Election Operations Assessment

Threat Trees and Matrices
and
Threat Instance Risk Analyzer (TIRA)

EAC Advisory Board and Standards Board Draft

Submitted by
University of South Alabama

December 23, 2009

Election Operations Assessment Project Overview

Overview

In September 2008, the Election Assistance Commission (EAC) conducted a procurement to obtain the services of an inter-disciplinary team to perform a scientifically founded Voting System Risk Assessment. The University of Southern Alabama team was competitively selected to conduct the analysis. The results of this project are intended to facilitate making informed decisions relative to future voting system standards by the EAC.

The project is organized in two phases. In the first phase, completed in May 2009, the project team conducted a literature search and created two sets of reference models that included an extensive glossary of election terms. The election process models define the operational context in which voting systems are used. Within the context established in the election system models, voting system models were created for seven voting technology types (direct recording electronic, precinct count optical scan, central count optical scan, vote by mail, vote by phone, internet voting, hand counted paper ballots) selected by the EAC to form the basis for the work on risk evaluation.

There are two goals of the project's second phase. The first of these is to analyze the voting system models to identify generic threats associated with each voting technology. We captured the outcome of this work as a set of threat trees using NIST 800-30 threat definitions, one threat tree for each technology type.

The second Phase II goal is to develop a tool to assist the EAC in evaluating the relative harm magnitude of identified threats and to facilitate cost-benefit analysis on the potential mitigations for those threats. We describe our tool at length in Section 9 below. Tool development was governed by project constraints that preclude any tool requiring assistance of experts with other than election specializations or to use restrictive proprietary data formats.

An essential element of each component of each phase of this project is peer and subject matter expert review. While many of the project artifacts were created by individual team members, every artifact was vetted through a four-tier review process that included at least one review at each of the following levels: the team level, the VSRA Advisory Board level, a formal review panel, and culminating with review and feedback from at least three EAC formal advisory bodies. The project team and advisory board members represent a broad spectrum of elections and technology expertise with members from many different states, thus ensuring breadth of experience and perspective in the vetting process. Additionally, several artifacts were sent to external reviewers for further comment. The project team carefully and systematically analyzed and incorporated comments into the project artifacts.

Tasks for the Board of Advisors and Standards Board

The project is nearing the completion of Phase 2. Here are some questions the EAC would like the Board of Advisors and Standards Board to consider while conducting their reviews:

- Are there any glaring risks or mitigations missing from the Risk Trees?
- How useful were the instructions provided?
- Was the tree structure consistent throughout all voting technologies?
- Were any of the risks identified non-applicable or out of scope?
- Did the explanations of the risk activities contain correct terminology and objective language?
- Was the same level of detail of risk applied to each voting technology?
- Were there terms that you didn't understand that need to be defined?
- Which of the three formats of presentation of the trees did you find easiest to follow? Is there another format that you think should be used?

Table of Contents

1 Introduction to Threat Trees and Matrices

A threat tree is a data structure for representing the steps that an attacker would take to exploit a vulnerability in order to accomplish malicious intent. While there has been much discussion of voting system threats and numerous voting system security vulnerability assessments, we are unaware of any systematic effort1 to catalog, specify, and validate voting system threat trees. Using threat trees as our foundation, we provide a voting system threat categorization approach, a voting system attack taxonomy, and a preliminary voting system threat tree development framework in this paper.

Our approach leverages three paradigms for representing voting system threat properties:

- Descriptively naming nodes as threat goals and steps
- Graphically expressing logical relationships between nodes and
- Defining attack goal and step semantic properties as nodal attributes.

Collectively these three approaches allow the abstraction and precision that are necessary to reason comparatively about fundamentally different threats.

For our purposes, a threat defines the process that one or more attackers might take to accomplish a malicious act in an election. The "tree" is a powerful abstraction that graphically captures relationships among nodes that are hierarchically connected by directional edges, while allowing analysts to express individual node properties as nodal attributes. The tree structure allows a systematic approach to threat analysis, including facilitating abstraction and decomposition and allows analysts to categorize goals and steps so they can focus on those that are most critical.

In order to leverage tree structures to represent threat processes, we define voting system threat trees so that their graphical properties capture important process relationship properties. We accomplish this by establishing the three node types of AND, OR, and TERMINAL. Subordination reflects specification through functional decomposition, so nodes higher in the tree are abstractions of subordinate nodes. All nodes that are immediately subordinate to an AND node must be carried out in order to meet higher level goals, while OR node subordinates reflect alternate means to accomplish an intended function. TERMINAL nodes have no subordinates, thus reflect the primitive operations (i.e. steps) that accomplish the modeled threat, while AND and OR nodes reflect intermediate attack goals.

The unit of evaluation for voting system threat trees is a threat instance, or equivalently, an attack, thus an attack is the realization of a threat. A threat tree represents many threat instances, or attacks, as a combination of TERMINAL nodes that satisfy the logical requirements of the tree.

We use goal nodes to abstract multiple sets of steps into a single logical unit of evaluation and thus mitigate this problem. Abstraction can reduce tree depth and make evaluation tractable. If we understood the properties of a node sufficiently to collapse it into a TERMINAL node, thus eliminating nodes. Thus, it may make sense to decompose goals in order to reason about them, but where that understanding is sufficiently detailed, to evaluate the tree at a higher abstraction level to reduce the evaluation state space.

Threat tree nodes may have many, sometimes seemingly contradictory, properties that dictate or influence a goal or step's occurrence LIKELIHOOD or its potential IMPACT. These are, of course, the two parameters for assessing voting system risk. Voting systems in the United States are highly complex. Consequently, risk LIKELIHOOD and IMPACT are varied and difficult to capture and express. It is not uncommon for two highly qualified election experts to disagree vehemently regarding the voting system risk.

While a threat tree consisting of well named AND, OR, and TERMINAL nodes can provide substantial information to an analyst at a glance, rigorous analysis in this complex environment demands much information. One mechanism for accomplishing this is to assign attributes to nodes that can be used to capture properties in greater detail than the name and structure can provide. For voting system risk analysis, these attributes represent properties that we can use to analyze risk LIKELIHOOD and IMPACT.

We highlight some voting system threat node attributes that capture a perspective of each of these properties in this section.

We may measure LIKELIHOOD and IMPACT as a continuous variable on a 0 to 1 scale. For the former, 0 (as the lower LIKELIHOOD extreme) would indicate that the event will not (or cannot) occur, while 1 (at the upper extreme) means that the event is certain to occur. For the latter, 0 would reflect no impact while a catastrophic result would represent the opposite extreme impact. Alternatively, a simple three step discrete metric of high, medium, and low could also represent LIKELIHOOD and/or IMPACT.

As we described earlier, we can capture the essence of every threat instance represented in a threat tree by only assigning metrics to TERMINAL nodes or steps. Since every step in a threat instance must be carried out to affect the attack it characterizes, we combine the step metrics for all steps in a threat instance to determine the cumulative measure. For example, if cost is the desired metric and if there is no overlapping cost between steps, then the cost of the threat instance is the sum of the cost of each step in the threat instance that is being evaluated.

Similarly, we may desire to represent a given threat tree at a higher abstraction level. If we have assigned metric values to the steps, we may be able to algorithmically compute the corresponding metric for a parent node using the values of its subordinates. For an AND node, again cost may be summed if there are no overlapping costs. For OR nodes, another approach, such as selecting the maximum or minimum cost, would be selected.

The only absolute in estimating risk likelihood is that there are no absolutes. Issues of relativity, temporality, uncertainty, and other qualifications render even the most intuitively accurate assumptions invalid, or worse yet, counterproductive. The best that we can hope for is to leverage heuristics to find metrics that incorporate best practice experience and offer analysts a chance at estimating comparative risk. We offer a few such prospective voting system risk assessment metrics below.

- Cost
- Necessary expertise
- Delectability
- Number of required participants

Generically, we think of threat IMPACT as the magnitude or degree of damage that will, or is expected to, occur as a result of a realized threat. In practice, IMPACT is context exclusive to the extent that the same voting system threat may have a catastrophic impact in one environment, but be essentially benign in a different environment. Assignment of the IMPACT metric is a major and important task of the analyst and requires significant subject matter expertise.

The two primary overarching goals of voting system attacks are either to impact election integrity or to influence public's perception about the election. Thus, we partition IMPACT metrics according to these two aspects and address IMPACT as the magnitude of the effect on voting system integrity or public perception.

Voting system integrity attacks are what we think of when we discuss election fraud, that is, integrity attacks maliciously influence a contest result in an election. This encompasses canonical election fraud issues, such as ballot stuffing.

Voting system integrity attack impact ranges from deleting one legal vote (or equivalently, injecting one illegal vote) with no impact on any contest selection, to controlling the selected candidate or issue decision in all contests. Voting system integrity issues are either related to vote counting (process where each voter selection is added to the total, one by one) or aggregation (where subtotals are combined to reflect the cumulative result).

The following metrics are illustrative (as opposed to comprehensive) and represent issues that are relevant to risk assessment. Without knowing a contest result a priori, an attack waged during the voting period has the best chance to be decisive if it can affect a large volume of votes. Such attacks are similar in many ways to wholesale purchasing tactics and the term "wholesale vote fraud" has become part of the election integrity vernacular. Wholesale attacks optimize effort-to-effect ratio, or more mathematically, retail attacks are linear in terms of the effort-to-effect ratio, while wholesale attacks are geometric (or exponential) in effort-to-effect ratio.

Since there are no well known metrics, metric validation is essential to the voting system risk assessment process. One way to approach validation is through comparing independent representations. With voting system threat trees, if metrics have suitable computational properties, we can use redundancy by comparing expert assessment against computed values. To accomplish this validation, an analyst would employ a five stage analysis.

1. Select a metric that that can be assigned based on expert opinion
2. Create an algorithm for computing a parent node's metric based on the child metric values
3. Apply expert metric evaluation rules to every node in the tree
4. Compute the metric value for each goal node and
5. For non-terminal nodes, compare the value assigned in Step 3 to the value that is vertically computed from its subordinate nodes in Step 4.

To illustrate, consider a simple threat tree with the (hypothetical) nodes: A: Intruder picks a lock B: Acquire lock picking skill C: Acquire private access to the lock D: Acquire information about the target lock E: Research approach for picking the target lock F: Determine when the room containing the safe will be empty G: Gain access to the room at an appropriate time. We now conduct the five stage analysis:

1. Select cost metric C
2. Compute the cost of a parent as the sum of the cost of the children
3. For instructional purposes, assume that the analyst opinion review assigns the cost of each node to be: (1) C(A) = 75, C(B) = 10, C(C) = 100, C(D) = 5, C(E) = 5, C(F) = 50, C(G) = 100
4. We compute the cost of the non-terminal nodes is: (2) C(A) = 160, C(B) = 10, C(C) = 150
5. Comparison of evaluations (3) and (4) reveals an inconsistency between the expert analysis and computed analysis at the highest level, which would not be surprising. It also reveals an inconsistency between the expert evaluation at the intermediate level for node C, suggesting reanalysis of assigned values for nodes F and G, or consideration of re-examining node C's decomposition.

1.1 Identifying Threats

In assessing risks to elections operations, a necessary first step is identifying threats. Let’s differentiate between risk and threat as we use these terms. Risk is the net negative Impact of the exercise of a Vulnerability, considering both the probability and the Impact of occurrence. A threat is the potential for a particular ThreatSource to successfully exercise a particular Vulnerability.

How did we identify voting system threats? They come from various sources such as our annotated bibliography, existing threat taxonomies, our phase 1 voting system models, which have been particularly helpful in identifying points of vulnerability, and the experts on our team, from whom threats were elicited in a facilitated group process, from research lead by the team and conducted by students, and resulting from three rounds of review. We have identified various threats, such as insider attacks, malware threats, and absentee ballot fraud, just to name a few.

1.2 Modeling Threats

When we identified threats, we needed to capture and model them in an organized manner that would be useful for later risk assessment. For this purpose, we used threat matrices and threat trees. Threats are identified as threat source – vulnerability pairs, in accordance with a widely cited government guideline for risk assessment, the NIST 800 dash 30. Vulnerabilities are simply weaknesses in voting systems, such as fragile or faulty equipment, the susceptibility to fraudulent acts by election officials, pollworkers, and voters, flawed processes, such as an error prone ballot counting procedure, or a lack of access protections on machines, ballots, and voters in the voting process. A Threat Source is any circumstance or event with the potential to cause harm to the system. Besides threat source and vulnerability, a third essential threat attribute, but no less important, is threat action. A threat action is the realization of a threat, whether by virtue of an intentional act or an accidental event. The threat action is the primary descriptive element when threats are depicted in a tree diagram. The threat tree and the threat matrix are the conceptual models that we use to specify threats against voting systems. The threat tree is a tree in the sense that it contains a root, branches, and leaves, all of which are also referred to as "nodes". There are two primary representations of threats. One is a graphical representation that you are looking at in a Microsoft Visio diagram. These diagrams depict the threat actions, although other threat attributes may also be laid out in this type of graphical depiction…inside of shapes that differentiate between AND, OR, and TERMINAL nodes. The [AND] means that the branches that connect to the root node are required actions rather than optional steps [OR]. Nodes not decomposed further are TERMINAL nodes. And gates, or gates, and circles are used to represent And, Or, and terminal nodes, respectively.

Let’s take a closer look at 3-2 PCOS Attack Voting Equipment. The root node of the sub-tree is at the top: 1-Attack voting equipment. Recall that this type of attack is one that requires specialized technical or insider knowledge of voting technology to launch an attack on an election. The outline number and threat action are shown in each shape. Each shape is a node in the tree, and has a corresponding row in the threat matrix that contains the remaining attribute values. Because an AND gate is used for 1-attack voting equipment, the children just below the root are required steps in the attack. So, the attack voting equipment threat is modeled as a series of three activities, all required: gather knowledge, gain insider access, and attack component. More generally, the attack includes intelligence, access, and execution steps. Let’s look at 1.2 – gain insider access. This one is an OR node, because the OR gate is used. So, its children are optional steps available to the attacker. Any one of these will accomplish the goal of gaining insider access. The attack may choose to gain access at a voting system vendor’s facility, in the supply chain, in the elections organization, by illegal insider entry, or by remote network access. Because all of these threats are depicted in a circle shape, they are all terminal nodes not broken down further. The 1.3 – attack component threat is interesting because it is broken down into threats of different types and at different depths. It is at this point in the attack equipment tree that we differentiate attacks by the four basic technical component types for computer-based systems. To attack a component means to attack eitherhardware, software, data, or communication links. To attack hardware means to either jam the PCOS scanner or attack a stored component. To attack a stored component is to either swap boot media, attack install, or destroy Removable Media. The next two children of attack component are an And node and an OR node, respectively. Although both trees are broken down, the sub-trees are not shown on this diagram.

1.3 Major Categories of Threats

Threat sources are said to exercise vulnerabilities, and include broad categories of human and nonhuman sources, such as malicious insiders and outsiders, nonmalicious insiders; and nonhuman threat sources.

Here are some of the types of voting system threats we’ve modeled. The first one on the list is attack voting equipment which are computer-based threats to elections operations. Election officials and pollworkers are the primary threat sources for perform insider attack. The subvert voting process sub-tree consists of situations where legal voters are complicit with attackers, because they either sell their vote, get intimidated to vote as the attacker would want, or they are a no-show at the polls. The commit errors in operations sub-tree includes pollworkers making honest mistakes. We've also got nonhuman threats represented, such as technical threats (software bugs and equipment failure) in the experience a technical failure sub-tree; and natural threats (earthquakes, and weather events) and environmental threats (power failure), which are both modeled in the disrupt operations sub-tree, along with terrorist threats.

Usefulness of Sub-tree Classification

We designed the tress so that we were able to place threats neatly into a category without a lot of overlap classification confusion, and enable a holistic understanding of a sub-tree that would generate a convergence of thought about the riskiness of its threats. Understanding a few broad trees, the analyst can then drill down into looking at different variations of threats within a tree, to more deeply assess risk.

1.4 Threat Tree Formats

Each of the trees is presented in three formats: outline, graphical, and matrix. The outline and graphical formats provide very similar information; the threat matrix contains all of the information from the outline and graphical forms as well as several additional columns of data.

Threat Trees - Outline

A second way that we depict threat trees is in outline form, and also stored in a spreadsheet. The outline structure is also hierarchical, outline-numbered, and indented. The outline shown includes the node type (an A, O, or T to the node's far left, representing AND, OR, or TERMINAL), the outline number with dot notation, and the threat action text, all indented from left to right according to the node's depth in the tree.

Let's look at part of the PCOS outline: 2 – Perform insider attack. The threat source for insider attacks are usually election officials, pollworkers, and sometimes voters. The threat has a sub-tree 2.2 execute insider attack, which is an OR node, denoted by the capital O at its left. This threat is broken down further into 2.2.1 attack at polling place and 2.2.2 attack at other than polling place. Attack at polling place, another OR node, is broken into discourage voters, and steal voter's vote. We will look at a specific node of this sub-tree when we review the threat matrices, next.

Threat Trees - Graphical

Technically speaking, threat trees are acyclic graphs (group of nodes connected by edges that cannot have cycles) in which each node in the graph has exactly one parent. The root of the tree is a parentless node. The node is a place to store information, and it's a connective element. The root is a node, the leaves are nodes, and the branches consist of nodes at the point where the branch splits in different directions.

Each node represents a threat at some level of abstraction. The root node represents the most general view of a threat, thought to encompass the entire set of actions to accomplish an attacker's goal or otherwise exercise the vulnerability. Nodes are decomposed by specifying the steps to complete the threat, i.e. to achieve the goal or to bring about the high-level result for that tree. The leaves (nodes without children) represent threats that are not broken down further, because further decomposition would not be useful in risk assessment. A threat tree represents many events that could happen. It is a model for a category of threats that are related by either the prospective attacker goals (nodes with children) or steps (nodes without children).

Threat Matrix (NIST 800-30)

Threats identified were cataloged in a threat matrix, implemented as a spreadsheet, tabular in form, and containing hundreds of entries.

The attributes chosen for describing threats were primarily motivated by the threat classification guidelines provided by NIST 800 dash 30. We document the threat source category, threat action, vulnerability, vulnerable element, scope, description, reference source, threat scenario, and recommended controls.

Let’s take a closer look at threat matrix entry for PCOS 2.2.1.1 discourage voters. Looking at the first three attributes, each threat, or node, begins with a node type - A, O, or T. The outline number is a unique number, providing a sequence of integers, one for each node down the branch leading to this node, starting from the root.

A longer, expanded version of the short threat action statement is included in the description field. In this case, “discourage voters” is expanded to “intentionally discourage voters from voting”. This threat references an item in the Jones taxonomy: #211- intimidation outside the polling place. The NIST 800-30 threat source category for discourage voters is human-deliberate insider, and the scope of the threat, according to our voting system activity model, is Voting System.

The final four attributes presented are vulnerable element, vulnerability, recommended controls, and threat scenario. The vulnerable element is the person, technology, or process that is vulnerable to the particular threat. In this case, the voting system process of check poll book for authentication is the vulnerable activity. The vulnerability, or weakness, is the unwillingness or inability of voters to appeal pollworkers' decisions. A number of recommended controls relevant to the discourage voters threat are listed. These come from the NIST 800-53 guidelines, where more detailed guidance can be found. It is not suggested that all these controls be selected, but they provide areas of possibilities for further analysis. The threat scenario provides a narrative story or more detailed description illustrating the threat action. In some cases, this scenario is based on actual past events.

1.5 Comprehensiveness of Trees

Evaluating the quality of the threat trees and matrices, a key question is one of completeness. “Are there threats missing?” is the key review question. It is a difficult issue because it is impossible to prove that there are no missing threats. With each additional round of review, a few more threats will undoubtedly be uncovered. In fact, risk assessment is not a one-time event, but should be conducted as a continuous process. Security is an escalating war. We prefer to say that the threat trees are comprehensive. By comprehensive, we mean that there is coverage from a number of points of view. That is, the threat trees…

- are defined for each of the seven voting technologies
- are representative of the Doug Jones taxonomy,
- provide coverage across the NIST 800 dash 30 threat source categories,
- address the various voting system activities modeled in Phase 1
- cite 54 reference sources, and
- exhausted ideas from our team in a summer brainstorming session.

In addition, the threat trees have also undergone three rounds of review: by our own team; by our advisory board; and by a panel of experts, including computer security experts, election officials, testing lab and vendor representatives, and academicians.
The thought we would like to leave you with is that a good faith effort was made to identify all known threats, through a rigorous process, and with the efforts of a variety of experts who provided feedback.

2 Direct Recording Electronic (DRE)

In this tree, we consider threats to voting systems that employ a direct recording electronic (DRE) voting machine, which interacts with the voter, typically through a touch screen. The DRE captures and counts each vote, and generates a persistent ballot image based on the voter interaction. We assume that the DRE's are used in a precinct-based polling place environment. We are also assuming the electronic ballot image exists, but no paper, such as VVPAT.

From a risk assessment standpoint, DRE has threats associated with the use of computer-based technology and polling places, but not paper ballots. The key technologies considered are the DRE terminals, which are used in the polling place but can also be brought outside the polling place in the case of curbside voting, particularly for disabled voters.

2.1 DRE Threat Tree

node type - outline number - threat action

```
A  1    attack voting equipment
   O  1.1   gather knowledge
      T  1.1.1   from insider
      A  1.1.2   from components
         O   1.1.2.1   access directly
                T   1.1.2.1.1   infiltrate as insider
                T   1.1.2.1.2   obtain a machine
                T   1.1.2.1.3   legally acquire machine
                T   1.1.2.1.4   study a machine in transit
                T   1.1.2.1.5   find source code
                T   1.1.2.1.6   compromise existing source code escrow
         T   1.1.2.2   directly examine
      T  1.1.3   from published reports
   O  1.2   gain insider access
      T  1.2.1   at voting system vendor
      T  1.2.2   in supply chain
      T  1.2.3   in elections org
      T  1.2.4   by illegal insider entry
      T  1.2.5   by remote network access
   O  1.3   attack component
      O  1.3.1   attack hardware
         O   1.3.1.1   attack stored components
                T   1.3.1.1.1   swap boot media
                T   1.3.1.1.2   attack install
                T   1.3.1.1.3   destroy RemovableMedia
      A  1.3.2   attack software
         T   1.3.2.1   develop malware
         O   1.3.2.2   select targets
                T   1.3.2.2.1   select precincts by expected voting pattern
                T   1.3.2.2.2   select all precincts
         O   1.3.2.3   inject malware
                T   1.3.2.3.1   by remote bug exploitation
                T   1.3.2.3.2   by local bug exploitation
                T   1.3.2.3.3   by human interface exploit
         O   1.3.2.4   execute malware
```

        - T 1.3.2.4.1 that alters artifact directly
        - T 1.3.2.4.2 that self-propagates
        - T 1.3.2.4.3 that remains resident
      - O 1.3.2.5 mitigate risk of detection
        - T 1.3.2.5.1 coerce testing staff
        - T 1.3.2.5.2 attack after testing
        - T 1.3.2.5.3 obtain cooperation of testers
        - T 1.3.2.5.4 acquire detailed knowledge of testing procedures and scripts
      - O 1.3.2.6 use infected component
        - O 1.3.2.6.1 supply cryptic knock
          - T 1.3.2.6.1.1 during logic and accuracy testing
          - T 1.3.2.6.1.2 during machine setup
          - T 1.3.2.6.1.3 during voting
          - T 1.3.2.6.1.4 as anti-knock
          - T 1.3.2.6.1.5 using AC power flicker
          - T 1.3.2.6.1.6 to detect realistic patterns of voting
          - T 1.3.2.6.1.7 to employ calendar/clock tricks
          - T 1.3.2.6.1.8 in ballot definition files
        - O 1.3.2.6.2 control/parameterize attack
          - T 1.3.2.6.2.1 voter enables attack as attacker
          - T 1.3.2.6.2.2 enable by unknowing voter
          - T 1.3.2.6.2.3 enable by technical consultant
          - T 1.3.2.6.2.4 employ unparameterized attack
          - T 1.3.2.6.2.5 add commands to ballot def file
    - O 1.3.3 attack data
      - O 1.3.3.1 using malware
        - O 1.3.3.1.1 select method and alter
          - T 1.3.3.1.1.1 by malware
          - T 1.3.3.1.1.2 by infected software
          - T 1.3.3.1.1.3 by infected config data
        - T 1.3.3.1.2 alter ballot definition file
        - T 1.3.3.1.3 alter device tallies
        - T 1.3.3.1.4 alter tabulation SW
      - O 1.3.3.2 modify data on storage medium
      - T 1.3.3.3 alter ballot creation software
        - T 1.3.3.2.1 modify tabulation data
        - O 1.3.3.2.2 modify data before use
          - T 1.3.3.2.2.1 pre-load votes
          - T 1.3.3.2.2.2 flip votes
          - T 1.3.3.2.2.3 alter config data
        - T 1.3.3.2.3 alter electronic ballots using administrator account access
    - O 1.3.4 attack comlinks
      - T 1.3.4.1 attack linked scanner/tabulator
      - T 1.3.4.2 attack wireless
- A 2 perform insider attack
  - O 2.1 form inside attack team
    - T 2.1.1 infiltrate as volunteer pollworker
    - T 2.1.2 infiltrate as observer
    - T 2.1.3 staff with attackers
    - T 2.1.4 collude with other insiders
    - T 2.1.5 allow pollworker rotation
  - O 2.2 execute insider attack
    - O 2.2.1 attack at polling place

  - O 2.2.1.1 discourage voters
    - O 2.2.1.1.1 challenge at CheckIn
      - T 2.2.1.1.1.1 falsely reject voter registration
      - T 2.2.1.1.1.2 falsely reject id check
      - T 2.2.1.1.1.3 selectively challenge voters
      - T 2.2.1.1.1.4 challenge voters on caging list
      - T 2.2.1.1.1.5 destroy registered cards
    - O 2.2.1.1.2 delay open/close
      - T 2.2.1.1.2.1 damage / tamper with electronic voting equipment
      - T 2.2.1.1.2.2 damage / tamper with artifacts
      - T 2.2.1.1.2.3 allocate insufficient resources
    - O 2.2.1.1.3 create long lines
      - T 2.2.1.1.3.1 work slowly to stymie
      - T 2.2.1.1.3.2 program the VVPAT to exhaust the paper supply
      - T 2.2.1.1.3.3 damage / tamper with electronic voting equipment
      - T 2.2.1.1.3.4 damage / tamper with artifacts
      - T 2.2.1.1.3.5 allocate insufficient resources
    - T 2.2.1.1.4 delay voters with poor assistance
    - T 2.2.1.1.5 stymie voters needing assistance
    - T 2.2.1.1.6 mislead w/phony ballot change
    - T 2.2.1.1.7 mislead w/one party only ruse
    - T 2.2.1.1.8 discourage provisional voting
    - T 2.2.1.1.9 impede voter access
    - T 2.2.1.1.10 persuade voter selections
    - T 2.2.1.1.11 send voter to wrong place
    - T 2.2.1.1.12 use faulty headsets
    - T 2.2.1.1.13 mispronounce names of candidates on audio ballot
  - A 2.2.1.2 alter voter's vote
    - O 2.2.1.2.1 obtain MarkedBallot
      - T 2.2.1.2.1.1 disable machine
      - T 2.2.1.2.1.2 mislead about committing ballot
      - T 2.2.1.2.1.3 take control of assisted voter terminals
    - O 2.2.1.2.2 subvert MarkedBallot of voter
      - T 2.2.1.2.2.1 mark undervote to create vote
      - T 2.2.1.2.2.2 mark vote to create overvote
      - T 2.2.1.2.2.3 flip voter's electronic vote
    - T 2.2.1.2.3 commit subverted ballot
  - T 2.2.1.3 send voter to subverted machine
- O 2.2.2 attack other than polls
  - A 2.2.2.1 attack ballots
    - T 2.2.2.1.1 access ballots
    - O 2.2.2.1.2 tamper with ballots
      - T 2.2.2.1.2.1 by subverting ballot rotation
      - T 2.2.2.1.2.2 by subverting provisional envelope
    - O 2.2.2.1.3 replace ballots
      - T 2.2.2.1.3.1 record voter's ballot as other than depicted on screen
      - T 2.2.2.1.3.2 swap provisional for non-provisional ballot
      - T 2.2.2.1.3.3 switch MarkedBallots during transport
      - T 2.2.2.1.3.4 discard / destroy MarkedBallots
      - T 2.2.2.1.3.5 damage MarkedBallots
  - T 2.2.2.2 damage electronic voting equipment
  - O 2.2.2.3 misinform about overvoting / undervoting
    - T 2.2.2.3.1 allow undervotes without warning

T 2.2.2.3.2 allow overvotes without warning
T 2.2.2.3.3 encourage voter override
O 2.2.2.4 confuse voters with poor ballot design
T 2.2.2.4.1 by splitting contests up
T 2.2.2.4.2 by spreading response options
T 2.2.2.4.3 by placing different contests on the same touch screen
T 2.2.2.4.4 by keeping disqualified candidates
T 2.2.2.4.5 with inconsistent formats
T 2.2.2.4.6 by omitting useful shading
O 2.2.2.4.7 by omitting use of bold
T 2.2.2.4.8 with complex instructions
O 2.2.2.4.9 with distant instructions
T 2.2.2.4.10 with no correction guidance
T 2.2.2.5 force least-objectionable choice
T 2.2.2.6 publish invalid sample ballots
T 2.2.2.7 stuff ballots after closing
T 2.2.2.8 stuff during canvass or recount
O 2.2.2.9 errors in ballot adjudication
T 2.2.2.9.1 incorrectly accept provisional ballots
T 2.2.2.9.2 incorrectly reject provisional ballots
O 2.2.2.10 subvert decision criteria
T 2.2.2.10.1 selectively recount
T 2.2.2.11 subvert tabulation
O 2.2.2.12 attack tabulated results
T 2.2.2.12.1 subvert reported results
T 2.2.2.12.2 falsely announce results
T 2.2.2.12.3 alter results transmission
A 3 subvert voting process
T 3.1 determine number of votes to target
O 3.2 target polling places
T 3.2.1 by expected voting pattern
T 3.2.2 where PollWorkers not likely to know Voters
T 3.2.3 that exploit Electoral College rules
T 3.2.4 where PollWorkers can be co-opted
T 3.2.5 with lax enforcement of procedures
T 3.2.6 staff polling place with attackers
T 3.2.7 allow rotation of poll worker roles
O 3.3 form attack team
A 3.3.1 use cell captains to execute deniable impersonation attack
T 3.3.1.1 recruit cell captains
T 3.3.1.2 motivate cell captains
T 3.3.1.3 educate cell captains
T 3.3.1.4 provide rewards for cell captains to distribute
T 3.3.1.5 recruit attackers
T 3.3.2 recruit attackers among LegalVoters
T 3.3.3 recruit brokers
O 3.4 commit vote fraud attack
A 3.4.1 perform impersonation attack
O 3.4.1.1 develop target voters list
O 3.4.1.1.1 create fraudulent voter registrations
T 3.4.1.1.1.1 register as a housemate
T 3.4.1.1.1.2 register as a dead person
T 3.4.1.1.1.3 register an ineligible person

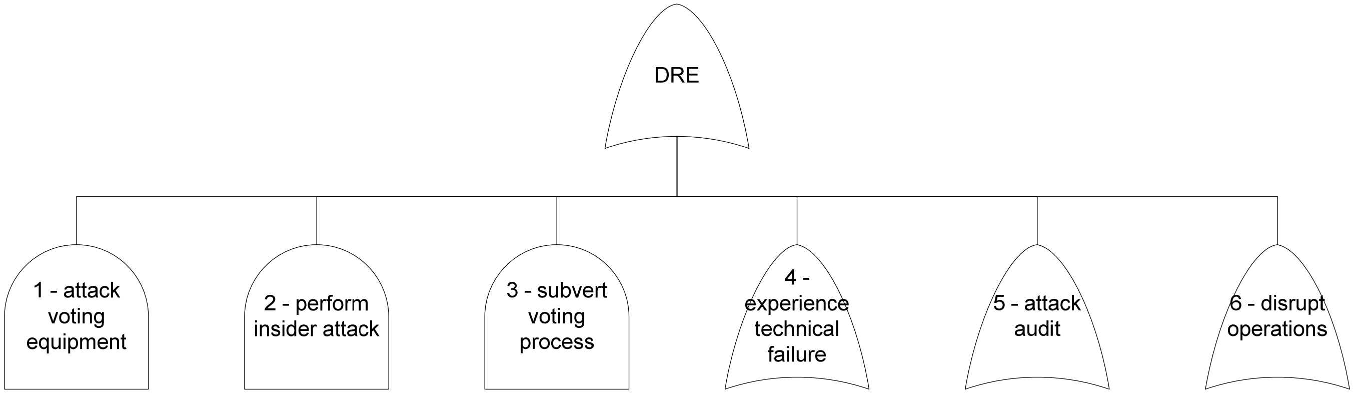
T	3.4.1.1.1.4	register as a fictitious person
T	3.4.1.1.2	create target list of LegalVoters to impersonate
O	3.4.1.2	execute impersonated voting
A	3.4.1.2.1	with fraudulent registrations
T	3.4.1.2.1.1	assign impersonator to voter
T	3.4.1.2.1.2	go to target voter's polling place
T	3.4.1.2.1.3	check in as the impersonated voter
T	3.4.1.2.1.4	vote in place of voter
T	3.4.1.2.1.5	supply rewards
A	3.4.1.2.2	with list of LegalVoters
O	3.4.1.2.2.1	create fraudulent CheckIns
T	3.4.1.2.2.1.1	
T	3.4.1.2.2.1.2	
T	3.4.1.2.2.2	mark VotableBallot
T	3.4.1.2.2.3	commit MarkedBallot
A	3.4.2	buy or coerce vote
O	3.4.2.1	motivate voter
O	3.4.2.1.1	pay
T	3.4.2.1.1.1	pay
T	3.4.2.1.1.2	promise to pay
O	3.4.2.1.2	coerce
T	3.4.2.1.2.1	promise to punish
T	3.4.2.1.2.2	punish and promise more
T	3.4.2.1.2.3	punish and promise repair
O	3.4.2.2	direct voters
T	3.4.2.2.1	to make specific votes
T	3.4.2.2.2	to not make specific votes
O	3.4.2.3	verify bought vote
T	3.4.2.3.1	by self-recorded casting
T	3.4.2.3.2	with phony voter assistant
T	3.4.2.3.3	using write-ins as code
T	3.4.2.3.4	by capturing electronic emanations
T	3.4.2.3.5	by headphone eavesdropping
T	3.4.2.3.6	by mapping votes to voters
T	3.4.2.4	supply rewards or punishment
O	3.4.3	vote more than once
T	3.4.3.1	vote using more than one method
T	3.4.3.2	vote in more than one place
O	3.4.3.3	engineer multiple access keys
T	3.4.3.3.1	create bogus authorization codes
T	3.4.3.3.2	program the smart card to ignore the deactivation command of the system
T	3.4.3.3.3	stuff ballot box using fraudulent smart cards
O	4	experience technical failure
O	4.1	experience operational error
T	4.1.1	by miscalibrating equipment
T	4.1.2	due to foreign substances
T	4.1.3	through erroneous settings
T	4.1.4	by mismatching precinct and actual
T	4.1.5	in software from bad data
T	4.1.6	causing hardware failure
T	4.1.7	causing device failure
T	4.1.8	due to manufacturer error
O	4.2	experience undetected tabulation errors

- T 4.2.1 in straight-party vote tabulation
- T 4.2.2 due to improper tabulation technique
- T 4.2.3 due to software error
- T 4.2.4 from mistakes by ballot designer
- T 4.2.5 due to flawed ballot creation software
- T 4.2.6 by omitting tallies from totals
- T 4.2.7 by adding tallies multiple times
- O 4.3 experience errors in ballot preparation
- T 4.3.1 encode incorrect contest counting rule
- T 4.3.2 supply erroneous ballot definition data
- T 4.3.3 supply erroneous voting equipment data
- T 4.3.4 misconfigure ballot by operator
- O 5 attack audit
- O 5.1 attack election evidence
- T 5.1.1 destroy ElectionArtifacts
- T 5.1.2 mishandle ElectionArtifacts
- T 5.1.3 add new fraudulent evidence
- O 5.1.4 modify ElectionArtifacts
- A 5.1.4.1 modify deliberately
- T 5.1.4.1.1 replace paper tape with fraud
- T 5.1.4.1.2 rewrite data on RemovableMedia
- T 5.1.4.1.3 modify poll books for audit
- T 5.1.4.1.4 modify logbooks and log data used in audit
- T 5.1.4.2 modify unintentionally
- T 5.1.4.3 modify deliberately by computer
- T 5.1.4.4 modify unintentionally by computer
- T 5.1.4.5 modify via malware attack
- T 5.1.4.6 modify via malware at artifact creation
- O 5.2 improperly select audit samples
- T 5.2.1 select audit units before election
- T 5.2.2 select non-randomly
- T 5.2.3 use subverted selection method
- T 5.2.4 ignore proper selections
- O 5.3 use poor audit process
- T 5.3.1 misguide auditors
- T 5.3.2 audit insufficient sample
- T 5.3.3 exploit variation in batch sizes
- T 5.3.4 establish single contest audit rule
- T 5.3.5 arrange contest audit
- T 5.3.6 select audited items before commit
- T 5.3.7 tamper with audit totals
- T 5.3.8 avoid correction
- T 5.3.9 overwhelm audit observers
- O 5.4 commit auditing error
- T 5.4.1 misanalyze discrepancies between electronic and paper results
- T 5.5 compromise auditors
- O 5.6 attack audit results
- T 5.6.1 mishandle media
- T 5.6.2 add fraudulent result data
- O 5.6.3 attack audit data
- T 5.6.3.1 modify deliberately
- T 5.6.3.2 modify unintentionally
- T 5.6.3.3 modify via malware attack

- T 5.6.4 publish bogus audit results

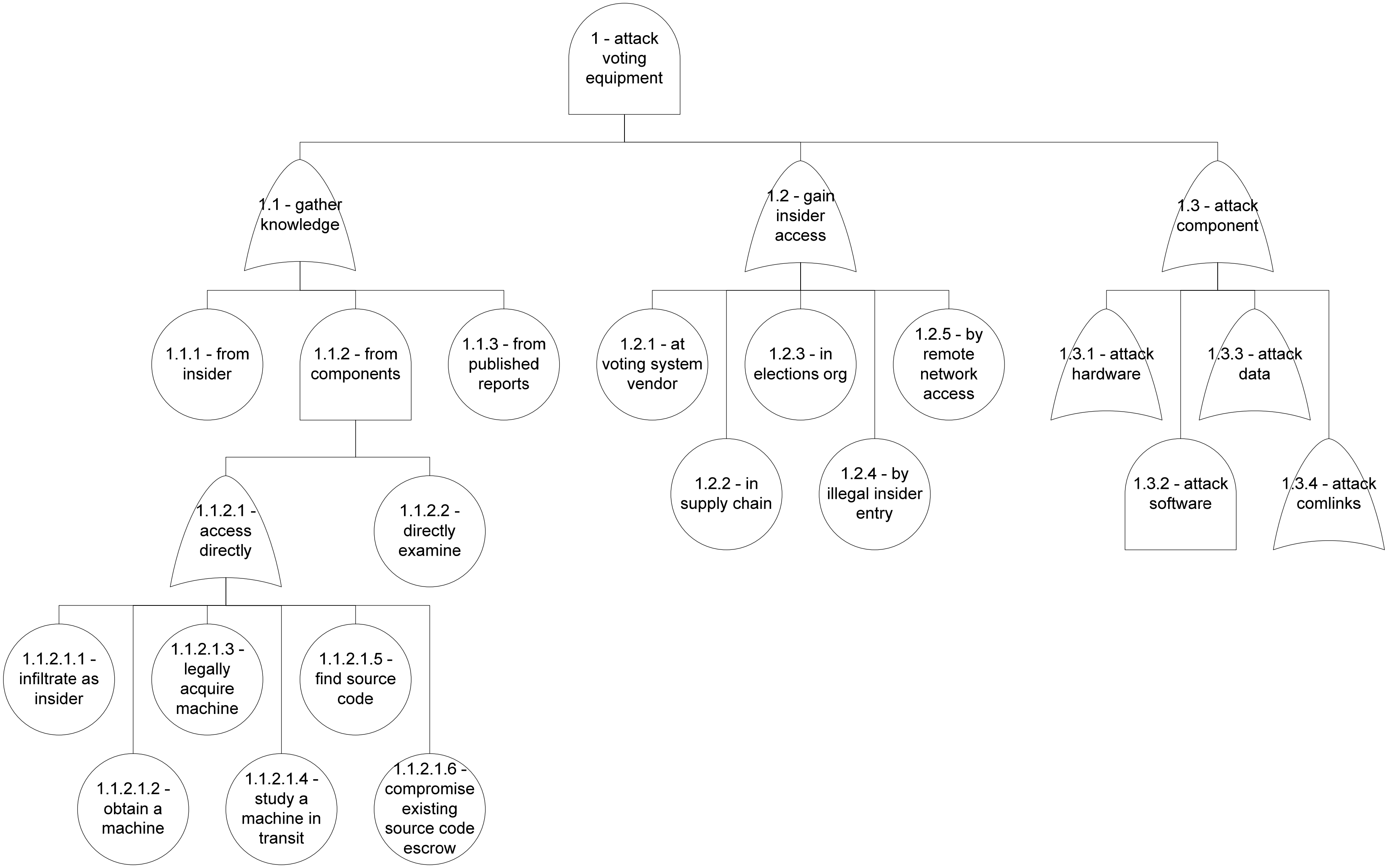
- O 6 disrupt operations
  - O 6.1 disruption from natural events
    - T 6.1.1 natural disaster
    - T 6.1.2 severe weather
  - O 6.2 disruption from environment events
    - T 6.2.1 environmental failures
    - T 6.2.2 hazardous accidents
  - O 6.3 disruption from human-created events
    - O 6.3.1 that damage equipment
      - T 6.3.1.1 render e-voting equipment inoperable
      - T 6.3.1.2 render removable media not working
      - T 6.3.1.3 render paper sensor inoperable
    - T 6.3.2 with environmental effects
  - O 6.4 discourage voter participation
    - T 6.4.1 misinform voters
    - T 6.4.2 threaten personal violence
    - T 6.4.3 threaten mass violence
    - T 6.4.4 commit an act of terror
    - T 6.4.5 intimidate to suppress turnout
    - T 6.4.6 create long lines

2.2 DRE Threat Tree - Graphic

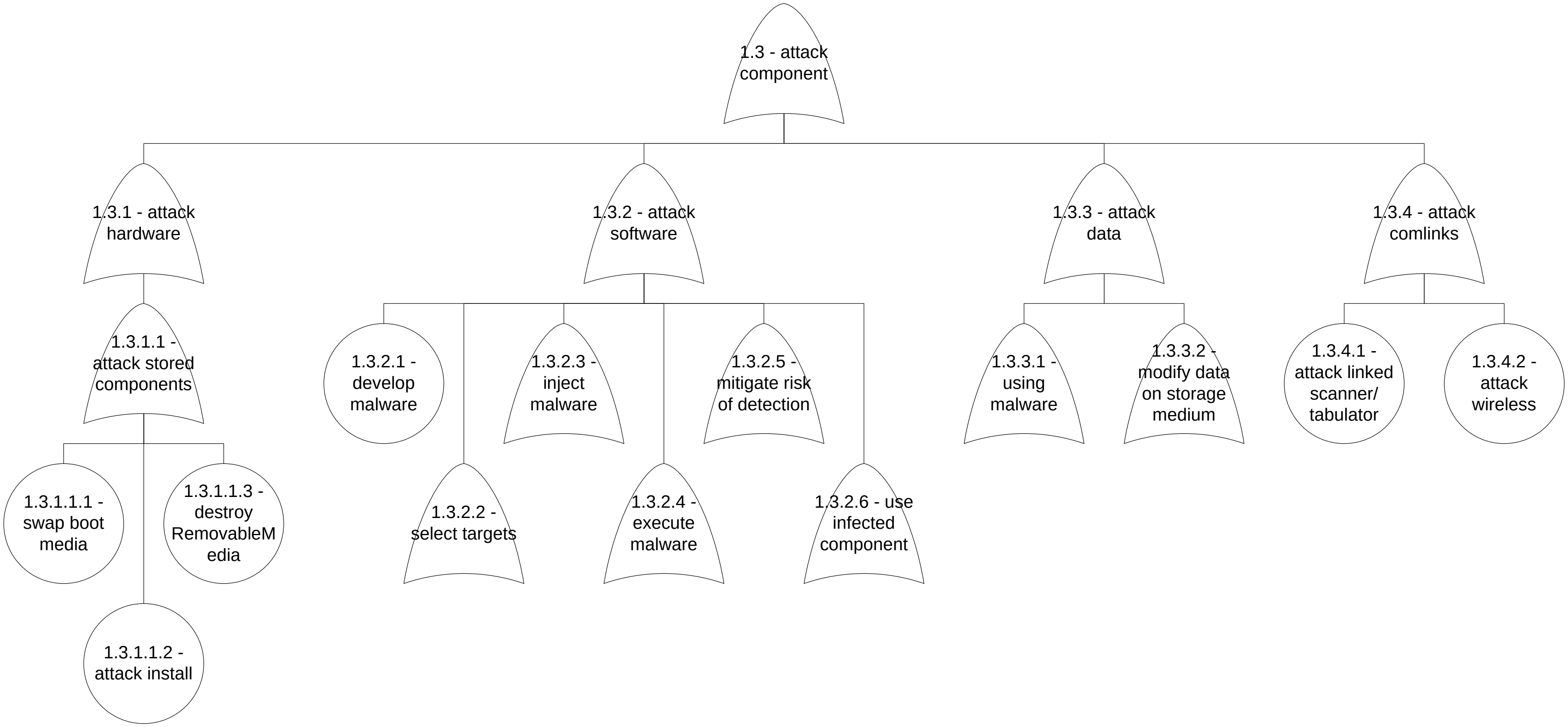

DRE
1 - attack voting equipment
2 - perform insider attack
3 - subvert voting process
4 - experience technical failure
5 - attack audit
6 - disrupt operations

2-1 DRE Overview[1]

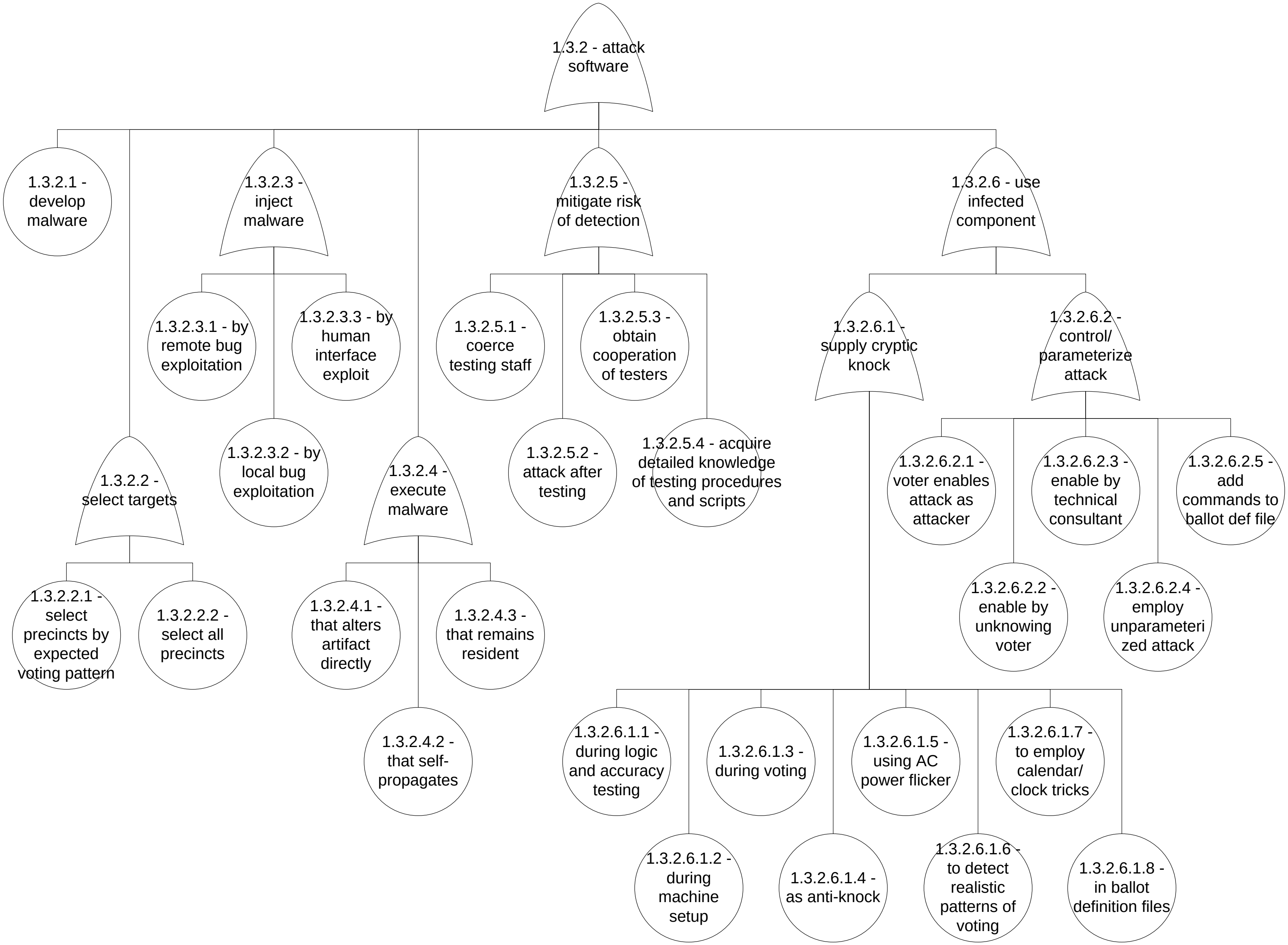
[1] A Key to Threat Tree Symbols is located in Section 11


1 - attack voting equipment
1.1 - gather knowledge
1.2 - gain insider access
1.3 - attack component
1.1.1 - from insider
1.1.2 - from components
1.1.3 - from published reports
1.2.1 - at voting system vendor
1.2.3 - in elections org
1.2.5 - by remote network access
1.3.1 - attack hardware
1.3.3 - attack data
1.2.2 - in supply chain
1.2.4 - by illegal insider entry
1.3.2 - attack software
1.3.4 - attack comlinks
1.1.2.1 - access directly
1.1.2.2 - directly examine
1.1.2.1.1 - infiltrate as insider
1.1.2.1.3 - legally acquire machine
1.1.2.1.5 - find source code
1.1.2.1.2 - obtain a machine
1.1.2.1.4 - study a machine in transit
1.1.2.1.6 - compromise existing source code escrow

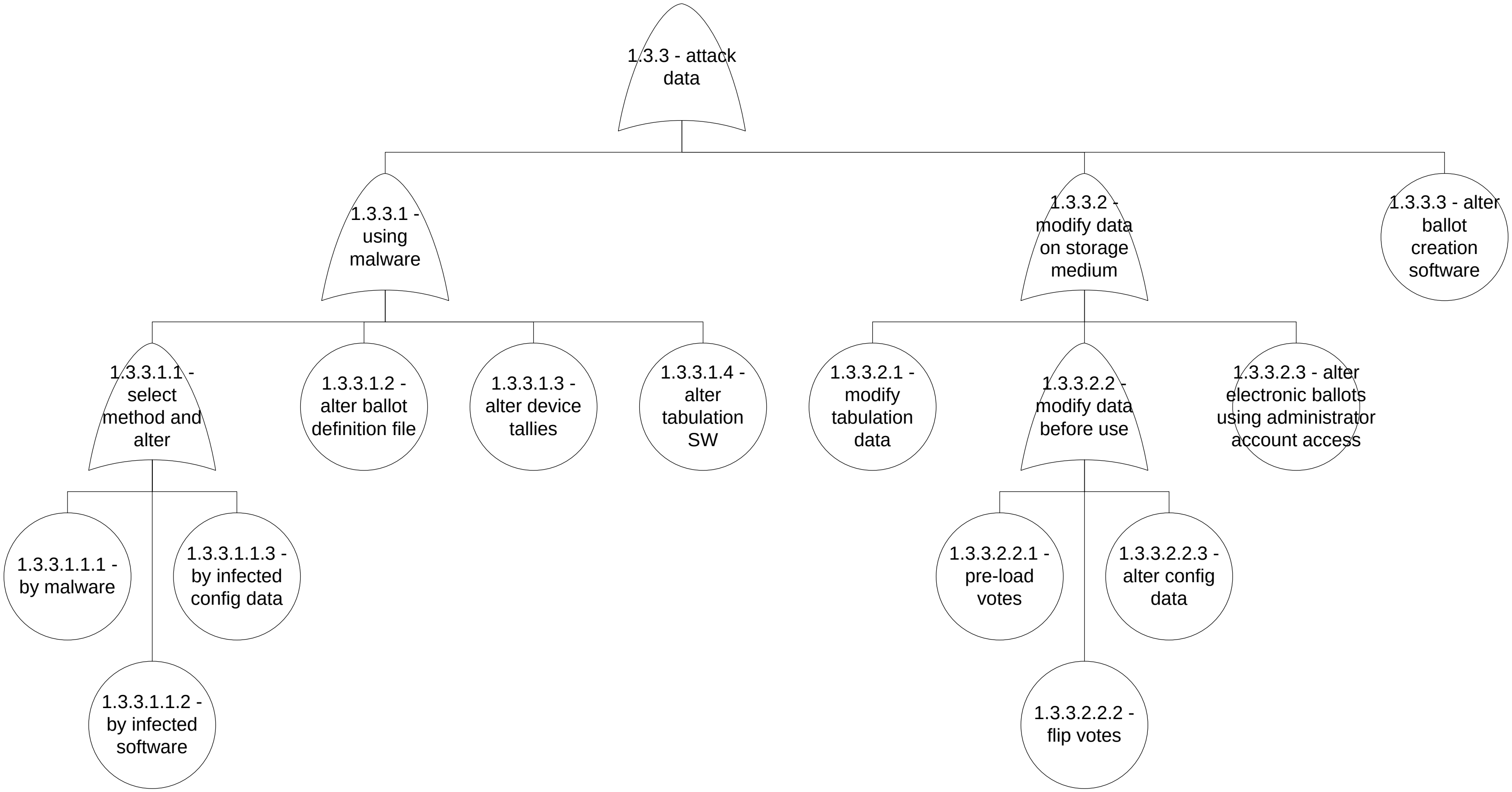
2-2 DRE Attack Voting Equipment


1.3 - attack component
1.3.1 - attack hardware
1.3.2 - attack software
1.3.3 - attack data
1.3.4 - attack comlinks
1.3.1.1 - attack stored components
1.3.1.1.1 - swap boot media
1.3.1.1.2 - attack install
1.3.1.1.3 - destroy RemovableMedia
1.3.2.1 - develop malware
1.3.2.2 - select targets
1.3.2.3 - inject malware
1.3.2.4 - execute malware
1.3.2.5 - mitigate risk of detection
1.3.2.6 - use infected component
1.3.3.1 - using malware
1.3.3.2 - modify data on storage medium
1.3.4.1 - attack linked scanner/ tabulator
1.3.4.2 - attack wireless

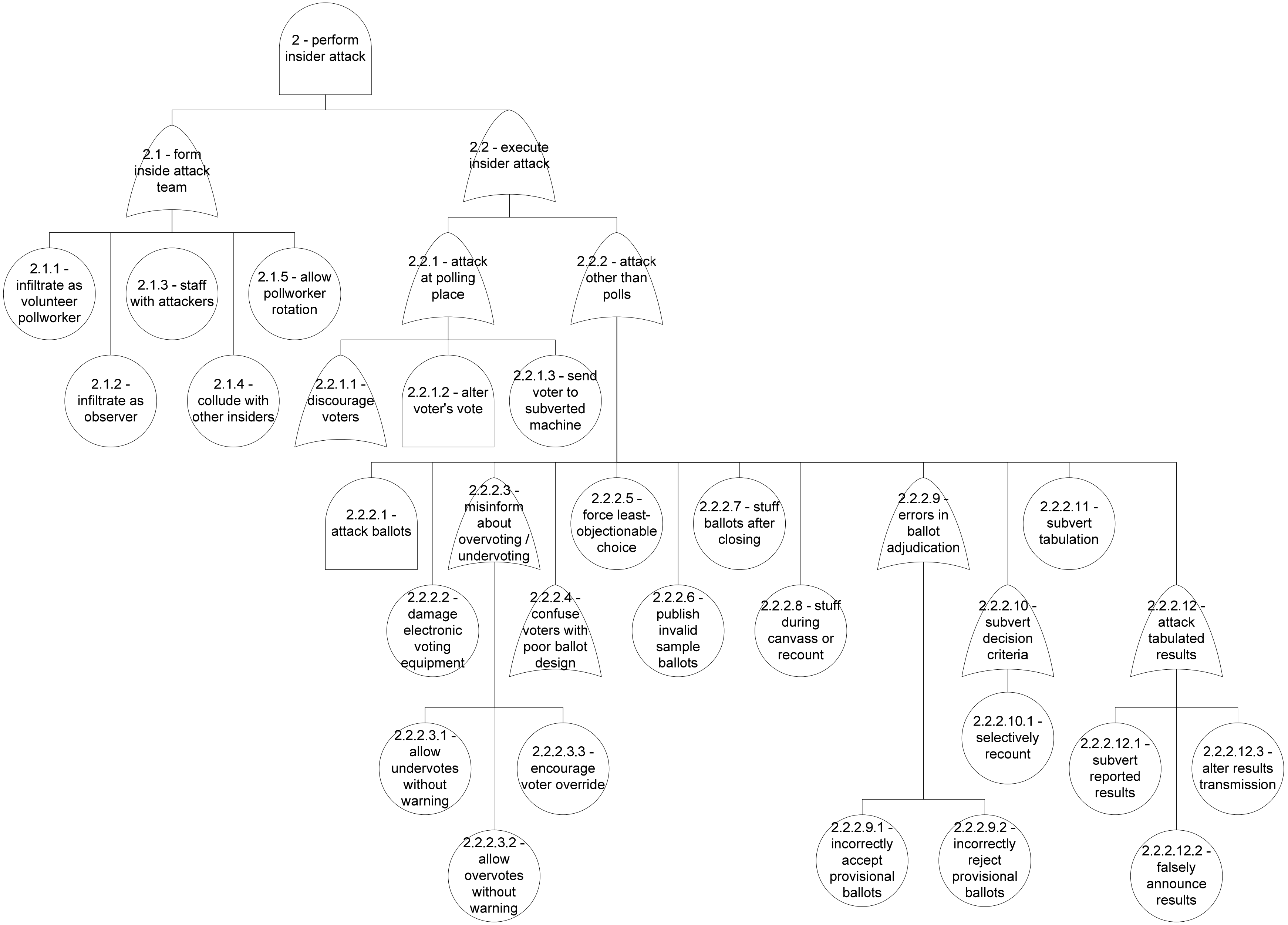
2-3 DRE Attack Component


1.3.2 - attack software
1.3.2.1 - develop malware
1.3.2.2 - select targets
1.3.2.2.1 - select precincts by expected voting pattern
1.3.2.2.2 - select all precincts
1.3.2.3 - inject malware
1.3.2.3.1 - by remote bug exploitation
1.3.2.3.2 - by local bug exploitation
1.3.2.3.3 - by human interface exploit
1.3.2.4 - execute malware
1.3.2.4.1 - that alters artifact directly
1.3.2.4.2 - that self-propagates
1.3.2.4.3 - that remains resident
1.3.2.5 - mitigate risk of detection
1.3.2.5.1 - coerce testing staff
1.3.2.5.2 - attack after testing
1.3.2.5.3 - obtain cooperation of testers
1.3.2.5.4 - acquire detailed knowledge of testing procedures and scripts
1.3.2.6 - use infected component
1.3.2.6.1 - supply cryptic knock
1.3.2.6.1.1 - during logic and accuracy testing
1.3.2.6.1.2 - during machine setup
1.3.2.6.1.3 - during voting
1.3.2.6.1.4 - as anti-knock
1.3.2.6.1.5 - using AC power flicker
1.3.2.6.1.6 - to detect realistic patterns of voting
1.3.2.6.1.7 - to employ calendar/ clock tricks
1.3.2.6.1.8 - in ballot definition files
1.3.2.6.2 - control/ parameterize attack
1.3.2.6.2.1 - voter enables attack as attacker
1.3.2.6.2.2 - enable by unknowing voter
1.3.2.6.2.3 - enable by technical consultant
1.3.2.6.2.4 - employ unparameterized attack
1.3.2.6.2.5 - add commands to ballot def file

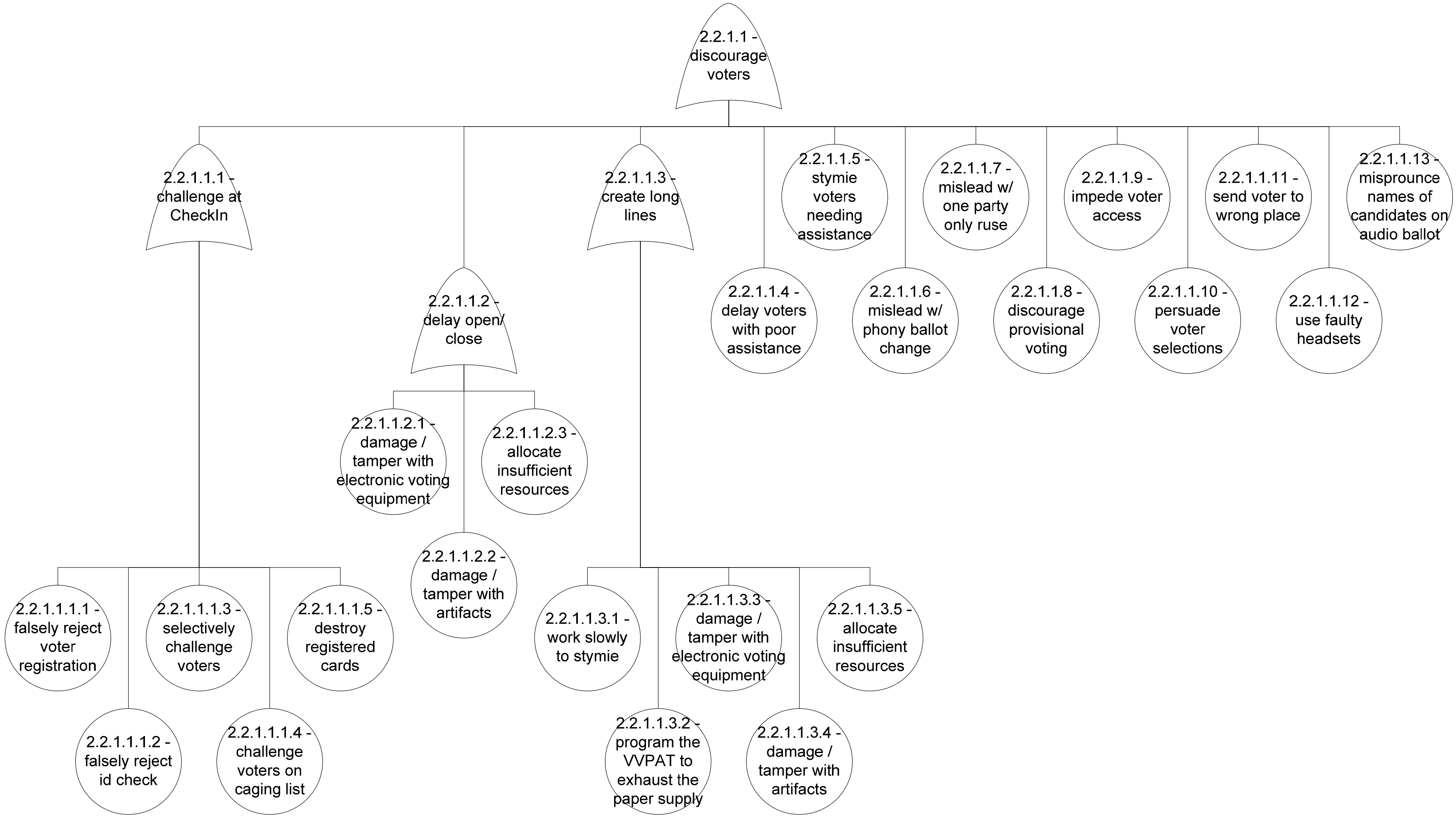
2-4 DRE Attack Software


1.3.3 - attack data
1.3.3.1 - using malware
1.3.3.2 - modify data on storage medium
1.3.3.3 - alter ballot creation software
1.3.3.1.1 - select method and alter
1.3.3.1.2 - alter ballot definition file
1.3.3.1.3 - alter device tallies
1.3.3.1.4 - alter tabulation SW
1.3.3.2.1 - modify tabulation data
1.3.3.2.2 - modify data before use
1.3.3.2.3 - alter electronic ballots using administrator account access
1.3.3.1.1.1 - by malware
1.3.3.1.1.3 - by infected config data
1.3.3.1.1.2 - by infected software
1.3.3.2.2.1 - pre-load votes
1.3.3.2.2.3 - alter config data
1.3.3.2.2.2 - flip votes

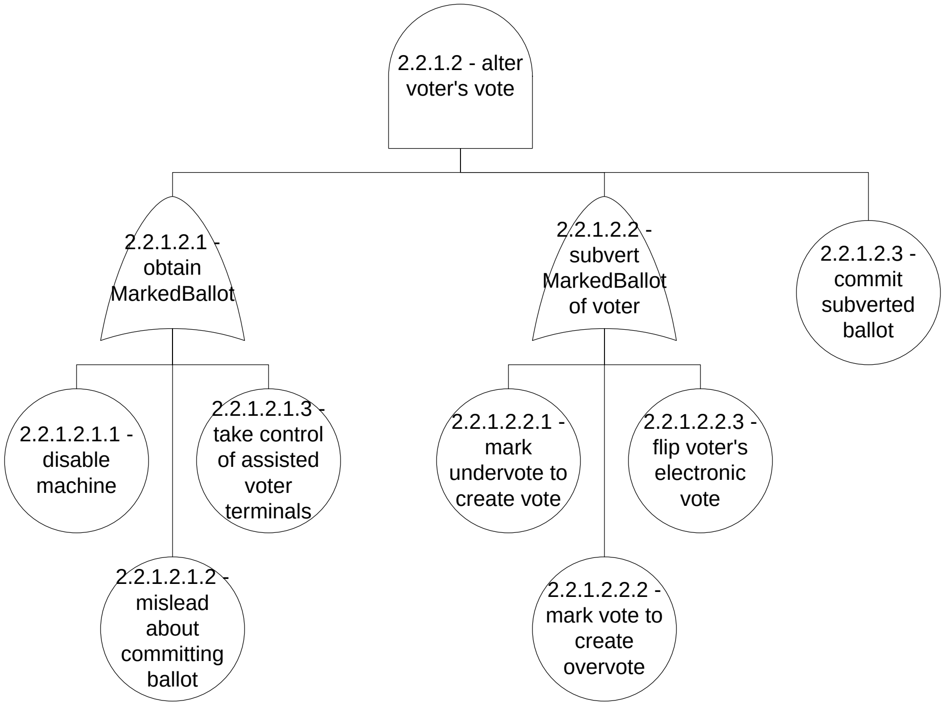
2-5 DRE Attack Data


2 - perform insider attack
2.1 - form inside attack team
2.2 - execute insider attack
2.1.1 - infiltrate as volunteer pollworker
2.1.2 - infiltrate as observer
2.1.3 - staff with attackers
2.1.4 - collude with other insiders
2.1.5 - allow pollworker rotation
2.2.1 - attack at polling place
2.2.2 - attack other than polls
2.2.1.1 - discourage voters
2.2.1.2 - alter voter's vote
2.2.1.3 - send voter to subverted machine
2.2.2.1 - attack ballots
2.2.2.2 - damage electronic voting equipment
2.2.2.3 - misinform about overvoting / undervoting
2.2.2.4 - confuse voters with poor ballot design
2.2.2.5 - force least-objectionable choice
2.2.2.6 - publish invalid sample ballots
2.2.2.7 - stuff ballots after closing
2.2.2.8 - stuff during canvass or recount
2.2.2.9 - errors in ballot adjudication
2.2.2.10 - subvert decision criteria
2.2.2.11 - subvert tabulation
2.2.2.12 - attack tabulated results
2.2.2.3.1 - allow undervotes without warning
2.2.2.3.2 - allow overvotes without warning
2.2.2.3.3 - encourage voter override
2.2.2.9.1 - incorrectly accept provisional ballots
2.2.2.9.2 - incorrectly reject provisional ballots
2.2.2.10.1 - selectively recount
2.2.2.12.1 - subvert reported results
2.2.2.12.2 - falsely announce results
2.2.2.12.3 - alter results transmission

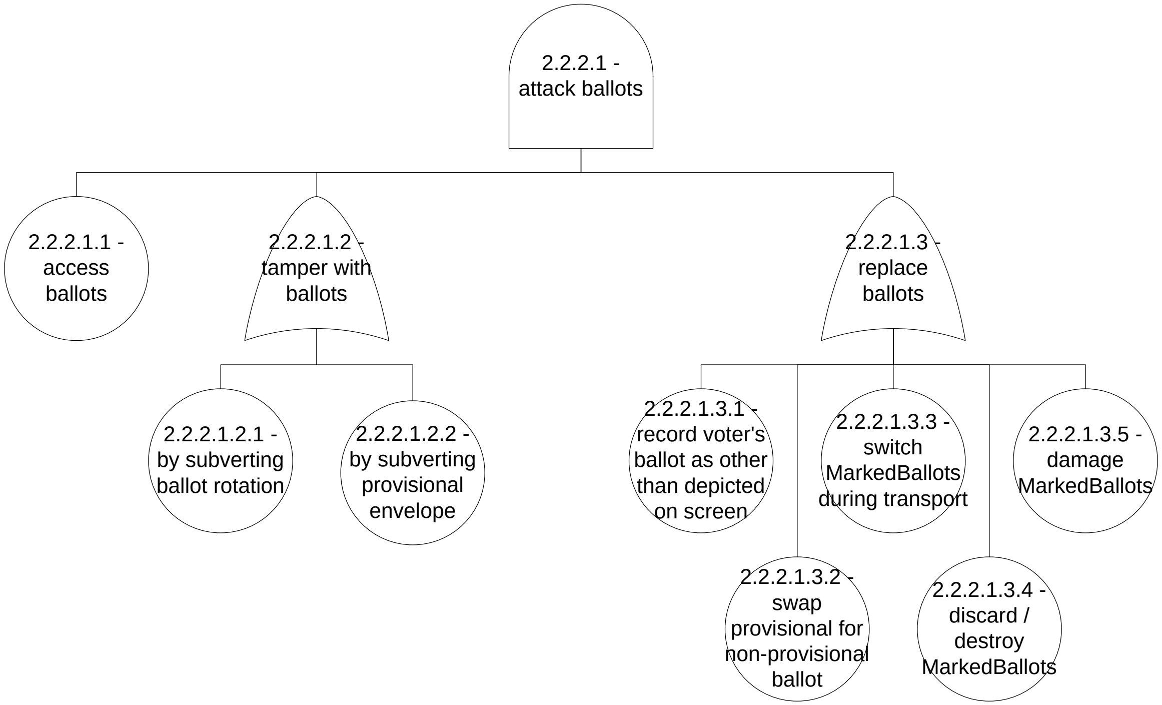
2-6 DRE Insider Attack


2.2.1.1 - discourage voters
2.2.1.1.1 - challenge at CheckIn
2.2.1.1.2 - delay open/ close
2.2.1.1.3 - create long lines
2.2.1.1.4 - delay voters with poor assistance
2.2.1.1.5 - stymie voters needing assistance
2.2.1.1.6 - mislead w/ phony ballot change
2.2.1.1.7 - mislead w/ one party only ruse
2.2.1.1.8 - discourage provisional voting
2.2.1.1.9 - impede voter access
2.2.1.1.10 - persuade voter selections
2.2.1.1.11 - send voter to wrong place
2.2.1.1.12 - use faulty headsets
2.2.1.1.13 - mispronounce names of candidates on audio ballot
2.2.1.1.2.1 - damage / tamper with electronic voting equipment
2.2.1.1.2.2 - damage / tamper with artifacts
2.2.1.1.2.3 - allocate insufficient resources
2.2.1.1.1.1 - falsely reject voter registration
2.2.1.1.1.2 - falsely reject id check
2.2.1.1.1.3 - selectively challenge voters
2.2.1.1.1.4 - challenge voters on caging list
2.2.1.1.1.5 - destroy registered cards
2.2.1.1.3.1 - work slowly to stymie
2.2.1.1.3.2 - program the VVPAT to exhaust the paper supply
2.2.1.1.3.3 - damage / tamper with electronic voting equipment
2.2.1.1.3.4 - damage / tamper with artifacts
2.2.1.1.3.5 - allocate insufficient resources

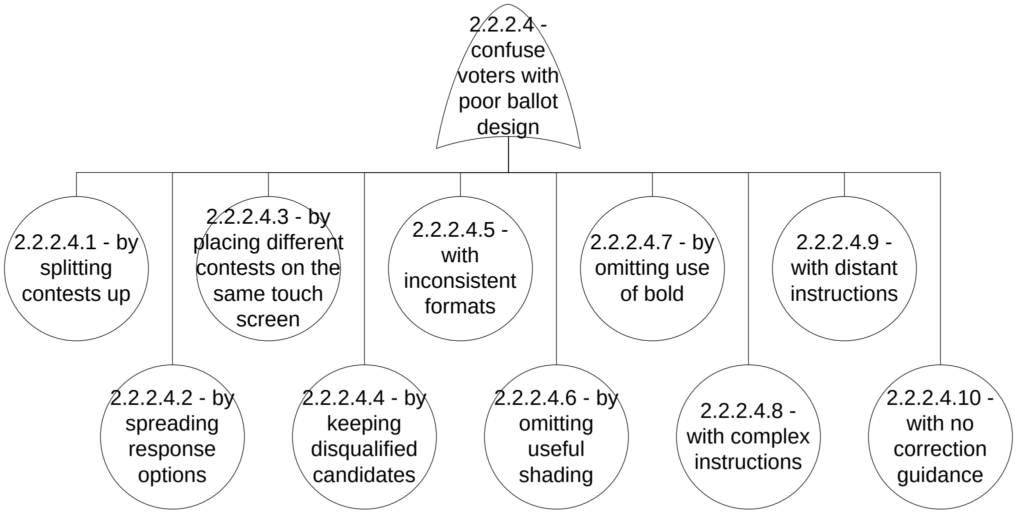
2-7 DRE Discourage Voters


2.2.1.2 - alter voter's vote
2.2.1.2.1 - obtain MarkedBallot
2.2.1.2.2 - subvert MarkedBallot of voter
2.2.1.2.3 - commit subverted ballot
2.2.1.2.1.1 - disable machine
2.2.1.2.1.3 - take control of assisted voter terminals
2.2.1.2.1.2 - mislead about committing ballot
2.2.1.2.2.1 - mark undervote to create vote
2.2.1.2.2.3 - flip voter's electronic vote
2.2.1.2.2.2 - mark vote to create overvote

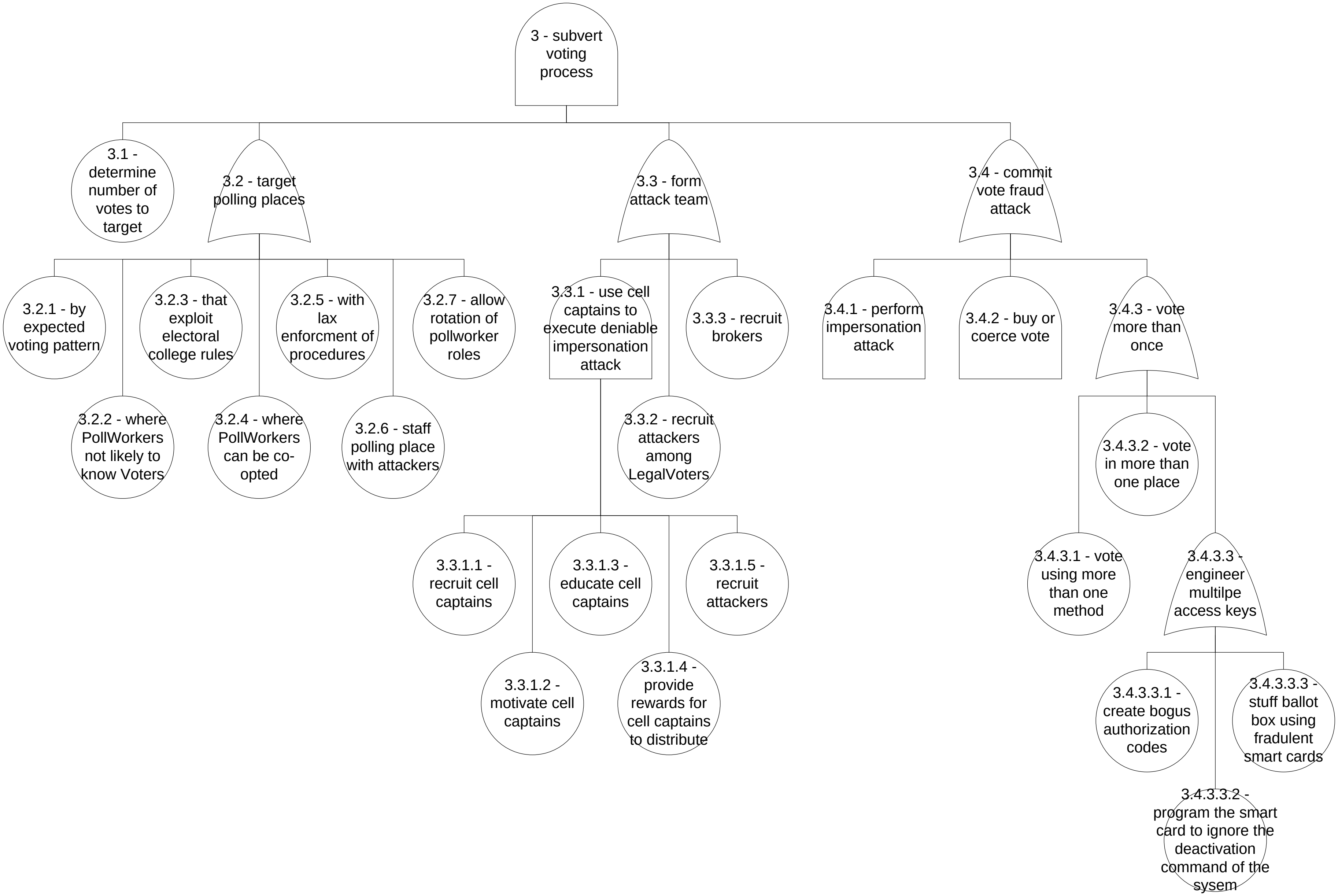
2-8 DRE Alter Voter’s Vote


2.2.2.1 - attack ballots
2.2.2.1.1 - access ballots
2.2.2.1.2 - tamper with ballots
2.2.2.1.3 - replace ballots
2.2.2.1.2.1 - by subverting ballot rotation
2.2.2.1.2.2 - by subverting provisional envelope
2.2.2.1.3.1 - record voter's ballot as other than depicted on screen
2.2.2.1.3.2 - swap provisional for non-provisional ballot
2.2.2.1.3.3 - switch MarkedBallots during transport
2.2.2.1.3.4 - discard / destroy MarkedBallots
2.2.2.1.3.5 - damage MarkedBallots

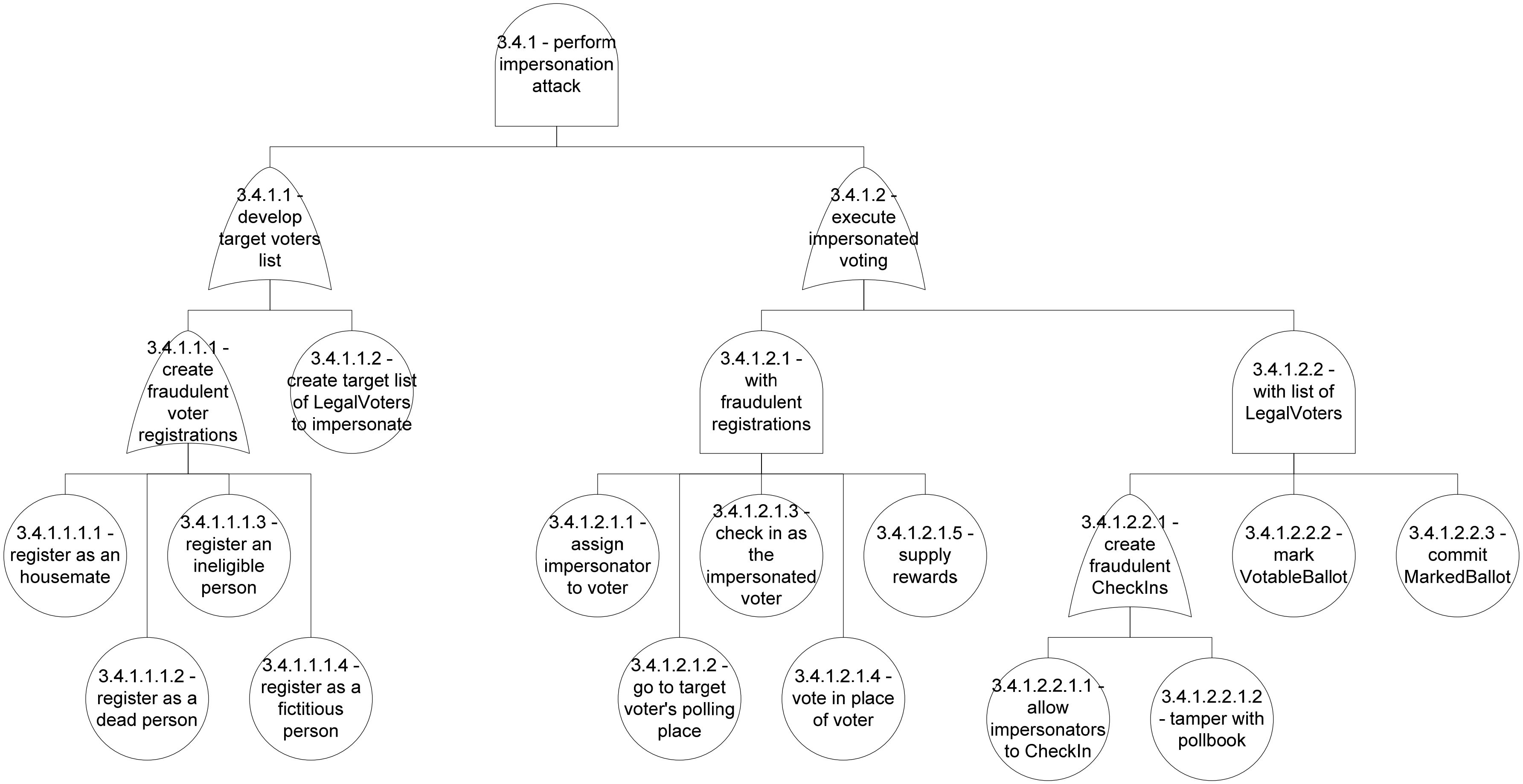
2-9 DRE Attack Ballots


2.2.2.4 - confuse voters with poor ballot design
2.2.2.4.1 - by splitting contests up
2.2.2.4.2 - by spreading response options
2.2.2.4.3 - by placing different contests on the same touch screen
2.2.2.4.4 - by keeping disqualified candidates
2.2.2.4.5 - with inconsistent formats
2.2.2.4.6 - by omitting useful shading
2.2.2.4.7 - by omitting use of bold
2.2.2.4.8 - with complex instructions
2.2.2.4.9 - with distant instructions
2.2.2.4.10 - with no correction guidance

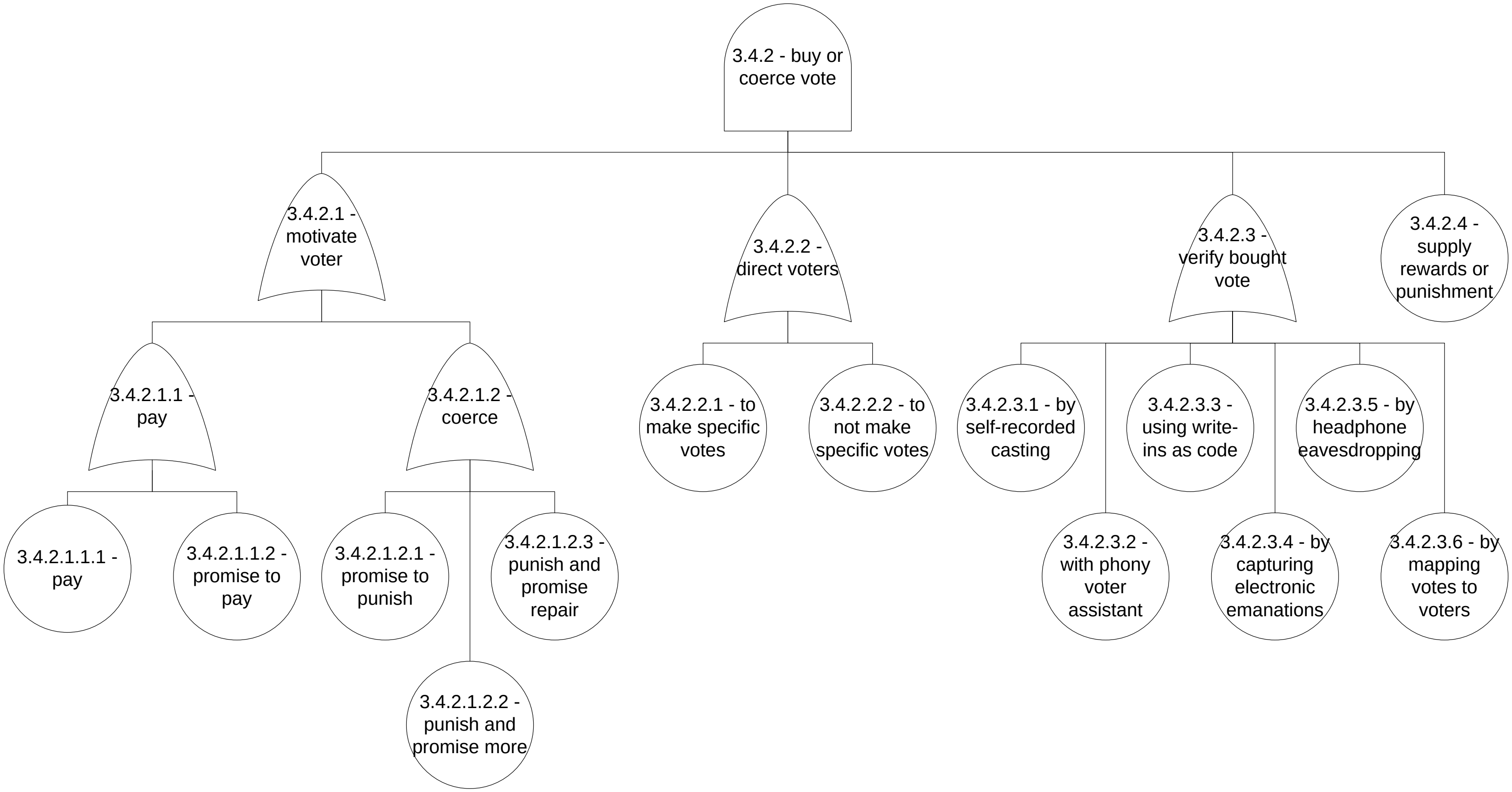
2-10 DRE Confuse Voters with Poor Ballot Design


3 - subvert voting process
3.1 - determine number of votes to target
3.2 - target polling places
3.3 - form attack team
3.4 - commit vote fraud attack
3.2.1 - by expected voting pattern
3.2.2 - where PollWorkers not likely to know Voters
3.2.3 - that exploit electoral college rules
3.2.4 - where PollWorkers can be co-opted
3.2.5 - with lax enforcment of procedures
3.2.6 - staff polling place with attackers
3.2.7 - allow rotation of pollworker roles
3.3.1 - use cell captains to execute deniable impersonation attack
3.3.2 - recruit attackers among LegalVoters
3.3.3 - recruit brokers
3.3.1.1 - recruit cell captains
3.3.1.2 - motivate cell captains
3.3.1.3 - educate cell captains
3.3.1.4 - provide rewards for cell captains to distribute
3.3.1.5 - recruit attackers
3.4.1 - perform impersonation attack
3.4.2 - buy or coerce vote
3.4.3 - vote more than once
3.4.3.1 - vote using more than one method
3.4.3.2 - vote in more than one place
3.4.3.3 - engineer multilpe access keys
3.4.3.3.1 - create bogus authorization codes
3.4.3.3.2 - program the smart card to ignore the deactivation command of the sysem
3.4.3.3.3 - stuff ballot box using fradulent smart cards

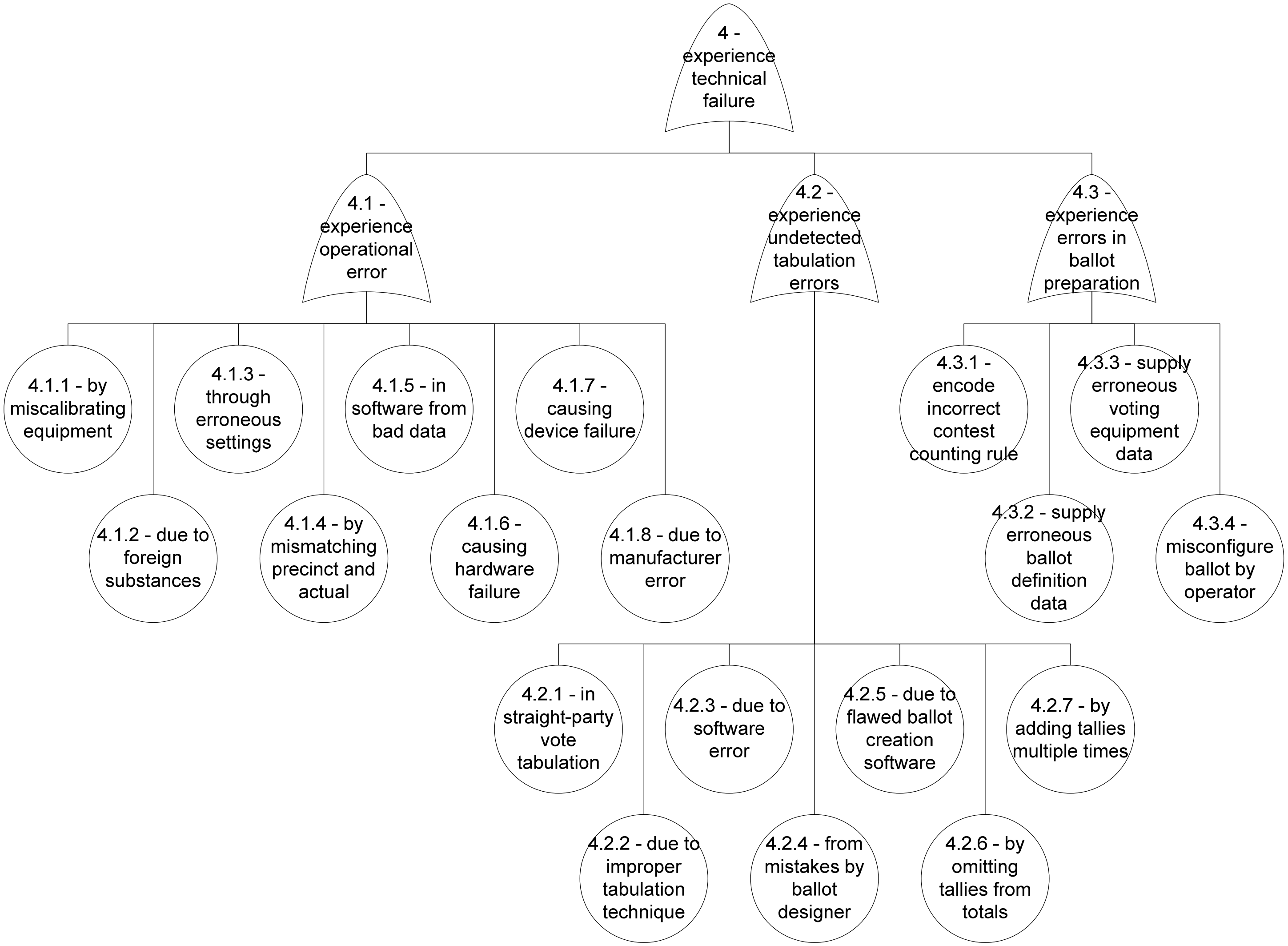
2-11 DRE Subvert Voting Process


3.4.1 - perform impersonation attack
3.4.1.1 - develop target voters list
3.4.1.2 - execute impersonated voting
3.4.1.1.1 - create fraudulent voter registrations
3.4.1.1.2 - create target list of LegalVoters to impersonate
3.4.1.2.1 - with fraudulent registrations
3.4.1.2.2 - with list of LegalVoters
3.4.1.1.1.1 - register as an housemate
3.4.1.1.1.3 - register an ineligible person
3.4.1.1.1.2 - register as a dead person
3.4.1.1.1.4 - register as a fictitious person
3.4.1.2.1.1 - assign impersonator to voter
3.4.1.2.1.3 - check in as the impersonated voter
3.4.1.2.1.5 - supply rewards
3.4.1.2.1.2 - go to target voter's polling place
3.4.1.2.1.4 - vote in place of voter
3.4.1.2.2.1 - create fraudulent CheckIns
3.4.1.2.2.2 - mark VotableBallot
3.4.1.2.2.3 - commit MarkedBallot
3.4.1.2.2.1.1 - allow impersonators to CheckIn
3.4.1.2.2.1.2 - tamper with pollbook

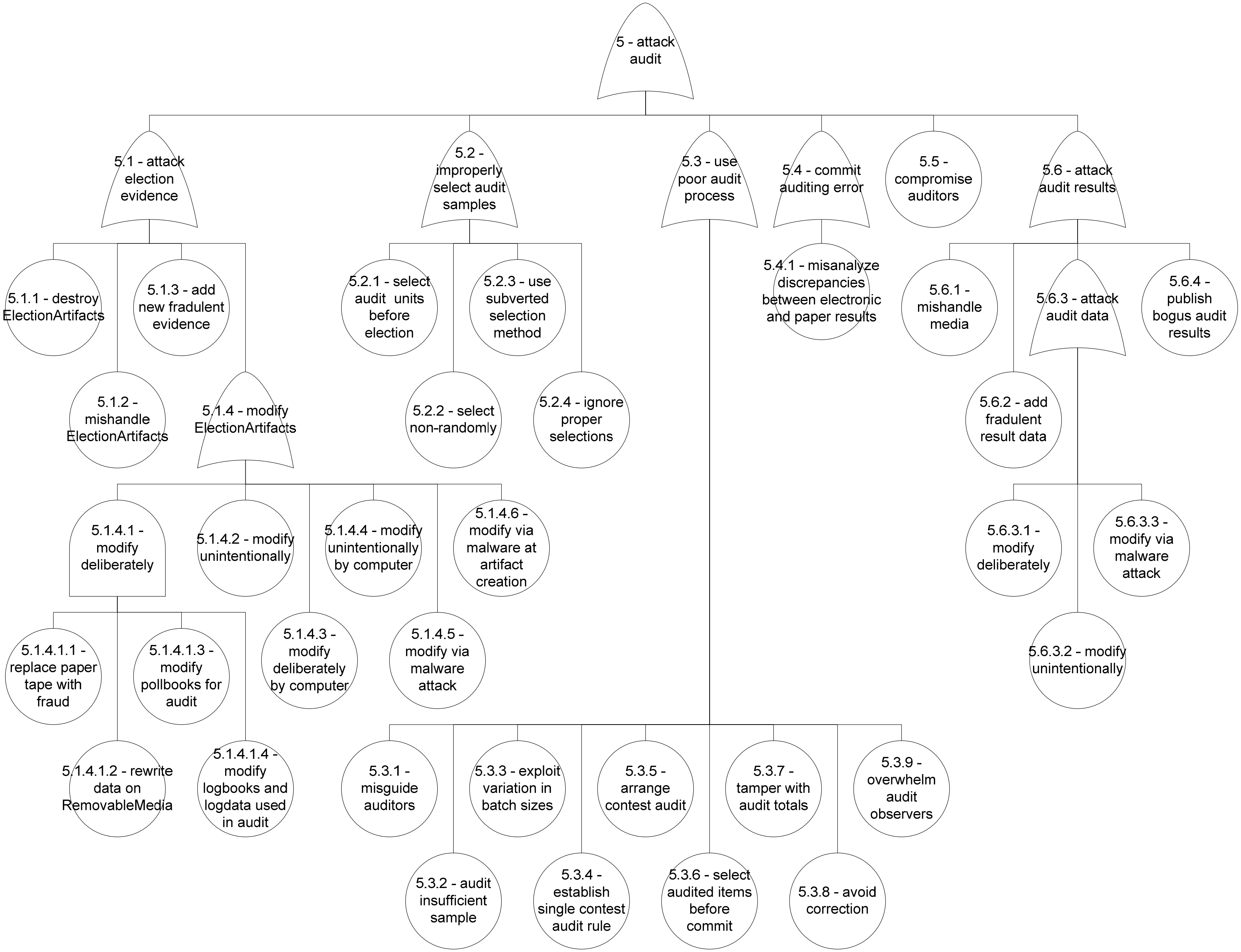
2-12 DRE Perform Impersonation Attack


3.4.2 - buy or coerce vote
3.4.2.1 - motivate voter
3.4.2.2 - direct voters
3.4.2.3 - verify bought vote
3.4.2.4 - supply rewards or punishment
3.4.2.1.1 - pay
3.4.2.1.2 - coerce
3.4.2.2.1 - to make specific votes
3.4.2.2.2 - to not make specific votes
3.4.2.3.1 - by self-recorded casting
3.4.2.3.3 - using write-ins as code
3.4.2.3.5 - by headphone eavesdropping
3.4.2.1.1.1 - pay
3.4.2.1.1.2 - promise to pay
3.4.2.1.2.1 - promise to punish
3.4.2.1.2.3 - punish and promise repair
3.4.2.3.2 - with phony voter assistant
3.4.2.3.4 - by capturing electronic emanations
3.4.2.3.6 - by mapping votes to voters
3.4.2.1.2.2 - punish and promise more

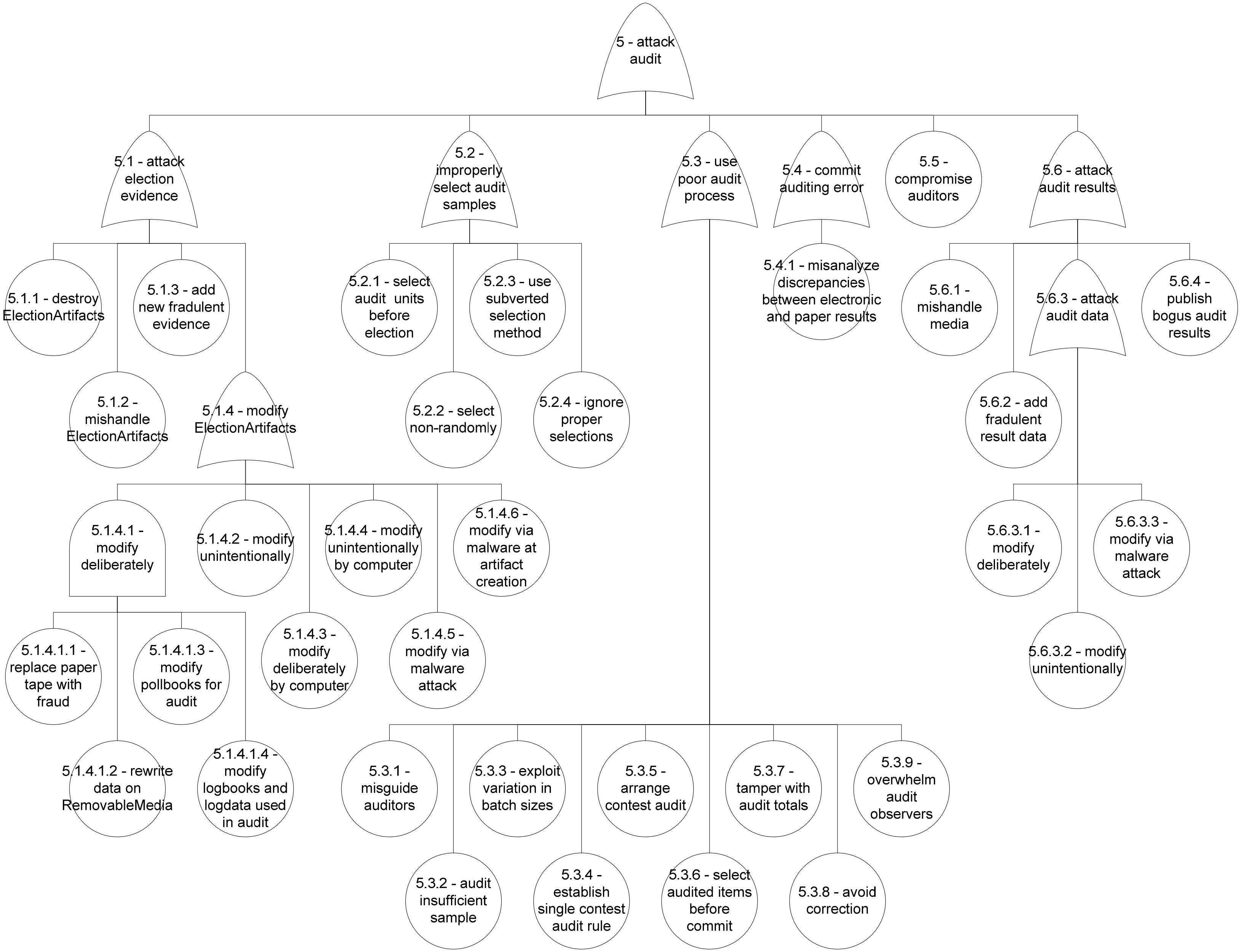
2-13 DRE Buy or Coerce Vote


4 - experience technical failure
4.1 - experience operational error
4.2 - experience undetected tabulation errors
4.3 - experience errors in ballot preparation
4.1.1 - by miscalibrating equipment
4.1.2 - due to foreign substances
4.1.3 - through erroneous settings
4.1.4 - by mismatching precinct and actual
4.1.5 - in software from bad data
4.1.6 - causing hardware failure
4.1.7 - causing device failure
4.1.8 - due to manufacturer error
4.3.1 - encode incorrect contest counting rule
4.3.2 - supply erroneous ballot definition data
4.3.3 - supply erroneous voting equipment data
4.3.4 - misconfigure ballot by operator
4.2.1 - in straight-party vote tabulation
4.2.2 - due to improper tabulation technique
4.2.3 - due to software error
4.2.4 - from mistakes by ballot designer
4.2.5 - due to flawed ballot creation software
4.2.6 - by omitting tallies from totals
4.2.7 - by adding tallies multiple times

2-14 DRE Experience Technical Failure


5 - attack audit
5.1 - attack election evidence
5.2 - improperly select audit samples
5.3 - use poor audit process
5.4 - commit auditing error
5.5 - compromise auditors
5.6 - attack audit results
5.1.1 - destroy ElectionArtifacts
5.1.3 - add new fradulent evidence
5.1.2 - mishandle ElectionArtifacts
5.1.4 - modify ElectionArtifacts
5.1.4.1 - modify deliberately
5.1.4.2 - modify unintentionally
5.1.4.4 - modify unintentionally by computer
5.1.4.6 - modify via malware at artifact creation
5.1.4.3 - modify deliberately by computer
5.1.4.5 - modify via malware attack
5.1.4.1.1 - replace paper tape with fraud
5.1.4.1.3 - modify pollbooks for audit
5.1.4.1.2 - rewrite data on RemovableMedia
5.1.4.1.4 - modify logbooks and logdata used in audit
5.2.1 - select audit units before election
5.2.3 - use subverted selection method
5.2.2 - select non-randomly
5.2.4 - ignore proper selections
5.3.1 - misguide auditors
5.3.3 - exploit variation in batch sizes
5.3.5 - arrange contest audit
5.3.7 - tamper with audit totals
5.3.9 - overwhelm audit observers
5.3.2 - audit insufficient sample
5.3.4 - establish single contest audit rule
5.3.6 - select audited items before commit
5.3.8 - avoid correction
5.4.1 - misanalyze discrepancies between electronic and paper results
5.6.1 - mishandle media
5.6.3 - attack audit data
5.6.4 - publish bogus audit results
5.6.2 - add fradulent result data
5.6.3.1 - modify deliberately
5.6.3.3 - modify via malware attack
5.6.3.2 - modify unintentionally

2-15 DRE Audit Attack


5 - attack audit
5.1 - attack election evidence
5.2 - improperly select audit samples
5.3 - use poor audit process
5.4 - commit auditing error
5.5 - compromise auditors
5.6 - attack audit results
5.1.1 - destroy ElectionArtifacts
5.1.2 - mishandle ElectionArtifacts
5.1.3 - add new fradulent evidence
5.1.4 - modify ElectionArtifacts
5.2.1 - select audit units before election
5.2.2 - select non-randomly
5.2.3 - use subverted selection method
5.2.4 - ignore proper selections
5.4.1 - misanalyze discrepancies between electronic and paper results
5.6.1 - mishandle media
5.6.2 - add fradulent result data
5.6.3 - attack audit data
5.6.4 - publish bogus audit results
5.1.4.1 - modify deliberately
5.1.4.2 - modify unintentionally
5.1.4.3 - modify deliberately by computer
5.1.4.4 - modify unintentionally by computer
5.1.4.5 - modify via malware attack
5.1.4.6 - modify via malware at artifact creation
5.6.3.1 - modify deliberately
5.6.3.2 - modify unintentionally
5.6.3.3 - modify via malware attack
5.1.4.1.1 - replace paper tape with fraud
5.1.4.1.2 - rewrite data on RemovableMedia
5.1.4.1.3 - modify pollbooks for audit
5.1.4.1.4 - modify logbooks and logdata used in audit
5.3.1 - misguide auditors
5.3.2 - audit insufficient sample
5.3.3 - exploit variation in batch sizes
5.3.4 - establish single contest audit rule
5.3.5 - arrange contest audit
5.3.6 - select audited items before commit
5.3.7 - tamper with audit totals
5.3.8 - avoid correction
5.3.9 - overwhelm audit observers

2-16 DRE Disrupt Operations

2.3 DRE Threat Matrix

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	1	attack voting equipment	attack on voting equipment; attack DRE hardware, software, communications links	LTM-USA Delivery 01a	human-deliberate	Voting System	Voting System	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish a chain of custody on VotingMachines; implement personnel security; and provide operational and technical safeguards	
O	1.1	gather knowledge	gather needed technical knowledge	LTM-USA Delivery 01a	human-deliberate	Election System	Voting Machine, sensitive tech data, tech insiders	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection	
T	1.1.1	from insider	hire existing vendor or testing lab insider	LTM-USA Delivery 01a	human-deliberate insider	Election System, Voting System	insider, technology	susceptibility of insiders to bribery and corruption; access that insiders have to voting machines and other election assets	personnel security, including thorough background checks on possible people who may have access to the voting machine	
A	1.1.2	from components	obtain knowledge from voting system components		human-deliberate	Election System, Voting System	Voting Machine	access to voting machines	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection	
O	1.1.2.1	access directly	obtain knowledge directly from a voting system		human-deliberate	Election System, Voting System	Voting Machine	access to voting machines	physical and environmental protection of voting equipment	
T	1.1.2.1.1	infiltrate as insider	get hired as vendor or lab insider	LTM-USA Delivery 01a	human-deliberate outsider	Election System, Voting System	Voting Machine, sensitive tech data	susceptibility of insiders to bribery and corruption; access to voting machine	personnel security, including thorough background checks on possible people who may have access to the voting machine, access controls, and media protection policies	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.2.1.2	obtain a machine	use illegal means to gain access that is available to insiders (e.g., breaking and entering warehouse)	LTM-USA Delivery 01a	human-deliberate	Election System, Voting System	Voting Machine	access to voting machine	physical and environmental protection of voting equipment, including use of tamper resistant or tamper evident seals and tracking of seal numbers, as in a chain of custody set of controls	reverse engineer a stolen machine
T	1.1.2.1.3	legally acquire machine	directly acquire voting system components including equipment, software installed on PC or on voting equipment or copied via network or as source code	LTM-USA Delivery 01a	human-deliberate	Election System	Voting Machine	access to voting equipment that is not controlled like arms, munitions, secrets etc	establish a chain of custody on VotingMachines, including access and personnel policies, audit logs, and media protection policies	Purchase a voting machine on eBay or study a machine in transit
T	1.1.2.1.4	study a machine in transit	steal machines - alter machine - attack machine	LTM-USA Delivery 01a	human-deliberate	Election System	Voting Machine	access to voting machine	thorough background checks on possible people who may have access to the voting machine	
T	1.1.2.1.5	find source code	Find or purchase source code		human-deliberate	Election System	Voting Machine	access to voting equipment that is not controlled like arms, munitions, secrets etc	establish a chain of custody on VotingMachines, including access and personnel policies, audit logs, and media protection policies	
T	1.1.2.1.6	compromise existing source code escrow	attacker obtains source code from existing source code escrow source (e.g., State Election Office)		human-deliberate	Election System	Voting Machine	access to voting equipment that is not controlled like arms, munitions, secrets etc	establish a chain of custody on VotingMachines, including access and personnel policies, audit logs, and media protection policies	
T	1.1.2.2	directly examine	directly examine voting system components to gain knowledge		human-deliberate	Election System, Voting System	Voting Machine	access to voting machines	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection	
T	1.1.3	from published reports	gather knowledge from published reports on the examination of voting machines		human-deliberate	Election System	Voting Machine	access to publicly available information	risk assessment	an attacker reads the California top-to-bottom reviews (TTBRs) of voting machines

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.2	gain insider access	obtain access for attack		human-deliberate outsider	Election System	Voting Machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection; establish system and services acquisition controls	
T	1.2.1	at voting system vendor	gain insider access at voting systems vendor in order to include in the product the ability to enable attacks		human-deliberate outsider	Election System	Voting Machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish chain of custody on VotingMachines	
T	1.2.2	in supply chain	gain insider access in the manufacturing chain, supply chain, or services/ support company, in order to be able to modify equipment and/ or SW install media		human-deliberate outsider	Election System	Voting Machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish chain of custody and system and services acquisition controls	
T	1.2.3	in elections org	gain insider access in elections organizations (and services such as transportation and storage of devices, IT support for PCs that run non-device SW) in order to modify delivered devices and installed SW		human-deliberate outsider	Election System	Voting Machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish chain of custody and system and services acquisition controls	
T	1.2.4	by illegal insider entry	use illegal means to gain access that is available to insiders (e.g., breaking and entering warehouse)		human-deliberate outsider	Election System	Voting Machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	physical and environmental protection of voting equipment	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.5	by remote network access	gain remote access via network-connected PCs running SW components of voting systems		human-deliberate outsider	Election System	Voting Machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	technical controls: access control, audit and accountability, identification and authentication, and system and communications protection	
O	1.3	attack component	perform attack on accessed voting system component, such as hardware, software, data, or communication link		human-deliberate	Election System, Voting System	Voting Machine, Testing, Voting, BallotDefinition	access to voting equipment, availability and willingness of insiders and outsiders, faulty testing, inability of audits / tests to detect	physical and environmental protection, incident response, maintenance, media protection policy and procedures, configuration management, testing	
O	1.3.1	attack hardware	perform physical attack on voting system hardware		human-deliberate	Election System, Voting System	Voting Machine	access to voting equipment	physical and environmental protection, incident response, maintenance, media protection policy and procedures	
O	1.3.1.1	attack stored components	attack storage of voting system components		human-deliberate	Election System, Voting System	Voting Machine	access to voting equipment	physical and environmental protection, incident response, maintenance, media protection policy and procedures	
T	1.3.1.1.1	swap boot media	physically swap boot media		human-deliberate	Election System, Voting System	Voting Machine	access to voting equipment	physical and environmental protection, including procedures limiting the ability of insiders to bring possible substitutes into physical environment; incident response, maintenance, media protection policy and procedures, including use of tamper-evident seals	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.1.1.2	attack install	physically swap install media, and re-install SW, or create situation in which someone else will re-install		human-deliberate	Election System, Voting System	Voting Machine	access to voting equipment	physical and environmental protection, including procedures limiting the ability of insiders to bring possible substitutes into physical environment; incident response; maintenance; media protection policy and procedures, including use of tamper-evident seals; and configuration management	
T	1.3.1.1.3	destroy RemovableMedia	destroy RemovableMedia		human-deliberate	Election System, Voting System	Voting Machine	access to voting equipment	physical and environmental protection, incident response, maintenance, media protection policy and procedures	
A	1.3.2	attack software	perform logical attack on voting system software		human-deliberate	Election System, Voting System	Voting Machine, Testing	access to voting equipment, availability and willingness of insiders and outsiders, faulty testing, inability of audits / tests to detect	system and service acquisition, system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection; and incident response	
T	1.3.2.1	develop malware	develop malware		human-deliberate	Election System	Voting Machine, Testing	ability of hackers to be able to develop new forms of malware	system and information integrity; incident response	
O	1.3.2.2	select targets	select targets for malware		human deliberate	Election System, Voting System		Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows.		

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2.2.1	select precincts by expected voting pattern	Attacker selects a precinct that follows a particular voting pattern making it easier for him to carry out the attack.	NA	human-deliberate	Voting	Polling Place	Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows.	PS2-Position Categorization,PS3-Personnel Sanctions	John is a poll worker. He selects a precinct of his choice to work on election day. He makes the selection based on the voting pattern the precinct follows. Doing so he can carry out the attacks he can on that particular voting pattern with ease. For example, if he is good at injecting malware into the systems with ease, he would select a precinct that uses internet voting pattern.
T	1.3.2.2.2	select all precincts	Attacker selects all precincts		human-deliberate					
O	1.3.2.3	inject malware	exploit existing vulnerability to inject malware	Jones(2005a) #2321	human-deliberate				system and service acquisition, system and information integrity, access control, audit and accountability, identification and authentication, and system and communications protection	An attacker gains physical access to a machine or its removable memory card for as little as a minute and installs malicious code. Voters cast their vote normally, but the malicious code inserted will steal the votes undetectably, modifying all the records, logs and counters to be consistent with the fraudulent vote counts it creates. The malicious code spreads automatically and silently from machine to machine during normal election activities - a VotingMachine virus
T	1.3.2.3.1	by remote bug exploitation	remotely exploit bug in voting system SW running on network-connected PC		human-deliberate				system and communications protection	
T	1.3.2.3.2	by local bug exploitation	locally exploit bug in voting system software that reads data from removable media (e.g., ballot definition files)		human-deliberate				system and communications protection; system and information integrity; media protection policy and procedures	
T	1.3.2.3.3	by human interface exploit	locally exploit bug in voting system software for human interface		human-deliberate				system and communications protection; system and information integrity; media protection policy and procedures	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.3.2.4	execute malware	exploit existing vulnerability to execute malware		human-deliberate				system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
T	1.3.2.4.1	that alters artifact directly	malware changes voting system code or configuration data directly		human-deliberate				system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
T	1.3.2.4.2	that self-propagates	malware installs itself to propagate virally to other instances of the same voting system component		human-deliberate				system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
T	1.3.2.4.3	that remains resident	malware remains resident during this power cycle only, in order to modify voting system code in memory, or tamper with data generated during this power cycle (e.g., vote data)		human-deliberate				system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
O	1.3.2.5	mitigate risk of detection	use procedural means to mitigate risk of detection during testing		human-deliberate				planning, personnel security, system and information integrity	
T	1.3.2.5.1	coerce testing staff	coerce testing staff to suppress information		human-deliberate				personnel security, system and information integrity	
T	1.3.2.5.2	attack after testing	perform malware attack after testing		human-deliberate				planning, system and information integrity, including random testing	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2.5.3	obtain cooperation of testers	bribing testers - tainted test results	LTM-USA Delivery 01a	human-deliberate	voting system	testing	easily bought or persuaded testers	ensure testers follow instructions completely to make sure that everything that you are testing to find is done	
T	1.3.2.5.4	acquire detailed knowledge of testing procedures and scripts	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system		access to knowledge of testing procedures	safeguard testing procedures; develop new testing procedures for each election	
O	1.3.2.6	use infected component	use voting system component that has been compromised by malware		human-deliberate				planning, system and information integrity	
O	1.3.2.6.1	supply cryptic knock	use malware features to mitigate risk of detection during testing, by determining when malware should be active		human-deliberate				planning, system and information integrity, including tests designed detect cryptic knocks, such as random testing, simulating election day volume, and setting date to election day	
T	1.3.2.6.1.1	during logic and accuracy testing	supply cryptic knock during logic and accuracy testing	LTM-USA Delivery 01a	human-deliberate	Voting System	Testing	inability to detect the clever insider's infiltration of the L&A test script; overcoming the defense against cryptic knocks	planning, system and information integrity, perform testing or random testing again after L&A scripts are completed, under the assumption that the test scripts may be compromised	
T	1.3.2.6.1.2	during machine setup	supply cryptic knock during machine setup	LTM-USA Delivery 01a	human-deliberate	Voting System	Poll Worker setup procedures	routine machine setup procedures of Poll Workers, when known, can be used to set off cryptic knock unknowingly	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine; review instructions from vendor for machine to check for possible abnormalities	
T	1.3.2.6.1.3	during voting	supply cryptic knock during voting	LTM-USA Delivery 01a	human-deliberate	Voting System	Voting	Low probability that tests will produce knock-like behavior	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2.6.1.4	as anti-knock	turn off fraud behavior with testing team anti-knock	LTM-USA Delivery 01a	human-deliberate	Voting System	Testing	ElectionOfficial's control over testing procedures	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.3.2.6.1.5	using AC power flicker	use AC power to flicker as knock	LTM-USA Delivery 01a	human-deliberate	Voting System	Testing	failure of tests to mimic knock action	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.3.2.6.1.6	to detect realistic patterns of voting	detect realistic patterns of voting	LTM-USA Delivery 01a	human-deliberate	Voting System	Testing	failure to test machines with realistic patterns of voting	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.3.2.6.1.7	to employ calendar/clock tricks	employ calendar/clock tricks	LTM-USA Delivery 01a	human-deliberate	Voting System	Testing	difficult to detect that the Trojan horse has circumvented the test	system and information integrity, with testing by setting the date to election day in advance	
T	1.3.2.6.1.8	in ballot definition files	deploy cryptic knock in ballot definition files	LTM-USA Delivery 01a	human-deliberate	Voting System	Testing	failure to use real ballot in testing	controls on ballot definition files, including audit and accountability, access control, media protection policy and procedures, physical and environmental protection, and system and information integrity	
O	1.3.2.6.2	control/parameterize attack	control/parameterize attack	LTM-USA Delivery 01a	human-deliberate	Voting System		extremely unlikely that voting pattern can be detected as a knock	physical and environmental protection, media protection policy and procedures, system and communications protection, personnel security, testing	
T	1.3.2.6.2.1	voter enables attack as attacker	voter knowingly enables attack	LTM-USA Delivery 01a	human-deliberate	Voting System		difficult or impossible to detect that a LegalVoter is setting off attack with their voting selections	personnel security, controls that prevent or detect voter impersonation	
T	1.3.2.6.2.2	enable by unknowing voter	voter unknowingly enables attack	LTM-USA Delivery 01a	human-deliberate	Voting System	Legal Voters, campaign	ability of voters to be fooled by false campaign	awareness and training, look for unusual or suspicious write-in campaigns	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2.6.2.3	enable by technical consultant	technical consultant at polling place enables attack during health check, repair, setup, or poll close	LTM-USA Delivery 01a	human-deliberate	Voting System		corrupt consultants to vendors	physical and environmental protection, media protection policy and procedures, including tamper controls, system and communications protection, including encrypted media	
T	1.3.2.6.2.4	employ unparameterized attack	employ unparameterized attack such as party-based attack	LTM-USA Delivery 01a	human-deliberate	Voting System		increased ease for attacker in employing attacks that do not need to know contest-specific parameters	thorough L&A testing and random testing that compares actual vs expected vote totals	
T	1.3.2.6.2.5	add commands to ballot def file	add steganographic commands to ballot definition file	LTM-USA Delivery 01a	human-deliberate	Voting System	Ballot Preparation	lack of supervision of ballot preparation	personnel security, including multi-person controls, and thorough L&A testing to detect mismatches	
O	1.3.3	attack data	perform logical attack on voting system data		human-deliberate				system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection; media protection policy and procedures; configuration management	
O	1.3.3.1	using malware	use malware to change data that effects election outcomes		human-deliberate				system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection, media protection policy and procedures	
O	1.3.3.1.1	select method and alter	select alteration method(s)		human-deliberate				system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection, media protection policy and procedures	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.3.1.1.1	by malware	direct alteration by malware resident with voting system device SW or non-device SW		human-deliberate				system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection	
T	1.3.3.1.1.2	by infected software	alteration by voting system SW that was modified by malware		human-deliberate				system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection	
T	1.3.3.1.1.3	by infected config data	alteration as a result of new configuration data that was modified by malware		human-deliberate				system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection, media protection policy and procedures	
T	1.3.3.1.2	alter ballot definition file	alter ballot definition file data (or predecessor data) to cause a device to record a vote in a particular location as a vote for a candidate/contest other than what is displayed on the ballot ("vote flipping")		human-deliberate				audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
T	1.3.3.1.3	alter device tallies	alter device tallies		human-deliberate				audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
T	1.3.3.1.4	alter tabulation SW	alter results of tabulation software		human-deliberate				audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.3.3.2	modify data on storage medium	use general purpose computer to modify data on the storage media		human-deliberate				physical and environmental protection, personnel security, media protection policy and procedures	
T	1.3.3.3	alter ballot creation software	modify the ballot creation software to produce a ballot that is different than the ballot that was intended	Review Panel	human-deliberate				audit and accountability, system and information integrity, logic and accuracy testing	
T	1.3.3.2.1	modify tabulation data	modify device vote tallies, tabulated vote totals, log data, after data was generated		human-deliberate				audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
O	1.3.3.2.2	modify data before use	modify data before use, to affect election results		human-deliberate				audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
T	1.3.3.2.2.1	pre-load votes	pre-load votes into a device before polls open		human-deliberate				personnel security: multi-person/multi-party observation at poll opening; configuration management: require a zero-count determination and documentation process	
T	1.3.3.2.2.2	flip votes	alter ballot definition file data (or predecessor data), windows manager or other component to cause a device to record a vote in a particular location as a vote for a candidate/contest other than what is displayed on the ballot ("vote flipping")		human-deliberate				planning, system and information integrity: thorough L&A testing and random testing that compares actual vs expected vote totals	John, who is a loyal supporter of Candidate Abby works for the vendor for DRE. He has access to the machine and alters the code to the window manager so votes can be switched to or defaulted to Candidate Abby.
T	1.3.3.2.2.3	alter config data	alter other configuration data of device		human-deliberate				planning, system and information integrity: through testing at multiple levels, including the use boundary analysis to develop test cases for detecting threshold errors	A vendor’s technician is bribed or forced by the political party workers to manipulate the configuration file of a voting machine in such a way that it credits one candidate even though the vote is intended for another candidate. This can be done prior to the election day.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.3.2.3	alter electronic ballots using administrator account access	Voter with technical knowledge can prepare administrators card and the enders card so as to gain access to the administrator account and make changes accordingly	Kohno (2004)	human-deliberate	Voting	Smartcard	lack of authentication process in the machine	installation of card reader that can identify duplicated cards,SC12-Cryptographic key establishment and management, SC13-Use of Cryptography	John is a voter. He is good at programming. Using his technical skills he manages to simulate the administrator's card and the enders card. Doing so he gains access to the administrator account and makes changes accordingly to the ballots.
O	1.3.4	attack comlinks	perform physical and/or logical attack on communications links		human-deliberate				access control and system and communications protection, including cryptography and public access protections	
T	1.3.4.1	attack linked scanner/tabulator	attack serial port connection while device is connected to central tabulator server		human-deliberate				access control and system and communications protection	
T	1.3.4.2	attack wireless	attack wireless communication vulnerability		human-deliberate			On Election Day, a LegalVoter executing a machine attack uses a wireless PDA to trigger malicious code	access control and system and communications protection, including cryptography and public access protections	
A	2	perform insider attack	intentional abuse of insider access and privileges		human-deliberate insider	Voting System	Voting System, Election Artifacts, Voters	insider access, availability and willingness of insiders, difficulty in detection	more transparency of the entire elections process; laws governing the bipartisan appointment of precinct officials and the distribution of duties within a polling place, the configuration of a polling place and access to it, criminalizing voter intimidation, caging; the abuse of the challenge process, training programs for election officials; more aggressive prosecution of violations; effective audits of elections and the ability to respond to attacks by investigating, prosecuting and correcting abuses after the fact	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.1	form inside attack team	form attack team of one or more attackers with insider privileges		human-deliberate insider	Election System, Voting System	Voting System	insider access, availability and willingness of insiders, difficulty in detection	personnel security, awareness and training, incident response, physical and environmental protection	
T	2.1.1	infiltrate as volunteer PollWorker	a lone attacker gains insider privilege by signing up as a PollWorker		human-deliberate insider				personnel security, awareness and training, incident response, physical and environmental protection	
T	2.1.2	infiltrate as observer	gain "insider" access as a poll observer, either by volunteering, or by qualifying, depending on state laws		human-deliberate insider				personnel security, awareness and training, incident response, physical and environmental protection	
T	2.1.3	staff with attackers	use insider privilege of ElectionOfficial to staff polling place or post-polling operations with attackers	Jones(2005a) #31	human-deliberate insider	Voting System	3-12 Check Poll Book for Authenticate Voter Activity Diagram	attacker access to polling place and fraudulent check-in enabled	improve the administration of voting on the election day	John is a poll worker having access to the poll books and he can verify the voter authentication. He can take advantage of this situation by allowing ineligible voters whose entry is not present in the poll book to vote by providing the VotableBallots.
T	2.1.4	collude with other insiders	collude with one or a few other insiders, possibly using bribery or coercion; either at the polling place, central operations, or between both		human-deliberate insider				personnel security, awareness and training, incident response, physical and environmental protection	an ElectionOfficial forms a collusive arrangement between a polling place and central operations, for the purpose of having either party overlook the potential abuses being committed by the other party
T	2.1.5	allow PollWorker rotation	allow rotation of PollWorker roles, as a single person PollWorker attacks are more likely when different duties are handled by the same person		human-deliberate insider	Voting	3-9 Elections Official / Poll Worker for Voter Check In Activity Diagram	poor election laws / policies / guidelines	establish chain of custody procedures on at-risk ElectionArtifacts; provide for both separation of duties, as well as multi-person, multi-party controls	John, a poll worker colludes with the election-official to subvert separation of duties. He handles the poll book and issues ballots to certain voters

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.2	execute insider attack			human-deliberate insider	Voting System	Voting System, Election Artifacts	insider access, availability and willingness of insiders, difficulty in detection	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1	attack at polling place	perform insider attack at polling place	LTM-USA Delivery 01a	human-deliberate insider	Voting System	voters		personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1.1	discourage voters	intentionally discourage voters from voting	Jones(2005a) # 211 Jones(2005a) #332	human-deliberate insider	Voting System	3-12 Check Poll Book for Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal Poll Workers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Poll workers intentionally refuse to allow the voter to vote even though voters name is present on the county register of voters.
O	2.2.1.1.1	challenge at CheckIn	challenge voters during CheckIn		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.1.1.1	falsely reject voter registration	falsely reject voter claiming they are not registered		human-deliberate insider	Voting System	3-12 Check Poll Book for Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal Poll Workers' decisions	provide appeal process for oversight of PollWorker	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.1.1.2	falsely reject id check	falsely reject voter on identification check		human-deliberate insider	Voting System	3-11 Provide Credential	unwillingness or inability of voters to appeal Poll Workers' decisions	provide appeal process for oversight of PollWorker	
T	2.2.1.1.1.3	selectively challenge voters	selectively challenge voters, such as "undesirable" voters in polling place	Jones #212	human-deliberate insider	Voting	Voter CheckIn	ability of Poll Workers or collusions of Poll Workers to control voter CheckIn; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A corrupt PollWorker may use race, gender, appearance of age, a person's attire, etc., as a means of "profiling" a voter, and then selectively challenge a person's voter status based upon the expectation that a person fitting that profile will vote contrary to attacker
T	2.2.1.1.1.4	challenge voters on caging list	creating a caging list and question voters' right to vote	Levitt (2007)	human-deliberate insider		Eligible Voters; SendToSeniorPW; 3-12	disclosing information of voters	chain of custody for voter lists, including access control policies	The attacker sends registered mail to addresses of registered voters that they've identified as likely to be unfriendly to their candidate. All mail that is returned as undeliverable is placed on what is called a caging list. Then this list is used to challenge the registration or right to vote of those names on it.
T	2.2.1.1.1.5	destroy registered cards	a third party working on behalf of voter registration encourages people to register and after the registration process destroy or discard their cards	Ballotpedia (2008)	human-deliberate insider		registered cards	lack of management oversight over third party	Get the details from third party and mail the voter Id's to the voters instead asking third party to handover the id's.	John volunteers to help register voters before the election. Unknowingly to the officials, he was bribed by the Candidate to destroy voters' cards after the registration process is over.

O	2.2.1.1.2	delay open/close	delay opening or close with plausible excuses; preventing the voters from voting by making long queues and working slowly leading the voters leave the polling place	Jones (2005a) #33	human-deliberate insider	Voting System	2.1 VotableBallot for Ballot State Transition Diagram;
							3.9 Authenticate Voter for Voter check In activity diagram;
							3-10 Authenticate Voter for Voter Check In Dataflow diagram.
								inability to detect that Poll Worker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A poll worker at a particular precinct works slowly e.g. he intentionally verifies the voter's authentication details slowly and issues the votable ballots to the voters slowly making the voters form long lines. Due to long waiting time few voters who cannot wait will leave the polling place without casting the vote.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.1.2.1	damage / tamper with electronic voting equipment	physical destruction of voting equipment; tampering with equipment	Jones (2005a) #231; 232	human-deliberate	Voting System	Voting Machine	access to equipment, fragility of computer-equipment	AC-3, AC-5, PE-3 physical access control , PE-6 monitoring physical access	
T	2.2.1.1.2.2	damage / tamper with artifacts	physical destruction of artifacts; tampering with artifacts		human-deliberate					malfunction of paper feed for VVPAT
T	2.2.1.1.2.3	allocate insufficient resources	allocate insufficient equipment or PollWorkers		human-deliberate					
O	2.2.1.1.3	create long lines	create long lines		human-deliberate insider	Voting	Voters		personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.1.3.1	work slowly to stymie	intentionally stymie voters by working slowly		human-deliberate insider	Voting System	Voting process	inability to detect that Poll Worker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.1.3.2	program the VVPAT to exhaust the paper supply	malicious software causes the VVPAT device to exhaust the paper supply thereby delaying poll opening.	Diebold TTBR (pp. 67)	human-deliberate	voting	3-14 One voter	malware can be injected into software	Inspection and testing	
T	2.2.1.1.3.3	damage / tamper with electronic voting equipment	physical destruction of voting equipment; tampering with equipment	Jones (2005a) #231; 232	human-deliberate	Voting System	Voting Machine	access to equipment, fragility of computer-equipment	AC-3, AC-5, PE-3 physical access control , PE-6 monitoring physical access	
T	2.2.1.1.3.4	damage / tamper with artifacts	physical destruction of artifacts; tampering with artifacts		human-deliberate					

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.1.3.5	allocate insufficient resources	allocate insufficient equipment or PollWorkers		human-deliberate					
T	2.2.1.1.4	delay voters with poor assistance	delay voters by failing to properly assist		human-unintentional				planning, including rules of behavior; PollWorker awareness and training; and personnel policies, including sanctions for poor performance	
T	2.2.1.1.5	stymie voters needing assistance	intentionally stymie voters needing assistance; voter manipulation - improper assistance to voters - improper advantage taken of voters with legitimate need for assistance	Jones (2005a) #332	human-deliberate insider	Voting System		lack of management oversight over poll workers designated to assist at polls	improve the administration of voting on the election day; let the voters be aware of the rules and regulations prior to the election day improve the PollWorker training	jam / interfere with telephone with headphone communication. John is a poll worker for a particular precincts election and is responsible for assisting voters who need help while marking the ballot. His main aim in this threat attack is to stymie the voters from voting. By working slowly he could stymie voters who need assistance who are waiting for him to be available or he could stymie all voters by occupying a voting station for an extended period or by making himself unavailable for other poll duties.
T	2.2.1.1.6	mislead w/phony ballot change	mislead voters by announcing phony last-minute ballot change		human-deliberate insider	voting	Eligible Voter, Signed In Voter	susceptibility of voters to believe what was being informed by the poll worker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	PollWorker passes out the activation keys to voters can tell them there has been a changed on the ballot.
T	2.2.1.1.7	mislead w/one party only ruse	mislead voters by announcing that only one party is allowed to vote		human-deliberate insider	voting	Eligible Voter, Signed In Voter	susceptibility of voters to believe what was being informed by the Poll Worker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker tells voters that only registered voters of one party is allowed to vote

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.1.8	discourage provisional voting	discourage provisional voting		human-deliberate insider	voting	3-12 Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal Poll Workers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker turns voter away by not issuing a provisional ballot
T	2.2.1.1.9	impede voter access	impede voter access to physical polling place; an attacker selectively prevents voters from some precincts, typically under some kind of color of authority.		human-deliberate insider	Voting	Voters and Voting	If a voter must be present at a particular location (e.g. precinct) to cast a ballot, it is possible to prevent the voter from voting by physical exclusion.	Physical security at polling places; public education	A sheriff in a rural jurisdiction, unlikely to be observed by media or activists, impedes some voters from getting to the polling place by conducting improper traffic stops outside select precincts
T	2.2.1.1.10	persuade voter selections	persuade the voter to vote a certain way	Jones(2005a) #332	human-deliberate insider	Voting	Voting Activity	lack of decisiveness in the voter, lack of management oversight over Poll Workers	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	PollWorker / ElectionOfficial / Voter during the day of election intrudes into personnel privacy of the voter and tries to persuade him to cast his vote a certain way with suggestive, though non-threatening remarks
T	2.2.1.1.11	send voter to wrong place	erroneously send voter to other polling place		human-unintentional				planning, including rules of behavior; PollWorker awareness and training; and personnel policies, including sanctions for poor performance	
T	2.2.1.1.12	use faulty headsets			Technical	Voting	voting equipment, voters	poor quality of equipment; failure to test properly	testing and vendor management	
T	2.2.1.1.13	mispronounce names of candidates on audio ballot	The pronunciation of a candidate's name is incorrect and voters do not recognize the candidate. Lost vote.		human-deliberate, unintentional	voting	3-14 One voter	Pronunciation of names is not standardized and subject to local accents		

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	2.2.1.2	alter voter's vote	steal voter's vote in polling place	LTM-USA Delivery 01a	human-deliberate insider	Voting System			personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1.2.1	obtain MarkedBallot	create plausible reason to obtain MarkedBallot before electronic commit		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.1.1	disable machine	disable the voter's DRE terminal before they commit ballot		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.1.2	mislead about committing ballot	mislead voters about correct commitment of ballot	http://www.lex18.com/Global/story.asp?S=10037216&nav=menu203_2	human-deliberate insider	voting	3-14 One voter	Poll Workers have discretion to instruct voters and voters do not tend to read informative signage	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	The PollWorkers told the voters to walk away after the first confirmation. After which, PollWorkers changed their votes.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.2.1.3	take control of assisted voter terminals	take advantage of voters needing assistance by seizing control of their DRE terminal		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1.2.2	subvert MarkedBallot of voter	subvert MarkedBallot of CheckedIn Voter at polls		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.1	mark undervote to create vote	mark undervote to create vote		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.2	mark vote to create overvote	mark vote to create overvote		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.2.2.3	flip voter's electronic vote	change voter's vote on the electronic Marked Ballot to some other vote; flip vote		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.3	commit subverted ballot	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones(2005a) #41	human-deliberate insider	Voting System	3-32 [[Absentee]] for Provide Credential (Remote) Activity Diagram	lack of supervision or other monitoring / poll observers	improved administration of voting on the election day; Video recording after the polls close	
T	2.2.1.3	send voter to subverted machine	direct targeted voters to use faulty machine		human-deliberate insider	Voting	CheckedIn Voter	voter dependence on instructions from Poll Workers	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	configure a terminal to operate test mode, and direct targeted voters to vote on those machines
O	2.2.2	attack other than polls	perform insider attack at other than polling place		human-deliberate insider	Voting System			election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
A	2.2.2.1	attack ballots	perform attacks on VotableBallots or MarkedBallots	Jones (2005a) #421	human-deliberate insider				establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.1.1	access ballots	access ballots as an insider		human-deliberate insider				establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
O	2.2.2.1.2	tamper with ballots	alter or destroy ballots obtained		human-deliberate insider				establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.2.1	by subverting ballot rotation	tamper with ballot design so that ballot rotation is subverted		human-deliberate insider				audit and accountability, system and information integrity, using testing that attempts to validate rotation	
T	2.2.2.1.2.2	by subverting provisional envelope	tamper with provisional ballot envelope to cause rejection; an envelope is altered to change it from an accepted ballot to a rejected ballot	Dallas (2008)	human-deliberate insider	Voting, Canvass	Committed provisional Ballot	access to / lack of control or custody of Committed Ballot	access controls, auditing and logging	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.2.2.1.3	replace ballots	switch legitimate ballots with tampered ballots		human-deliberate insider				establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.3.1	record voter's ballot as other than depicted on screen	attacker miscalibrates the hardware and software of the voting machine so ballot image will capture fraud data	FLCVEF(1994)	human intentional or unintentional	Voting	3-24 Mark Ballot for HCI Select Activity Diagram	Software and hardware could have been miscalibrated	AC-1 access control policy and procedures, AC-3 access enforcement	Polly cast her vote for Candidate A, however the tampered DRE recorded her vote for Candidate B.
T	2.2.2.1.3.2	swap provisional for non-provisional ballot	malicious software prints VVPAT receipt for provisional ballot for favored candidate. It then takes the next non-provisional ballot for the disfavored candidate and prints a provisional receipt.	Diebold TTBR (pp. 23 #4)	human-deliberate	voting	3-14 One voter	malware can be injected into software	Educate voters to verify their VVPAT	
T	2.2.2.1.3.3	switch MarkedBallots during transport	substitute memory card (add, delete, change memory card) during transport to central location	Jones(2005a) #413	human-deliberate insider	precinct closeout	3-35 One voter (Remote) Activity Diagram - Ballot Delivery, 3-36 One Voter (Remote) Data Flow Diagram	failure to take the details of the person transferring the votes to the central location	physical and environmental protection-Delivery and Removal, , personnel security-Third Party personnel security	Person responsible for transporting the envelopes swaps out cards or entire envelopes.
T	2.2.2.1.3.4	discard / destroy MarkedBallots	use private access to discard or destroy a memory card	Dill (2008)	human-deliberate insider	State Accumulation, Canvass, Post Certification	Precinct Closeout, Deliver To Jurisdiction, etc. Any activity where one person or a group of collaborating people, can gain private access to a physical ballot box.	corrupt poll-worker / election-official	Ballot accounting, chain of custody, personnel screening	John is a PollWorker at a precinct that follows DRE voting system pattern. He has access to the memory card. He somehow manages to steal the secure digital (SD) memory card which contains the information on the cast votes. This could be a large scale election theft that could change an election outcome.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.1.3.5	damage MarkedBallots	damage memory card		human-deliberate insider	State Accumulation, Canvass, Post Certification	Precinct Closeout, Deliver To Jurisdiction, etc. Any activity where one person or a group of collaborating people, can gain private access to a physical ballot box.	corrupt poll-worker / election-official	Ballot accounting, chain of custody, personnel screening	
T	2.2.2.2	damage electronic voting equipment	physical destruction of voting equipment	Jones (2005a) #231	human-unintentional	Voting System	Voting Machine	fragility of computer equipment, mishandling	PL-4 PollWorker rules of behavior, PE-3 physical access control , PE-6 monitoring physical access	a voter wearing golf spikes steps on a power strip
O	2.2.2.3	misinform about overvoting / undervoting	provide incorrect information about overvotes and undervotes		human-unintentional				planning, including rules of behavior; PollWorker awareness and training; and personnel policies, including sanctions for poor performance	
T	2.2.2.3.1	allow undervotes without warning	allow undervotes without warning		human-unintentional				planning, including rules of behavior; PollWorker awareness and training; and personnel policies, including sanctions for poor performance	Poor ballot format caused voters to miss the 2006 Thirteenth Congressional District race while paging through their electronic ballots. The touch screen system failed to warn voters of the undervote before casting the ballot.
T	2.2.2.3.2	allow overvotes without warning	allow overvotes without warning		human-unintentional				planning, including rules of behavior; PollWorker awareness and training; and personnel policies, including sanctions for poor performance	
T	2.2.2.3.3	encourage voter override	encourage voter override of over/under-votes		human-unintentional				planning, including rules of behavior; PollWorker awareness and training; and personnel policies, including sanctions for poor performance	
O	2.2.2.4	confuse voters with poor ballot design	poor ballot design that confuses or misleads voters during Voting process, or fails to prevent voter errors in marking ballot	Norden (2008)	human-unintentional	Ballot Preparation	Validate Ballot Style, 3-3, CheckedInVoter	weak reviewing process of a ballot design	use ballot design checklist, implement usability testing, review and amend election laws	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.4.1	by splitting contests up	split candidates for the same office onto different pages or columns	Norden (2008) #1 p. 20	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	use ballot design checklist, implement usability testing, review and amend election laws (* note the above also applies to thread id # 557 - 568), list all candidates for the same race on the same page in the same column	The 2000 presidential race in Palm Beach county, Florida has high residual vote rate due to confusing ballot design that displayed candidates in separate columns with response options in the center - hence the term "butterfly ballot".
T	2.2.2.4.2	by spreading response options	place response options on both sides of candidate names	Norden (2008) #3 p. 28	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	place response options (such as fill-in-the-ovals) in a consistent place on the ballot, such as one side of candidate names or ballot or ballot question choices	Response options placed on both sides of the candidate's name caused confusion among Hamilton county voters in Illinois. Voters tend to mark the arrow to the right of the candidate's name when they were supposed to mark the arrows on the left.
T	2.2.2.4.3	by placing different contests on the same touch screen	poor ballot design	Norden (2008) #2 p. 24, Frisina (2008)	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	place only one contest on the each screen, at least for federal and statewide races.	Ballot format was to blame for the large undervote in the 2006 Thirteenth Congressional District race in Sarasota county. Voters were confused as they were presented with two different contests on the same screen. As a result, Democrat Christine Jennings lost the race to Republican Vern Buchanan by a certified margin of 369 votes.
T	2.2.2.4.4	by keeping disqualified candidates	leave columns or rows for disqualified candidates	Norden (2008) #5 p. 32	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	Failure to remove disqualified candidates from ballot; Failure to inform voters of disqualified candidates	remove the entire column or row for any candidate or party that has been withdrawn or disqualified (not just the candidate or party name)	The 2004 Presidential race in Montgomery county, Ohio has a higher overvote rate when the name of Ralph Nader was replaced with the words "Candidate Removed"
T	2.2.2.4.5	with inconsistent formats	inconsistently design ballots in formatting and style	Norden (2008) #6 p. 36, Frisina (2008)	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	use consistent format and style for every contest and voting action	The inconsistent use of colors in Sarasota county ballot caused voters to skip the Thirteenth Congressional District race. The second page shows "State" highlighted in teal which is the same as the first page's "Congressional" word. Thus, it was easy to overlook the congressional district race.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.4.6	by omitting useful shading	omit shading to help voters differentiate between voting tasks	Norden (2008) #7 p. 40	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	shade certain text, such as office name to help voters to differentiate between voting tasks	Failure to shade office titles on ballot result in higher residual vote rate in Escambia county, Florida. The affected races were Attorney General and Commissioner of Agriculture.
O	2.2.2.4.7	by omitting use of bold	omit bold text to help voters differentiate between voting tasks	Norden (2008) #8 p. 44	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	bold certain text, such as office name to help voters to differentiate between voting tasks	Misused of bold-faced text on the Franklin county ballot in Illinois made it difficult for voters to differentiate contests within each type. Hence, the residual votes were higher for the Attorney General and the Secretary of State races.
T	2.2.2.4.8	with complex instructions	fail to write short, simple instructions	Norden (2008) #9 p. 46	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	write short instructions with simple words	The 2004 presidential race in Kansas experienced high residual vote rate due to the long and confusing instruction on the ballot. For example, they used complicated words such as "Deface" and "wrongfully mark" instead of "make a mistake".
O	2.2.2.4.9	with distant instructions	place Instructions far from related actions	Norden (2008) #10 p. 48	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	place specific instructions and related actions together.	Nonpartisan voters in Los Angeles county, California were told to indicate their party choice before voting in partisan contests. Failure to do so, votes cast for party contest will not count.
T	2.2.2.4.10	with no correction guidance	fail to inform voters how to correct paper ballots	Norden (2008) #11 p. 54	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	include information of how to correct paper ballots if voters make mistakes	Lincoln county, Tennessee had a high residual vote rate compared to the state's residual vote rate for the 2002 Senate race. The ballots in Lincoln did not have instructions for voters who wished to correct their ballots if mistakes were made.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.5	force least-objectionable choice	force least-objectionable candidate voting	VNOTA (2009)	operational	Ballot Preparation	Votable Ballot	lack of acceptable candidates running for office	system and information integrity-9, allow for "none-of-the above" choices in contests	After incumbent governor Buddy Roemer finished 3rd in the general election, Louisiana voters were faced with a lesser-of-two-evils choice between Edwin Edwards, long dogged by allegations of corruption, and David Duke, the former Ku Klux Klan leader, in the 1991 gubernatorial run-off. Without a none-of-the-above choice, voters could either undervote or choose. Edwards won and eventually went to prison for racketeering.
T	2.2.2.6	publish invalid sample ballots	publish sample ballots different from actual ballots	Norden (2008) #13 p. 58	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	publish actual ballots that looks the same as the sample ballots	The actual ballot used on the election day in Sarasota county looked very different from the sample ballot. Almost all voters saw the confusing ballot layout for the first time when they were in the voting booth.
T	2.2.2.7	stuff ballots after closing	stuff ballot box after the polls close	Jones (2005a) #413	human-deliberate insider				election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Person responsible for sealing the envelopes slips in extra memory cards while other PollWorkers were occupied with other closeout activities.
T	2.2.2.8	stuff during canvass or recount	inject ballot box (of physical ballots) during canvass or recount	Epstein (2007), Greenmeier (2008)	human-deliberate insider	Canvas, Post Certification Audit	Validate Total, Process Remote Ballots	After the election, during the validate process, ballot boxes may be placed where they will be found in storage rooms, elections officials' cars, etc.	Ballot watermarking, ballot accounting, registration reconciliation	1. During a recount, an elections official places and then "finds" a memory card in a key-controlled storage room and presents the card to the canvassing board for inclusion in the count. 2. During a recount, a poll worker places, and then finds, a memory card in the trunk of their car and presents these ballots to the canvassing board for inclusion in the count.
O	2.2.2.9	errors in ballot adjudication			human-unintentional				planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.9.1	incorrectly accept provisional ballots	incorrectly accept provisional ballots enclosed in envelopes with disqualifying information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #5	human-unintentional	Canvass	3-50 Validate Precinct Results, 3-51 Resolve Provisional Ballots, Reconcile Voter Feedback	lack of oversight; human error; lack of voter being informed; inability of voter to protest	PollWorker training, labeling provisional ballots or other distinguishing them from other ballots, audit provisional ballot data	In King County, Washington in 2005, it was alleged that election officials were counting provisional ballots in parallel with absentee ballots, which could have resulted in accepting provisional ballots for voters who had already voted absentee
T	2.2.2.9.2	incorrectly reject provisional ballots	incorrectly reject provisional ballots in envelopes with fully compliant information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #6	human-unintentional, operational	Canvass	3-50 Validate Precinct Results, 3-51 Resolve Provisional Ballots, Reconcile Voter Feedback	fallibility of human judgment; misinterpretation of rules	training; auditing and logging	In a 2005 Washington governor's race, King County election officials admitted that 348 provisional ballots had been improperly counted before the voters' registration status could be determined.
O	2.2.2.10	subvert decision criteria	subvert ballot decision criteria		human-deliberate insider				election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	2.2.2.10.1	selectively recount	selectively recount by county or precinct		human-deliberate insider	Canvass, State Accumulation, Post Certification Audit	Validate Total, Recount	Election law	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	An elections official or political operative may trigger selective recounts in order to capture additional votes, expecting that changes in the selected counties will favor their candidate.
T	2.2.2.11	subvert tabulation	intentionally commit errors in tabulation (i.e., counting)		human-deliberate insider, human-unintentional, operational				election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	precinct submitted twice without warning from system
O	2.2.2.12	attack tabulated results	attack results of tabulation process	Jones (2005a) #6	human-deliberate insider				security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.12.1	subvert reported results	impersonate PollWorker reporting preliminary precinct results; malicious outsider threatens the PollWorker to disclose false results to the jurisdiction so as to change the election outcome.	Jones(2005a) #51	human-deliberate insider	Canvass	3-49 Get Precinct Results Flow Chart	Poll Worker impersonation to alter the precinct result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	John is a malicious outsider. He tries to threaten the PollWorker who is responsible for reporting the preliminary precinct results to the jurisdiction. Being threatened by the attacker the PollWorker announces false results by not considering few ballots like provisional ballots and absentee ballots changing the outcome of the election.
T	2.2.2.12.2	falsely announce results	falsely announce tabulation results; announcement of tabulation result ignoring actual ballots	Jones (2005a) #51	human-deliberate insider	Canvass, State Accumulation	3-48 UnofficialResults, 3-54 ReportResults	dependence on key election official(s) with centralized power to announce / certify result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, separation of duties, physical access controls, auditing and accountability, such as verifying results against tabulated; incident monitoring and reporting; making whole process more transparent to media and public	
T	2.2.2.12.3	alter results transmission	Results will be transmitted to county elections department on the election night. There are chances that the precinct results might be altered before transmitting them to the elections department.	Jones(2005a) #611	human-deliberate insider	precinct closeout	Precinct Result	Attacker can alter the transmission of precinct results by adding a counterfeit ballot box, ignoring the provisional votes etc.	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	John is a PollWorker responsible for tabulating the votes on the election night. This includes all kinds of votes like the absentee ballots, early votes, provisional ballots etc. He can use his influence and try to manipulate the precinct results by ignoring the ballots or by adding counterfeit ballots so as to match the original count of votes since the precinct results will be telephoned to the election department by the inspector prior to transmission.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	3	subvert voting process	subvert polling place voting process		human-deliberate, operational	Voting System, Election System	Voting, Voters, Ballots, Poll Workers, Polling Places	susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	planning, risk assessment, awareness and training, incident response, media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
T	3.1	determine number of votes to target			human-deliberate	Voting System, Election System	Voters, Polling Places	availability of information to aid attack strategy	risk assessment, incident response, personnel security	
O	3.2	target polling places			human-deliberate	Voting System, Election System	Poll Workers, Polling Places	availability of information to aid attack strategy	risk assessment, incident response, personnel security	
T	3.2.1	by expected voting pattern	select a precinct that follows a particular voting pattern making it easier to carry out the attack	NA	human-deliberate	Voting	Polling Place	Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows	personnel security, including Position Categorization and Personnel Sanctions	John is a poll worker. He selects a precinct of his choice to work on election day. He makes the selection based on the voting pattern the precinct follows. Doing so he can carry out the attacks he can on that particular voting pattern with ease. For example, if he is good at injecting malware into the systems with ease, he would select a precinct that uses internet voting pattern.
T	3.2.2	where PollWorkers not likely to know Voters	target polling places where poll workers are not likely to know voters		human-deliberate		Poll Workers, Authenticate Voter, 3-9, 3-10	Poll Workers do not know voters	risk assessment, incident response	
T	3.2.3	that exploit electoral college rules	use winner-take-all electoral college design to tempt a selective attack in a tight presidential race	Campbell (2008), p. 337	human-deliberate	Voting System, Election System	Voting System, Election System	availability of polling data enables careful calculation of the number of votes needed to win, which can be leveraged by the winner-take-all electoral design	recommend that states award electoral votes in proportion to popular vote	Several tight presidential elections (1844, 1876, 1884, 1888, 1960, and 2000) could have been turned by fraud in a few selected areas (Campbell 2008, p. 337)
T	3.2.4	where PollWorkers can be co-opted			human-deliberate				risk assessment, incident response	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.5	with lax enforcement of procedures			human-deliberate				risk assessment, incident response	
T	3.2.6	staff polling place with attackers	voter manipulation- allowing ineligible individuals to vote by staffing polling places with attackers	Jones(2005a) #31	human-deliberate	voting system	3-12 Check Poll Book for Authenticate Voter Activity Diagram	attacker access to polling place and fraudulent CheckIn enabled	improve the administration of voting on the election day	John is a poll worker having access to the poll books and he can verify the voter authentication. He can take advantage of this situation by allowing ineligible voters whose entry is not present in the poll book to vote by providing the votable ballots.
T	3.2.7	allow rotation of PollWorker roles	a single person PollWorker attacks are more likely when different duties are handled by the same person		human-deliberate	Voting	3-9 Elections Official / Poll Worker for Voter Check In Activity Diagram	poor election laws / policies / guidelines	AC-5 separation of duties	John, a poll worker colludes with the election-official to subvert separation of duties. He handles the poll book and issues ballots to certain voters
O	3.3	form attack team	recruit sufficient impersonating attackers		human-deliberate	Election System	potential recruits, Eligible Voters	availability and willingness of recruits	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
A	3.3.1	use cell captains to execute deniable impersonation attack	use cell captains to execute deniable impersonation attack	Jones (2005a) #31	human-deliberate	Voting System	Authenticate Voter, 3-9, 3-10	political influence / power of political leaders or election officials	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.3.1.1	recruit cell captains	recruit cell captains		human-deliberate	people being recruited		corruptibility or vulnerability of political loyalists of political leader	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.3.1.2	motivate cell captains	educate and motivate cell captains in deniable ways		human-deliberate	people being recruited		insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.3.1.3	educate cell captains	educate captains in deniable ways		human-deliberate	people being recruited		insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.3.1.4	provide rewards for cell captains to distribute	provide cell captains with rewards to distribute		human-deliberate	people being recruited		insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.3.1.5	recruit attackers	cell captains recruit more attackers	Jones (2005a) #311	human-deliberate	Voters		corruptibility of potential impersonators; resources of attackers	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.3.2	recruit attackers among LegalVoters	subvertible voters are gathered to increase the impact of a voting attack	Jones (2005b)	human-deliberate	Voting System		susceptibility of voters to being bribed or intimidated	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.3.3	recruit brokers	recruit brokers to buy voters; attacker recruits loyal followers, giving them cash bills to buy votes on behalf of attacker's choices	Campbell (2006) pp. 278, 282, 337	human-deliberate	Voting System, Election System	Eligible Voter, Signed In Voter	attacker's power to acquire significant resources	expand campaign finance reform to cover wholesale vote-buying; prosecute voting conspiracies, including vote haulers and voters; maintain ballot secrecy	A Dodge County, GA, county commissioner used $15,000 in $20 bills, giving $4,000 to one vote "hauler" to buy votes at the $20 going rate; one county commissioner forced his road department employees to work on the campaign or else lose their jobs (Campbell 2008, p. 282)
O	3.4	commit vote fraud attack			human-deliberate	Voting System, Election System	Voting, Voters, Ballots, Poll Workers, Polling Places	susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	chain of custody controls on ballots, polling place security, multi-party observers	
A	3.4.1	perform impersonation attack	perform voter impersonation attack	LTM-USA Delivery 01a	human-deliberate	Voting System	Voting System, 3-1,3-2	accessibility of lists of voters not likely to vote; soft voter authentication process; Poll Workers don't know voters; willingness of Poll Workers to engage in fraud	media protection policy and procedures, personnel security, access control, audit and accountability, identification and authentication	Tom is a party worker who has contacts with ElectionOfficial. Getting EligibleVoters' personal information is an easy task for Tom. He can even prepare a list of EligibleVoters who are unlikely to vote this time through his contacts. After preparing a list, he then prepares fake Id's and bribes a group of loyal followers to impersonate the voters on his list. He sends impersonators to the polling places where PollWorkers are not likely to recognize them.
O	3.4.1.1	develop target voters list			human-deliberate					
O	3.4.1.1.1	create fraudulent voter registrations		Jones(2005a) #1	human-deliberate	Election System			strengthen the controls in the ElectionSystem	
T	3.4.1.1.1.1	register as an housemate	recruit registers impersonators as housemates / roommates	Jones(2005a) #11, 12	human-deliberate	Voting System	people being recruited	corruptibility or vulnerability of recruits	strengthen the controls in the ElectionSystem	A party worker may hire non voters from different state, prepare fake IDs and register them as housemates of LegalVoters and ask them to vote for his/her party candidate.
T	3.4.1.1.1.2	register as a dead person	register as a deceased or incapacitated person	Jones(2005a) #12	human-deliberate				strengthen the controls in the ElectionSystem	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.1.1.1.3	register an ineligible person	register as an unregistered but ineligible person (e.g., non-citizens, felons)	Jones(2005a) #1	human-deliberate				strengthen the controls in the ElectionSystem	
T	3.4.1.1.1.4	register as a fictitious person	use a fake Id to register as a fictitious voter	Jones(2005a) #11,12	human-deliberate	Voting System	Authenticate Voter, 3-9, 3-10	soft verification process	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	
T	3.4.1.1.2	create target list of LegalVoters to impersonate	make lists of voters very unlikely to vote this election or likely to vote late in the day		human-deliberate		voter registration databases	access to voter lists and ability to determine voters not likely to vote	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election participation records by voter are available. Attacker parses data to detect voting patterns and prepares a list of EligibleVoters who are unlikely to vote this time through his contacts.
O	3.4.1.2	execute impersonated voting			human-deliberate					
A	3.4.1.2.1	with fraudulent registrations			human-deliberate				physical and environmental protection, audit and accountability, identification and authentication	
T	3.4.1.2.1.1	assign impersonator to voter	supply attackers with information about unlikely voter (e.g., name and gender)		human-deliberate	Voting System	Poll Workers, Authenticate Voter, 3-9, 3-10	Poll Workers fooled by unknown attacker with valid voter information	physical and environmental protection, audit and accountability, identification and authentication	
T	3.4.1.2.1.2	go to target voter's polling place	impersonator goes to polling place of target voter	Jones(2005a) #311	human-deliberate		voters	susceptibility of insiders to bribery and corruption	physical and environmental protection, including patrolling polling places, looking for suspicious activity	
T	3.4.1.2.1.3	check in as the impersonated voter	attacker has friends vote for the fake housemates	Jones(2005a) #311	human-deliberate	Voting System	Poll Workers, Authenticate Voter, 3-9, 3-10	Poll Workers fooled by unknown attacker with valid voter information	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.1.2.1.4	vote in place of voter	impersonate and vote in the place of an EligibleVoter; a list of voters who are unlikely to vote may be prepared and people may be recruited to vote for that person. A polling place where a PollWorkers are not likely to know voters may be targeted.	Jones (2005a) #311	human-deliberate	Voting System	Authenticate Voter, 3-9, 3-10	access to lists of voters not likely to vote; Poll Workers don't know voters; corrupt Poll Worker	require Credentials at polling places; conduct precise and careful purges on voter lists to remove duplicate names, people who have moved, died, or are otherwise ineligible.	
T	3.4.1.2.1.5	supply rewards	cell captain provides all required rewards out of own pocket		human-deliberate		voters	susceptibility of insiders to bribery and corruption	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers, physical and environmental protection, limiting access to polling place and providing polling place patrols	
A	3.4.1.2.2	with list of LegalVoters		Jones (2005a) #311 Jones (2005a) #312 Wvvotes.com (2008)	human-deliberate insider	Voting System	3-12 Check Poll Book for Authenticate Voter Activity Diagram	unsecured poll book; corrupt official who coerces other poll workers	limited/no access to the ballot boxes to the PollWorkers after the polls close improve administration of the PollWorkers on the election day	John as a poll worker has the responsibility of recording the voters in the poll book. He uses his position and influence, and fills the polling place with attackers letting them vote for no-show voters.
O	3.4.1.2.2.1	create fraudulent CheckIns			human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	3.4.1.2.2.1.1	allow impersonators to CheckIn	allow impersonators to fraudulently CheckIn for LegalVoters		human-deliberate insider					

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.1.2.2.1.2	tamper with poll book	tamper with poll book to reduce the risk of detection either during the day or after the polls close		human-deliberate insider	Voting System	Poll book	unsecured poll book; lack of supervision	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	3.4.1.2.2.2	mark VotableBallot	mark VotableBallot		human-deliberate insider				personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	a PollWorker casts fraudulent votes on the way to or from the poll to a curbside voting event
T	3.4.1.2.2.3	commit MarkedBallot	commit MarkedBallot		human-deliberate insider					
A	3.4.2	buy or coerce vote	motivate voters to either (a) stay away from polls or (b) vote in compliance with attacker demands	Dekel (2004), Fund (2004), Jones(2005a) #21	human-deliberate outsider	Voting System, Election System	Eligible Voter	susceptibility of voters to buying and coercion; breach of voter privacy; ability to attribute vote	maintain voter privacy; limit access to polling place	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
O	3.4.2.1	motivate voter	motivate voter with bribes or threats		human-deliberate	Voting	Eligible Voter	human susceptibility to being bribed or coerced	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers, physical and environmental protection, limiting access to polling place and providing polling place patrols	"Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future." (Fund 2004)

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	3.4.2.1.1	pay	make a direct payment to voters using cash or some other desirable exchange	Fund (2004), Dekel (2004), Campbell (2006) pp. 144, 282, Estep (2009), Campbell (2006) pp. 278, 283	human-deliberate	Voting	Eligible Voter	human susceptibility to being bribed	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers, maintain ballot secrecy	I had no choice. I was hungry that day,' Thomas Felder told the Miami Herald in explaining why he illegally voted in a mayoral election. 'You wanted the money; you were told who to vote for.'"(Fund 2004) In 1910, the price of a vote was "a drink of whiskey" (Campbell 2006, p. 144); in 2002, two Clay County, KY, election officers allegedly used the prescription painkiller OxyContin to buy votes (Estep 2009) In a 1987 Kentucky race, the price for a vote reached $200, while in 1996 Dodge County, Georgia, the going rate was $20 per vote (Campbell 2008)
T	3.4.2.1.1.1	pay	make a direct payment to voters using cash or some other desirable exchange	Fund (2004), Dekel (2004), Campbell (2006) pp. 144, 282, Estep (2009), Campbell (2006) pp. 278, 283	human-deliberate	Voting	Eligible Voter	human susceptibility to being bribed	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers, maintain ballot secrecy	'I had no choice. I was hungry that day,' a voter told the Miami Herald 'You wanted the money, you were told who to vote for.'(Fund 2004) In 1910, the price of a vote was "a drink of whiskey" (Campbell 2006, p. 144); in 2002, two Clay County, KY, election officers allegedly used OxyContin to buy votes (Estep 2009) In a 1987 Kentucky race, the price for a vote reached $200, while in 1996 Dodge County, Georgia, the going rate was $20 per vote (Campbell 2008)
T	3.4.2.1.1.2	promise to pay	promise payment later or promise payment based on subsequent verifiability of voter's carry out attacker's voting demands	Jones(2005a) #311	human-deliberate	Voting	Eligible Voter	susceptibility of voters to bribery	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	3.4.2.1.2	coerce	coerce the voter to vote for the attacker's candidate(s)		human-deliberate	Voting	Eligible Voter	human susceptibility to being coerced	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers	Off-duty policemen were hired to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters; a consent decree forswearing all such 'ballot security' programs in the future was signed. (Fund 2004)
T	3.4.2.1.2.1	promise to punish	promise some form of punishment in order to coerce voter	Van Acker	human-deliberate	Voting	Eligible Voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers	An incumbent candidate seeking reelection sends a loyal confederate to the polls accompanying the incumbents' employees, who are coerced to vote for the incumbent, once they receive their votable ballots
T	3.4.2.1.2.2	punish and promise more	provide a real punishment, and then promise more punishment of not compliant		human-deliberate	Voting	Eligible Voter		personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers	
T	3.4.2.1.2.3	punish and promise repair	provide a real punishment, and then promise a repair of punishment		human-deliberate	Voting	Eligible Voter		personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers	
O	3.4.2.2	direct voters		Jones (2005a) #32, Jones(2005b)	human-deliberate	Voting	Eligible Voter	corrupt Poll Worker or voter who can easily be intimidated; Poll Workers and poll observers unable to detect concealed ballots	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.2.2.1	to make specific votes	direct voter to make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	Voting	Eligible Voter	corrupt Poll Worker or voter who can easily be intimidated; Poll Workers and poll observers unable to detect concealed ballots	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
T	3.4.2.2.2	to not make specific votes	direct voter to not make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	Voting	Eligible Voter	corrupt Poll Worker or voter who can easily be intimidated; Poll Workers and poll observers unable to detect concealed ballots	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
O	3.4.2.3	verify bought vote	assess voter compliance with direction		human-deliberate	Voting	Voter	inability to prevent voter attribution	prevent voter attribution with ballot secrecy, preventing stray marks, and making sure that voter assistance is legitimately needed	to ascertain that a bribed voter goes along with the vote fraud, attacker attempts to verify that voter voted for attacker's choices
T	3.4.2.3.1	by self-recorded casting	use a secret camera to self-record voter's ballot casting	Dekel (2004)	human-deliberate	Voting	Eligible Voter, Signed In Voter	secret ballot	Tighten the security of voting system	Voter manages to capture video of his ballot casting, produces it to the attacker as evidence.
T	3.4.2.3.2	with phony voter assistant	assist voter at precinct to verify bought vote; voter requests assistance in order to earn reward from assistant	Jones (2005a) #333	human-deliberate	Voting	3-12 SignPollBook, 3-48 Validate Precinct Results	failure to authenticate voter's assistant; failure to detect unusual patterns of assistance (same assistant, higher than normal assistance)	audit and accountability audit precinct results and investigate any unusual voting patterns, such as a high percentage of voter assistance or repeated assistance by the same assistant; prevent by asking voter for reason assistance needed	A man wearing dark glasses and appearing to be sight-impaired shows up with an assistant to help him vote. Following the procedures for check-in, the voter and the assistant obtain a VotableBallot, which is then marked and committed with the full knowledge and help of the assistant, who provides a cash payoff afterwards.
T	3.4.2.3.3	using write-ins as code	write in a candidate name that provides voter attribution		human-deliberate	Voting	Votable Ballot	ability of voter to take advantage of free-form entry in write-in	investigate unusual patterns of write-ins	voter votes for attacker candidates and then votes for a write-in candidate by writing in a predetermined code word intended for an inside confederate to see and verify the bought vote

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.2.3.4	by capturing electronic emanations	eavesdropping on voter's vote using electronic emanations	Fishcher (2003), Review Panel	human-deliberate	Voting	Voting Machine	Lack of use of recent technology to stop electronic emanation from being compromised	use of latest technology for protecting of exploitation of electromagnetic emanation,AC18-Wireless Access Restrictions,SC14-Public Access Protections	John is a malicious outsider. He bribes or intimidates the voters on the election day to cast them to member of his choice. John makes use of compromising electronic emanations from voting machines to reproduce DRE screens in a vehicle near the polling place. He intimidates or corrupts the voters to make certain combinations of selections and changes to enable perpetrator to identify which voter is using which machine to keep track of the votes cast by them.
T	3.4.2.3.5	by headphone eavesdropping	eavesdropping headphone output		human-deliberate	Voting			polling place security; not allowing electronic devices that could be eavesdropping into the polling place	
T	3.4.2.3.6	by mapping votes to voters	record the voter sequence and read the corresponding VVPAT records	Wallach (Review Panel)	human-deliberate	Voting	Secret Ballot		personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and PollWorkers	Voters are instructed to use a specific voting booth. The sequence of voters is recorded for that voting booth. The VVPAT record is examined using the voter sequence to read the votes.
T	3.4.2.4	supply rewards or punishment	provide promised rewards or punishments based on voter compliance		human-deliberate	Voting			personnel security, including sanctions against violators	
O	3.4.3	vote more than once	a LegalVoter votes more than once; ballot box stuffing by the voter		human-deliberate	Voting	Voting	inability of voting system to capture duplicate votes by a voter	system and information integrity, identification and authentication	
T	3.4.3.1	vote using more than one method	vote early and regular, or absentee and provisional as a form of ballot box stuffing	Jones (2005a) #41, TIRA panel	human-deliberate	Voting	3-33 Authenticate Voter (remote), 3-31 Voter List, Voter Information, Authenticate Voter, Authentication Rules, Jurisdiction	inability to or failure to cross-check poll books for different voting methods within a single place (jurisdiction)	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	a voter casts an absentee ballot but then votes again at the polling place on election day

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.3.2	vote in more than one place	vote in two neighboring states or multiple precincts with registrations in more than one place	Jones (2005a) #11, 312	human-deliberate	Voting	3-31 Voter List, Voter Information, Authenticate Voter, AuthenticationRules, Jurisdiction	inability to or failure to cross-check voter lists across multiple jurisdictions	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	a husband and wife who move from Pensacola, FL to Mobile, AL prior to a federal election registers and votes in Alabama, then drives to Pensacola on same election day, voting in the precinct for their former address
O	3.4.3.3	engineer multiple access keys			human-deliberate					
T	3.4.3.3.1	create bogus authorization codes	Voter guesses authentication code (perhaps 4 digit code) and votes multiple times		human-deliberate	voting	3-14 One voter	Authorization codes could be easily guessable	Use sufficiently large and random authorization codes	
T	3.4.3.3.2	program the smart card to ignore the deactivation command of the system	Voter will simulate a smart card using his technical skills and use it for casting the vote	Kohno (2004)	human-deliberate	Voting	Smartcard	lack of cryptography, lack of authentication of the card by the machine	SC12-Cryptographic key establishment and management,SC13-Use of Cryptography	John is a voter. He is good at programming. He uses his technical skills to prepare a smart card by himself and programs it in such a way that the machine he uses to vote doesn't deactivate the smart card after voting. This way he uses his card repeatedly casting multiple votes.
T	3.4.3.3.3	stuff ballot box using fraudulent smart cards	voter manipulation-voter can create a valid smart card that matches the DREs requirements, he might be able to cast multiple votes	Jones (2005a) #311	human-deliberate	Voting	Voting Activity	Duplicate the smartcards	PE6-Monitoring Physical Access	With the knowledge of hard coded key used with voter cards, it is possible to forge valid voter cards. Also, between the time a voter's voter card is activated by the poll worker and used, it can be duplicated and used multiple times, without any knowledge of the hard coded key. Smart card duplication equipment can be hidden easily on a voter's person.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	4	experience technical failure	experience a unintentional technical failure		technical				certification, accreditation, and security assessments, planning, system and services acquisition, awareness and training, configuration management, contingency planning, incident response, maintenance, media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, system and communications protection	
O	4.1	experience operational error	experience or commit voting equipment operational errors		technical				system and services acquisition, system and information integrity, maintenance, awareness and training, physical and environmental protection, contingency planning	
T	4.1.1	by miscalibrating equipment	calibration failures or errors		technical				system and services acquisition, system and information integrity, maintenance, awareness and training, physical and environmental protection, contingency planning, testing (as part of polling place opening and periodically while polls are open)	A PollWorker can surreptitiously re-calibrate the screen in a way that allows most input to behave normally but that denies access to specific regions or a terminal can be maliciously re-calibrated to prevent voting for certain candidates or to cause voter input for one candidate to be recorded for another
T	4.1.2	due to foreign substances	paper feed mis-calibration, foreign objects, dust/dirt/grit		technical				maintenance	
T	4.1.3	through erroneous settings	erroneous date/time settings, precinct ID setting, other election specific settings		technical				DM, system and information integrity, awareness and training	
T	4.1.4	by mismatching precinct and actual	mis-match of device's programmed precinct and actual precinct		technical				system and information integrity	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.1.5	in software from bad data	software errors from incorrect data in removable media, due to flaws in ballot creation software		technical				system and services acquisition, system and information integrity	
T	4.1.6	causing hardware failure	hardware errors, both spontaneous or induced, such as liquid spills, static charge to memory units		technical				physical and environmental protection, contingency planning	
T	4.1.7	causing device failure	device operator error, including incorrect cabling, or bring-up in test mode		technical				awareness and training	
T	4.1.8	due to manufacturer error	manufacturing error causes device not to conform with technical specifications		technical				system and services acquisition, system and information integrity: testing at the state or county level	
O	4.2	experience undetected tabulation errors	experience un-detected tabulation errors		human-unintentional, technical, operational				system and information integrity, system and services acquisition, configuration management, awareness and training	
T	4.2.1	in straight-party vote tabulation	due to use of incorrect rules for straight-party vote interpretation		human-unintentional				logic and accuracy tests that include straight-party voting tests that test actual vs. expected counts	
T	4.2.2	due to improper tabulation technique	due to use of incorrect selection of tabulation algorithm		human-unintentional			possibility that late testing will not detect, because actual vs. expected counts will match because both assume erroneous algorithm is the correct one	system and information integrity, including expert review of algorithm selection decision	during the tabulation of results, the incorrect instant run-off voting algorithm is selected
T	4.2.3	due to software error	due to software error including data loss, or incorrect tabulation algorithms		technical			possibility that late testing will not detect, because actual vs. expected counts will match because both assume erroneous algorithm is the correct one	system and information integrity, including expert review of algorithm selection decision; data backups or other redundancies	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.2.4	from mistakes by ballot designer	due to operator error in ballot creation software (e.g., selection of contest counting rules; choosing to vote for no more than 4 votes when the real rule is no more than three)		human-unintentional				system and information integrity, including verifying correct rules chosen, and then testing the application of rule on test ballot sets	
T	4.2.5	due to flawed ballot creation software	due to flaws in ballot creation software		technical				system and services acquisition controls that hold vendors accountable for testing	
T	4.2.6	by omitting tallies from totals	due to human error in omitting some tallies from vote total		human-unintentional				multi-person controls to verify correctness of human decisions	
T	4.2.7	by adding tallies multiple times	due to human error in including some tallies from vote total multiple times		human-unintentional				multi-person controls to verify correctness of human decisions	
O	4.3	experience errors in ballot preparation	experience software errors, or commit operational errors, in software that prepares ballots, device "programming", ballot definition files, and other election-specific software or data artifacts		human-unintentional			poor testing procedures, making last-minute changes to ballots and not re-testing; poorly trained workers	careful planning of tests at all levels; system and services acquisition controls; system and information integrity controls, including logic and accuracy testing; configuration management, including tracking and documentation of changes, particularly after testing; regression testing; and awareness and training of election officials and PollWorkers in ballot creation, testing procedures, and the use of equipment	
T	4.3.1	encode incorrect contest counting rule	encoding an incorrect contest counting rule		human-unintentional				logic and accuracy tests designed to detect contest counting flaws	
T	4.3.2	supply erroneous ballot definition data	incorrect encoding of other ballot definition file data that influences tabulation		human-unintentional				logic and accuracy testing	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.3.3	supply erroneous voting equipment data	incorrect encoding of other election equipment data that can cause technical malfunction		human-unintentional				comprehensive testing	
T	4.3.4	misconfigure ballot by operator	operator error making incorrect choices among configuration alternatives, e.g. vote-counting algorithms, setting to notify voters of undervotes, etc.		human-unintentional				comprehensive testing	
O	5	attack audit	render routine statistical audit ineffective	LTM-USA Delivery 01a	human-deliberate	Voting System	Election Artifacts	no separation of duties; control by election officials over audit procedures, access to Election Artifacts	media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication	An ElectionOfficial with the help of some auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited ElectionArtifacts. Then proceed to publish the election results.
O	5.1	attack election evidence	election evidence includes ElectionArtifacts, such as ballots, BallotPreparation data and artifacts, relevant PollBooks, PhysicalVoteRecords, PollWorker logs, VotingMachine audit logs, voter feedback, VotingMachines themselves, etc.		human-deliberate	Voting System	Election Artifacts	access to uncontrolled, accessible Election Artifacts	establish a chain of custody for all ElectionArtifacts used in audits; include separation of duties, access policies, audit logs, personnel policies, and media protections	
T	5.1.1	destroy ElectionArtifacts	physically destroy ElectionArtifacts, including electronic artifacts or electronic media, ballot destruction, VVPAT	Jones(2005) #6, Norden(2006) #9	human-deliberate	Voting System	3-43 (Deliver To Jurisdiction)	poor security during Election Artifacts delivery	Implement chain of custody and strong physical security during delivery	An ElectionOfficial destroys Paper Tape or RemovableMedia during delivery of the ElectionArtifacts to the central location.
T	5.1.2	mishandle ElectionArtifacts	swap, replace, hide, mislay, or mislabel ElectionArtifacts containing election evidence		human-deliberate				implementation chain of custody on ElectionArtifacts including media protection policies	John, a newly hired poll worker, is responsible for labeling batches of audit data. Unfortunately, he mislabeled one of the batches due to his inexperience.
T	5.1.3	add new fraudulent evidence		Jones(2005) #421	human-deliberate	results of the tabulation process	3-2 (Votable Ballots)	Real Votable Ballots has limited physical security		

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	5.1.4	modify ElectionArtifacts	modify poll books for audit; modify logbooks and log data used in audit		human-deliberate	Voting, Precinct Closeout	3-12 Check Poll Book for Authenticate Voter Activity Diagram, 3-43 Poll Worker Logs for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	audit monitoring, analysis, and reporting	John, a corrupted poll worker, has access to the poll book and authority to authenticate a voter. John alters the poll books so the number of eligible voters matches the number of CommittedBallots which includes fraud ballots.
A	5.1.4.1	modify deliberately	deliberately modify physical evidence		human-deliberate				implement strong physical security and chain of custody on ElectionArtifacts, including tamper resistant and tamper evident seals	
T	5.1.4.1.1	replace paper tape with fraud	results manipulation - change real Paper Tape with fraudulent Paper Tape	Jones (2005) #612 #62	human-deliberate	results of the tabulation process	3-45 (Paper Tape of Machine Totals Printed), (Removable memory card total generated), (Paper Tape totals of machine count reconciled to removable memory card total)	lack of management oversight over Poll Worker and Observers	implement strong physical security and chain of custody; report the MachineCount and check the number of AcceptedBallots against the number of registered voters; conduct thorough background checks on PollWorkers, ElectionOfficials, and Observers	This attack assumes at least three participants in this attack. PollWorker A rewrites data on the memory card while PollWorker B replaces the Paper Tape with fraudulent tape to cover the tracks of the attack on the RemovableMedia. The Observer(s) are in cahoots with the corrupted PollWorkers in order to successfully execute the attack with little or no suspicion. Note: Machine Totals reflect the total on the memory card after the attack is performed.
T	5.1.4.1.2	rewrite data on RemovableMedia	rewrite data on RemovableMedia	Jones (2005) #6	human-deliberate	results of the tabulation process	3-45 (Precinct Data)	poor security during election artifacts delivery	implement chain of custody and strong physical security during delivery	A corrupted ElectionOfficial or an Outsider steals or destroys Paper Tape RemovableMedia during delivery of the ElectionArtifacts to the central location.
T	5.1.4.1.3	modify poll books for audit	poll worker or election-official changes poll books to avoid fraud detection		human-deliberate	Voting, Precinct Closeout	3-12 Check Poll Book for Authenticate Voter Activity Diagram, 3-43 Poll Worker Logs for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	AU-6 audit monitoring, analysis, and reporting	John, a corrupted poll worker, has access to the poll book and authority to authenticate a voter. John alters the poll books so the number of eligible voters matches the number of CommittedBallots which includes fraud ballots.
T	5.1.4.1.4	modify logbooks and log data used in audit	poll worker or election-official changes logbooks and log data to avoid fraud detection		human-deliberate	Precinct Closeout	3-43 Poll Worker Logs for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	AU-6 audit monitoring, analysis, and reporting	Jane, a corrupted election-official, has access to logbooks and log data. She alters the content in the logbooks and log data so auditors would not be able to detect any fraud.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.1.4.2	modify unintentionally	unintentionally damage physical or electronic evidence		human-deliberate				physical and environmental protection; personnel security, including sanctions against policy violators, awareness and training	
T	5.1.4.3	modify deliberately by computer	use a computer to modify electronic evidence; implement attack code or misconfiguration at voting terminal, and replace real CommittedBallots with fraudulent CommittedBallots	Jones(2005) #611	human-deliberate	Voting System	3-1 (Voting) 3-43 (Deliver To Jurisdiction)	lack of management oversight over Poll Workers during transit and limited physical security on Committed Ballots and voting machine	add more security features to the real CommittedBallots and implement chain of custody and strong physical security on voting terminal and CommittedBallots	This attack assumes at least two corrupted PollWorkers. PollWorker A injects malware into the voting terminal just before the election. After the election is over, PollWorker B replaces real CommittedBallots with fraudulent CommittedBallots.
T	5.1.4.4	modify unintentionally by computer	unintentionally modify evidence via computer operator error		human-unintentional				personnel security, system and information integrity, awareness and training	
T	5.1.4.5	modify via malware attack	modify electronic evidence using a computer infected with malware, and/or vulnerable to network-based attacks		human-deliberate				personnel security, access control, audit and accountability, identification and authentication, system and communications protection	
T	5.1.4.6	modify via malware at artifact creation	modify electronic evidence at point of creation using infected voting equipment		human-deliberate				personnel security, access control, audit and accountability, identification and authentication, system and communications protection	
O	5.2	improperly select audit samples	use improper methods of selecting the scope of audit		human-deliberate	Election Audit	Election Audit	difficulty in discovery	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	
T	5.2.1	select audit units before election	audit manipulation - select audited items dishonestly	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	lack of basic audit in effect	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.2.2	select non-randomly	use non-random selection methods		human-deliberate	Precinct Closeout	Audit Data	poor auditing practices or procedures; failure to follow procedures; lack of management oversight over auditing practices	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	break randomization pattern to leverage voting pattern of a precinct
T	5.2.3	use subverted selection method	use selection methods subject to outside influence (e.g., malware infected or attacked via network connection)		human-deliberate				access control, audit and accountability, identification and authentication, system and communications protection	a computer that is malware-infected, perhaps by network-connected, is used to select audit units, and does so in a manner that makes it less likely that the primary attack can be detected
T	5.2.4	ignore proper selections	ignore randomly sampled audit units and audit something else		human-deliberate				personnel security, audit and accountability	An auditor ignores properly (randomly or scientifically) selected audit units and instead audits other units
O	5.3	use poor audit process	use poor auditing processes and procedures		human-deliberate	Election Audit	Election Audit, Validate Precinct Results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	Inside attacker, an ElectionOfficial, institutes poor auditing practices which are unlikely to detect the primary threat; Note: election Auditors may or may not be willing co-conspirators in these attacks
T	5.3.1	misguide auditors	give improper instructions to Auditors to render audit ineffective, and avoid detecting subverted VotingMachines	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor policies allows Election Official to specify their own rules	revise policies to ensure that ElectionOfficial follows the guidelines for auditing process	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors thus resulting in undetected subverted VotingMachines. Note Auditors may or may not be in cahoots with the ElectionOfficial.
T	5.3.2	audit insufficient sample	audit manipulation - audit insufficient of sample to avoid tampered audit unit detected	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	An ElectionOfficial gives improper or unclear instructions to Auditors to audit insufficient data thus resulting in undetected tampered audit units.
T	5.3.3	exploit variation in batch sizes	audit manipulation - random sampling from large variation of audit unit size minimize the risk of detection	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	An ElectionOfficial gives improper or unclear instructions to Auditors by creating a big variation in audit unit size so that tampered audit units will not likely be selected during sampling.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.3.4	establish single contest audit rule	election law manipulation - select a race randomly - assume audit untampered race only	Jones(2005) #612; LTM-Deliverable	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	Get a law or regulation in place that says that only one randomly selected race will be audited and assume your race will not be audited.
T	5.3.5	arrange contest audit	arrange selection of a non-subverted contest for audit	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	In a state that allows (but does not require) the auditing of only one randomly selected race, a dishonest election official could change procedures and institute an audit that is very unlikely to detect fraud.
T	5.3.6	select audited items before commit	tabulation manipulation - clean up data automatically based on operator	Jones(2005) #612	human-deliberate	tabulation server	3-48 (AccumulateTotals) 3-55 (Election Artifacts), (Contest Audit)	lack of tabulation server security	increase security features of tabulators	An ElectionOfficial with the help of some Auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited items. Then proceed to publish the election results.
T	5.3.7	tamper with audit totals	corrupt precinct-level data but not the machine-level data; election results manipulation - precinct total do not add up to machine totals	Jones(2005) #612 Norden(2006) #3	human-deliberate	results of the tabulation process	1-1 (Precinct Accumulation), (VoteTabulatingMachine), 3-43 (PrecinctAudit Data), (Machine Accumulation),	poor auditing practices or procedures	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	An ElectionOfficial releases precinct-level data that reflects the fraudulent results without tampering the MachineCount. Thus, the precinct total does not tally with the machine total, which can be published in a way (across hundreds of pages of paper) that is difficult for anyone to count quickly
T	5.3.8	avoid correction	when audits reveal mismatches, avoid calling for a recount or other corrective measures by making excuses; election results manipulation - give reasons for mismatch - avoid recount, examining voting terminals, and fraud audit items detection	Jones(2005) #612	human-deliberate	results of the tabulation process	3-54 (ValidateJurisdiction Results)	poor election laws / policies / guidelines	implement a policy that requires ElectionOfficial to give non-obscure reasons for result discrepancies and take corrective measures to avoid fraud	During the validation of the Jurisdiction results, a mismatch was found. The corrupted ElectionOfficial tries to offer obscure reasons to hide the actual attack.
T	5.3.9	overwhelm audit observers	overwhelm observers with too many auditors - auditor manipulation - incompetent Auditors ballot manipulation - dishonest audit	Jones(2005) #5,#6	human-deliberate	ballot tabulation process / results of the tabulation process	3-48 (Validate Precinct Results)	lack of management oversight over Election Officials and Auditors	implement a policy that specifies only certain number of Auditors can be employed so that Observers can perform their duty efficiently	An ElectionOfficial hires as many incompetent or corrupt Auditors as possible knowing that an Observer can only monitor a limited number of Auditors at a time.

node type	**outline number**	**threat action**	**Description**	**Reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
O	5.4	commit auditing error	human errors in following correct audit procedures, or overlooking errors		human-deliberate	Election Audit	Ballot Box Accounting, Machine Accumulation	Election Official has limited knowledge on discrepancies issues	personnel security, including personnel sanctions; awareness and training: auditor training	
T	5.4.1	misanalyze discrepancies between electronic and paper results	results discrepancies - totals do not tally - failed to correctly analyze the discrepancies	Jones(2005) #6	human-deliberate	results of the tabulation process	3-42 / 3-43 (Ballot Box Accounting), (Machine Accumulation)	Election Official has limited knowledge on discrepancies issues	Provide training or courses to equip ElectionOfficial with up-to-date knowledge on election materials, or hire experienced ElectionOfficial	An ElectionOfficial was recently hired to run the PollingPlace at a local Precinct. His experience as ElectionOfficial is somewhat limited as he has just begun his job not too long ago. After the election is over, he was being informed that the totals from the paper and electronic do not match. Because of his lack of experience, he misanalyzes and offers ambiguous reasons for discrepancies.
T	5.5	compromise auditors	suborn (bribe, threaten) auditors to intentionally misreport or suppress discrepancies between election results and audit results		human-deliberate	Election Audit	auditors	willingness of auditors to be bribed or coerced	personnel security	
O	5.6	attack audit results	attack audit-related computing process and electronic data representing audit results		human-deliberate	Election Audit	Election Audit	lack of control over audit results	physical and environmental protection, media protection policy and procedures	
T	5.6.1	mishandle media	swap, replace, hide, mislay, or mislabel media containing audit data; e.g. poll worker or election-official incorrectly labels batch of audit data		human-deliberate, human-unintentional	Precinct Closeout	3-43 PrecinctAudit Data for Precinct Closeout Data Flow Diagram	unintentional - vulnerability to human error due to carelessness; intentional - mislabel batch to cover fraud from being detected	audit monitoring, analysis, and reporting	John, a newly hired poll worker, is responsible for labeling batches of audit data. Unfortunately, he mislabeled one of the batches due to his inexperience.
T	5.6.2	add fraudulent result data	use illegal voting terminal to add tampered votes; inject fake votes to a back-end tabulating authority by impersonating a legitimate voting terminal	Kohno (2008)	human-deliberate	Voting	Voting Machines	poor physical and network security on voting terminals	increase physical and network security;	Just a day before the poll was open for election, John the election official and a few corrupted poll workers switched the certified voting machines with illegal voting machine so they could insert votes to the back-end of the tabulating authority.
O	5.6.3	attack audit data	poll worker changes audit data		human-deliberate	Precinct Closeout	3-43 PrecinctAudit Data for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	audit monitoring, analysis, and reporting	Jane, a corrupted election-official, has access to audit data and modifies it during delivery to the jurisdiction.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.6.3.1	modify deliberately			human-deliberate				establish a chain of custody on all ElectionArtifacts, including personnel security, physical and environmental protection, media protection policy and procedures	
T	5.6.3.2	modify unintentionally	modify audit data via operator error		human-unintentional				establish a chain of custody on all ElectionArtifacts, including personnel security, physical and environmental protection, media protection policy and procedures	
T	5.6.3.3	modify via malware attack	install malware in auditing device through physical access or network access; voting system manipulation - install malware to tamper results	Jones(2005) # 612 Norden(2006) #2,#3	human-deliberate	Voting System / auditing device	3-42 / 3-43 (Ballot Box Accounting), (Machine Accumulation)	corrupt officials using unsecured and non-certified voting system or custom device as audit device	use only certified voting system or secured custom device and implement a policy that requires ElectionOfficials to reconcile totals from HandCount and ManualCount	An ElectionOfficial avoids manual audit by giving excuses (such as MachineCount is more accurate than HandCount), and instructs Auditors to use Totals from the MachineCount.
T	5.6.4	publish bogus audit results	penetrate jurisdiction web site and publish bogus audit results to hide attack	Jones(2005) #62	human-deliberate	results of the tabulation process	1-1 (Canvass), (Official Report), 3-54 (Report Results)	lack of publishing system security that leads to obscure results	increase security in both areas - tabulator and publication website	An outsider penetrates into the jurisdiction website and changes the audit results of the election.
O	6	disrupt operations			human-deliberate, natural, environmental	Election System, Voting System	Voting Machines, Polling Place, Voting	exposure to natural or environmental events, fragility of computer equipment, susceptibility of voters to threats and intimidation	disaster planning, contingency planning, physical and environmental protection, incident response, and personnel security	
O	6.1	disruption from natural events	voting system failures attributable to natural events	Rackleff 2007	natural	Election System, Voting System	Voting Machines, Polling Place, Voting	exposure to natural events	disaster recovery planning; physical and environmental protection policies, incident response with coordination among government entities	
T	6.1.1	natural disaster	polling place hit by tornado, hurricane, tsunami, flood, earthquake, landslide, wildfire, lightening, strike, etc	Rackleff 2007	natural	Election System, Voting System	Voting machines, polling places, displaced voters	exposure to natural or accidental events	disaster recovery planning; hurricane and flood protection; contingency planning; incident response with coordination among government entities	Hurricane Katrina destroyed voting equipment and polling places, displaced voters, and caused elections to be postponed; many of the displaced voters were difficult to find even after basic utilities were restored

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.1.2	severe weather	polling place access impaired by severe weather conditions and side effects such as public transportation closure		natural	Voting	Voting Machines, Polling Place		contingency planning, such as use of alternate polling places or voting methods	a severe weather threat, including a tornado watch, was forecast for Super Tuesday in 2008; severe weather could have caused power outages or otherwise negatively impacted turnout in several states, including Alabama and Tennessee
O	6.2	disruption from environment events			environmental	Voting	Voting Machines, Polling Place	exposure to environment events	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
T	6.2.1	environmental failures	polling place facilities failures including power failure, electrical fire, kitchen fire, burst water pipes		environmental		Voting System		disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
T	6.2.2	hazardous accidents	polling place access impaired by nearby hazards including chemical spill, power wire fall, gas main explosion		environmental		Voting System		disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
O	6.3	disruption from human-created events	disruption from human-created events		human-deliberate, human-unintentional	Voting	Voting Machine	fragility of computer equipment, mishandling	planning; physical and environmental protection, access control	
O	6.3.1	that damage equipment	directly damage electronic voting equipment	Jones (2005a) #231	human-deliberate, human-unintentional	Voting System	Voting Machine	fragility of computer equipment, mishandling	planning: PollWorker rules of behavior, physical and environmental protection: physical access control and monitoring physical access	a voter wearing golf spikes steps on a power strip
T	6.3.1.1	render e-voting equipment inoperable	render electronic voting equipment inoperable		human-deliberate, human-unintentional				physical and environmental protection, access control	
T	6.3.1.2	render removable media not working	render removable media not working		human-deliberate, human-unintentional				physical and environmental protection, access control, media protection policy and procedures; chain of custody of media	

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.3.1.3	render paper sensor inoperable	during transportation, the rolls became loose and so the machine registered that it was out of paper when it was not - an attacker could intentionally tamper with rolls in transit or when loading the paper and delay opening of the polls		human-deliberate, human-unintentional, technical	voting	3-14 One voter	Physical attributes of thermal paper roll	physical and environmental protection: physical access control and monitoring physical access; VotingMachine chain of custody procedures	
T	6.3.2	with environmental effects	intentionally create environmental events to affect voting equipment or polling place operation		human-deliberate				physical and environmental protection	
O	6.4	discourage voter participation	discourage voter participation		human-deliberate	Voting	Voter	susceptibility of voters to violence, intimidation, fear	awareness and training, planning, contingency planning, incident response, physical and environmental protection	
T	6.4.1	misinform voters	misinformation about polling places or transportation		human-deliberate				awareness and training: voter education, utilize new media to counteract misinformation campaign	
T	6.4.2	threaten personal violence	threaten personal violence, such as in blackmailing a voter to be a no-show or to vote for attacker's candidate; attacker focuses on a particular voter threatens him to vote against his will	Van Acker	human-deliberate	Voting System	Eligible Voter	susceptibility of voters to intimidation; lack of voter privacy	planning, strengthen laws against such crimes; physical and environmental security; voter privacy	a type of voter suppression that involves deliberate acts to cause fear in EligibleVoters, thus deterring them from coming out to vote.
T	6.4.3	threaten mass violence	violence to prevent voting, (i.e., bomb scare, mail contamination scare (do not open mail), perhaps even targeting areas (by zip code)	Foxnews.com (2005)	human-deliberate	Voting	Voters	voters' fear for their safety	contingency planning contingency planning, incident response incident response, physical and environmental protection physical and environmental protection	In January, 2005, an Australian polling station for Iraqi exiles voting in their homeland's historic first post-Sadaam election was closed for an hour after a riot broke out and a suspicious bag prompted a bomb scare. The overall turnout was affected, it was thought. Many of Australia's estimated 80,000 Iraqis declined to register for the election, fearing their votes would make relatives in Iraq terrorist targets.

node type	outline number	threat action	Description	Reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.4.4	commit an act of terror			human-deliberate	Polling Place	Voters, Election Officials, Voting Equipment	exposure to terrorist acts of violence	physical and environmental protection: arms and ammunitions should not be allowed in the polling area. Unclaimed items should be continuously checked. Regular police patrolling required.	
T	6.4.5	intimidate to suppress turnout	coerce the voter to stay away from polls with threats and intimidation	Van Acker	human-deliberate	Voting System	Eligible Voter	susceptibility of voters to intimidation; lack of voter privacy	awareness and training, strengthen the election law against such crimes	"Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future." (Fund 2004)
T	6.4.6	create long lines	long lines are created by voters occupying the equipment for extended periods	Wallach (Review Panel)	human-deliberate	Voting System	Eligible Voter	voter's inability to wait to cast their vote	awareness and training, strengthen the election law against such crimes	Even in jurisdictions where there is a maximum amount of time a voter is allowed to occupy a voting booth, a large number of voters using the maximum time could create long lines

3 Precinct Count Optical Scan

In this tree, we consider threats to voting systems that employ marks sense technology to scan and count committed ballots recorded on a physical medium, such as pre-printed paper ballots, at precinct-based polling places. The primary technology used is a precinct-count optical scan (PCOS) device, used at polling places. A distinctive feature of PCOS devices is that it can be programmed to identify and reject undervotes and overvotes on ballots that it scans.

From a risk assessment standpoint, PCOS has threats associated with the use of computer-based technology, polling places, and paper ballots. The key technologies considered are the PCOS scanning machines, vote tabulators, and ballot creation software. The use of computer-based technologies introduces two categories of threats: attacks on voting equipment and technical failure. We consider threats that occur at polling places and at central operations. This voting system includes physical (paper) ballots, and the provisional ballot process is considered as well.

3.1 PCOS Threat Tree

node type - outline number - threat action

A	1	attack voting equipment
O	1.1	gather knowledge
T	1.1.1	from insider
A	1.1.2	from components
O	1.1.2.1	access directly
T	1.1.2.1.1	infiltrate as insider
T	1.1.2.1.2	obtain a machine
T	1.1.2.1.3	legally acquire machine
T	1.1.2.1.4	study a machine in transit
T	1.1.2.1.5	find source code
T	1.1.2.1.6	compromise existing source code escrow
T	1.1.2.2	directly examine
T	1.1.3	from published reports
O	1.2	gain insider access
T	1.2.1	at voting system vendor
T	1.2.2	in supply chain
T	1.2.3	in elections org
T	1.2.4	by illegal insider entry
T	1.2.5	by remote network access
O	1.3	attack component
O	1.3.1	attack hardware
T	1.3.1.1	jam PCOS scanner
T	1.3.1.2	attack scanner with goop pen
O	1.3.1.3	attack stored components
T	1.3.1.3.1	swap boot media
T	1.3.1.3.2	attack install
T	1.3.1.3.3	destroy Removable Media
A	1.3.2	attack software
T	1.3.2.1	develop malware
O	1.3.2.2	select targets
T	1.3.2.2.1	select precincts by expected voting pattern
T	1.3.2.2.2	select all precincts
O	1.3.2.3	inject malware
T	1.3.2.3.1	by remote bug exploitation

T	1.3.2.3.2	by local bug exploitation
T	1.3.2.3.3	by human interface exploit
O	1.3.2.4	execute malware
T	1.3.2.4.1	that alters artifact directly
T	1.3.2.4.2	that self-propagates
T	1.3.2.4.3	that remains resident
O	1.3.2.5	mitigate risk of detection
T	1.3.2.5.1	coerce testing staff
T	1.3.2.5.2	attack after testing
T	1.3.2.5.3	obtain cooperation of testers
T	1.3.2.5.4	access testing scripts
O	1.3.2.6	use infected component
O	1.3.2.6.1	supply cryptic knock
T	1.3.2.6.1.1	during logic and accuracy testing
T	1.3.2.6.1.2	during machine setup
T	1.3.2.6.1.3	during voting
T	1.3.2.6.1.4	as anti-knock
T	1.3.2.6.1.5	using AC power flicker
T	1.3.2.6.1.6	to detect realistic patterns of voting
T	1.3.2.6.1.7	to employ calendar/clock tricks
T	1.3.2.6.1.8	in ballot definition files
O	1.3.2.6.2	control/parameterize attack
T	1.3.2.6.2.1	voter enables attack as attacker
T	1.3.2.6.2.2	enable by unknowing voter
T	1.3.2.6.2.3	enable by technical consultant
T	1.3.2.6.2.4	employ unparameterized attack
T	1.3.2.6.2.5	add commands to ballot def file
O	1.3.3	attack data
O	1.3.3.1	using malware
O	1.3.3.1.1	select method and alter
T	1.3.3.1.1.1	by malware
T	1.3.3.1.1.2	by infected software
T	1.3.3.1.1.3	by infected config data
T	1.3.3.1.2	alter ballot definition file
T	1.3.3.1.3	alter device tallies
T	1.3.3.1.4	alter tabulation SW
O	1.3.3.2	modify data on storage medium
T	1.3.3.2.1	modify tabulation data
O	1.3.3.2.2	modify data before use
T	1.3.3.2.2.1	pre-load votes
T	1.3.3.2.2.2	flip votes
T	1.3.3.2.2.3	alter config data
O	1.3.4	attack comlinks
T	1.3.4.1	attack linked scanner/tabulator
T	1.3.4.2	attack wireless
A	2	perform insider attack
O	2.1	form inside attack team
T	2.1.1	infiltrate as volunteer pollworker
T	2.1.2	infiltrate as observer
T	2.1.3	staff with attackers
T	2.1.4	collude with other insiders
T	2.1.5	allow pollworker rotation
O	2.2	execute insider attack

O	2.2.1	attack at polling place
O	2.2.1.1	discourage voters
O	2.2.1.1.1	challenge at CheckIn
T	2.2.1.1.1.1	falsely reject voter registration
T	2.2.1.1.1.2	falsely reject id check
T	2.2.1.1.1.3	selectively challenge voters
T	2.2.1.1.1.4	falsely challenge voters on target list
T	2.2.1.1.1.5	destroy registered cards
T	2.2.1.1.2	delay open/close with excuses
T	2.2.1.1.3	create long lines
T	2.2.1.1.4	stymie voters needing assistance
T	2.2.1.1.5	issue incorrect ballot style
T	2.2.1.1.6	mislead w/phony ballot change
T	2.2.1.1.7	mislead w/one party only ruse
T	2.2.1.1.8	discourage provisional voting
T	2.2.1.1.9	impede voter access
T	2.2.1.1.10	persuade voter selections
A	2.2.1.2	alter voter's vote
O	2.2.1.2.1	access ballots to alter votes
T	2.2.1.2.1.1	obtain VotableBallot
O	2.2.1.2.1.2	obtain MarkedBallot
T	2.2.1.2.1.2.1	jam / shutdown machine
T	2.2.1.2.1.2.2	mislead about committing ballot
T	2.2.1.2.1.2.3	collect ballots from voters
A	2.2.1.2.1.3	steal provisional ballot
T	2.2.1.2.1.3.1	force provisional vote
T	2.2.1.2.1.3.2	obtain provisional ballot
T	2.2.1.2.1.4	obtain ballot of assisted voter
O	2.2.1.2.2	tamper with ballots
A	2.2.1.2.2.1	subvert no-show vote
O	2.2.1.2.2.1.1	conceal pollbook tampering
T	2.2.1.2.2.1.1.1	
T	2.2.1.2.2.1.1.2	
T	2.2.1.2.2.1.1.3	
T	2.2.1.2.2.1.2	mark VotableBallot
T	2.2.1.2.2.1.3	tamper with pollbook
O	2.2.1.2.2.2	subvert MarkedBallot of voter
T	2.2.1.2.2.2.1	mark undervote to create vote
T	2.2.1.2.2.2.2	mark vote to create overvote
T	2.2.1.2.2.2.3	swap ballot with new MarkedBallot
T	2.2.1.2.3	commit subverted ballot
O	2.2.2	attack other than polls
A	2.2.2.1	attack ballots
T	2.2.2.1.1	access ballots
O	2.2.2.1.2	tamper with ballots
T	2.2.2.1.2.1	with unobtrusive defects
T	2.2.2.1.2.2	with faint pre-marks
T	2.2.2.1.2.3	with invisible ink pre-marks
T	2.2.2.1.2.4	by subverting ballot rotation
T	2.2.2.1.2.5	by marking ballot
T	2.2.2.1.2.6	with invalidating marks
T	2.2.2.1.2.7	by undoing voter marks
T	2.2.2.1.2.8	by subverting provisional envelope

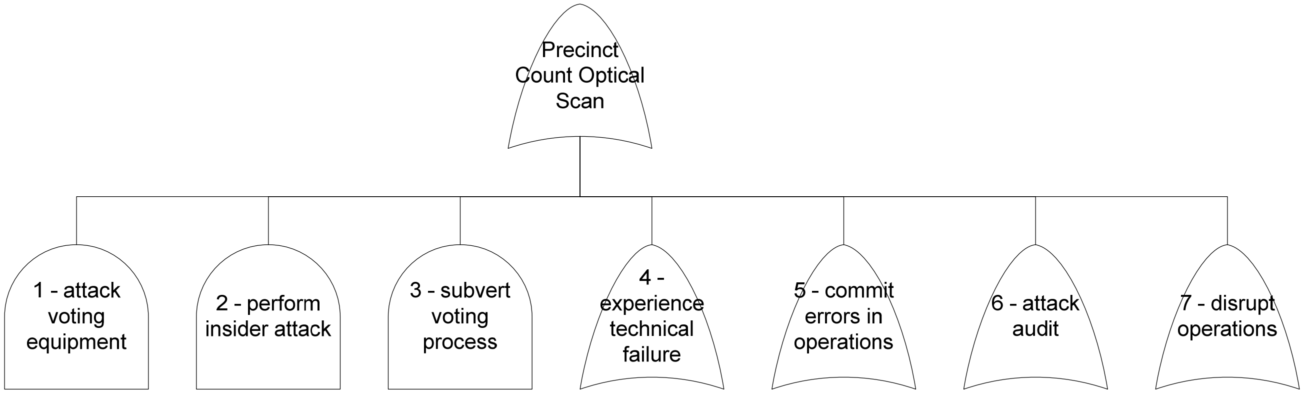
```
                                T           2.2.2.1.2.9     with physical damage
                      O         2.2.2.1.3   replace ballots
                                T           2.2.2.1.3.1     switch valid ballots with tampered ones
                                T           2.2.2.1.3.2     switch box during transport
                                T           2.2.2.1.3.3     discard / destroy MarkedBallots
              T       2.2.2.2   stuff ballots after closing
              T       2.2.2.3   stuff during canvass or recount
              T       2.2.2.4   selectively recount
              T       2.2.2.5   subvert tabulation
              O       2.2.2.6   attack tabulated results
                      T         2.2.2.6.1   subvert reported results
                      T         2.2.2.6.2   falsely announce results
                      T         2.2.2.6.3   alter results transmission
A   3   subvert voting process
    O   3.1   target polling places
        T     3.1.1   by expected voting pattern
        T     3.1.2   where PollWorkers not likely to know Voters
        T     3.1.3   that exploit electoral college rules
        T     3.1.4   where PollWorkers can be co-opted
        T     3.1.5   with lax enforcement of procedures
    O   3.2   form attack team
        A     3.2.1   use cell captains
              T       3.2.1.1   recruit cell captains
              T       3.2.1.2   motivate cell captains
              T       3.2.1.3   educate cell captains
              T       3.2.1.4   provide rewards for cell captains to distribute
              T       3.2.1.5   recruit attackers
        T     3.2.2   recruit attackers among LegalVoters
        T     3.2.3   recruit brokers
    O   3.3   commit vote fraud attack
        A     3.3.1   perform chain vote
              T       3.3.1.1   acquire VotableBallot
              T       3.3.1.2   vote with pre-marked ballot
              T       3.3.1.3   smuggle VotableBallot out
        O     3.3.2   perform impersonation attack
              O       3.3.2.1   create fraudulent voter registrations
                      T         3.3.2.1.1   register as an housemate
                      T         3.3.2.1.2   register as a dead person
                      T         3.3.2.1.3   register an ineligible person
                      T         3.3.2.1.4   register as a fictitious person
              O       3.3.2.2   create target list of voters to impersonate
                      T         3.3.2.2.1   fraudulent registrations
                      T         3.3.2.2.2   unlikely voters
                      T         3.3.2.2.3   voters likely to vote late in the day
              A       3.3.2.3   execute impersonated voting
                      T         3.3.2.3.1   assign impersonator to voter
                      T         3.3.2.3.2   go to target voter's polling place
                      T         3.3.2.3.3   check in as the impersonated voter
                      T         3.3.2.3.4   vote in place of voter
                      T         3.3.2.3.5   supply rewards
        A     3.3.3   buy or coerce vote
              O       3.3.3.1   motivate voter
                      O         3.3.3.1.1   pay
```

O 3.3.3.1.1 pay for candidate support
T 3.3.3.1.1.1.1 use drugs, alcohol as payment
T 3.3.3.1.1.1.2 pay voters cash
T 3.3.3.1.1.2 promise to pay
O 3.3.3.1.2 coerce
T 3.3.3.1.2.1 promise to punish
T 3.3.3.1.2.2 punish and promise more
T 3.3.3.1.2.3 punish and promise repair
O 3.3.3.2 direct voters
T 3.3.3.2.1 to make specific votes
T 3.3.3.2.2 to not make specific votes
O 3.3.3.3 verify bought vote
T 3.3.3.3.1 by self-recorded casting
T 3.3.3.3.2 with phony voter assistant
T 3.3.3.3.3 with encoded stray marks
T 3.3.3.3.4 through PollWorker ballot chaining
T 3.3.3.4 supply rewards or punishment
O 3.3.4 vote more than once
T 3.3.4.1 vote using more than one method
T 3.3.4.2 vote in more than one place
T 3.3.4.3 insert unauthorized physical ballots into the ballot box
O 4 experience technical failure
O 4.1 experience operational error
T 4.1.1 by miscalibrating scanner
T 4.1.2 due to foreign substances
T 4.1.3 through erroneous settings
T 4.1.4 by mismatching precinct and actual
T 4.1.5 in software from bad data
T 4.1.6 causing hardware failure
T 4.1.7 causing device failure
T 4.1.8 due to manufacturer error
O 4.2 experience undetected tabulation errors
T 4.2.1 due to excessive variance
T 4.2.2 in straight-party vote tabulation
T 4.2.3 due to improper tabulation technique
T 4.2.4 due to software error
T 4.2.5 from mistakes by ballot designer
T 4.2.6 due to flawed ballot creation software
T 4.2.7 by omitting tallies from totals
T 4.2.8 by adding tallies multiple times
T 4.2.9 from simultaneous multiple scan feeding tabulator
O 4.3 experience errors in ballot preparation
T 4.3.1 encode incorrect contest counting rule
T 4.3.2 incorrectly map candidate's mark position
T 4.3.3 supply erroneous ballot definition data
T 4.3.4 supply erroneous voting equipment data
T 4.3.5 misconfigure ballot by operator
T 4.4 fail to warn voter of overvotes / undervotes
T 4.5 failure of batteries
O 5 commit errors in operations
O 5.1 commit errors in polling place operations
O 5.1.1 unintentionally discourage voting
T 5.1.1.1 create long lines by working slowly

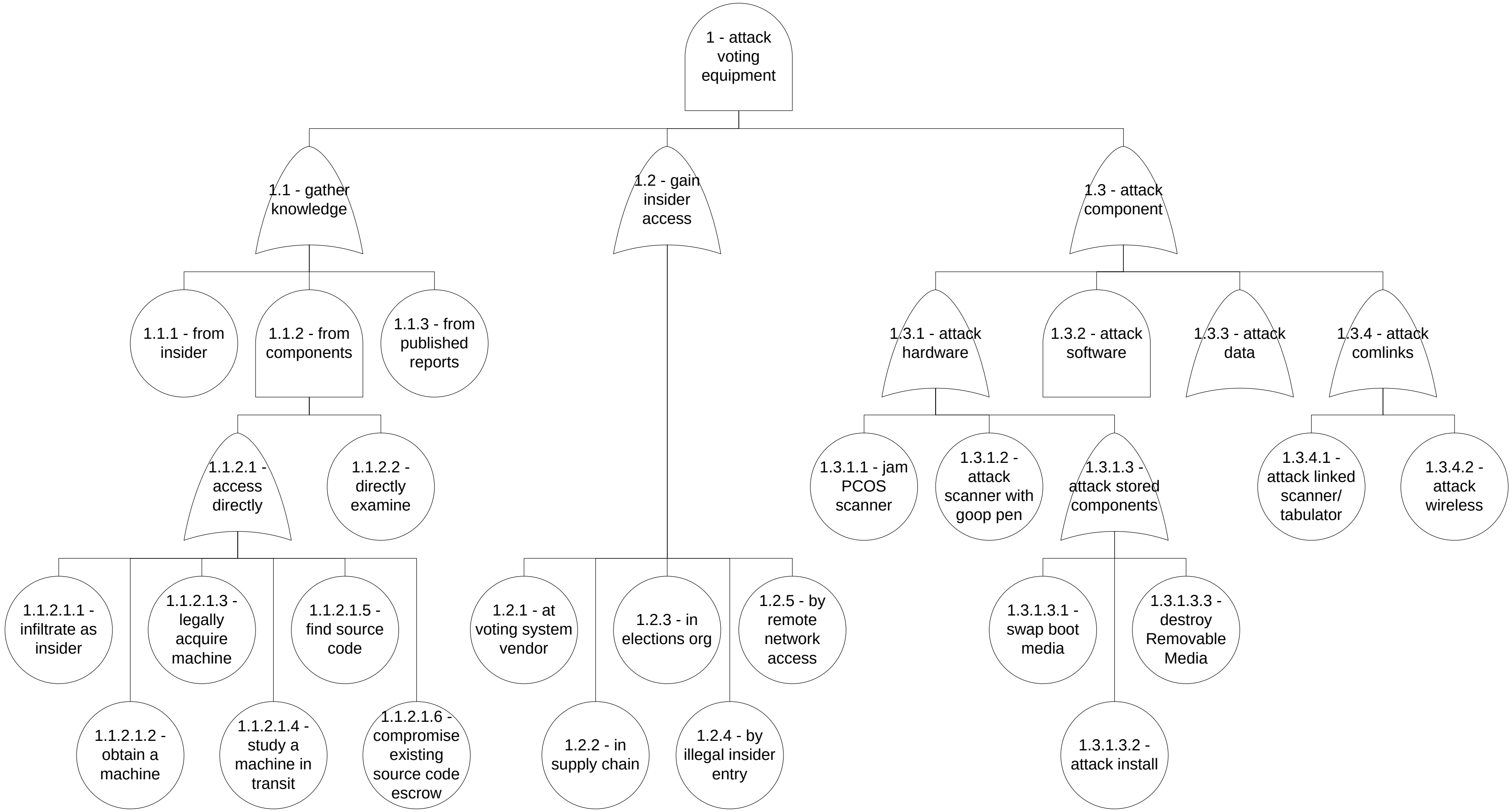
            - T 5.1.1.2 mistakenly challenge voters at CheckIn
            - T 5.1.1.3 delay opening or closing
            - T 5.1.1.4 delay voters with poor assistance
            - T 5.1.1.5 send voter to wrong place
            - T 5.1.1.6 require provisional by mistake
        - T 5.1.2 supply incompatible marking device
        - O 5.1.3 misinform about overvoting / undervoting
            - T 5.1.3.1 allow undervotes without warning
            - T 5.1.3.2 allow overvotes without warning
            - T 5.1.3.3 encourage voter override
        - O 5.1.4 issue erroneous VotableBallot
            - T 5.1.4.1 of the incorrect ballot style
            - T 5.1.4.2 with errors in contests or candidates
            - T 5.1.4.3 with errors in selection rules
        - O 5.1.5 confuse voters with poor ballot design
            - T 5.1.5.1 by splitting contests up
            - T 5.1.5.2 by spreading response options
            - T 5.1.5.3 with complete-the-arrow
            - T 5.1.5.4 by keeping disqualified candidates
            - T 5.1.5.5 with inconsistent formats
            - T 5.1.5.6 by omitting useful shading
            - O 5.1.5.7 by omitting use of bold
            - T 5.1.5.8 with complex instructions
            - O 5.1.5.9 with distant instructions
            - T 5.1.5.10 with no correction guidance
            - T 5.1.5.11 force least-objectionable choice
            - T 5.1.5.12 publish invalid sample ballots
        - O 5.1.6 mishandle ballots
            - T 5.1.6.1 lose ballots by accident
            - T 5.1.6.2 abuse ballots by accident
            - T 5.1.6.3 stuff, swap, or lose the ballot box
            - T 5.1.6.4 run out of ballots
    - O 5.2 make mistakes in ballot adjudication
        - T 5.2.1 incorrectly accept provisional ballots
        - T 5.2.2 incorrectly reject provisional ballots
        - T 5.2.3 reject ballots without retry
- O 6 attack audit
    - O 6.1 attack election evidence
        - T 6.1.1 destroy ElectionArtifacts
        - T 6.1.2 mishandle ElectionArtifacts
        - T 6.1.3 add new fraudulent evidence
        - O 6.1.4 modify ElectionArtifacts
            - A 6.1.4.1 modify deliberately
                - T 6.1.4.1.1 replace paper tape with fraud
                - T 6.1.4.1.2 rewrite data on Removable Media
            - T 6.1.4.2 modify unintentionally
            - T 6.1.4.3 modify deliberately by computer
            - T 6.1.4.4 modify unintentionally by computer
            - T 6.1.4.5 modify via malware attack
            - T 6.1.4.6 modify via malware at artifact creation
    - O 6.2 improperly select audit samples
        - T 6.2.1 select audit units before election
        - T 6.2.2 select non-randomly

- T 6.2.3 use subverted selection method
- T 6.2.4 ignore proper selections
- O 6.3 use poor audit process
  - T 6.3.1 misguide auditors
  - T 6.3.2 audit insufficient sample
  - T 6.3.3 exploit variation in batch sizes
  - T 6.3.4 establish single contest audit rule
  - T 6.3.5 arrange contest audit
  - T 6.3.6 select audited items before commit
  - T 6.3.7 tamper with audit totals
  - T 6.3.8 avoid correction
  - T 6.3.9 overwhelm audit observers
- T 6.4 commit auditing error
- T 6.5 compromise auditors
- O 6.6 attack audit results
  - T 6.6.1 mishandle media
  - T 6.6.2 add fraudulent result data
  - O 6.6.3 attack audit data
    - T 6.6.3.1 modify deliberately
    - T 6.6.3.2 modify unintentionally
    - T 6.6.3.3 modify via malware attack
  - T 6.6.4 publish bogus audit results
- O 7 disrupt operations
  - O 7.1 disruption from natural events
    - T 7.1.1 natural disaster
    - T 7.1.2 severe weather
  - O 7.2 disruption from environmental events
    - O 7.2.1 environmental failures
      - T 7.2.1.1 experience a fire
      - T 7.2.1.2 experience power disruptions
      - T 7.2.1.3 experience effects of humidity
    - T 7.2.2 hazardous accidents
  - O 7.3 disruption from human-created events
    - O 7.3.1 that damage equipment
      - T 7.3.1.1 render e-voting equipment inoperable
      - T 7.3.1.2 render removable media not working
      - T 7.3.1.3 render paper sensor inoperable
    - T 7.3.2 deploy faulty equipment
    - T 7.3.3 with environmental effects
  - O 7.4 discourage voter participation
    - T 7.4.1 misinform voters
    - T 7.4.2 threaten personal violence
    - T 7.4.3 threaten mass violence
    - T 7.4.4 commit an act of terror
    - T 7.4.5 intimidate to suppress turnout

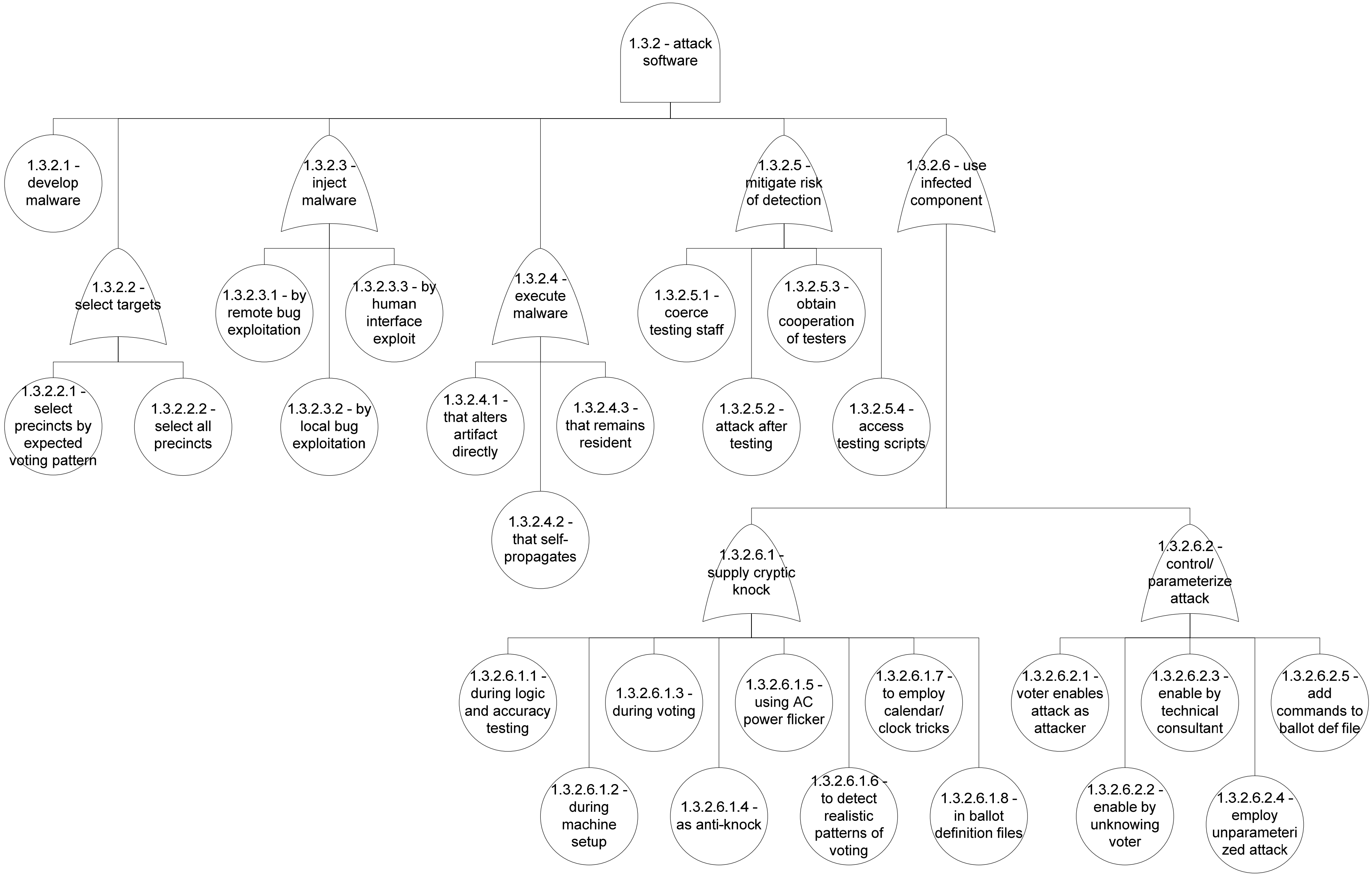
3.2 PCOS Threat Tree – Graphic


Precinct Count Optical Scan
1 - attack voting equipment
2 - perform insider attack
3 - subvert voting process
4 - experience technical failure
5 - commit errors in operations
6 - attack audit
7 - disrupt operations

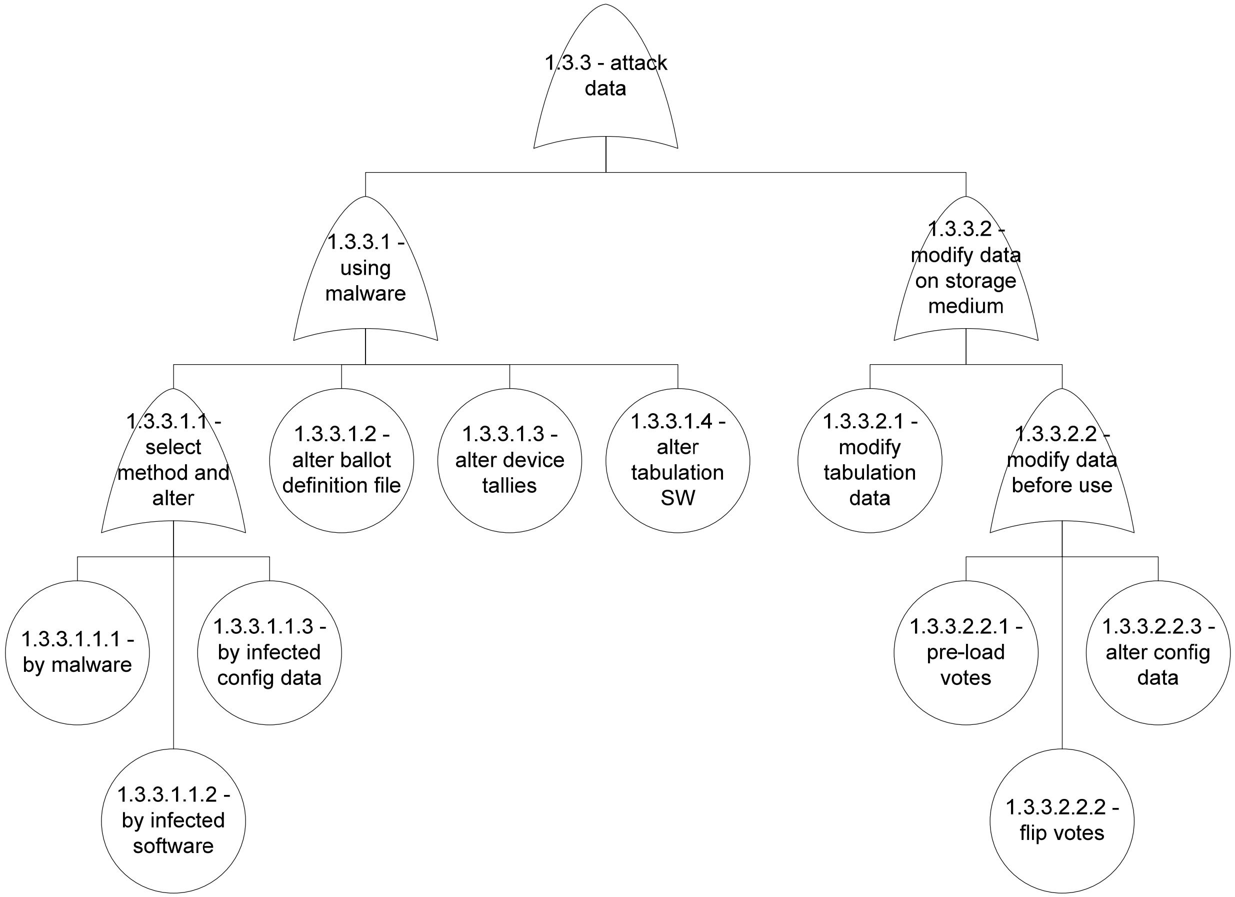
3-1 PCOS Overview


1 - attack voting equipment
1.1 - gather knowledge
1.2 - gain insider access
1.3 - attack component
1.1.1 - from insider
1.1.2 - from components
1.1.3 - from published reports
1.3.1 - attack hardware
1.3.2 - attack software
1.3.3 - attack data
1.3.4 - attack comlinks
1.1.2.1 - access directly
1.1.2.2 - directly examine
1.3.1.1 - jam PCOS scanner
1.3.1.2 - attack scanner with goop pen
1.3.1.3 - attack stored components
1.3.4.1 - attack linked scanner/ tabulator
1.3.4.2 - attack wireless
1.1.2.1.1 - infiltrate as insider
1.1.2.1.3 - legally acquire machine
1.1.2.1.5 - find source code
1.2.1 - at voting system vendor
1.2.3 - in elections org
1.2.5 - by remote network access
1.3.1.3.1 - swap boot media
1.3.1.3.3 - destroy Removable Media
1.1.2.1.2 - obtain a machine
1.1.2.1.4 - study a machine in transit
1.1.2.1.6 - compromise existing source code escrow
1.2.2 - in supply chain
1.2.4 - by illegal insider entry
1.3.1.3.2 - attack install

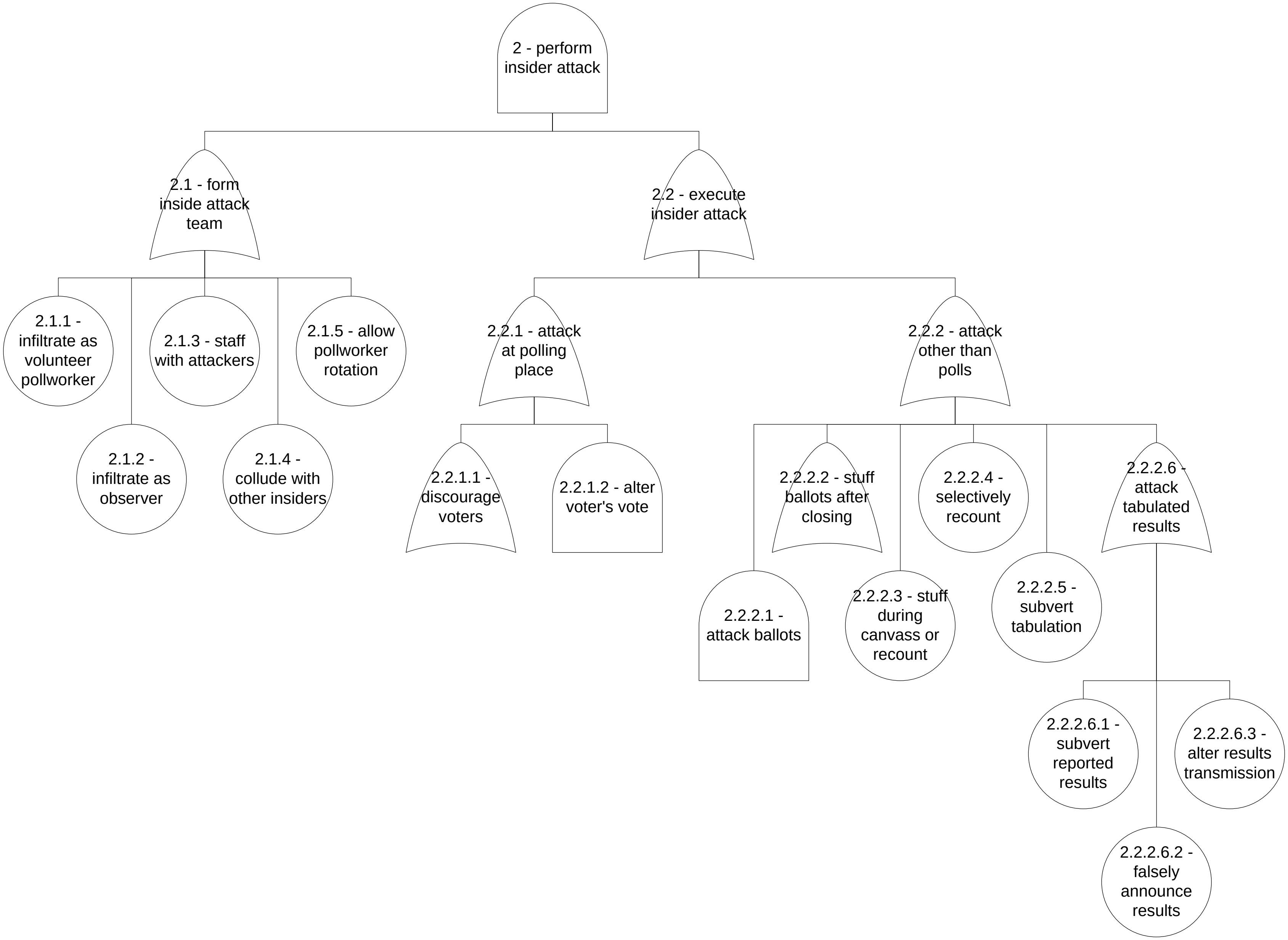
3-2 PCOS Attack Voting Equipment


1.3.2 - attack software
1.3.2.1 - develop malware
1.3.2.2 - select targets
1.3.2.2.1 - select precincts by expected voting pattern
1.3.2.2.2 - select all precincts
1.3.2.3 - inject malware
1.3.2.3.1 - by remote bug exploitation
1.3.2.3.2 - by local bug exploitation
1.3.2.3.3 - by human interface exploit
1.3.2.4 - execute malware
1.3.2.4.1 - that alters artifact directly
1.3.2.4.2 - that self-propagates
1.3.2.4.3 - that remains resident
1.3.2.5 - mitigate risk of detection
1.3.2.5.1 - coerce testing staff
1.3.2.5.2 - attack after testing
1.3.2.5.3 - obtain cooperation of testers
1.3.2.5.4 - access testing scripts
1.3.2.6 - use infected component
1.3.2.6.1 - supply cryptic knock
1.3.2.6.1.1 - during logic and accuracy testing
1.3.2.6.1.2 - during machine setup
1.3.2.6.1.3 - during voting
1.3.2.6.1.4 - as anti-knock
1.3.2.6.1.5 - using AC power flicker
1.3.2.6.1.6 - to detect realistic patterns of voting
1.3.2.6.1.7 - to employ calendar/ clock tricks
1.3.2.6.1.8 - in ballot definition files
1.3.2.6.2 - control/ parameterize attack
1.3.2.6.2.1 - voter enables attack as attacker
1.3.2.6.2.2 - enable by unknowing voter
1.3.2.6.2.3 - enable by technical consultant
1.3.2.6.2.4 - employ unparameteri zed attack
1.3.2.6.2.5 - add commands to ballot def file

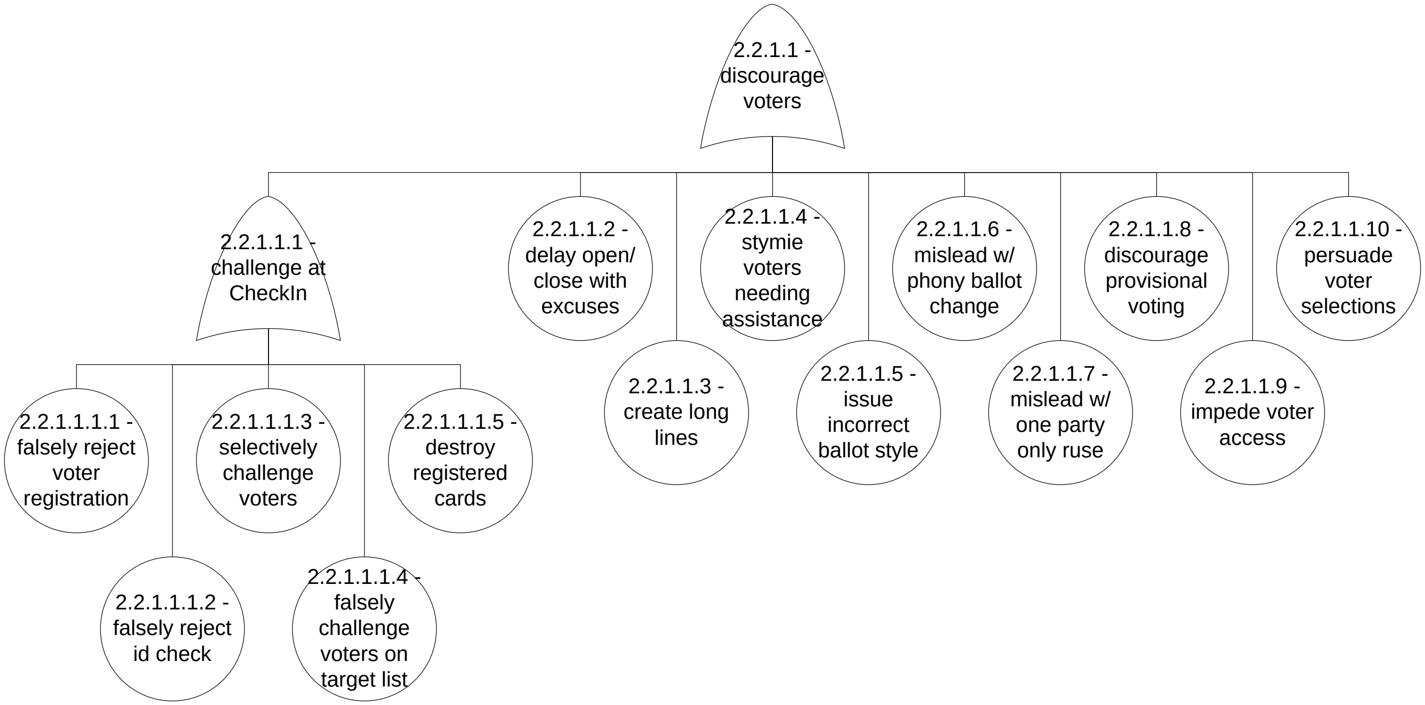
3-3 PCOS Attack Software


1.3.3 - attack data
1.3.3.1 - using malware
1.3.3.2 - modify data on storage medium
1.3.3.1.1 - select method and alter
1.3.3.1.2 - alter ballot definition file
1.3.3.1.3 - alter device tallies
1.3.3.1.4 - alter tabulation SW
1.3.3.2.1 - modify tabulation data
1.3.3.2.2 - modify data before use
1.3.3.1.1.1 - by malware
1.3.3.1.1.3 - by infected config data
1.3.3.1.1.2 - by infected software
1.3.3.2.2.1 - pre-load votes
1.3.3.2.2.3 - alter config data
1.3.3.2.2.2 - flip votes

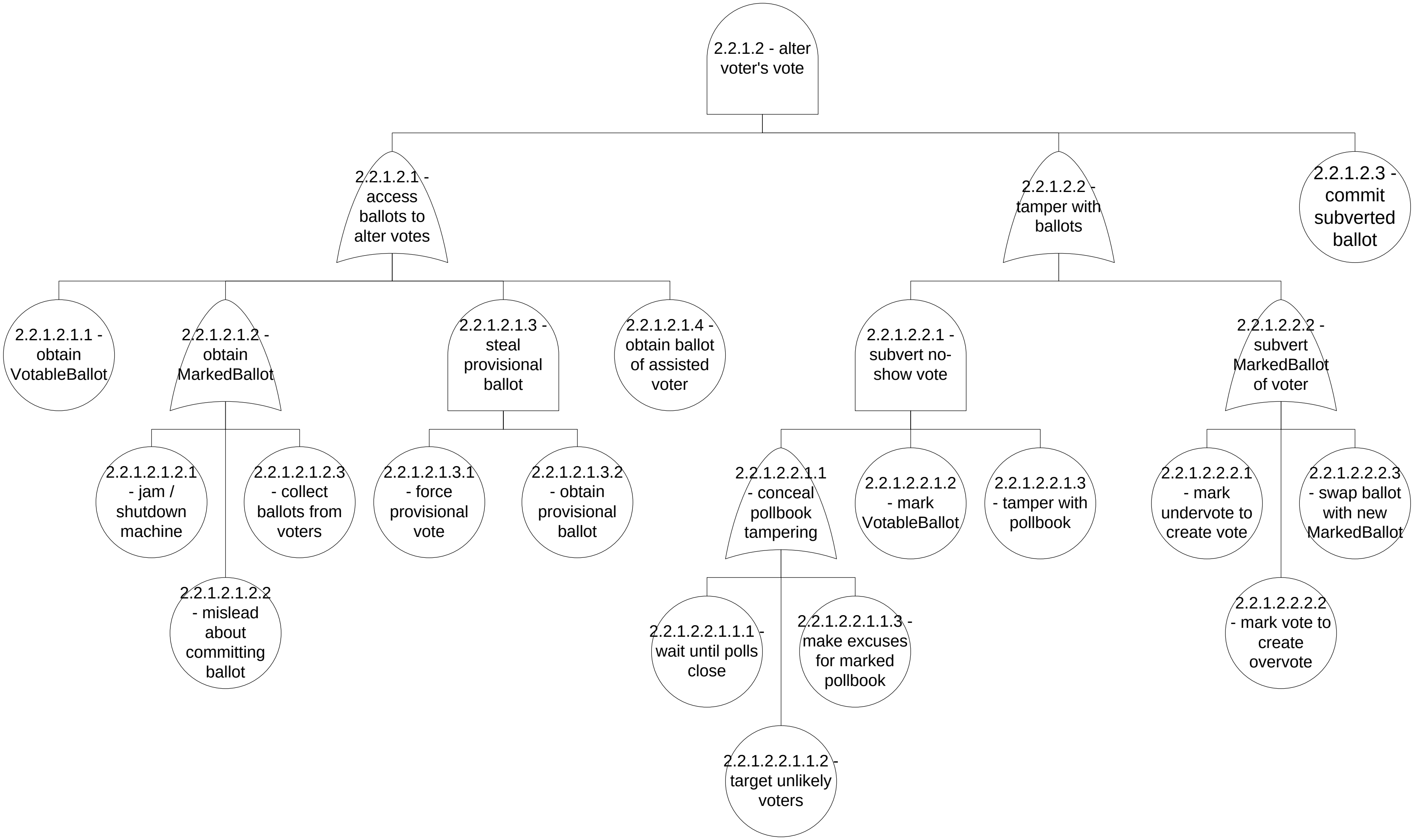
3-4 PCOS Attack Data


2 - perform insider attack
2.1 - form inside attack team
2.2 - execute insider attack
2.1.1 - infiltrate as volunteer pollworker
2.1.2 - infiltrate as observer
2.1.3 - staff with attackers
2.1.4 - collude with other insiders
2.1.5 - allow pollworker rotation
2.2.1 - attack at polling place
2.2.2 - attack other than polls
2.2.1.1 - discourage voters
2.2.1.2 - alter voter's vote
2.2.2.1 - attack ballots
2.2.2.2 - stuff ballots after closing
2.2.2.3 - stuff during canvass or recount
2.2.2.4 - selectively recount
2.2.2.5 - subvert tabulation
2.2.2.6 - attack tabulated results
2.2.2.6.1 - subvert reported results
2.2.2.6.2 - falsely announce results
2.2.2.6.3 - alter results transmission

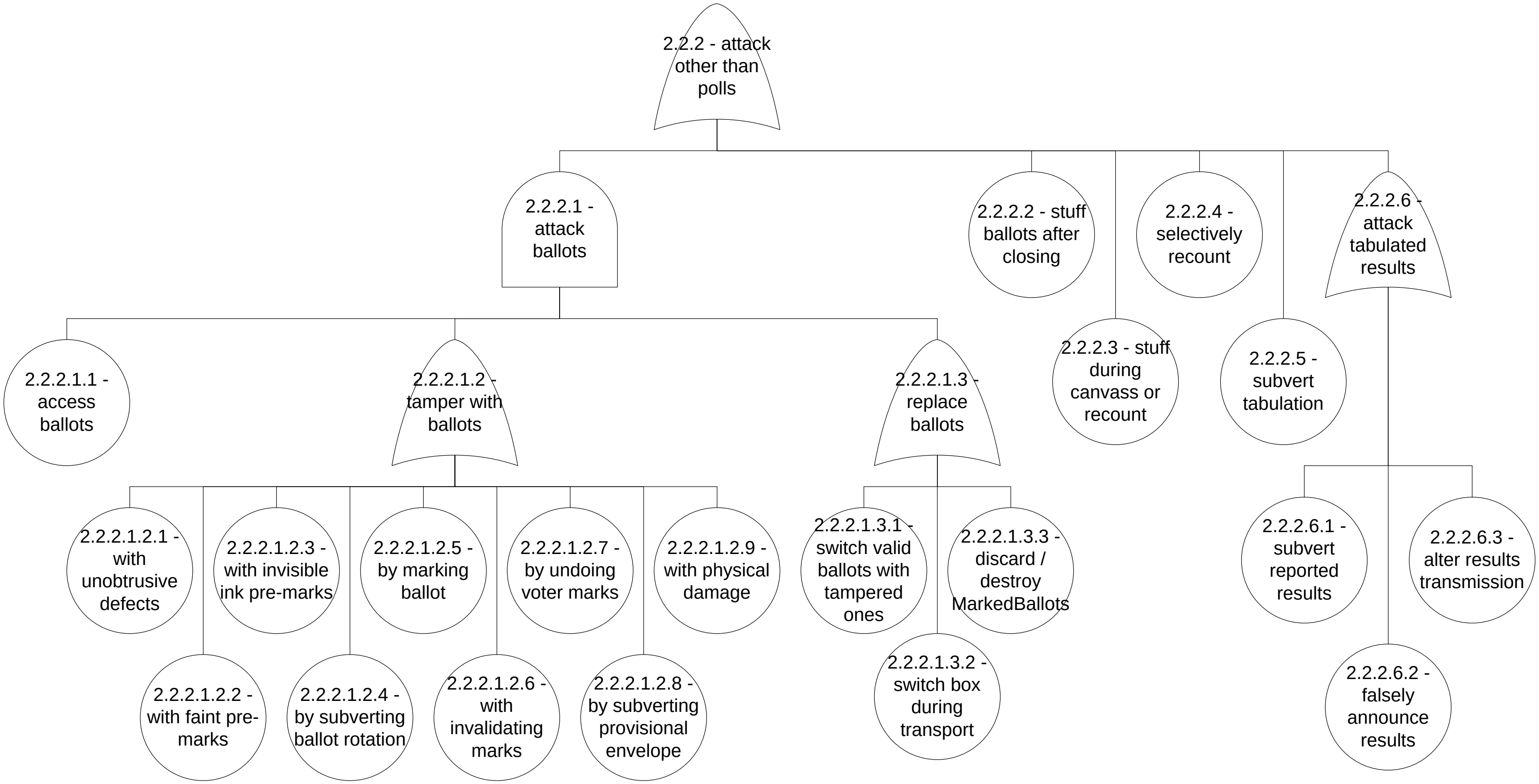
3-5 PCOS Perform Insider Attack


2.2.1.1 - discourage voters
2.2.1.1.1 - challenge at CheckIn
2.2.1.1.2 - delay open/ close with excuses
2.2.1.1.3 - create long lines
2.2.1.1.4 - stymie voters needing assistance
2.2.1.1.5 - issue incorrect ballot style
2.2.1.1.6 - mislead w/ phony ballot change
2.2.1.1.7 - mislead w/ one party only ruse
2.2.1.1.8 - discourage provisional voting
2.2.1.1.9 - impede voter access
2.2.1.1.10 - persuade voter selections
2.2.1.1.1.1 - falsely reject voter registration
2.2.1.1.1.2 - falsely reject id check
2.2.1.1.1.3 - selectively challenge voters
2.2.1.1.1.4 - falsely challenge voters on target list
2.2.1.1.1.5 - destroy registered cards

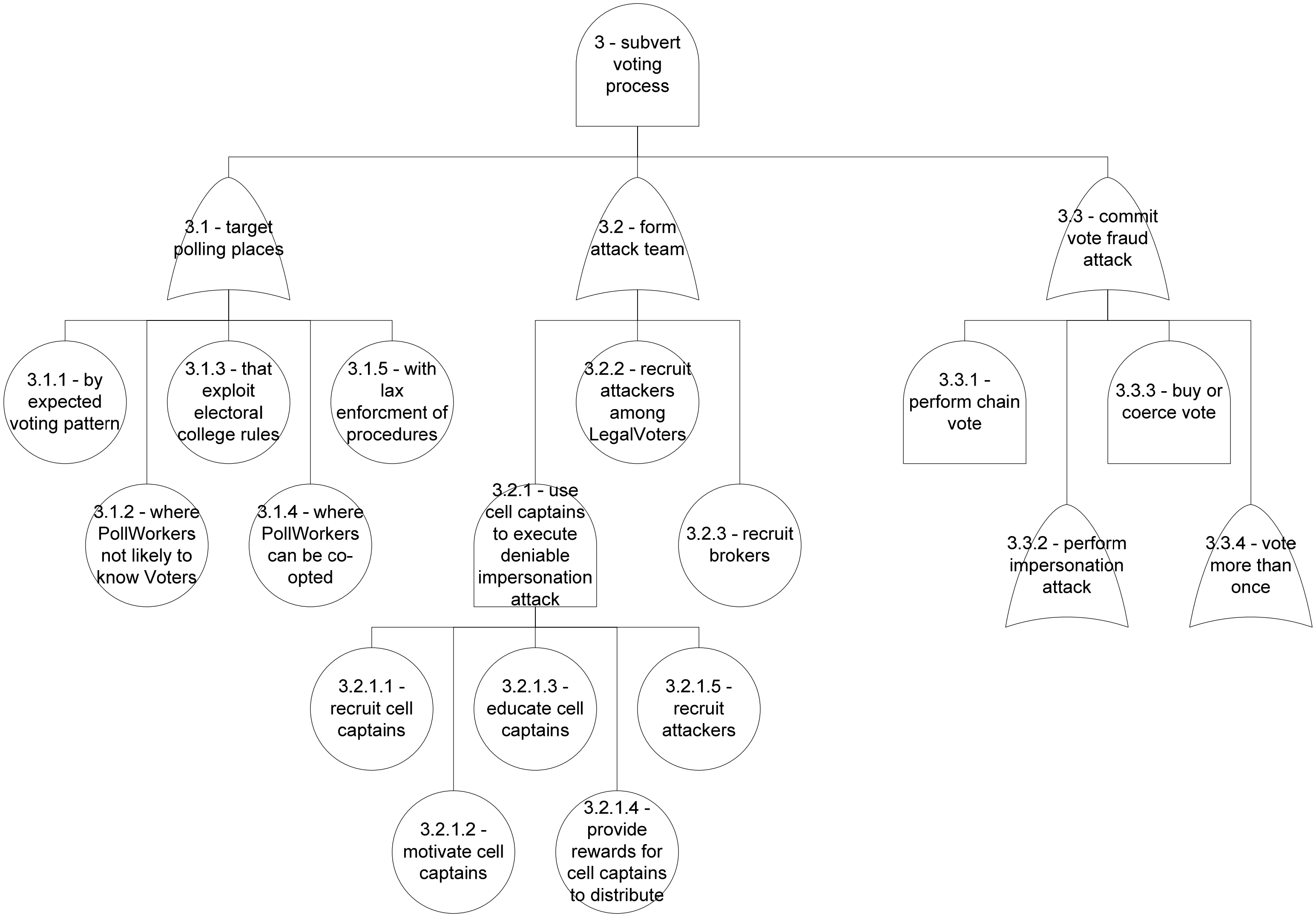
3-6 PCOS Discourage Voters


2.2.1.2 - alter voter's vote
2.2.1.2.1 - access ballots to alter votes
2.2.1.2.2 - tamper with ballots
2.2.1.2.3 - commit subverted ballot
2.2.1.2.1.1 - obtain VotableBallot
2.2.1.2.1.2 - obtain MarkedBallot
2.2.1.2.1.3 - steal provisional ballot
2.2.1.2.1.4 - obtain ballot of assisted voter
2.2.1.2.2.1 - subvert no-show vote
2.2.1.2.2.2 - subvert MarkedBallot of voter
2.2.1.2.1.2.1 - jam / shutdown machine
2.2.1.2.1.2.3 - collect ballots from voters
2.2.1.2.1.3.1 - force provisional vote
2.2.1.2.1.3.2 - obtain provisional ballot
2.2.1.2.2.1.1 - conceal pollbook tampering
2.2.1.2.2.1.2 - mark VotableBallot
2.2.1.2.2.1.3 - tamper with pollbook
2.2.1.2.2.2.1 - mark undervote to create vote
2.2.1.2.2.2.3 - swap ballot with new MarkedBallot
2.2.1.2.1.2.2 - mislead about committing ballot
2.2.1.2.2.1.1.1 - wait until polls close
2.2.1.2.2.1.1.3 - make excuses for marked pollbook
2.2.1.2.2.2.2 - mark vote to create overvote
2.2.1.2.2.1.1.2 - target unlikely voters

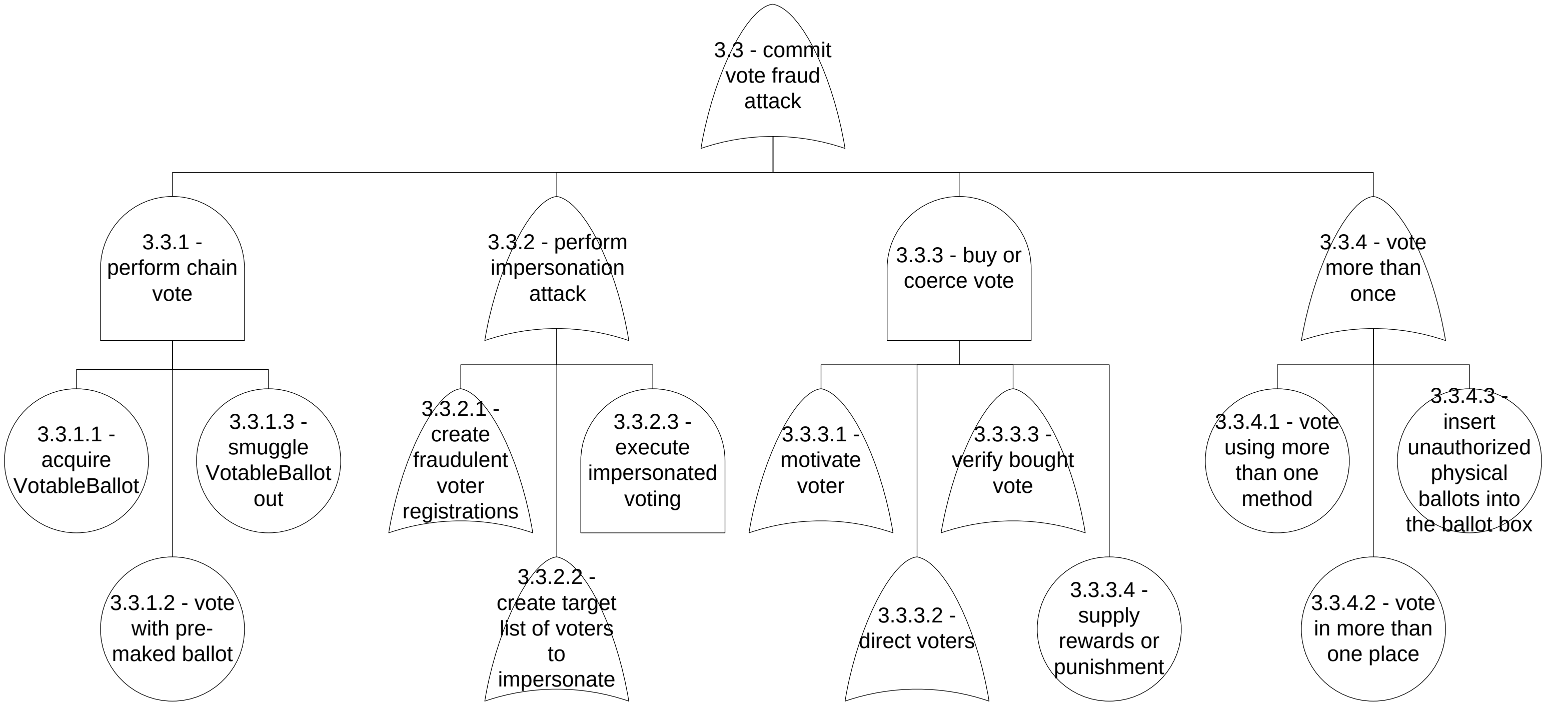
3-7 PCOS Alter Voter's Vote


2.2.2 - attack other than polls
2.2.2.1 - attack ballots
2.2.2.2 - stuff ballots after closing
2.2.2.3 - stuff during canvass or recount
2.2.2.4 - selectively recount
2.2.2.5 - subvert tabulation
2.2.2.6 - attack tabulated results
2.2.2.1.1 - access ballots
2.2.2.1.2 - tamper with ballots
2.2.2.1.3 - replace ballots
2.2.2.1.2.1 - with unobtrusive defects
2.2.2.1.2.2 - with faint pre-marks
2.2.2.1.2.3 - with invisible ink pre-marks
2.2.2.1.2.4 - by subverting ballot rotation
2.2.2.1.2.5 - by marking ballot
2.2.2.1.2.6 - with invalidating marks
2.2.2.1.2.7 - by undoing voter marks
2.2.2.1.2.8 - by subverting provisional envelope
2.2.2.1.2.9 - with physical damage
2.2.2.1.3.1 - switch valid ballots with tampered ones
2.2.2.1.3.2 - switch box during transport
2.2.2.1.3.3 - discard / destroy MarkedBallots
2.2.2.6.1 - subvert reported results
2.2.2.6.2 - falsely announce results
2.2.2.6.3 - alter results transmission

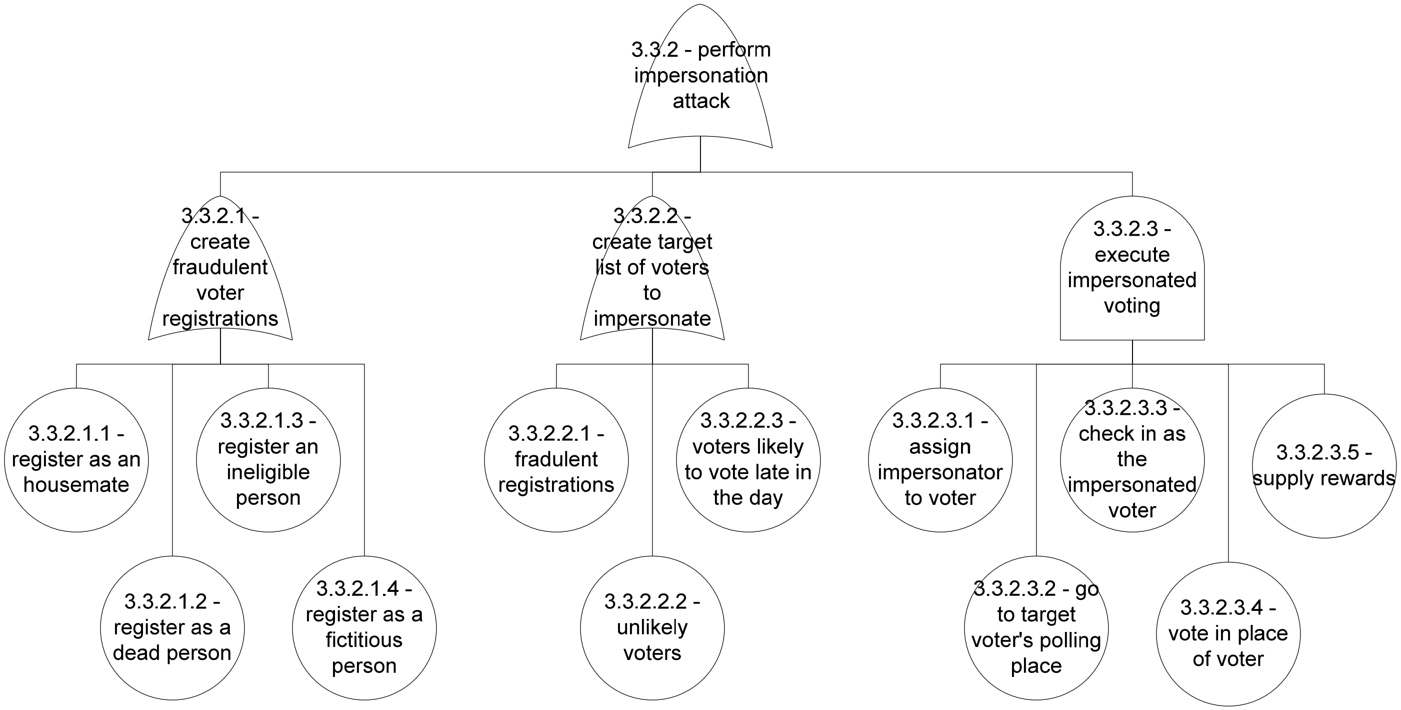
3-8 PCOS Attack Other than Polls


3 - subvert voting process
3.1 - target polling places
3.2 - form attack team
3.3 - commit vote fraud attack
3.1.1 - by expected voting pattern
3.1.2 - where PollWorkers not likely to know Voters
3.1.3 - that exploit electoral college rules
3.1.4 - where PollWorkers can be co-opted
3.1.5 - with lax enforcment of procedures
3.2.1 - use cell captains to execute deniable impersonation attack
3.2.2 - recruit attackers among LegalVoters
3.2.3 - recruit brokers
3.2.1.1 - recruit cell captains
3.2.1.2 - motivate cell captains
3.2.1.3 - educate cell captains
3.2.1.4 - provide rewards for cell captains to distribute
3.2.1.5 - recruit attackers
3.3.1 - perform chain vote
3.3.2 - perform impersonation attack
3.3.3 - buy or coerce vote
3.3.4 - vote more than once

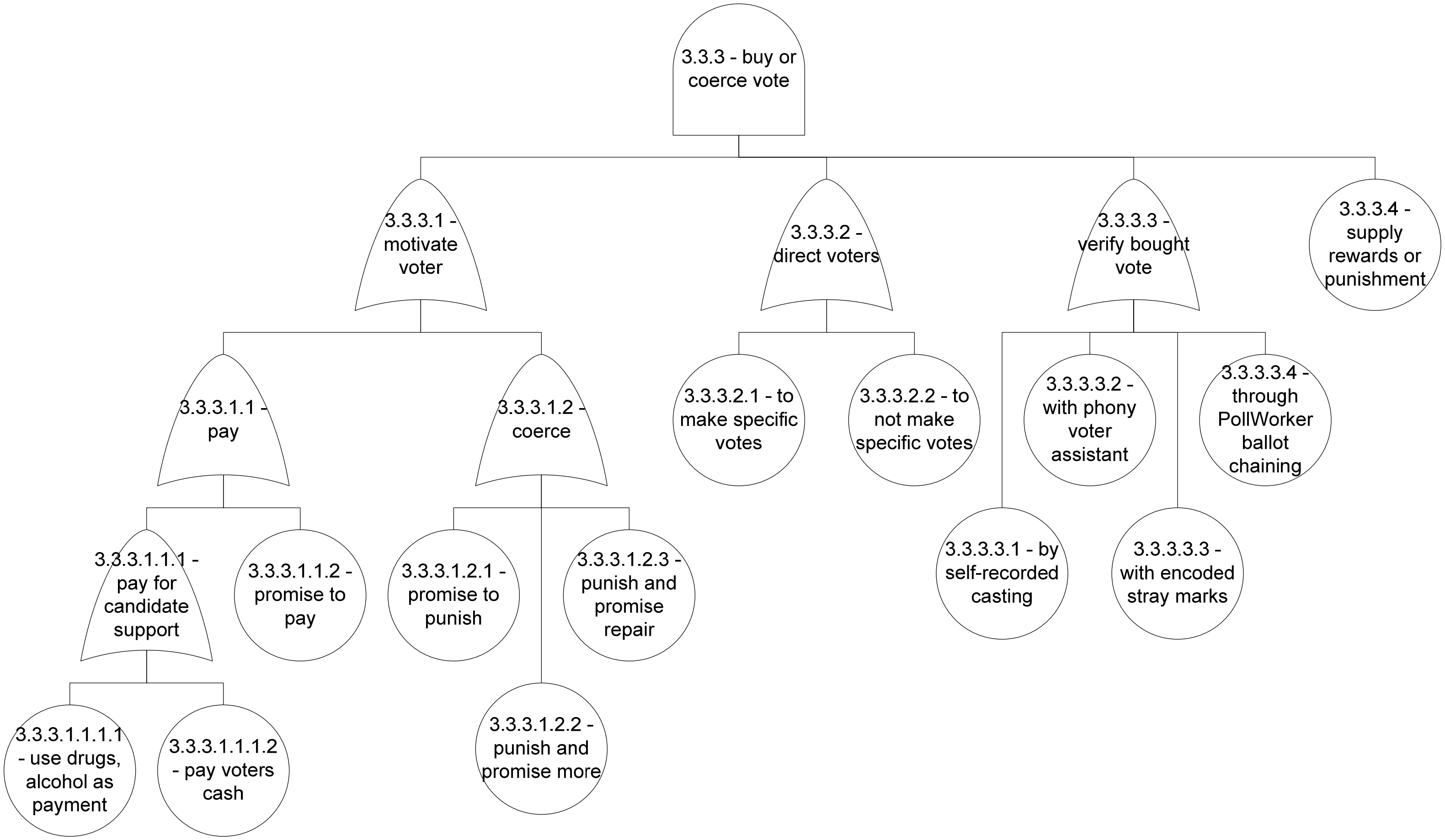
3-9 PCOS Subvert Voting Process


3.3 - commit vote fraud attack
3.3.1 - perform chain vote
3.3.2 - perform impersonation attack
3.3.3 - buy or coerce vote
3.3.4 - vote more than once
3.3.1.1 - acquire VotableBallot
3.3.1.3 - smuggle VotableBallot out
3.3.1.2 - vote with pre-maked ballot
3.3.2.1 - create fraudulent voter registrations
3.3.2.3 - execute impersonated voting
3.3.2.2 - create target list of voters to impersonate
3.3.3.1 - motivate voter
3.3.3.3 - verify bought vote
3.3.3.2 - direct voters
3.3.3.4 - supply rewards or punishment
3.3.4.1 - vote using more than one method
3.3.4.3 - insert unauthorized physical ballots into the ballot box
3.3.4.2 - vote in more than one place

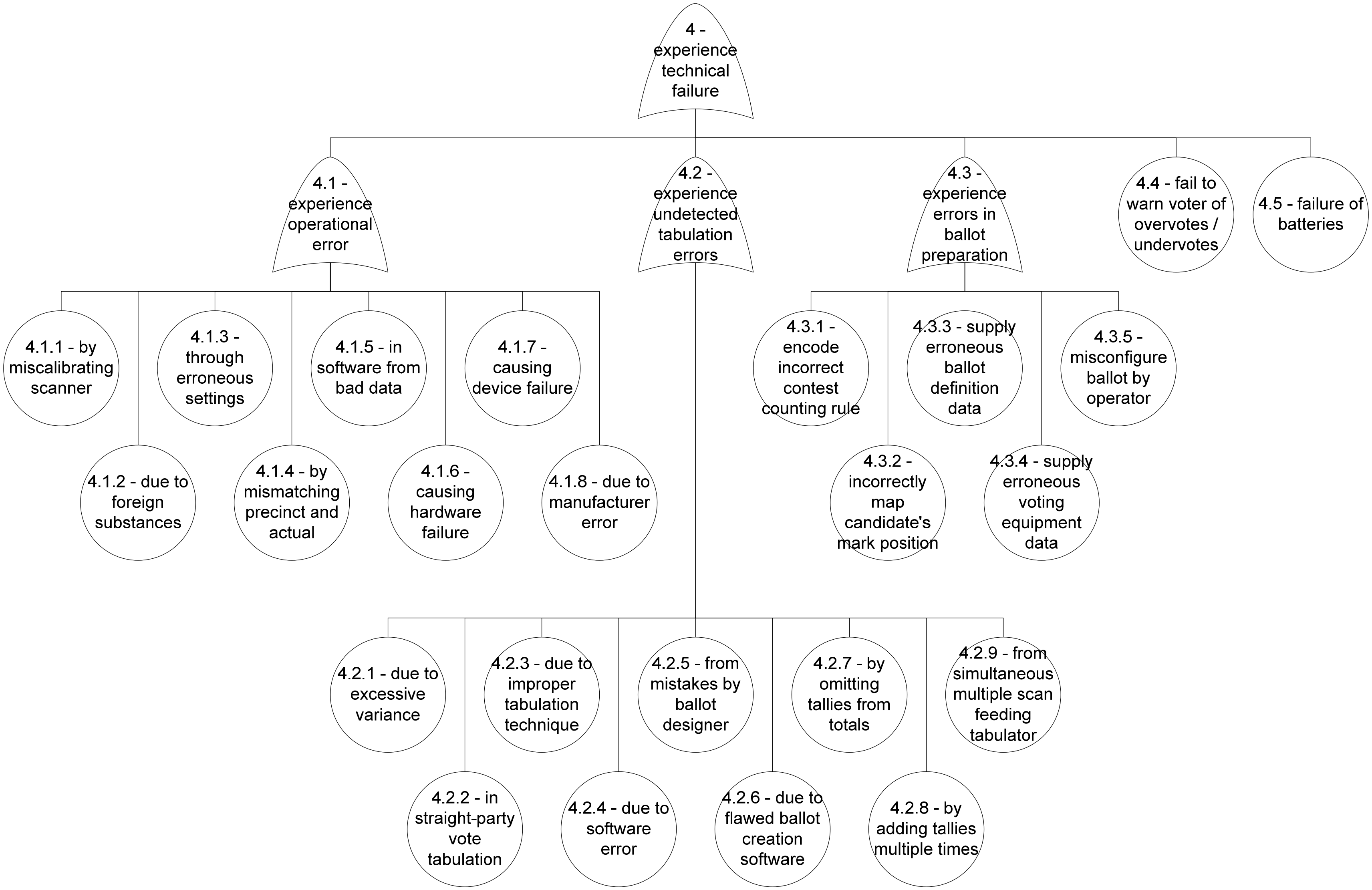
3-10 PCOS Commit Vote Fraud Attack


3.3.2 - perform impersonation attack
3.3.2.1 - create fraudulent voter registrations
3.3.2.2 - create target list of voters to impersonate
3.3.2.3 - execute impersonated voting
3.3.2.1.1 - register as an housemate
3.3.2.1.2 - register as a dead person
3.3.2.1.3 - register an ineligible person
3.3.2.1.4 - register as a fictitious person
3.3.2.2.1 - fradulent registrations
3.3.2.2.2 - unlikely voters
3.3.2.2.3 - voters likely to vote late in the day
3.3.2.3.1 - assign impersonator to voter
3.3.2.3.2 - go to target voter's polling place
3.3.2.3.3 - check in as the impersonated voter
3.3.2.3.4 - vote in place of voter
3.3.2.3.5 - supply rewards

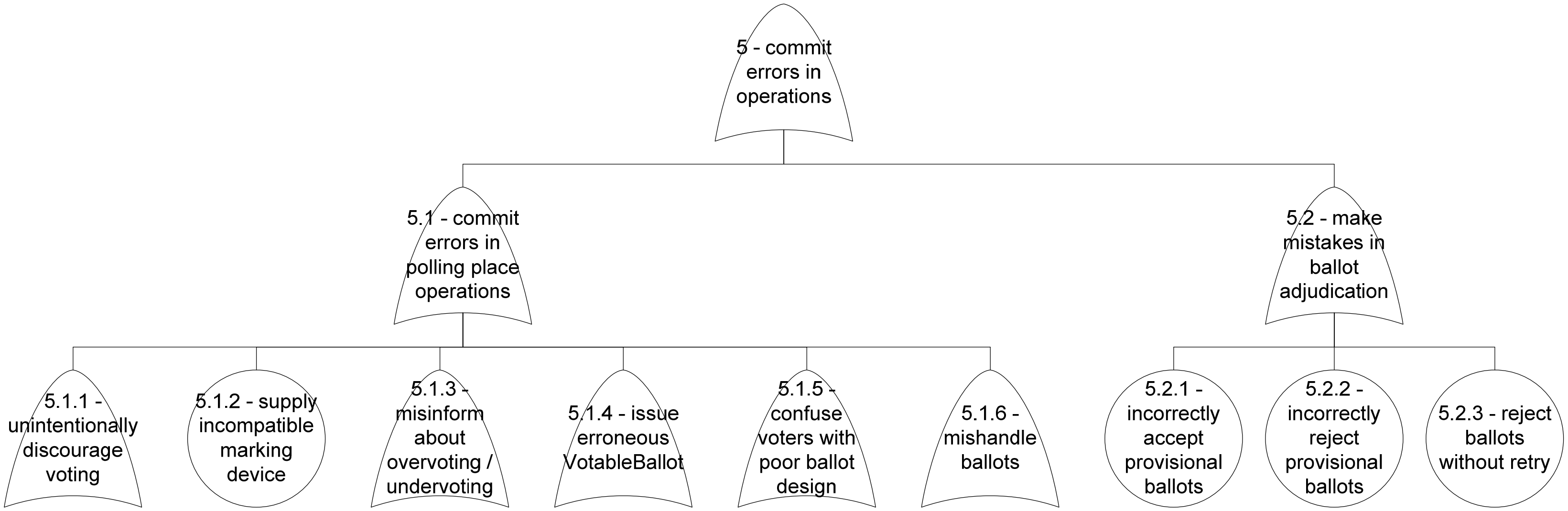
3-11 PCOS Perform Impersonation Attack


3.3.3 - buy or coerce vote
3.3.3.1 - motivate voter
3.3.3.2 - direct voters
3.3.3.3 - verify bought vote
3.3.3.4 - supply rewards or punishment
3.3.3.1.1 - pay
3.3.3.1.2 - coerce
3.3.3.2.1 - to make specific votes
3.3.3.2.2 - to not make specific votes
3.3.3.3.2 - with phony voter assistant
3.3.3.3.4 - through PollWorker ballot chaining
3.3.3.1.1.1 - pay for candidate support
3.3.3.1.1.2 - promise to pay
3.3.3.1.2.1 - promise to punish
3.3.3.1.2.3 - punish and promise repair
3.3.3.3.1 - by self-recorded casting
3.3.3.3.3 - with encoded stray marks
3.3.3.1.1.1.1 - use drugs, alcohol as payment
3.3.3.1.1.1.2 - pay voters cash
3.3.3.1.2.2 - punish and promise more

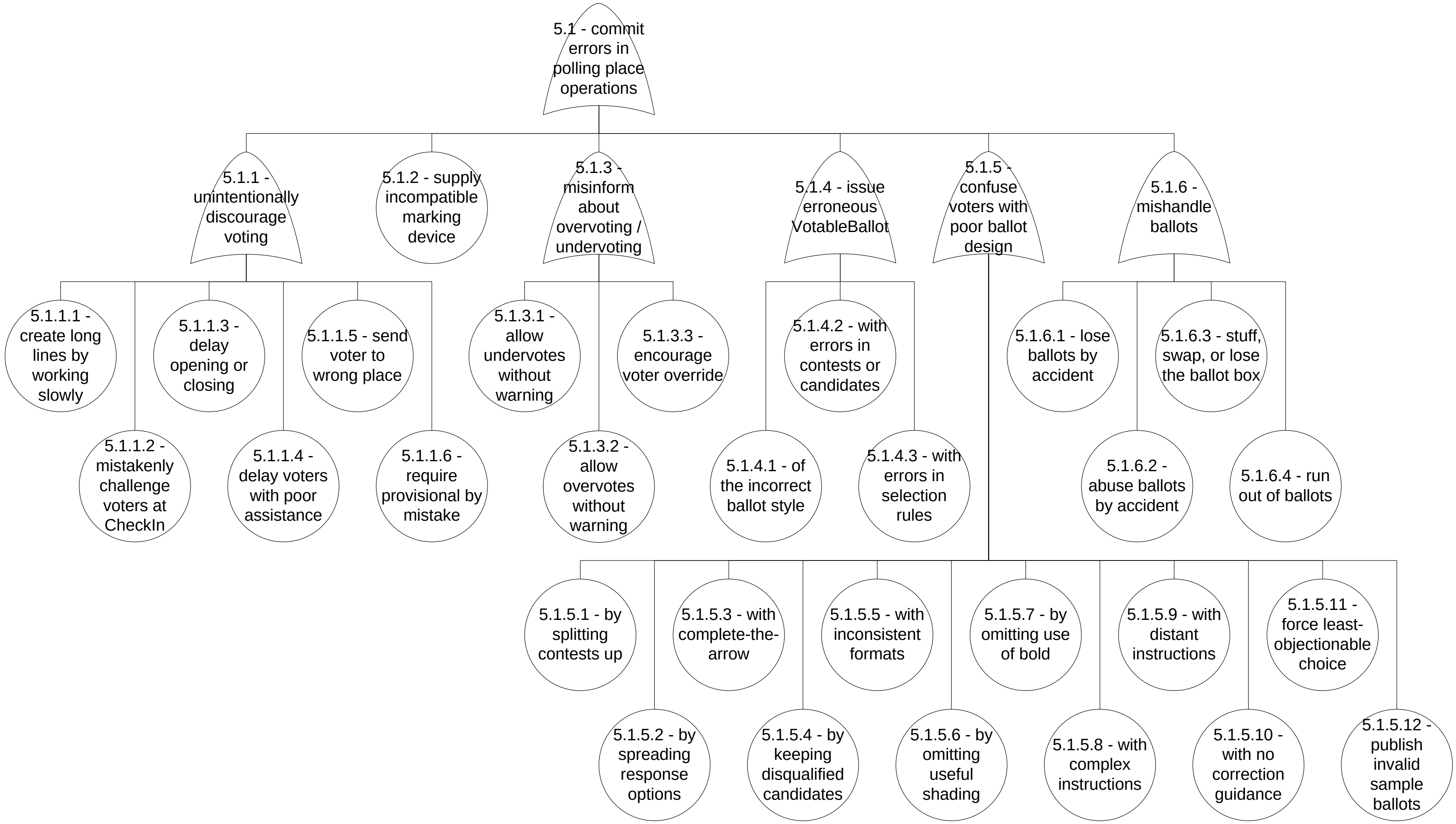
3-12 PCOS Buy or Coerce Vote


4 - experience technical failure
4.1 - experience operational error
4.2 - experience undetected tabulation errors
4.3 - experience errors in ballot preparation
4.4 - fail to warn voter of overvotes / undervotes
4.5 - failure of batteries
4.1.1 - by miscalibrating scanner
4.1.2 - due to foreign substances
4.1.3 - through erroneous settings
4.1.4 - by mismatching precinct and actual
4.1.5 - in software from bad data
4.1.6 - causing hardware failure
4.1.7 - causing device failure
4.1.8 - due to manufacturer error
4.3.1 - encode incorrect contest counting rule
4.3.2 - incorrectly map candidate's mark position
4.3.3 - supply erroneous ballot definition data
4.3.4 - supply erroneous voting equipment data
4.3.5 - misconfigure ballot by operator
4.2.1 - due to excessive variance
4.2.2 - in straight-party vote tabulation
4.2.3 - due to improper tabulation technique
4.2.4 - due to software error
4.2.5 - from mistakes by ballot designer
4.2.6 - due to flawed ballot creation software
4.2.7 - by omitting tallies from totals
4.2.8 - by adding tallies multiple times
4.2.9 - from simultaneous multiple scan feeding tabulator

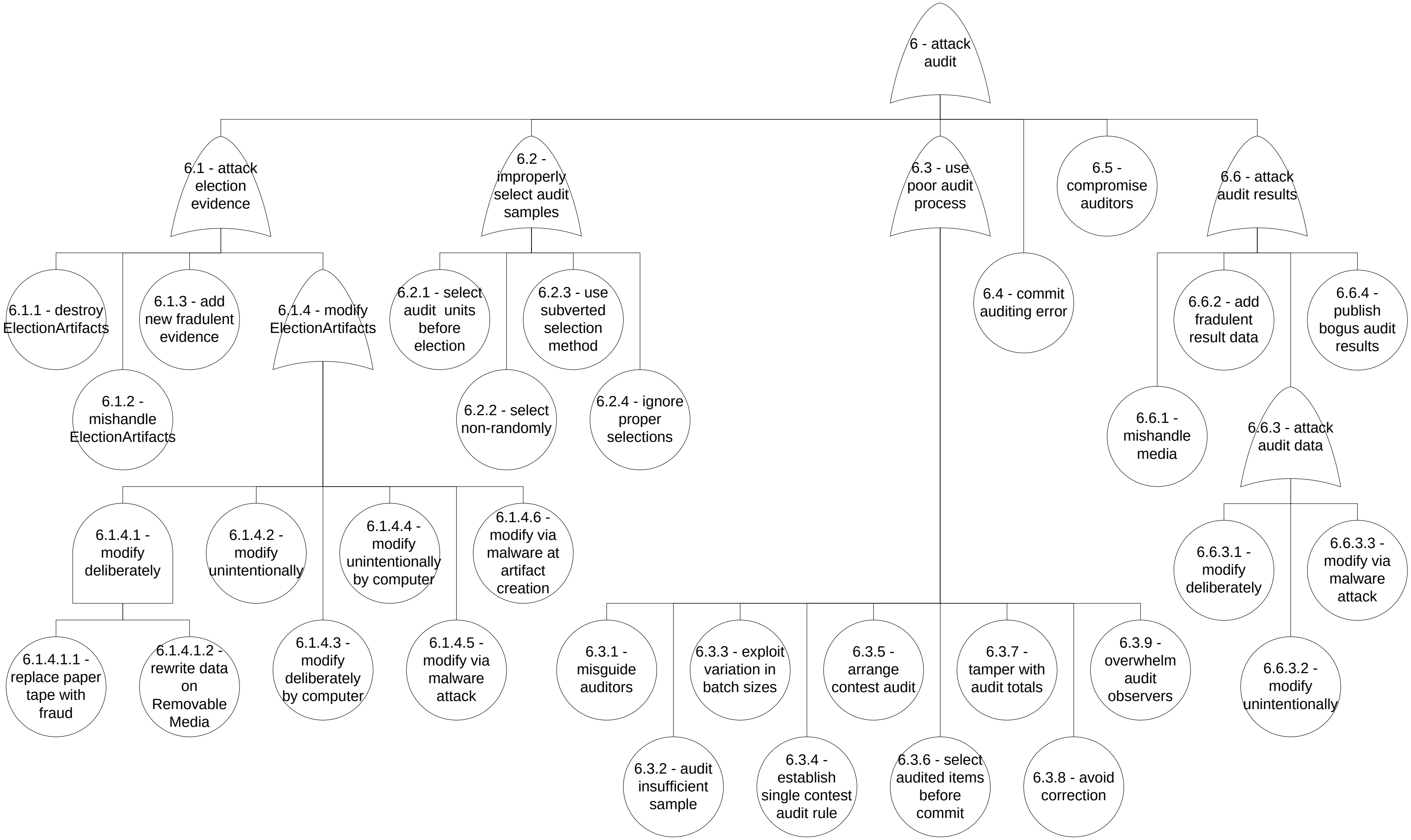
3-13 PCOS Experience Technical Failure


5 - commit errors in operations
5.1 - commit errors in polling place operations
5.2 - make mistakes in ballot adjudication
5.1.1 - unintentionally discourage voting
5.1.2 - supply incompatible marking device
5.1.3 - misinform about overvoting / undervoting
5.1.4 - issue erroneous VotableBallot
5.1.5 - confuse voters with poor ballot design
5.1.6 - mishandle ballots
5.2.1 - incorrectly accept provisional ballots
5.2.2 - incorrectly reject provisional ballots
5.2.3 - reject ballots without retry

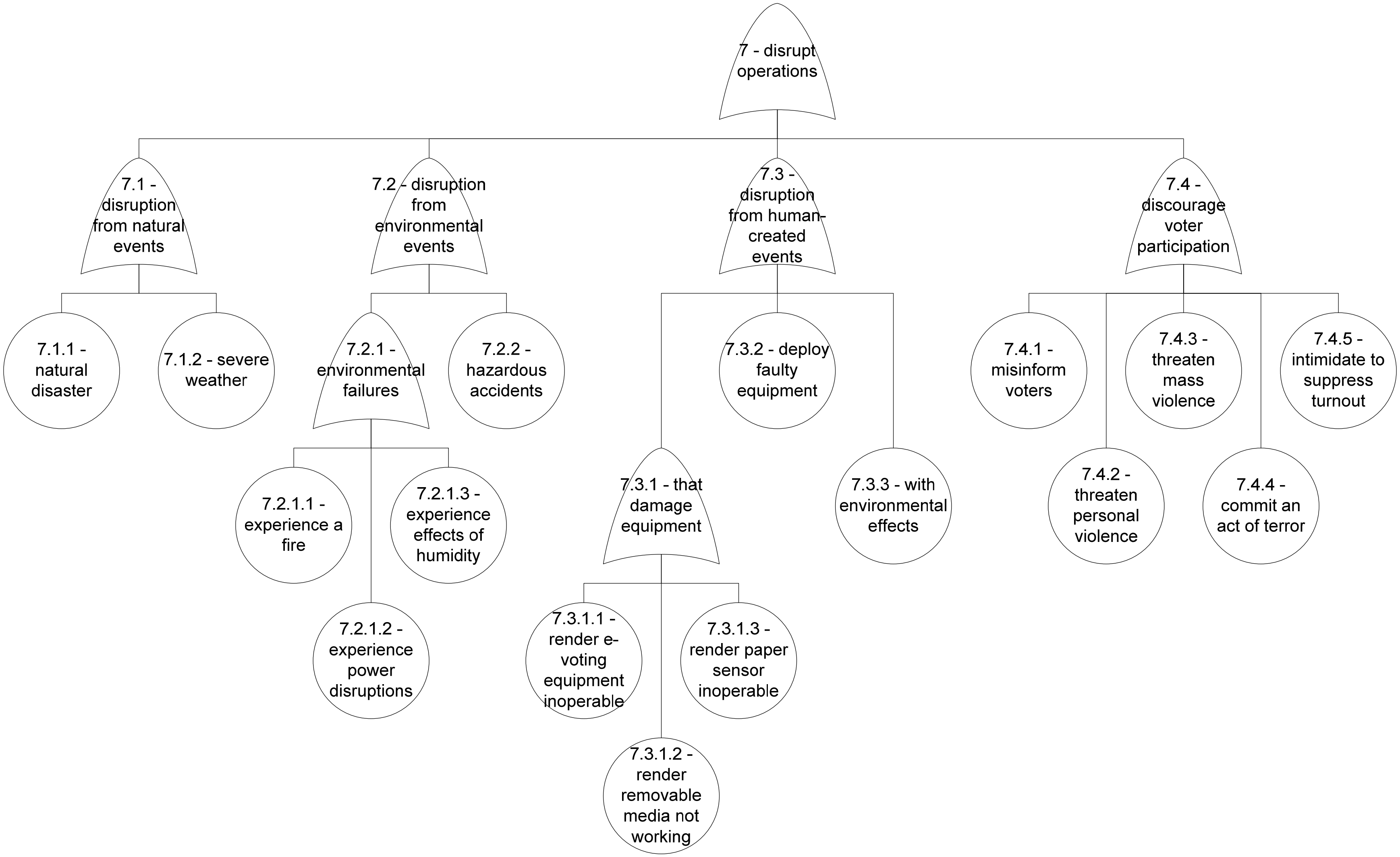
3-14 PCOS Commit Errors in Operations


5.1 - commit errors in polling place operations
5.1.1 - unintentionally discourage voting
5.1.2 - supply incompatible marking device
5.1.3 - misinform about overvoting / undervoting
5.1.4 - issue erroneous VotableBallot
5.1.5 - confuse voters with poor ballot design
5.1.6 - mishandle ballots
5.1.1.1 - create long lines by working slowly
5.1.1.2 - mistakenly challenge voters at CheckIn
5.1.1.3 - delay opening or closing
5.1.1.4 - delay voters with poor assistance
5.1.1.5 - send voter to wrong place
5.1.1.6 - require provisional by mistake
5.1.3.1 - allow undervotes without warning
5.1.3.2 - allow overvotes without warning
5.1.3.3 - encourage voter override
5.1.4.1 - of the incorrect ballot style
5.1.4.2 - with errors in contests or candidates
5.1.4.3 - with errors in selection rules
5.1.6.1 - lose ballots by accident
5.1.6.2 - abuse ballots by accident
5.1.6.3 - stuff, swap, or lose the ballot box
5.1.6.4 - run out of ballots
5.1.5.1 - by splitting contests up
5.1.5.2 - by spreading response options
5.1.5.3 - with complete-the-arrow
5.1.5.4 - by keeping disqualified candidates
5.1.5.5 - with inconsistent formats
5.1.5.6 - by omitting useful shading
5.1.5.7 - by omitting use of bold
5.1.5.8 - with complex instructions
5.1.5.9 - with distant instructions
5.1.5.10 - with no correction guidance
5.1.5.11 - force least-objectionable choice
5.1.5.12 - publish invalid sample ballots

3-15 PCOS Commit Errors in Polling Place Operations


6 - attack audit
6.1 - attack election evidence
6.2 - improperly select audit samples
6.3 - use poor audit process
6.5 - compromise auditors
6.6 - attack audit results
6.1.1 - destroy ElectionArtifacts
6.1.3 - add new fradulent evidence
6.1.4 - modify ElectionArtifacts
6.2.1 - select audit units before election
6.2.3 - use subverted selection method
6.4 - commit auditing error
6.6.2 - add fradulent result data
6.6.4 - publish bogus audit results
6.1.2 - mishandle ElectionArtifacts
6.2.2 - select non-randomly
6.2.4 - ignore proper selections
6.6.1 - mishandle media
6.6.3 - attack audit data
6.1.4.1 - modify deliberately
6.1.4.2 - modify unintentionally
6.1.4.4 - modify unintentionally by computer
6.1.4.6 - modify via malware at artifact creation
6.6.3.1 - modify deliberately
6.6.3.3 - modify via malware attack
6.1.4.1.1 - replace paper tape with fraud
6.1.4.1.2 - rewrite data on Removable Media
6.1.4.3 - modify deliberately by computer
6.1.4.5 - modify via malware attack
6.3.1 - misguide auditors
6.3.3 - exploit variation in batch sizes
6.3.5 - arrange contest audit
6.3.7 - tamper with audit totals
6.3.9 - overwhelm audit observers
6.6.3.2 - modify unintentionally
6.3.2 - audit insufficient sample
6.3.4 - establish single contest audit rule
6.3.6 - select audited items before commit
6.3.8 - avoid correction

3-16 PCOS Attack Audit


7 - disrupt operations
7.1 - disruption from natural events
7.2 - disruption from environmental events
7.3 - disruption from human-created events
7.4 - discourage voter participation
7.1.1 - natural disaster
7.1.2 - severe weather
7.2.1 - environmental failures
7.2.2 - hazardous accidents
7.3.2 - deploy faulty equipment
7.4.1 - misinform voters
7.4.3 - threaten mass violence
7.4.5 - intimidate to suppress turnout
7.2.1.1 - experience a fire
7.2.1.3 - experience effects of humidity
7.3.1 - that damage equipment
7.3.3 - with environmental effects
7.4.2 - threaten personal violence
7.4.4 - commit an act of terror
7.2.1.2 - experience power disruptions
7.3.1.1 - render e-voting equipment inoperable
7.3.1.3 - render paper sensor inoperable
7.3.1.2 - render removable media not working

3-17 PCOS Disrupt Operations

3.3 PCOS Threat Matrix

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	1	attack voting equipment	attack on voting equipment; attack PCOS hardware, software, communications links	LTM-USA Delivery 01a	human-deliberate	voting system	voting system	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish a chain of custody on VotingMachines; implement personnel security; and provide operational and technical safeguards	
O	1.1	gather knowledge	gather needed technical knowledge	LTM-USA Delivery 01a	human-deliberate	election system	voting machine, sensitive tech data, tech insiders	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection	
T	1.1.1	from insider	hire existing vendor or testing lab insider	LTM-USA Delivery 01a	human-deliberate insider	election system	insider, technology	susceptibility of insiders to bribery and corruption; access that insiders have to voting machines and other election assets	personnel security, including thorough background checks on possible people who may have access to the voting machine	
A	1.1.2	from components	obtain knowledge from voting system components		human-deliberate	election system, voting system	voting machine	access to voting machines	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection	
O	1.1.2.1	access directly	obtain knowledge directly from a voting system		human-deliberate	election system, voting system	voting machine	access to voting machines	physical and environmental protection of voting equipment	
T	1.1.2.1.1	infiltrate as insider	get hired as vendor or lab insider	LTM-USA Delivery 01a	human-deliberate outsider	election system, voting system	voting machine, sensitive tech data	susceptibility of insiders to bribery and corruption; access to voting machine	personnel security, including thorough background checks on possible people who may have access to the voting machine, access controls, and media protection policies	
T	1.1.2.1.2	obtain a machine	use illegal means to gain access that is available to insiders (e.g., breaking and entering warehouse)	LTM-USA Delivery 01a	human-deliberate	election system, voting system	voting machine	access to voting machine	physical and environmental protection of voting equipment, including use of tamper resistant or tamper evident seals and tracking of seal numbers, as in a chain of custody set of controls	reverse engineer a stolen machine
T	1.1.2.1.3	legally acquire machine	directly acquire voting system components including equipment, software installed on PC or on voting equipment or copied via network or as source code	LTM-USA Delivery 01a	human-deliberate	election system	voting machine	access to voting equipment that is not controlled like arms, munitions, secrets etc	establish a chain of custody on VotingMachines, including access and personnel policies, audit logs, and media protection policies	Purchase a voting machine on eBay or study a machine in transit

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.2.1.4	study a machine in transit	steal machines - alter machine - attack machine	LTM-USA Delivery 01a	human-deliberate	election system	voting machine	access to voting machine	thorough background checks on possible people who may have access to the voting machine	
T	1.1.2.1.5	find source code	find or purchase source code		human-deliberate	election system	voting machine	access to voting equipment that is not controlled like arms, munitions, secrets etc	establish a chain of custody on VotingMachines, including access and personnel policies, audit logs, and media protection policies	
T	1.1.2.1.6	compromise existing source code escrow	attacker obtains source code from existing source code escrow source (e.g., State Election Office)		human-deliberate	election system	voting machine	access to voting equipment that is not controlled like arms, munitions, secrets etc	establish a chain of custody on VotingMachines, including access and personnel policies, audit logs, and media protection policies	
T	1.1.2.2	directly examine	directly examine voting system components to gain knowledge		human-deliberate	election system, voting system	voting machine	access to voting machines	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection	
T	1.1.3	from published reports	gather knowledge from published reports on the examination of voting machines		human-deliberate	election system	voting machine	access to publicly available information	risk assessment	an attacker reads the California top-to-bottom reviews (TTBRs) of voting machines
O	1.2	gain insider access	obtain access for attack		human-deliberate outsider	election system	voting machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection; establish system and services acquisition controls	
T	1.2.1	at voting system vendor	gain insider access at voting systems vendor in order to include in the product the ability to enable attacks		human-deliberate outsider	election system	voting machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish chain of custody on VotingMachines	
T	1.2.2	in supply chain	gain insider access in the manufacturing chain, supply chain, or services/ support company, in order to be able to modify equipment and/ or SW install media		human-deliberate outsider	election system	voting machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish chain of custody and system and services acquisition controls	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.3	in elections org	gain insider access in elections organizations (and services such as transportation and storage of PCOS devices, IT support for PCs that run non-device SW) in order to modify delivered devices and installed SW		human-deliberate outsider	election system	voting machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish chain of custody and system and services acquisition controls	
T	1.2.4	by illegal insider entry	use illegal means to gain access that is available to insiders (e.g., breaking and entering warehouse)		human-deliberate outsider	election system	voting machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	physical and environmental protection of voting equipment	
T	1.2.5	by remote network access	gain remote access via network-connected PCs running SW components of voting systems		human-deliberate outsider	election system	voting machine	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	technical controls: access control, audit and accountability, identification and authentication, and system and communications protection	
O	1.3	attack component	perform attack on accessed voting system component, such as hardware, software, data, or communication link		human-deliberate	election system, voting system	voting machine, testing, voting, ballot definition	access to voting equipment, availability and willingness of insiders and outsiders, faulty testing, inability of audits / tests to detect	physical and environmental protection, incident response, maintenance, media protection policy and procedures, and configuration management	
O	1.3.1	attack hardware	perform physical attack on voting system hardware		human-deliberate	election system, voting system	voting machine	access to voting equipment	physical and environmental protection, incident response, maintenance, media protection policy and procedures	
T	1.3.1.1	jam PCOS scanner	jam PCOS scanner so it will not be able to accept any ballots		human-deliberate	election system, voting system	voting machine	access to voting equipment	physical and environmental protection, incident response, maintenance	
T	1.3.1.2	attacker scanner with goop pen	use an invalid marking device with goop ink to render scan head unreadable		human-deliberate	voting	voting machine	inability to detect easily, and difficulty preventing voters from using their own marking device	incident response, maintenance, close inspection of ballots before scanning	a voter, using his own 'goop' pen with a Vaseline-mixed or other odd ink, intentionally executes a denial of service attack by rendering entire columns of a ballot unreadable by disabling the read head in that location; aka spitball attack
O	1.3.1.3	attack stored components	attack storage of voting system components		human-deliberate	election system, voting system	voting machine	access to voting equipment	physical and environmental protection, incident response, maintenance, media protection policy and procedures	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.1.3.1	swap boot media	physically swap boot media		human-deliberate	election system, voting system	voting machine	access to voting equipment	physical and environmental protection, including procedures limiting the ability of insiders to bring possible substitutes into physical environment; incident response, maintenance, media protection policy and procedures, including use of tamper-evident seals	
T	1.3.1.3.2	attack install	physically swap install media, and re-install SW, or create situation in which someone else will re-install		human-deliberate	election system, voting system	voting machine	access to voting equipment	physical and environmental protection, including procedures limiting the ability of insiders to bring possible substitutes into physical environment; incident response; maintenance; media protection policy and procedures, including use of tamper-evident seals; and configuration management	
T	1.3.1.3.3	destroy Removable Media	destroy RemovableMedia		human-deliberate	election system, voting system	voting machine	access to voting equipment	physical and environmental protection, incident response, maintenance, media protection policy and procedures	
A	1.3.2	attack software	perform logical attack on voting system software		human-deliberate	election system, voting system	voting machine, testing	access to voting equipment, availability and willingness of insiders and outsiders, faulty testing, inability of audits / tests to detect	system and service acquisition, system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection; and incident response	
T	1.3.2.1	develop malware	develop malware		human-deliberate	election system	voting machine, testing	ability of hackers to be able to develop new forms of malware	system and information integrity; incident response	
O	1.3.2.2	select targets	select targets for malware		human deliberate	election system, voting system	polling place	Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows.	risk assessment	
T	1.3.2.2.1	select precincts by expected voting pattern	attacker selects a precinct that follows a particular voting pattern making it easier for him to carry out the attack.	NA	human-deliberate	election system	polling place	Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows.	Position Categorization, Personnel Sanctions	John is a poll worker. He selects a precinct of his choice to work on election day. He makes the selection based on the voting pattern the precinct follows. Doing so he can carry out the attacks he can on that particular voting pattern with ease. For example, if he is good at injecting malware into the systems with ease, he would select a precinct that uses internet voting pattern.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2.2.2	select all precincts	attacker selects all precincts		human-deliberate	election system	polling place	Increasing availability (i.e. web-based) of information about precincts	risk assessment	
O	1.3.2.3	inject malware	exploit existing vulnerability to inject malware		human-deliberate	election system	voting machine	poor physical and network security on voting terminals	system and service acquisition, system and information integrity, access control, audit and accountability, identification and authentication, and system and communications protection	
T	1.3.2.3.1	by remote bug exploitation	remotely exploit bug in voting system SW running on network-connected PC		human-deliberate	election system	voting machine	poor physical and network security on voting terminals	system and communications protection	
T	1.3.2.3.2	by local bug exploitation	locally exploit bug in voting system software that reads data from removable media (e.g., ballot definition files)		human-deliberate	election system	voting machine	access to voting equipment	system and communications protection; system and information integrity; media protection policy and procedures	
T	1.3.2.3.3	by human interface exploit	locally exploit bug in voting system software for human interface		human-deliberate	election system	voting machine	access to voting equipment	system and communications protection; system and information integrity; media protection policy and procedures	
O	1.3.2.4	execute malware	exploit existing vulnerability to execute malware		human-deliberate	election system	voting machine	access to voting equipment	system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
T	1.3.2.4.1	that alters artifact directly	malware changes voting system code or configuration data directly		human-deliberate	voting system	voting machine	access to voting equipment	system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
T	1.3.2.4.2	that self-propagates	malware installs itself to propagate virally to other instances of the same voting system component		human-deliberate	voting system	voting machine	access to voting equipment	system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	
T	1.3.2.4.3	that remains resident	malware remains resident during this power cycle only, in order to modify voting system code in memory, or tamper with data generated during this power cycle (e.g., vote data)		human-deliberate	voting system	voting machine	access to voting equipment	system and information integrity, including logic and accuracy testing; audit and accountability; identification and authentication; system and communications protection; and incident response	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.3.2.5	mitigate risk of detection	use procedural means to mitigate risk of detection during testing		human-deliberate	voting system	voting machine, election officials, testers, test scripts	insider knowledge of testing procedures and access to equipment	planning, personnel security, system and information integrity	
T	1.3.2.5.1	coerce testing staff	coerce testing staff to suppress information		human-deliberate	voting system	election officials	susceptibility of insiders to bribery or corruption	personnel security, system and information integrity	
T	1.3.2.5.2	attack after testing	perform malware attack after testing		human-deliberate	voting system	voting machine	limits of one-time tests that are not repeated	planning, system and information integrity, including random testing	
T	1.3.2.5.3	obtain cooperation of testers	bribing testers - tainted test results	LTM-USA Delivery 01a	human-deliberate	voting system	testers	easily bought or persuaded testers	ensure testers follow instructions completely to make sure that everything that you are testing to find is done	
T	1.3.2.5.4	access testing scripts	acquire detailed knowledge of testing procedures and scripts	LTM-USA Delivery 01a	human-deliberate	voting system	test scripts	access to knowledge of testing procedures	safeguard testing procedures; develop new testing procedures for each election	
T	1.3.2.6	use infected component	use voting system component that has been compromised by malware		human-deliberate	voting system	voting	inability of computer user to detect malware during use	planning, system and information integrity	
O	1.3.2.6.1	supply cryptic knock	use malware features to mitigate risk of detection during testing, by determining when malware should be active		human-deliberate	voting system	voting system	difficulty in detecting malware that has not yet been activated by knock	planning, system and information integrity, including tests designed detect cryptic knocks, such as random testing, simulating election day volume, and setting date to election day	
T	1.3.2.6.1.1	during logic and accuracy testing	supply cryptic knock during logic and accuracy testing	LTM-USA Delivery 01a	human-deliberate	voting system	testing	inability to detect the clever insider's infiltration of the L&A test script; overcoming the defense against cryptic knocks	planning, system and information integrity, perform testing or random testing again after L&A scripts are completed, under the assumption that the test scripts may be compromised	
T	1.3.2.6.1.2	during machine setup	supply cryptic knock during machine setup	LTM-USA Delivery 01a	human-deliberate	voting system	pollworker setup procedures	routine machine setup procedures of pollworkers, when known, can be used to set off cryptic knock unknowingly	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine; review instructions from vendor for machine to check for possible abnormalities	
T	1.3.2.6.1.3	during voting	supply cryptic knock during voting	LTM-USA Delivery 01a	human-deliberate	voting system	voting	unlikeliness of tests to produce knock-like behavior	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.3.2.6.1.4	as anti-knock	turn off fraud behavior with testing team anti-knock	LTM-USA Delivery 01a	human-deliberate	voting system	testing	election official's control over testing procedures	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.3.2.6.1.5	using AC power flicker	use AC power to flicker as knock	LTM-USA Delivery 01a	human-deliberate	voting system	testing	failure of tests to mimic knock action	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2.6.1.6	to detect realistic patterns of voting	detect realistic patterns of voting	LTM-USA Delivery 01a	human-deliberate	voting system	testing	failure to test machines with realistic patterns of voting	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.3.2.6.1.7	to employ calendar/clock tricks	employ calendar/clock tricks	LTM-USA Delivery 01a	human-deliberate	voting system	testing	difficult to detect that the Trojan horse has circumvented the test	system and information integrity, with testing by setting the date to election day in advance	
T	1.3.2.6.1.8	in ballot definition files	deploy cryptic knock in ballot definition files	LTM-USA Delivery 01a	human-deliberate	voting system	testing	failure to use real ballot in testing	controls on ballot definition files, including audit and accountability, access control, media protection policy and procedures, physical and environmental protection, and system and information integrity	
O	1.3.2.6.2	control/parameterize attack	control/parameterize attack	LTM-USA Delivery 01a	human-deliberate	voting system	testing, voting, voters	extremely unlikely that voting pattern can be detected as a knock	physical and environmental protection, media protection policy and procedures, system and communications protection, personnel security	
T	1.3.2.6.2.1	voter enables attack as attacker	voter knowingly enables attack	LTM-USA Delivery 01a	human-deliberate	voting system	voting	difficult or impossible to detect that a LegalVoter is setting off attack with their voting selections	personnel security, controls that prevent or detect voter impersonation	
T	1.3.2.6.2.2	enable by unknowing voter	voter unknowingly enables attack	LTM-USA Delivery 01a	human-deliberate	voting system	legal voters, campaign	ability of voters to be fooled by false campaign	awareness and training, look for unusual or suspicious write-in campaigns	
T	1.3.2.6.2.3	enable by technical consultant	technical consultant at polling place enables attack during health check, repair, setup, or poll close	LTM-USA Delivery 01a	human-deliberate	voting system	consultants	corrupt consultants to vendors	physical and environmental protection, media protection policy and procedures, including tamper controls, system and communications protection, including encrypted media	
T	1.3.2.6.2.4	employ unparameterized attack	employ unparameterized attack such as party-based attack	LTM-USA Delivery 01a	human-deliberate	voting system	voting system	increased ease for attacker in employing attacks that do not need to know contest-specific parameters	thorough L&A testing and random testing that compares actual vs expected vote totals	
T	1.3.2.6.2.5	add commands to ballot def file	add steganographic commands to ballot definition file	LTM-USA Delivery 01a	human-deliberate	voting system	ballot preparation	lack of supervision of ballot preparation	personnel security, including mutli-person controls, and thorough L&A testing to detect mismatches	
O	1.3.3	attack data	perform logical attack on voting system data		human-deliberate	voting system	election artifacts	access to components	system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection; media protection policy and procedures; configuration management	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.3.3.1	using malware	use malware to change data that effects election outcomes		human-deliberate	voting system	election artifacts	access to components	system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection, media protection policy and procedures	
O	1.3.3.1.1	select method and alter	select alteration method(s)		human-deliberate	voting system	election artifacts	access to components	system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection, media protection policy and procedures	
T	1.3.3.1.1.1	by malware	direct alteration by malware resident with voting system device SW or non-device SW		human-deliberate	voting system	election artifacts	access to components	system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection	
T	1.3.3.1.1.2	by infected software	alteration by voting system SW that was modified by malware		human-deliberate	voting system	election artifacts	access to components	system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection	
T	1.3.3.1.1.3	by infected config data	alteration as a result of new configuration data that was modified by malware		human-deliberate	voting system	election artifacts	access to components	system and information integrity, personnel security, audit and accountability, identification and authentication, physical and environmental protection, media protection policy and procedures	
T	1.3.3.1.2	alter ballot definition file	alter ballot definition file data (or predecessor data) to cause a PCOS device to record a vote in a particular location as a vote for a candidate/contest other than what is displayed on the ballot (‘vote flipping’) *REPEAT??		human-deliberate	voting system	election artifacts	access to components	audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
T	1.3.3.1.3	alter device tallies	alter PCOS device tallies		human-deliberate	voting system	election artifacts	access to components	audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
T	1.3.3.1.4	alter tabulation SW	alter results of tabulation software		human-deliberate	voting system	election artifacts	access to components	audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.3.3.2	modify data on storage medium	use general purpose computer to modify data on the storage media		human-deliberate	voting system	election artifacts	access to components	physical and environmental protection, personnel security, media protection policy and procedures	
T	1.3.3.2.1	modify tabulation data	modify device vote tallies, tabulated vote totals, log data, after data was generated		human-deliberate	voting system	election artifacts	access to components	audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
O	1.3.3.2.2	modify data before use	modify data before use, to affect election results		human-deliberate	voting system	election artifacts	access to components	audit and accountability, system and information integrity, using testing that attempts to reconcile separate tallies	
T	1.3.3.2.2.1	pre-load votes	pre-load votes into a PCOS device before polls open		human-deliberate	voting system	election artifacts	access to components	personnel security: multi-person/multi-party observation at poll opening; configuration management: require a zero-count determination and documentation process	
T	1.3.3.2.2.2	flip votes	alter ballot definition file data (or predecessor data) to cause a PCOS device to record a vote in a particular location as a vote for a candidate/contest other than what is displayed on the ballot ('vote flipping')		human-deliberate	voting system	election artifacts	access to components	planning, system and information integrity: thorough L&A testing and random testing that compares actual vs expected vote totals	
T	1.3.3.2.2.3	alter config data	alter other configuration data of PCOS device (e.g., threshold values for identifying ballot mark)		human-deliberate	voting system	election artifacts	access to components	planning, system and information integrity: through testing at multiple levels, including the use boundary analysis to develop test cases for detecting threshold errors	
O	1.3.4	attack comlinks	perform physical and/or logical attack on communications links		human-deliberate	voting system	voting machine	ease of access to components via networked connections for hackers	access control and system and communications protection, including cryptography and public access protections	
T	1.3.4.1	attack linked scanner/tabulator	attack serial port connection while PCOS scanner is connected to central tabulator server		human-deliberate	voting system	voting machine	ease of access to components via networked connections for hackers	access control and system and communications protection	
T	1.3.4.2	attack wireless	attack wireless communication vulnerability		human-deliberate	voting system	voting machine	ease of remote wireless accessibility for hackers	access control and system and communications protection, including cryptography and public access protections	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	2	perform insider attack	intentional abuse of insider access and privileges		human-deliberate insider	voting system	voting sytem, election artifacts, voters	insider access, availability and willingness of insiders, difficulty in detection	more transparency of the entire elections process, laws governing the bipartisan appointment of precinct officials and the distribution of duties within a polling place, laws dictating the configuration of a polling place and access to it, laws criminalizing voter intimidation, caging and the abuse of the challenge process, training programs for election officials at the national, state and local levels, including enhanced training of precinct officials and more aggressive prosecution of violations; effective audits of elections and the ability to respond to attacks by investigating, prosecuting and correcting abuses after the fact	
O	2.1	form inside attack team	form attack team of one or more attackers with insider privileges		human-deliberate insider	election system, voting system	voting system	insider access, availability and willingness of insiders, difficulty in detection	personnel security, awareness and training, incident response, physical and environmental protection	
T	2.1.1	infiltrate as volunteer pollworker	a lone attacker gains insider privilege by signing up as a pollworker		human-deliberate insider	election system, voting system	election officials	difficulty in discovering infiltrators	personnel security, awareness and training, incident response, physical and environmental protection	
T	2.1.2	infiltrate as observer	gain 'insider' access as a poll observer, either by volunteering, or by qualifying, depending on state laws		human-deliberate insider	election system, voting system	election officials	difficulty in discovering infiltrators	personnel security, awareness and training, incident response, physical and environmental protection	
T	2.1.3	staff with attackers	use insider privilege of ElectionOfficial to staff polling place or post-polling operations with attackers	Jones(2005a) #31	human-deliberate insider	voting system	pollworkers	power of election official over polling place operations	transparency of polling place activities, presence of observers	
T	2.1.4	collude with other insiders	collude with one or a few other insiders, possibly using bribery or coercion; either at the polling place, central operations, or between both		human-deliberate insider	election system	election officials	removal of potential means of detection	personnel security, awareness and training, incident response, physical and environmental protection	an ElectionOfficial forms a collusive arrangement between a polling place and central operations, for the purpose of having either party overlook the potential abuses being committed by the other party
T	2.1.5	allow pollworker rotation	allow rotation of pollworker roles, as a single person pollworker attacks are more likely when different duties are handled by the same person		human-deliberate insider	voting	elections official / pollworker for voter checkin	poor election laws / policies / guidelines	establish chain of custody procedures on at-risk election artifacts; provide for both separation of duties, as well as multi-person, multi-party controls	John, a poll worker colludes with the election-official to subvert separation of duties. He handles the pollbook and issues ballots to certain voters

node type	**outline number**	**threat action**	**description**	**reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
O	2.2	execute insider attack	execute insider attack		human-deliberate insider	voting system	voting system, election artifacts	insider access, availability and willingness of insiders, difficulty in detection	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1	attack at polling place	perform insider attack at polling place	LTM-USA Delivery 01a	human-deliberate insider	voting system	voters, ballots, voting system	power and control of insiders over elections operations	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1.1	discourage voters	intentionally discourage voters from voting	Jones(2005a) # 211	human-deliberate insider	voting system	checkin, check poll book, authenticate voter	unwillingness or inability of voters to appeal pollworkers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Poll workers intentionally refuse to allow the voter to vote even though voters name is present on the county register of voters.
O	2.2.1.1.1	challenge at CheckIn	challenge voters during CheckIn		human-deliberate insider	checkin	checkin	unwillingness or inability of voters to appeal pollworkers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.1.1.1	falsely reject voter registration	falsely reject voter claiming they are not registered		human-deliberate insider	voting system	checkin, check poll book, authenticate voter	unwillingness or inability of voters to appeal pollworkers' decisions	provide appeal process for oversight of pollworker	
T	2.2.1.1.1.2	falsely reject id check	falsely reject voter on identification check		human-deliberate insider	voting system	provide credential	unwillingness or inability of voters to appeal pollworkers' decisions	provide appeal process for oversight of pollworker	
T	2.2.1.1.1.3	selectively challenge voters	selectively challenge voters, such as ‘undesirable’ voters in polling place	Jones #212	human-deliberate insider	voting	voter checkin	ability of pollworkers or collusions of pollworkers to control voter checkin; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A corrupt pollworker may use race, gender, appearance of age, a person's attire, etc., as a means of ‘profiling’ a voter, and then selectively challenge a person's voter status based upon the expectation that a person fitting that profile will vote contrary to attacker

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.1.1.4	falsely challenge voters on target list	creating a target list and question voters' right to vote	Levitt (2007)	human-deliberate insider	election system	eligible voters; send to senior pw;	disclosing information of voters	chain of custody for voter lists, including access control policies	The attacker sends registered mail to addresses of registered voters that they've identified as likely to be unfriendly to their candidate. All mail that is returned as undeliverable is placed on what is called a caging list. Then this list is used to challenge the registration or right to vote of those names on it.
T	2.2.1.1.1.5	destroy registered cards	a third party working on behalf of voter registration encourages people to register and after the registration process destroy or discard their cards	Ballotpedia (2008)	human-deliberate insider	election system	registered cards	lack of management oversight over third party	Get the details from third party and mail the voter Id's to the voters instead asking third party to handover the id's.	John volunteers to help register voters before the election. Unknowingly to the officials, he was bribed by the Candidate to destroy voters' cards after the registration process is over.
O	2.2.1.1.2	delay open/close with excuses	delay opening or close with plausible excuses; preventing the voters from voting by making long queues and working slowly leading the voters leave the polling place	Jones (2005a) #33	human-deliberate insider	voting system	votable ballot, authenticate voter for voter check in	inability to detect that pollworker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A poll worker at a particular precinct works slowly e.g. he intentionally verifies the voter's authentication details slowly and issues the votable ballots to the voters slowly making the voters form long lines. Due to long waiting time few voters who cannot wait will leave the polling place without casting the vote.
T	2.2.1.1.3	create long lines	create long lines		human-deliberate insider	voting system	voting process	lack of oversight, lack of voter awareness; inability to detect that pollworker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	intentionally stymie voters by working slowly
T	2.2.1.1.4	stymie voters needing assistance	intentionally stymie voters needing assistance; voter manipulation - improper assistance to voters - improper advantage taken of voters with legitimate need for assistance	Jones (2005a) #332	human-deliberate insider	voting system	feed attempt for PCOS	lack of management oversight over poll workers designated to assist at polls	improve the administration of voting on the election day; let the voters be aware of the rules and regulations prior to the election day	John is a poll worker for a particular precincts election and is responsible for assisting the voter say 'X' needing help while marking the ballot or inserting the marked ballot into the scanner. His main aim in this threat attack is to stymie the voters from voting or vote for the voters who ask for help. If X has trouble inserting the marked ballot into the scanner(assume the scanner rejects the vote showing over votes), John can take advantage of the situation and change the ballot or simply without revising insert the ballot into the scanner resulting in the loss or cancellation of vote.
T	2.2.1.1.5	issue incorrect ballot style	issue voter an incorrect ballot style		human-deliberate insider	voter checkin	voter	possibility that threat will go undetected by voter	personnel security, voter education	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.1.6	mislead w/phony ballot change	mislead voters by announcing phony last-minute ballot change		human-deliberate insider	voting	eligible voter, signed in voter	susceptibility of voters to believe what was being informed by the poll worker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker passes out the ballots to voters and tell them there has been a change on the ballot.
T	2.2.1.1.7	mislead w/one party only ruse	mislead voters by announcing that only one party is allowed to vote		human-deliberate insider	voting	eligible voter, signed in voter	susceptibility of voters to believe what was being informed by the pollworker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker tells voters that only registered voters of one party is allowed to vote
T	2.2.1.1.8	discourage provisional voting	discourage provisional voting		human-deliberate insider	voting	authenticate voter	unwillingness or inability of voters to appeal pollworkers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker turns voter away by not issuing a provisional ballot
T	2.2.1.1.9	impede voter access	impede voter access to physical polling place; an attacker selectively prevents voters from some precincts, typically under some kind of color of authority.		human-deliberate insider	voting	voters and voting	If a voter must be present at a particular location (e.g. precinct) to cast a ballot, it is possible to prevent the voter from voting by physical exclusion.	Physical security at polling places; public education	A sheriff in a rural jurisdiction, unlikely to be observed by media or activists, impedes some voters from getting to the polling place by conducting improper traffic stops outside select precincts
T	2.2.1.1.10	persuade voter selections	persuade the voter to vote a certain way	Jones(2005a) #332	human-deliberate insider	voting	voting activity	lack of decisiveness in the voter, lack of management oversight over pollworkers	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Pollworker/election official/voter during the day of election intrudes into personnel privacy of the voter and tries to persuade him to cast his vote a certain way with suggestive, though non-threatening remarks
A	2.2.1.2	alter voter's vote	alter voter's vote in polling place	LTM-USA Delivery 01a	human-deliberate insider	voting system	voter, one voter	pollworker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.2.1.2.1	access ballots to alter votes	access ballots, either Marked, Provisional, or assisted, to steal votes		human-deliberate insider	election system, voting system	one voter	pollworker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	steal votes through improperly accessed ballots
T	2.2.1.2.1.1	obtain VotableBallot	obtain VotableBallot		human-deliberate insider	election system	one voter	pollworker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1.2.1.2	obtain MarkedBallot	create plausible reason to obtain MarkedBallot		human-deliberate insider	voting	one voter	pollworker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.1.2.1	jam / shutdown machine	jam or shutdown machine		human-deliberate insider	voting	one voter	pollworker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.1.2.2	mislead about committing ballot	mislead voters about correct commitment of ballot	http://www.lex18.com/Global/story.asp?S=10037216&nav=menu203_2	human-deliberate insider	voting	one voter	pollworkers have discretion to instruct voters and voters do not tend to read informative signs	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	The pollworkers told the voters to walk away after the first confirmation. After which, pollworkers changed their votes.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.2.1.2.3	collect ballots from voters	collect ballots from legitimate voters		human-deliberate insider	voting	one voter	pollworkers have discretion to instruct voters and voters do not tend to read informative signs	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
A	2.2.1.2.1.3	steal provisional ballot	poll worker forces the voter to vote on provisional ballot-vote manipulation	Jones(2005a) #21	human-deliberate insider	voting system	check poll book for authenticate voter	unwillingness or inability of voters to appeal pollworkers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Irrespective of the valid information provided by the voter, Poll worker forces voter to vote on provisional ballots. Since the provisional ballots are counted after the voter verification is done, the poll worker can tamper with the provisional ballots before turning them in with other election materials.
T	2.2.1.2.1.3.1	force provisional vote	force voter to vote on provisional ballot; voter manipulation- not allowing the eligible voters to vote as the registration information is not available	Jones (2005a) #3	human-deliberate insider	voting	check poll book for authenticate voter	unwillingness or inability of voters to appeal pollworkers' decisions	1) An election official at the polling place shall notify the individual that the individual may cast a provisional ballot in that election.	John is a poll worker at particular precinct elections. He has the access to the poll book where he can verify the voter's authentication to check the eligibility to vote. If the voters name is not present in the poll book or voters hold on to a voter ID card from many years ago which listed an incorrect precinct, it is John's responsibility to issue a provisional ballot to the voter. John here can take advantage of not issuing the provisional ballot to the voter thus resulting in loss of vote.
T	2.2.1.2.1.3.2	obtain provisional ballot	tamper with provisional ballots; ballot manipulation - neglect to seal the provisional ballot envelops-not writing the reason on the envelop	Jones(2005a) #33	human-deliberate insider	voting system	ballot	no monitoring or checking or observing PollWorker actions	eliminate barriers to voter registration so as to reduce the use of provisional voting	The poll worker should direct the voter to place the provisional ballot inner envelop into the provisional ballot outer envelope and seal the envelope and cross verify if the ballot is sealed properly. The poll worker here can be negligent or intentionally not seal the envelopes so that the vote can be disregarded.
T	2.2.1.2.1.4	obtain ballot of assisted voter	steal votes of voters needing assistance		human-deliberate insider	voting	votable or marked ballot	vulnerability of voter in need of assistance to the abuses of malicious pollworker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.2.1.2.2	tamper with ballots	tamper with ballots before they are scanned		human-deliberate insider	voting	votable or marked ballot	lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
A	2.2.1.2.2.1	subvert no-show vote	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones (2005a) #311	human-deliberate insider	voting system	check poll book for authenticate voter	unsecured poll book; corrupt official who coerces other poll workers	limited/no access to the ballot boxes to the pollworkers after the polls close	responsibility of recording the voters
O	2.2.1.2.2.1.1	conceal pollbook tampering	conceal pollbook tampering to reduce the risk of detection		human-deliberate insider	voting, precinct closeout	pollbook	lack of access controls on pollbook	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.1.1.1	wait until polls close	wait until polls close to tamper with pollbook		human-deliberate insider	voting, precinct closeout	pollbook	lack of access controls on pollbook	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.1.1.2	target unlikely voters	make list of unlikely voters		human-deliberate insider	election system	voter registration databases	access to voter lists and ability to determine voters not likely to vote	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.1.1.3	make excuses for marked pollbook	make excuses in case voters show up, and the pollbook is pre-signed		human-deliberate insider	voter CheckIn	election official	difficulty in determining the truth when pollworkers are lying	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.2.2.1.2	mark VotableBallot	mark VotableBallot		human-deliberate insider	voting, precinct closeout	voter	inability to verify voters vote due to lack of voter attribution	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.1.3	tamper with poll book	tamper with poll book to add no-show voters		human-deliberate insider	voting, precinct closeout	poll book	unsecured poll book; lack of supervision	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	2.2.1.2.2.2	subvert MarkedBallot of voter	subvert MarkedBallot of CheckedIn Voter at polls		human-deliberate insider	voting, precinct closeout	voter, marked ballot	inability to verify vote with voter, lack of management oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A Ballot Stuffer will cast votes on behalf of the people who did not show up to the polls ;sometimes, votes will even be cast by those who are long dead or fictitious characters often referred to as impersonation
T	2.2.1.2.2.2.1	mark undervote to create vote	mark undervote to create vote		human-deliberate insider	voting, precinct closeout	voter	inability to verify voters vote due to lack of voter attribution	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.2.2.2	mark vote to create overvote	mark vote to create overvote		human-deliberate insider	voting, precinct closeout	voter	inability to verify voters vote due to lack of voter attribution	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.2.2.2.3	swap ballot with new MarkedBallot	swap ballot with new MarkedBallot		human-deliberate insider	voting, precinct closeout	marked ballot	lack of management oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	2.2.1.2.3	commit subverted ballot	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones(2005a) #41	human-deliberate insider	voting, precinct closeout	[absentee] for provide credential (remote)	lack of supervision or other monitoring / poll observers	improved administration of voting on the election day	
O	2.2.2	attack other than polls	perform insider attack at other than polling place		human-deliberate insider	voting system	contest artifacts	insider access to contest artifacts	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
A	2.2.2.1	attack ballots	perform attacks on VotableBallots or MarkedBallots	Jones (2005a) #421	human-deliberate insider	voting system	votable ballots	access to ballots, difficulty of detection	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.1	access ballots	access ballots as an insider		human-deliberate insider	voting system	votable ballots	access to ballots	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
O	2.2.2.1.2	tamper with ballots	alter or destroy ballots obtained		human-deliberate insider	voting system	votable ballots	access to ballots	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.1.2.1	with unobtrusive defects	create unobtrusive defects on VotableBallots designed to change contest result		human-deliberate insider	ballot preparation, voting	votable ballots	lack of ballot custody controls	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.2.2	with faint pre-marks	tamper with preprinted ballot stock by making faint machine-readable marks		human-deliberate insider	ballot preparation, voting	votable ballots	difficulty for humans to detect machine-readable marks	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.2.3	with invisible ink pre-marks	pre-mark a ballot using invisible ink that is machine-readable		human-deliberate insider	ballot preparation, voting	votable ballots	difficulty for humans to detect machine-readable marks	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.2.4	by subverting ballot rotation	tamper with ballot design so that ballot rotation is subverted		human-deliberate insider	ballot preparation	votable ballots	inability for human to detect how machine counts marks; failure of tests to detect all anomalies	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.1.2.5	by marking ballot	alter MarkedBallots by marking selections that either exploit undervotes or cause overvotes	Jones (2005a) #421	human-deliberate insider	voting system	precinct closeout, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to physical ballots.	Paper ballots have no 'final form' status. That is, they can be marked after the voter has cast the ballot. For any system based on physical ballots, each ballot is a constrained data item (CDI). It is a well known security principle that the more CDIs there are, the more difficult it is to protect them.	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	After the polls close, poll worker(s) remove(s) ballots from the ballot box. If anytime thereafter they, or with a group of collaborators, gain private access to the paper ballots, they may selectively mark ballots to favor one or more candidates by exploiting undervotes (marking contests where voters did not make a selection) or to create overvotes in contests where voters selected the opponent of a preferred candidate. This could happen at the polling place, between the polling place and the jurisdiction's central site.
T	2.2.2.1.2.6	with invalidating marks	alter physical ballots by making illegal marks that will invalidate ballots during hand count or hand recount.	Jones (2005a) #421	human-deliberate insider	voting system	precinct closeout, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to physical ballots.	Paper ballots have no 'final form' status. That is, they can be marked after the voter has cast the ballot. For any system based on physical ballots, each ballot is a constrained data item (CDI). It is a well known security principle that the more CDIs there are, the more difficult it is to protect them.	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	After the polls close, poll worker(s) remove(s) ballots from the ballot box. If anytime thereafter they, or with a group of collaborators, gain private access to the paper ballots, they may selectively apply stray or identifying marks to ballots that are marked in support of the opponent of a preferred candidate. This could happen at the polling place, between the polling place and the jurisdiction's central site, etc.
T	2.2.2.1.2.7	by undoing voter marks	undo a voter's valid mark on a completed mark-sense ballot; To be properly recognized and interpreted by the scanner, mark sense ballots must have clear and unobscured marks. Proper marks can be obscured by applying stickers. White stickers will be effective, but may be easily detected. Some apparently clear stickers might be sufficient to interfere with the scanner but be hard to detect.	TMB, possible in Saltman	human-deliberate insider	ballot preparation, voting	marked ballots, especially prior to counting	insider access to ballots; lack of oversight / chain of custody of ballots	ballot chain of custody procedures; post-election review of ballots	Persons with access to marked ballots can obscure voter's marks by applying opaque stickers over the marks. This is possible even if indelible pens are used to mark the ballots (compare to erasure of pencil marks). In CCOS and remote voting environments the stickers could be applied in large numbers before the ballots are scanned the first time and could result in significant vote total changes. In PCOS environments there will be more limited possibilities of applying stickers before the initial scan. Nevertheless, applying stickers after the initial scan could result in audit and recount exceptions that would undermine voter confidence even if the outcome was not changed.
T	2.2.2.1.2.8	by subverting provisional envelope	tamper with provisional ballot envelope to cause rejection; an envelope is altered to change it from an accepted ballot to a rejected ballot	Dallas (2008)	human-deliberate insider	voting, canvass	committed provisional ballot	access to / lack of control or custody of CommittedBallot	access controls, auditing and logging	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.1.2.9	with physical damage	tamper with ballots by doing physical damage	CA TTBR	human-deliberate insider	voting	one voter	Unobserved physical access to paper	physical access controls	Damage paper/paper roll by pouring chemicals onto paper
O	2.2.2.1.3	replace ballots	switch legitimate ballots with tampered ballots		human-deliberate insider	voting system	ballots	access to ballots; lack of management oversight	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.3.1	switch valid ballots with tampered ones	switch a set of valid ballots with the ones the tampered ballots		human-deliberate insider	voting system	ballots	access to ballots; lack of management oversight	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	2.2.2.1.3.2	switch box during transport	substitute ballot box (add, delete, change ballots) during transport to central location	Jones(2005a) #413	human-deliberate insider	precinct closeout	one voter(remote), ballot delivery, one voter(remote)	failure to take the details of the person transferring the votes to the central location	physical and environmental protection-Delivery and Removal, , personnel security-Third Party personnel security	John is a pollworker responsible for tabulating the votes on the election night. This includes all kinds of votes like the absentee ballots, early votes, provisional ballots etc. He can use his influence and try to manipulate the precinct results by ignoring the ballots or by adding counterfeit ballots so as to match the original count of votes since the precinct results will be telephoned to the election department by the inspector prior to transmission.
T	2.2.2.1.3.3	discard / destroy MarkedBallots	use private access to discard or destroy a box of MarkedBallots (fail to replace)		human-deliberate insider	state accumulation, canvass, post certification	precinct closeout, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to a physical ballot box.	For any system based on physical ballots, each ballot is a constrained data item (CDI). It is a well known security principle that the more CDIs there are, the more difficult it is to protect them.	Ballot accounting, chain of custody, personnel screening	During precinct closeout, an elections official may remove a box of ballots from the controlled area and discard it, e.g. in a trash bin.
O	2.2.2.2	stuff ballots after closing	stuff ballot box after the polls close	Jones (2005a) #413	human-deliberate insider	voting g, precinct closeout	ballots, ballot box	access to ballots, ballot box; lack of management oversight	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.3	stuff during canvass or recount	inject ballot box (of physical ballots) during canvass or recount	2004 Washington Governor Contest	human-deliberate insider	canvas, post certification audit	validate total, process remote ballots	After the election, during the validate process, ballot boxes may be placed where they will be found in storage rooms, elections officials' cars, etc.	Ballot watermarking, ballot accounting, registration reconciliation	1. During a recount, an elections official places and then 'finds' a box of ballots in a key-controlled storage room and presents these ballots to the canvassing board for inclusion in the count. 2. During a recount, a poll worker places, and then finds, a box of ballots in the trunk of their car and presents these ballots to the canvassing board for inclusion in the count.
T	2.2.2.4	selectively recount	selectively recount by county or precinct		human-deliberate insider	canvass, state accumulation, post certification audit	validate total, recount	Election law	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	An elections official or political operative may trigger selective recounts in order to capture additional votes, expecting that changes in the selected counties will favor their candidate.
T	2.2.2.5	subvert tabulation	intentionally commit errors in tabulation (i.e., counting)		human-deliberate insider	precinct closeout, canvass, state accumulation	election artifacts	dependence on key election official(s) with centralized power to announce / certify result	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	precinct submitted twice without warning from system
O	2.2.2.6	attack tabulated results	attack results of tabulation process	Jones (2005a) #6	human-deliberate insider	precinct closeout, canvass, state accumulation	election artifacts	dependence on key election official(s) with centralized power to announce / certify result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	
T	2.2.2.6.1	subvert reported results	impersonate pollworker reporting preliminary precinct results; malicious outsider threatens the pollworker to disclose false results to the jurisdiction so as to change the election outcome.	Jones(2005a) #51	human-deliberate insider	precinct closeout, canvass, state accumulation	get precinct results flow chart	pollworker impersonation to alter the precinct result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	John is a malicious outsider. He tries to threaten the pollworker who is responsible for reporting the preliminary precinct results to the jurisdiction. Being threatened by the attacker the pollworker announces false results by not considering few ballots like provisional ballots, absentee ballots changing the outcome of the election.
T	2.2.2.6.2	falsely announce results	falsely announce tabulation results; announcement of tabulation result ignoring actual ballots	Jones (2005a) #51	human-deliberate insider	canvass, state accumulation	unofficial results, report results	dependence on key election official(s) with centralized power to announce / certify result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, separation of duties, physical access controls, auditing and accountability, such as verifying results against tabulated; incident monitoring and reporting; making whole process more transparent to media and public	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.2.6.3	alter results transmission	Results will be transmitted to county elections department on the election night. There are chances that the precinct results might be altered before transmitting them to the elections department.	Jones(2005a) #611	human-deliberate insider	precinct closeout	precinct result	Attacker can alter the transmission of precinct results by adding a counterfeit ballot box, ignoring the provisional votes etc.	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	John is a pollworker responsible for tabulating the votes on the election night. This includes all kinds of votes like the absentee ballots, early votes, provisional ballots etc. He can use his influence and try to manipulate the precinct results by ignoring the ballots or by adding counterfeit ballots so as to match the original count of votes since the precinct results will be telephoned to the election department by the inspector prior to transmission.
A	3	subvert voting process	subvert polling place voting process		human-deliberate, operational	voting system, election system	voting, voters, ballots, pollworkers, polling places	susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	planning, risk assessment, awareness and training, incident response, media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
O	3.1	target polling places	target polling places to attack		human-deliberate	voting system, election system	pollworkers, polling places	availability of information to aid attack strategy	risk assessment, incident response, personnel security	
T	3.1.1	by expected voting pattern	select a precinct that follows a particular voting pattern making it easier to carry out the attack	NA	human-deliberate	voting	polling place	Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows	personnel security, including Position Categorization and Personnel Sanctions	John is a poll worker. He selects a precinct of his choice to work on election day. He makes the selection based on the voting pattern the precinct follows. Doing so he can carry out the attacks he can on that particular voting pattern with ease. For example, if he is good at injecting malware into the systems with ease, he would select a precinct that uses internet voting pattern.
T	3.1.2	where PollWorkers not likely to know Voters	target polling places where poll workers are not likely to know voters		human-deliberate	voting	pollworkers, authenticate voter	pollworkers do not know voters	risk assessment, incident response	
T	3.1.3	that exploit electoral college rules	use winner-take-all electoral college design to tempt a selective attack in a tight presidential race	Campbell (2008), p. 337	human-deliberate	voting system, election system	voting system, election system	availability of polling data enables careful calculation of the number of votes needed to win, which can be leveraged by the winner-take-all electoral design	recommend that states award electoral votes in proportion to popular vote	Several tight presidential elections (1844, 1876, 1884, 1888, 1960, and 2000) could have been turned by fraud in a few selected areas (Campbell 2008, p. 337)
T	3.1.4	where PollWorkers can be co-opted	target polling places where poll workers can be co-opted		human-deliberate	voting	polling place, election official	susceptibility to exploitation by attackers	risk assessment, incident response	
T	3.1.5	with lax enforcement of procedures	target polling places with lax enforcement of procedures		human-deliberate	voting	polling place, election official	susceptibility to exploitation by attackers	risk assessment, incident response	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	3.2	form attack team	recruit sufficient impersonating attackers		human-deliberate	election system	potential recruits, eligible voters	availability and willingness of recruits	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
A	3.2.1	use cell captains to execute deniable impersonation attack	use cell captains to execute deniable impersonation attack	Jones (2005a) #31	human-deliberate	voting system	authenticate voter, ,	political influence / power of political leaders or election officials	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.2.1.1	recruit cell captains	recruit cell captains		human-deliberate	election system	people being recruited	corruptibility or vulnerability of political loyalists of political leader	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.2.1.2	motivate cell captains	educate and motivate cell captains in deniable ways		human-deliberate	election system	people being recruited	insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.2.1.3	educate cell captains	educate captains in deniable ways		human-deliberate	election system	people being recruited	insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.2.1.4	provide rewards for cell captains to distribute	provide cell captains with rewards to distribute		human-deliberate	election system	people being recruited	insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.2.1.5	recruit attackers	cell captains recruit more attackers	Jones (2005a) #311	human-deliberate	election system	voters	corruptibility of potential impersonators; resources of attackers	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.2	recruit attackers among LegalVoters	subvertible voters are gathered to increase the impact of chain voting or a group of attackers carry out chain voting attack	Jones (2005b)	human-deliberate	voting system	legal voters	susceptibility of voters to being bribed or intimidated	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	3.2.3	recruit brokers	recruit brokers to buy voters; attacker recruits loyal followers, giving them cash bills to buy votes on behalf of attacker's choices	Campbell (2006) pp. 278, 282, 337	human-deliberate	voting system, election system	eligible voter, signed in voter	attacker's power to acquire significant resources	expand campaign finance reform to cover wholesale vote-buying; prosecute voting conspiracies, including vote haulers and voters; maintain ballot secrecy	A Dodge County, GA, county commissioner used $15,000 in $20 bills, giving $4,000 to one vote 'hauler' to buy votes at the $20 going rate; one county commissioner forced his road department employees to work on the campaign or else lose their jobs (Campbell 2008, p. 282)
O	3.3	commit vote fraud attack	commit vote fraud attack	Campbell (2006)	human-deliberate	voting system, election system	voting, voters, ballots, pollworkers, polling places	susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	chain of custody controls on ballots, polling place security, multi-party observers	
A	3.3.1	perform chain vote	perform chain voting scheme	Jones (2005b)	human-deliberate	voting system	pollworkers, election officials	susceptibility of voters to being bribed or intimidated; lack of polling place security	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	
T	3.3.1.1	acquire VotableBallot	an outside attacker smuggles a VotableBallot or an election insider takes an absentee ballot and uses it for chain voting	Jones (2005b)	human-deliberate	voting system	ballot stock	lack of polling place security, lack of ballot custody	chain of ballot custody procedures, polling place security, including observers	
T	3.3.1.2	vote with pre-marked ballot	subverted voter takes MarkedBallot to polling place and votes with it, while also legally obtaining VotableBallot	Jones (2005b)	human-deliberate	voting system	commit ballot	lack of polling place security; voter privacy measures helps attacker conceal ballots	chain of ballot custody procedures, polling place security, including observers	
T	3.3.1.3	smuggle VotableBallot out	voter smuggles VotableBallot out of polling place and takes it to attacker to enable next cycle of chain voting	Jones (2005b)	human-deliberate	voting system	ballot stock	lack of polling place security; voter privacy measures helps attacker conceal ballots	chain of ballot custody procedures, polling place security, including observers	
O	3.3.2	perform impersonation attack	perform voter impersonation attack	LTM-USA Delivery 01a	human-deliberate	voting system	voting system	accessibility of lists of voters not likely to vote; soft voter authentication process; pollworkers don't know voters; willingness of pollworkers to engage in fraud	media protection policy and procedures, personnel security, access control, audit and accountability, identification and authentication	Tom is a party worker who has contacts with ElectionsOfficial. Getting EligibleVoters' personal information is an easy task for Tom. He can even prepare a list of EligibleVoters who are unlikely to vote this time through his contacts. After preparing a list, he then prepares fake Id's and bribes a group of loyal followers to impersonate the voters on his list. He sends impersonators to the polling places where PollWorkers are not likely to recognize them.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	3.3.2.1	create fraudulent voter registrations	create fraudulent voter registrations	Jones(2005a) #1	human-deliberate	election system	election system	poor vetting process, lack of resources, legal constraints on voter registration process	strengthen the controls in the ElectionSystem	
T	3.3.2.1.1	register as an housemate	recruit registers impersonators as housemates / roommates	Jones(2005a) #11, 12	human-deliberate	voting system	people being recruited	corruptibility or vulnerability of recruits	strengthen the controls in the ElectionSystem	A party worker may hire non voters from different state, prepare fake IDs and register them as housemates of LegalVoters and ask them to vote for his/her party candidate.
T	3.3.2.1.2	register as a dead person	register as a deceased or incapacitated person	Jones(2005a) #12	human-deliberate	election system	election system	lack of records management	strengthen the controls in the ElectionSystem	
T	3.3.2.1.3	register an ineligible person	register as an unregistered but ineligible person (e.g., non-citizens, felons)	Jones(2005a) #1	human-deliberate	election system	election system	lack of records management	strengthen the controls in the ElectionSystem	
T	3.3.2.1.4	register as a fictitious person	use a fake Id to register as a fictitious voter	Jones(2005a) #11,12	human-deliberate	voting system	authenticate voter	soft verification process	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	
O	3.3.2.2	create target list of voters to impersonate	create target list of voters to impersonate		human-deliberate	election system	voter lists	access to voter lists	chain of custody controls on voter registration lists, if not public information	
T	3.3.2.2.1	fraudulent registrations	create fraudulent voter registrations		human-deliberate	election system	voters lists	access to voter lists	chain of custody controls on voter registration lists, if not public information	
T	3.3.2.2.2	unlikely voters	make lists of voters very unlikely to vote this election	Jones (2005a) #311	human-deliberate	election system	voter lists	access to voter lists and ability to determine voters not likely to vote	chain of custody controls on voter registration lists, if not public information	Unlikely voters for an election might include infrequent voters, or voters that are absent or overseas
T	3.3.2.2.3	voters likely to vote late in the day	make lists of voters likely to vote late in the day		human-deliberate	election system	voter lists	access to voter lists and ability to identify target voters	chain of custody controls on voter registration lists, if not public information	
T	3.3.2.3	execute impersonated voting	execute impersonated voting		human-deliberate	voting	authenticate voter	failure of election day administration to foil attack	physical and environmental protection, audit and accountability, identification and authentication	
T	3.3.2.3.1	assign impersonator to voter	supply attackers with information about unlikely voter (e.g., name and gender)		human-deliberate	voting system	pollworkers, authenticate voter	pollworkers fooled by unknown attacker with valid voter information	physical and environmental protection, audit and accountability, identification and authentication	
T	3.3.2.3.2	go to target voter's polling place	impersonator goes to polling place of target voter	Jones(2005a) #311	human-deliberate	voting	voters	susceptibility of insiders to bribery and corruption	physical and environmental protection, including patrolling polling places, looking for suspicious activity	
T	3.3.2.3.3	check in as the impersonated voter	attacker has friends vote for the fake housemates	Jones(2005a) #311	human-deliberate	voter CheckIn	pollworkers, authenticate voter	pollworkers fooled by unknown attacker with valid voter information	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.3.2.3.4	vote in place of voter	impersonate and vote in the place of an EligibleVoter; a list of voters who are unlikely to vote may be prepared and people may be recruited to vote for that person. A polling place where a poll workers are not likely to know voters may be targeted.	Jones (2005a) #311	human-deliberate	voting	authenticate voter	access to lists of voters not likely to vote; PollWorkers don't know voters; corrupt PollWorker	require Credentials at polling places; conduct precise and careful purges on voter lists to remove duplicate names, people who have moved, died, or are otherwise ineligible.	
T	3.3.2.3.5	supply rewards	cell captain provides all required rewards out of own pocket		human-deliberate	election system	voters	susceptibility of insiders to bribery and corruption	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers, physical and environmental protection, limiting access to polling place and providing polling place patrols	
A	3.3.3	buy or coerce vote	motivate voters to either (a) stay away from polls or (b) vote in compliance with attacker demands	Dekel (2004), Fund (2004), Jones(2005a) #21	human-deliberate outsider	voting system, election system	eligible voter, signed in voter	susceptibility of voters to buying and coercion; breach of voter privacy; ability to attribute vote	maintain voter privacy; limit access to polling place	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
O	3.3.3.1	motivate voter	motivate voter with bribes or threats		human-deliberate	voting system	voter	human susceptibility to being bribed or coerced	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers, physical and environmental protection, limiting access to polling place and providing polling place patrols	‘Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future.’ (Fund 2004)
O	3.3.3.1.1	pay	motivate voter with pay		human-deliberate	election system	voter	human susceptibility to being bribed	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers	
O	3.3.3.1.1.1	pay for candidate support	make a direct payment to voters to support a particular candidate; attacker promises to bribe voters if they prove the attacker with evidence that they voted to the particular candidate supported by attacker.	Fund (2004), Dekel (2004)	human-deliberate	voting system	eligible voter, signed in voter	susceptibility of voters to bribery	Educate the voters about the importance of voting	‘Democrats are far more skilled at encouraging poor people — who need money — to participate in shady vote-buying schemes. 'I had no choice. I was hungry that day,' Thomas Felder told the Miami Herald in explaining why he illegally voted in a mayoral election. ‘You wanted the money; you were told who to vote for. (Fund 2004)

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.3.3.1.1.1.1	use drugs, alcohol as payment	use drugs or alcohol as payment for votes; attacker promises and exchanges drugs or alcohol in exchange for voting for attacker's candidates	Campbell (2006) pp. 144, 282, Estep (2009)	human-deliberate	voting system, election system	eligible voter, signed in voter	susceptibility of voters with substance abuse to bribery	maintain ballot secrecy	In 1910, the price of a vote was 'a drink of whiskey' (Campbell 2006, p. 144); in 2002, two Clay County, KY, election officers allegedly used the prescription painkiller OxyContin to buy votes (Estep 2009)
T	3.3.3.1.1.1.2	pay voters cash	pay the 'market' rate for a vote in direct cash payment	Campbell (2006) pp. 278, 283	human-deliberate	voting system, election system	eligible voter, signed in voter	susceptibility of voters to bribery	prosecute voters who sell their vote; throw out illegal votes; maintain ballot secrecy	In a 1987 Kentucky race, the price for a vote reached $200, while in 1996 Dodge County, Georgia, the going rate was $20 per vote (Campbell 2008)
T	3.3.3.1.1.2	promise to pay	promise payment later or promise payment based on subsequent verifiability of voter's carry out attacker's voting demands	Jones(2005a) #311	human-deliberate	voting	voters	susceptibility of voters to bribery	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers	
O	3.3.3.1.2	coerce	coerce the voter to vote for the attacker's candidate(s)		human-deliberate	election system	voters	human susceptibility to being coerced	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers	
T	3.3.3.1.2.1	promise to punish	promise some form of punishment in order to coerce voter	Van Acker	human-deliberate	election system	eligible voter, signed in voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers	An incumbent candidate seeking reelection sends a loyal confederate to the polls accompanying the incumbents' employees, who are coerced to vote for the incumbent, once they receive their votable ballots
T	3.3.3.1.2.2	punish and promise more	provide a real punishment, and then promise more punishment of not compliant		human-deliberate	election system	eligible voter, signed in voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers	
T	3.3.3.1.2.3	punish and promise repair	provide a real punishment, and then promise a repair of punishment		human-deliberate	election system	eligible voter, signed in voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and pollworkers	
O	3.3.3.2	direct voters	direct voters to vote a certain way	Jones (2005a) #32, Jones(2005b)	human-deliberate	voting	eligible voter	corrupt Poll Worker or voter who can easily be intimidated; Poll Workers and poll observers unable to detect concealed ballots	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.3.3.2.1	to make specific votes	direct voter to make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	paper ballot systems	folded marked ballot,	corrupt PollWorker or voter who can easily be intimidated; PollWorkers and poll observers unable to detect concealed ballots	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
T	3.3.3.2.2	to not make specific votes	direct voter to not make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	voting	eligible voter	corrupt Poll Worker or voter who can easily be intimidated; Poll Workers and poll observers unable to detect concealed ballots	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
O	3.3.3.3	verify bought vote	assess voter compliance with direction		human-deliberate	voting system	voter	inability to prevent voter attribution	prevent voter attribution with ballot secrecy, preventing stray marks, and making sure that voter assistance is legitimately needed	to ascertain that a bribed voter goes along with the vote fraud, attacker attempts to verify that voter voted for attacker's choices
T	3.3.3.3.1	by self-recorded casting	use a secret camera to self-record voter's ballot casting	Dekel (2004)	human-deliberate	voting system	eligible voter, signed in voter	breech of voter privacy in polling place	Tighten the security of voting system	Voter manages to capture video of his ballot casting, produces it to the attacker as evidence.
T	3.3.3.3.2	with phony voter assistant	assist voter at precinct to verify bought vote; voter requests assistance in order to earn reward from assistant	Jones (2005a) #333	human-deliberate	voting, canvass	sign pollbook, validate precinct results	failure to authenticate voter's assistant; failure to detect unusual patterns of assistance (same assistant, higher than normal assistance)	audit and accountability audit precinct results and investigate any unusual voting patterns, such as a high percentage of voter assistance or repeated assistance by the same assistant; prevent by asking voter for reason assistance needed	A man wearing dark glasses and appearing to be sight-impaired shows up with an assistant to help him vote. Following the procedures for check-in, the voter and the assistant obtain a VotableBallot, which is then marked and committed with the full knowledge and help of the assistant, who provides a cash payoff afterwards.
T	3.3.3.3.3	with encoded stray marks	make stray ballot mark for voter attribution		human-deliberate	voting	votable ballot	ability of voter to mark ballot freely	use ballot marking that prevents stray marks; clear plastic ballot sleeve	voter votes for attacker candidates and then votes for a write-in candidate by writing in a predetermined code word intended for an inside confederate to see and verify the bought vote
T	3.3.3.3.4	through PollWorker ballot chaining	voter feeds the pre MarkedBallot into the scanner and returns the empty VotableBallot to the attacker	Jones (2005a) #32, Jones(2005b)	human-deliberate	paper ballot systems	folded marked ballot,	corrupt PollWorker or voter who can easily be intimidated; PollWorkers and poll observers unable to detect concealed ballots	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
T	3.3.3.4	supply rewards or punishment	provide promised rewards or punishments based on voter compliance		human-deliberate	election system	post certification audit	difficulty in tracing payments	personnel security, including sanctions against violators	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	3.3.4	vote more than once	a LegalVoter votes more than once; ballot box stuffing by the voter		human-deliberate	voting	voting	inability of voting system to capture duplicate votes by a voter	system and information integrity, identification and authentication	
T	3.3.4.1	vote using more than one method	vote early and regular, or absentee and provisional as a form of ballot box stuffing	Jones (2005a) #41, TIRA panel	human-deliberate	voting	authenticate voter (remote), voter list, voter information, authenticate voter, authentication rules, jurisdiction	inability to or failure to cross-check pollbooks for different voting methods within a single place (jurisdiction)	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	a voter casts an absentee ballot but then votes again at the polling place on election day
T	3.3.4.2	vote in more than one place	vote in two neighboring states or multiple precincts with registrations in more than one place	Jones (2005a) #11, 312	human-deliberate	voting	VoterList, voter information, authenticate voter, authentication rules, jurisdiction	inability to or failure to cross-check voter lists across multiple jurisdictions	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	a husband and wife who move from Pensacola, FL to Mobile, AL prior to a federal election registers and votes in Alabama, then drives to Pensacola on same election day, voting in the precinct for their former address
T	3.3.4.3	insert unauthorized physical ballots into the ballot box	insert unauthorized physical ballots into the ballot box	NA	human-deliberate	voting	commit ballot	Cannot bind a paper ballot to a voter. For a physical ballot box with a slot, a voter may stack several ballots and insert them at the same time. For a PCOS system, the scanner attendant, must ensure that voter's only submit one ballot.	Ballot box attendant, probably not particular effective	A voter may acquire ballot copies, pre-mark them, and insert them into a ballot box with their legal ballot.
O	4	experience technical failure	experience a nondeliberate technical failure		technical	election system, voting system	voting machine	hardware wears rout, erroneous data entry, human error, poor testing	certification, accreditation, and security assessments, planning, system and services acquisition, awareness and training, configuration management, contingency planning, incident response, maintenance, media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, system and communications protection	
O	4.1	experience operational error	experience or commit voting equipment operational errors		technical	election system, voting system	voting machine	human error, poor testing	system and services acquisition, system and information integrity, maintenance, awareness and training, physical and environmental protection, contingency planning	
T	4.1.1	by miscalibrating scanner	PCOS scanner calibration failures or errors		technical	election system, voting system	voting machine	poor testing	system and services acquisition, system and information integrity	
T	4.1.2	due to foreign substances	PCOS paper feed mis-calibration, foreign objects, dust/dirt/grit		technical	voting	voting machine	difficulty in detection during operation	maintenance	
T	4.1.3	through erroneous settings	erroneous date/time settings, precinct ID setting, other election specific settings		technical	election system, ballot preparation	voting machine	human error, poor testing	DM, system and information integrity, awareness and training	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.1.4	by mismatching precinct and actual	mis-match of device's programmed precinct and actual precinct		technical	election system, ballot preparation	voting machine	human error, poor testing	system and information integrity	
T	4.1.5	in software from bad data	software errors from incorrect data in removable media, due to flaws in ballot creation software		technical	election system, ballot preparation	voting machine	erroneous data entry	system and services acquisition, system and information integrity	
T	4.1.6	causing hardware failure	hardware errors, both spontaneous or induced, such as liquid spills, static charge to memory units		technical	voting system	voting machine	hardware wear out	physical and environmental protection, contingency planning	
T	4.1.7	causing device failure	device operator error, including incorrect cabling, or bring-up in test mode		technical	voting system	voting machine	human error	awareness and training	
T	4.1.8	due to manufacturer error	ballot manufacturer incorrectly programming the ballot scanner		technical	election system	voting machine	human error, poor testing	system and services acquisition, system and information integrity: testing at the state or county level	
O	4.2	experience undetected tabulation errors	experience un-detected tabulation errors		human-unintentional, technical, operational	voting system, precinct closeout	voting machine	software bugs, human error, poor testing	system and information integrity, system and services acquisition, configuration management, awareness and training	
T	4.2.1	due to excessive variance	due to excessive variance requirement (* needs more explanation)		technical, operational	voting system, precinct closeout	voting machine	poor testing	system and information integrity	
T	4.2.2	in straight-party vote tabulation	due to use of incorrect rules for straight-party vote interpretation		human-unintentional	voting system, precinct closeout	contest results, candidates, political parties	poor testing	logic and accuracy tests that include straight-party voting tests that test actual vs. expected counts	
T	4.2.3	due to improper tabulation technique	due to use of incorrect selection of tabulation algorithm (e.g., IRV variants)		human-unintentional	voting system, precinct closeout	contest results, candidates, political parties	possibility that late testing will not detect, because actual vs. expected counts will match because both assume erroneous algorithm is the correct one	system and information integrity, including expert review of algorithm selection decision	
T	4.2.4	due to software error	due to software error including data loss, or incorrect tabulation algorithms		technical	voting system, precinct closeout	voting machine	possibility that late testing will not detect, because actual vs. expected counts will match because both assume erroneous algorithm is the correct one	system and information integrity, including expert review of algorithm selection decision; data backups or other redundancies	
T	4.2.5	from mistakes by ballot designer	due to operator error in ballot creation software (e.g., selection of contest counting rules; choosing to vote for no more than 4 votes when the real rule is no more than three)		human-unintentional	voting system, precinct closeout	votable ballots	human error and lack of testing	system and information integrity, including verifying correct rules chosen, and then testing the application of rule on test ballot sets	
T	4.2.6	due to flawed ballot creation software	due to flaws in ballot creation software		technical	voting system, precinct closeout	votable ballots	software bugs	system and services acquisition controls that hold vendors accountable for testing	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.2.7	by omitting tallies from totals	due to human error in omitting some tallies from vote total		human-unintentional	voting system, precinct closeout	contest results, candidates, political parties	human counting errors and poor testing	multi-person controls to verify correctness of human decisions	
T	4.2.8	by adding tallies multiple times	due to human error in including some tallies from vote total multiple times		human-unintentional	voting system, precinct closeout	contest results, candidates, political parties	human counting errors and poor testing	multi-person controls to verify correctness of human decisions	
T	4.2.9	from simultaneous multiple scan feeding tabulator	error caused due to multiple scanners feeding data into the tabulation system all at once		operational	voting system, precinct closeout	voting machine	technical limitations in handling high rate / volume of input	planning: setting up a procedure to avoid bottlenecks or procedures to monitor and detect bottlenecks and perform a retry	
O	4.3	experience errors in ballot preparation	experience software errors, or commit operational errors, in software that prepares ballots, device 'programming', ballot definition files, and other election-specific software or data artifacts		human-unintentional	ballot preparation	votable ballots	poor testing procedures, making last-minute changes to ballots and not re-testing; poorly trained workers	careful planning of tests at the state/local/precinct levels; system and services acquisition controls; system and information integrity controls, including comprehensive logic and accuracy tests designed to detect various errors; configuration management, including careful tracking and documentation of changes, particularly after testing, and the performance of regression testing; and awareness and training of election officials and pollworkers in ballot creation, testing procedures, and the use of equipment	
T	4.3.1	encode incorrect contest counting rule	encoding an incorrect contest counting rule		human-unintentional	ballot preparation	votable ballot	human error and lack of testing	logic and accuracy tests designed to detect contest counting flaws	
T	4.3.2	incorrectly map candidate's mark position	encoding incorrect mapping of ballot mark position to contest/candidate		human-unintentional	ballot preparation	votable ballot, candidate, contest	human error and lack of testing	systematic testing of marked ballots after contests are defined and that are designed to test the mark positions of each candidate for each contest	
T	4.3.3	supply erroneous ballot definition data	incorrect encoding of other ballot definition file data that influences tabulation		human-unintentional	ballot preparation	voting machine	human error and lack of testing	testing that includes matching machine tabulated counts against expected counts	
T	4.3.4	supply erroneous voting equipment data	incorrect encoding of other election equipment data that can cause technical malfunction		human-unintentional	ballot preparation	voting machine	human error and lack of testing	comprehensive testing	
T	4.3.5	misconfigure ballot by operator	operator error making incorrect choices among configuration alternatives, e.g. vote-counting algorithms, setting to notify voters of undervotes, etc.		human-unintentional	ballot preparation	votable ballot	human error and lack of testing	comprehensive testing	
T	4.4	fail to warn voter of overvotes / undervotes	failure of scanners to detect or warn the voter of overvotes or undervotes		technical	voting	voting machine	poor testing procedures	system and information integrity, system and services acquisition, configuration management, awareness and training	a voting machine fails to warn voters when they overvote or undervote, and the precinct or county experiences a disproportionate residual rate and rejected ballot rate

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.5	failure of batteries	failure of batteries during voting		technical	voting	voting machine	limited, unpredictable battery life	battery indicators, spare batteries on hand, replace before they go out	
O	5	commit errors in operations	commit unintentional errors in polling place operations		human-unintentional	voting system	pollworkers, voters, ballots, voting system activities	inadequate training, flawed processes, poor working conditions	certification, accreditation, and security assessments, planning, system and services acquisition, awareness and training, contingency planning, incident response, media protection policy and procedures, personnel security	
O	5.1	commit errors in polling place operations	commit errors in polling place operations		human-unintentional	ballot preparation, voting	pollworkers, voters, ballots, ballot preparation, voting	inadequate training, flawed processes, poor working conditions	certification, accreditation, and security assessments, planning, system and services acquisition, awareness and training, contingency planning, incident response, media protection policy and procedures, personnel security	
O	5.1.1	unintentionally discourage voting	unintentionally discourage the voter from voting		human-unintentional	voting	voter	poor election administration	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.1.1	create long lines by working slowly	create long lines by working too slowly		human-unintentional	voting	voter	inadequate pollworker training, staffing levels, voter constraints on time, impatience	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.1.2	mistakenly challenge voters at CheckIn	mistakenly challenge voters during CheckIn		human-unintentional	voting	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.1.3	delay opening or closing	delay opening or closing polls due to mistakes or slow working		human-unintentional	voting	voter	poor election administration	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.1.4	delay voters with poor assistance	delay voters by failing to properly assist		human-unintentional	voting	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.1.5	send voter to wrong place	erroneously send voter to other polling place		human-unintentional	voting	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.1.6	require provisional by mistake	erroneously require a voter to vote provisionally		human-unintentional	voting	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.1.2	supply incompatible marking device	provide paper ballot marking devices that are incompatible with ballot scanner		human-unintentional	voting	MarkedBallot	sensitivity of machines to ink color; difficulty with controlling use of marking device used by voter	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	Some voters vote with their own pens rather than the ones supplied; some machines are sensitive to blue ink
O	5.1.3	misinform about overvoting / undervoting	provide incorrect information about overvotes and undervotes		human-unintentional	voting	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.3.1	allow undervotes without warning	allow undervotes without warning		human-unintentional	voting	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
T	5.1.3.2	allow overvotes without warning	allow overvotes without warning		human-unintentional	voting	pollworker	lack of oversight of pollworkers	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	with long lines at the polling place, the pollworker might override the machine's overvote warning, rather than informing the voter
T	5.1.3.3	encourage voter override	encourage voter override of over/under-votes		human-unintentional	perform override	voter	poor pollworker performance; lack of oversight	planning, including rules of behavior; pollworker awareness and training; and personnel policies, including sanctions for poor performance	
O	5.1.4	issue erroneous VotableBallot	issue an erroneous VotableBallot to the voter		human-unintentional	IssueBallot	voter	possibility that voter will not catch error	personnel sanctions	
T	5.1.4.1	of the incorrect ballot style	issue an incorrect ballot style, that is, a ballot for a different precinct		human-unintentional	IssueBallot	voter	possibility that voter will not catch error	pollworker awareness and training	voter gets the ballot for voters of a different precinct, and consequently votes on incorrect set of contests
T	5.1.4.2	with errors in contests or candidates	issue ballot with mistakes in the contests or candidates		human-unintentional	IssueBallot	voter	possibility that voter will not catch error	pre-election ballot validation	ballot designer leaves off a contest or a candidate, or includes a disqualified candidate on the ballot
T	5.1.4.3	with errors in selection rules	issue ballot with errors in selection rules		human-unintentional	IssueBallot	voter	possibility that voter will not catch error	pre-election ballot validation	election official mistakenly designs ballot with incorrect counting rules, such as choosing to vote for no more than 4 votes when the real rule is no more than three
O	5.1.5	confuse voters with poor ballot design	poor ballot design that confuses or misleads voters during Voting process, or fails to prevent voter errors in marking ballot	Norden (2008)	human-unintentional	ballot preparation	validate ballot style, checkedin voter	weak reviewing process of a ballot design	use ballot design checklist, implement usability testing, review and amend election laws	
T	5.1.5.1	by splitting contests up	split candidates for the same office onto different pages or columns	Norden (2008) #1 p. 20	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	* use ballot design checklist, implement usability testing, review and amend election laws (* note the above also applies to thread id # 557 - 568), list all candidates for the same race on the same page in the same column	The 2000 presidential race in Palm Beach county, Florida has high residual vote rate due to confusing ballot design that displayed candidates in separate columns with response options in the center - hence the term ‘butterfly ballot’.

node type	**outline number**	**threat action**	**description**	**reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
T	5.1.5.2	by spreading response options	place response options on both sides of candidate names	Norden (2008) #3 p. 28	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	place response options (such as fill-in-the-ovals) in a consistent place on the ballot, such as one side of candidate names or ballot or ballot question choices	Response options placed on both sides of the candidate's name caused confusion among Hamilton county voters in Illinois. Voters tend to mark the arrow to the right of the candidate's name when they were supposed to mark the arrows on the left.
T	5.1.5.3	with complete-the-arrow	use complete-the-arrow instead of fill-the-oval response options	Norden (2008) #4 p. 30	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	use the fill-the-oval response option for selecting a choice in a contest	Polk county, Iowa uses optical scan system that requires voters to 'complete-the-arrow' to cast votes. Unfortunately, voters are more familiar with 'fill-in-the-oval' which has lesser residual vote rate compared to 'complete-the-arrow' response option.
T	5.1.5.4	by keeping disqualified candidates	leave columns or rows for disqualified candidates	Norden (2008) #5 p. 32	human-unintentional	ballot preparation	validate ballot style for ballot preparation	Failure to remove disqualified candidates from ballot; Failure to inform voters of disqualified candidates	remove the entire column or row for any candidate or party that has been withdrawn or disqualified (not just the candidate or party name)	The 2004 Presidential race in Montgomery county, Ohio has a higher overvote rate when the name of Ralph Nader was replaced with the words 'Candidate Removed'
T	5.1.5.5	with inconsistent formats	inconsistently design ballots in formatting and style	Norden (2008) #6 p. 36, Frisina (2008)	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	use consistent format and style for every contest and voting action	The inconsistent use of colors in Sarasota county ballot caused voters to skip the Thirteenth Congressional District race. The second page shows 'State' highlighted in teal which is the same as the first page's 'Congressional' word. Thus, it was easy to overlook the congressional district race.
T	5.1.5.6	by omitting useful shading	omit shading to help voters differentiate between voting tasks	Norden (2008) #7 p. 40	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	shade certain text, such as office name to help voters to differentiate between voting tasks	Failure to shade office titles on ballot result in higher residual vote rate in Escambia county, Florida. The affected races were Attorney General and Commissioner of Agriculture.
O	5.1.5.7	by omitting use of bold	omit bold text to help voters differentiate between voting tasks	Norden (2008) #8 p. 44	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	bold certain text, such as office name to help voters to differentiate between voting tasks	Misused of bold-faced text on the Franklin county ballot in Illinois made it difficult for voters to differentiate contests within each type. Hence, the residual votes were higher for the Attorney General and the Secretary of State races.
T	5.1.5.8	with complex instructions	fail to write short, simple instructions	Norden (2008) #9 p. 46	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	write short instructions with simple words	The 2004 presidential race in Kansas experienced high residual vote rate due to the long and confusing instruction on the ballot. For example, they used complicated words such as 'Deface' and 'wrongfully mark' instead of 'make a mistake'.
O	5.1.5.9	with distant instructions	place Instructions far from related actions	Norden (2008) #10 p. 48	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	place specific instructions and related actions together.	Nonpartisan voters in Los Angeles county, California were told to fill out an oval to indicate their party choice before voting in partisan contests. Failure to do so, votes cast for party contest will not count.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.1.5.10	with no correction guidance	fail to inform voters how to correct paper ballots	Norden (2008) #11 p. 54	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	include information of how to correct paper ballots if voters make mistakes	Lincoln county, Tennessee had a high residual vote rate compared to the state's residual vote rate for the 2002 Senate race. The ballots in Lincoln did not have instructions for voters who wished to correct their ballots if mistakes were made.
T	5.1.5.11	force least-objectionable choice	force least-objectionable candidate voting	VNOTA (2009)	operational	ballot preparation	votable ballot	lack of acceptable candidates running for office	system and information integrity-9, allow for 'none-of-the above' choices in contests	After incumbent governor Buddy Roemer finished 3rd in the general election, Louisiana voters were faced with a lesser-of-two-evils choice between Edwin Edwards, long dogged by allegations of corruption, and David Duke, the former Ku Klux Klan leader, in the 1991 gubernatorial run-off. Without a none-of-the-above choice, voters could either undervote or choose. Edwards won and eventually went to prison for racketeering.
T	5.1.5.12	publish invalid sample ballots	publish sample ballots different from actual ballots	Norden (2008) #13 p. 58	human-unintentional	ballot preparation	validate ballot style for ballot preparation	weak reviewing process of a ballot design	publish actual ballots that looks the same as the sample ballots	The actual ballot used on the election day in Sarasota county looked very different from the sample ballot. Almost all voters saw the confusing ballot layout for the first time when they were in the voting booth.
O	5.1.6	mishandle ballots	mishandle ballots		human-unintentional	voting system	ballots, voting	poor polllworker training, performance, lack of oversight	physical and environmental protection, media protection policy and procedures, personnel security, awareness and training, ballot accounting / reconciliation	
T	5.1.6.1	lose ballots by accident	unintentionally lose or misplace ballots, including close-polls filing errors		human-unintentional	voting, canvass	ballots	poor planning	awareness and training awareness and training,; personnel security personnel policies; audit and accountability audit and accountability; system and information integrity accuracy tests; planning	misplace a box of ballots before they are scanned during counting or recounting
T	5.1.6.2	abuse ballots by accident	unintentionally tamper with, mark, abuse ballots, including during close-polls operations		human-unintentional	voting system	ballots	poor pollworker performance; lack of oversight	physical and environmental protection, media protection policy and procedures, personnel security, awareness and training	
T	5.1.6.3	stuff, swap, or lose the ballot box	scan ballots more than once, by accident		human-unintentional, operational	voting, canvass	voting	poor planning	awareness and training awareness and training,; personnel security personnel policies; audit and accountability audit and accountability; system and information integrity accuracy tests; planning	
T	5.1.6.4	run out of ballots	run out of Votable Ballot stock		human-unintentional	ballot preparation, voting	votable ballot stock	poor planning; process whereby ballots must be preprinted	plan well and print plenty of ballots; fewer ballot styles; ballot on demand	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	5.2	make mistakes in ballot adjudication	make mistakes in ballot adjudication		human-unintentional	precinct closeout, canvass, state accumulation	canvass	human error; lack of oversight; low voter awareness	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	
T	5.2.1	incorrectly accept provisional ballots	incorrectly accept provisional ballots enclosed in envelopes with disqualifying information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #5	human-unintentional	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	lack of oversight; human error; lack of voter being informed; inability of voter to protest	pollworker training, labeling provisional ballots or other distinguishing them from other ballots, audit provisional ballot data	In King County, Washington in 2005, it was alleged that election officials were counting provisional ballots in parallel with absentee ballots, which could have resulted in accepting provisional ballots for voters who had already voted absentee
T	5.2.2	incorrectly reject provisional ballots	incorrectly reject provisional ballots in envelopes with fully compliant information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #6	human-unintentional, operational	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	fallibility of human judgment; misinterpretation of rules	training; auditing and logging	In a 2005 Washington governor's race, King County election officials admitted that 348 provisional ballots had been improperly counted before the voters' registration status could be determined.
T	5.2.3	reject ballots without retry	reject ballots for overvote, stray mark without retry; accidentally ignoring overvotes and undervotes shown by the scanner leading to rejection of votes	Jones(2005a) #33	human-unintentional, operational	voting, precinct closeout	feed attempt for PCOS scanner	failure to recognize the overvotes and undervotes by the scanner	add non-counting scanners to CCOS precincts; incident response Incident handling, incident response Incident reporting	John is an pollworker at a particular precinct. He is responsible for observing the ballots scanned through the scanner. He accidentally ignores them even when he should have been able to detect overvotes or undervotes
O	6	attack audit	render routine statistical audit ineffective	LTM-USA Delivery 01a	human-deliberate	voting system	election artifacts	no separation of duties; control by election officials over audit procedures, access to Election Artifacts	media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication	An ElectionOfficial with the help of some auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited ElectionArtifacts. Then proceed to publish the election results.
O	6.1	attack election evidence	election evidence includes ElectionArtifacts, such as ballots, BallotPreparation data and artifacts, relevant PollBooks, PhysicalVoteRecords, PollWorker logs, VotingMachine audit logs, voter feedback, VotingMachines themselves, etc.		human-deliberate	voting system	election artifacts	access to uncontrolled, accessible Election Artifacts	establish a chain of custody for all election artifacts used in audits; include separation of duties, access policies, audit logs, personnel policies, and media protections	
T	6.1.1	destroy ElectionArtifacts	physically destroy ElectionArtifacts, including electronic artifacts or electronic media, ballot destruction	Jones(2005) #6, Norden(2006) #9	human-deliberate	voting system	(deliver to jurisdiction)	poor security during Election Artifacts delivery	Implement chain of custody and strong physical security during delivery	An ElectionOfficial destroys Paper Tape RemovableMedia during delivery of the ElectionArtifacts to the central location.
T	6.1.2	mishandle ElectionArtifacts	swap, replace, hide, mislay, or mislabel ElectionArtifacts containing election evidence		human-deliberate	voting system	election artifacts	access to Election Artifacts	implementation chain of custody on election artifacts including media protection policies	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.1.3	add new fraudulent evidence	replace real VotableBallots with VotableBallots designed to match the electronic and audit in warehouse; results manipulation	Jones(2005) #421	human-deliberate	voting system	votable ballots	access to Votable Ballots	add more security features to the real VotableBallots to discourage attackers to duplicate VotableBallots, implement chain of custody and strong physical security	After the VotableBallots are printed, an insider who has access to the warehouse replaces the real VotableBallots with tampered VotableBallots.
O	6.1.4	modify ElectionArtifacts	modify pollbooks for audit; modify logbooks and log data used in audit		human-deliberate	voting, precinct closeout	check poll book for authenticate voter, pollworker logs for precinct closeout	lack of management oversight over PollWorker, election-official, auditor	audit monitoring, analysis, and reporting	John, a corrupted poll worker, has access to the poll book and authority to authenticate a voter. John alters the pollbooks so the number of eligible voters matches the number of CommittedBallots which includes fraud ballots.
A	6.1.4.1	modify deliberately	deliberately modify physical evidence		human-deliberate	voting, precinct closeout	election artifacts	access to Election Artifacts	implement strong physical security and chain of custody on election artifacts, including tamper resistant and tamper evident seals	
T	6.1.4.1.1	replace paper tape with fraud	results manipulation - change real Paper Tape with fraudulent Paper Tape	Jones (2005) #612 #62	human-deliberate	precinct closeout	(paper tape of machine totals printed), (removable memory card total generated), (paper tape totals of machine count reconciled to removable memory card total)	lack of management oversight over PollWorker and Observers	implement strong physical security and chain of custody; report the MachineCount and check the number of AcceptedBallots against the number of registered voters; conduct thorough background checks on PollWorkers, ElectionOfficials, and Observers	This attack assumes at least three participants in this attack. PollWorker A rewrites data on the memory card while PollWorker B replaces the Paper Tape with fraudulent tape to cover the tracks of the attack on the RemovableMedia. The Observer(s) are in cahoots with the corrupted Pollworkers in order to successfully execute the attack with little or no suspicion. Note: Machine Totals reflect the total on the memory card after the attack is performed.
T	6.1.4.1.2	rewrite data on Removable Media	rewrite data on RemovableMedia	Jones (2005) #6	human-deliberate	precinct closeout	(precinct data)	poor security during election artifacts delivery	implement chain of custody and strong physical security during delivery	A corrupted ElectionOfficial or an Outsider steals or destroys Paper Tape RemovableMedia during delivery of the ElectionArtifacts to the central location.
T	6.1.4.2	modify unintentionally	unintentionally damage physical or electronic evidence		human-deliberate	precinct closeout	election artifacts	fallibility of pollworkers and election officials with access to Election Artifacts	physical and environmental protection; personnel security, including sanctions against policy violators, awareness and training	
T	6.1.4.3	modify deliberately by computer	use a computer to modify electronic evidence; implement attack code or misconfiguration at voting terminal, and replace real CommittedBallots with fraudulent CommittedBallots	Jones(2005) #611	human-deliberate	precinct closeout	(voting) (deliver to jurisdiction)	lack of management oversight over PollWorkers during transit and limited physical security on CommittedBallots and voting machine	add more security features to the real CommittedBallots and implement chain of custody and strong physical security on voting terminal and CommittedBallots	This attack assume a at least two corrupted PollWorkers. PollWorker A injects malware into the voting terminal just before the election. After the election is over, PollWorker B replaces real CommittedBallots with fraudulent CommittedBallots.
T	6.1.4.4	modify unintentionally by computer	unintentionally modify evidence via computer operator error		human-unintentional	voting, precinct closeout	election artifacts	fallibility of pollworkers and election officials with access to Election Artifacts	personnel security, system and information integrity, awareness and training	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.1.4.5	modify via malware attack	modify electronic evidence using a computer infected with malware, and/or vulnerable to network-based attacks		human-deliberate	voting, precinct closeout	election artifacts	difficulty in detecting malware during computer use	personnel security, access control, audit and accountability, identification and authentication, system and communications protection	
T	6.1.4.6	modify via malware at artifact creation	modify electronic evidence at point of creation using infected voting equipment		human-deliberate	voting, precinct closeout	election artifacts	difficulty in detecting malware during computer use	personnel security, access control, audit and accountability, identification and authentication, system and communications protection	
O	6.2	improperly select audit samples	use improper methods of selecting the scope of audit		human-deliberate	election audit	election audit	difficulty in discovery	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	
T	6.2.1	select audit units before election	audit manipulation - select audited items dishonestly	Jones(2005) #612	human-deliberate	results of the tabulation process	(validate precinct results)	lack of basic audit in effect	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	
T	6.2.2	select non-randomly	use non-random selection methods		human-deliberate	precinct closeout	audit data	poor auditing practices or procedures; failure to follow procedures; lack of management oversight over auditing practices	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	break randomization pattern to leverage voting pattern of a precinct
T	6.2.3	use subverted selection method	use selection methods subject to outside influence (e.g., malware infected or attacked via network connection)		human-deliberate	election system, voting system	election artifacts	difficulty in detecting malware during computer use	access control, audit and accountability, identification and authentication, system and communications protection	a computer that is malware-infected, perhaps by network-connected, is used to select audit units, and does so in a manner that makes it less likely that the primary attack can be detected
T	6.2.4	ignore proper selections	ignore randomly sampled audit units and audit something else		human-deliberate	election audit	validate precinct results	susceptibility of audit process to discretion of election officials	personnel security, audit and accountability	An auditor ignores properly (randomly or scientifically) selected audit units and instead audits other units
O	6.3	use poor audit process	use poor auditing processes and procedures		human-deliberate	election audit	election audit, validate precinct results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	Inside attacker, an ElectionOfficial, institutes poor auditing practices which are unlikely to detect the primary threat; Note: election Auditors may or may not be willing co-conspirators in these attacks
T	6.3.1	misguide auditors	give improper instructions to Auditors to render audit ineffective, and avoid detecting subverted VotingMachines	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor policies allows Election Official to specify their own rules	revise policies to ensure that ElectionOfficial follows the guidelines for auditing process	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors thus resulting in undetected subverted VotingMachines. Note Auditors may or may not be in cahoots with the ElectionOfficial.
T	6.3.2	audit insufficient sample	audit manipulation - audit insufficient of sample to avoid tampered audit unit detected	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	An ElectionOfficial gives improper or unclear instructions to Auditors to audit insufficient data thus resulting in undetected tampered audit units.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.3.3	exploit variation in batch sizes	audit manipulation - random sampling from large variation of audit unit size minimize the risk of detection	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	An ElectionOfficial gives improper or unclear instructions to Auditors by creating a big variation in audit unit size so that tampered audit units will not likely be selected during sampling.
T	6.3.4	establish single contest audit rule	election law manipulation - select a race randomly - assume audit untampered race only	Jones(2005) #612; LTM-Deliverable	human-deliberate	election audit	validate precinct results	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	Get a law or regulation in place that says that only one randomly selected race will be audited and assume your race will not be audited.
T	6.3.5	arrange contest audit	arrange selection of a non-subverted contest for audit	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	In a state that allows (but does not require) the auditing of only one randomly selected race, a dishonest election official could change procedures and institute an audit that is very unlikely to detect fraud.
T	6.3.6	select audited items before commit	tabulation manipulation - clean up data automatically based on operator	Jones(2005) #612	human-deliberate	election audit, accumulate totals	vote tabulating machine, election artifacts	lack of tabulation server security	increase security features of tabulators	An ElectionOfficial with the help of some Auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited items. Then proceed to publish the election results.
T	6.3.7	tamper with audit totals	corrupt precinct-level data but not the machine-level data; election results manipulation - precinct total do not add up to machine totals	Jones(2005) #612 Norden(2006) #3	human-deliberate	accumulate totals	(precinct accumulation), (vote tabulating machine), (precinct audit data), (machine accumulation),	poor auditing practices or procedures	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	An ElectionOfficial releases precinct-level data that reflects the fraudulent results without tampering the MachineCount. Thus, the precinct total does not tally with the machine total, which can be published in a way (across hundreds of pages of paper) that is difficult for anyone to count quickly
T	6.3.8	avoid correction	when audits reveal mismatches, avoid calling for a recount or other corrective measures by making excuses; election results manipulation - give reasons for mismatch - avoid recount, examining voting terminals, and fraud audit items detection	Jones(2005) #612	human-deliberate	accumulate totals	(validate jurisdiction results)	poor election laws / policies / guidelines	implement a policy that requires ElectionOfficial to give non-obscure reasons for result discrepancies and take corrective measures to avoid fraud	During the validation of the Jurisdiction results, a mismatch was found. The corrupted ElectionOfficial tries to offer obscure reasons to hide the actual attack.
T	6.3.9	overwhelm audit observers	overwhelm observers with too many auditors - auditor manipulation - incompetent Auditors ballot manipulation - dishonest audit	Jones(2005) #5,#6	human-deliberate	accumulate totals	(validate precinct results)	lack of management oversight over Election Officials and Auditors	implement a policy that specifies only certain number of Auditors can be employed so that Observers can perform their duty efficiently	An ElectionOfficial hires as many incompetent or corrupt Auditors as possible knowing that an Observer can only monitor a limited number of Auditors at a time.
T	6.4	commit auditing error	human errors in following correct audit procedures, or overlooking errors	Jones(2005) #6	human-unintentional insider	election audit	ballot box accounting, machine accumulation	Election Official has limited knowledge on discrepancies issues	personnel security, including personnel sanctions; awareness and training: auditor training; Provide training or courses to equip ElectionOfficial with up-to-date knowledge on election materials, or hire experienced ElectionOfficial	An ElectionOfficial was recently hired to run the PollingPlace at a local Precinct. His experience as ElectionOfficial is somewhat limited as he has just begun his job not too long ago. After the election is over, he was being informed that the totals from the paper and electronic do not match. Because of his lack of experience, he misanalyzes and offers ambiguous reasons for discrepancies.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.5	compromise auditors	suborn (bribe, threaten) auditors to intentionally misreport or suppress discrepancies between election results and audit results		human-deliberate	election audit	auditors	willingness of auditors to be bribed or coerced	personnel security, including sanctions against violators	
O	6.6	attack audit results	attack audit-related computing process and electronic data representing audit results		human-deliberate	election audit	election audit	lack of control over audit results	physical and environmental protection, media protection policy and procedures	
T	6.6.1	mishandle media	swap, replace, hide, mislay, or mislabel media containing audit data; e.g. poll worker or election-official incorrectly labels batch of audit data		human-deliberate, human-unintentional	precinct closeout	precinct audit data for precinct closeout	unintentional - vulnerability to human error due to carelessness; intentional - mislabel batch to cover fraud from being detected	audit monitoring, analysis, and reporting	John, a newly hired poll worker, is responsible for labeling batches of audit data. Unfortunately, he mislabeled one of the batches due to his inexperience.
T	6.6.2	add fraudulent result data	use illegal voting terminal to add tampered votes; inject fake votes to a back-end tabulating authority by impersonating a legitimate voting terminal	Kohno (2008)	human-deliberate	voting	voting machines	poor physical and network security on voting terminals	increase physical and network security;	Just a day before the poll was open for election, John the election official and a few corrupted poll workers switched the certified voting machines with illegal voting machine so they could insert votes to the back-end of the tabulating authority.
O	6.6.3	attack audit data	poll worker changes audit data		human-deliberate	precinct closeout	precinct audit data for precinct closeout	lack of management oversight over PollWorker, election-official, auditor	audit monitoring, analysis, and reporting	Jane, a corrupted election-official, has access to audit data and modifies it during delivery to the jurisdiction.
T	6.6.3.1	modify deliberately	deliberately modify audit data		human-deliberate	precinct closeout	election artifacts	lack of management oversight over PollWorker, election-official, auditor	establish a chain of custody on all election artifacts, including personnel security, physical and environmental protection, media protection policy and procedures	
T	6.6.3.2	modify unintentionally	modify audit data via operator error		human-unintentional	precinct closeout	election artifacts	lack of management oversight over PollWorker, election-official, auditor	establish a chain of custody on all election artifacts, including personnel security, physical and environmental protection, media protection policy and procedures	
T	6.6.3.3	modify via malware attack	install malware in auditing device through physical access or network access; voting system manipulation - install malware to tamper results	Jones(2005) # 612 Norden(2006) #2,#3	human-deliberate	voting system	/ (ballot box accounting), (machine accumulation)	corrupt officials using unsecured and non-certified voting system or custom device as audit device	use only certified voting system or secured custom device and implement a policy that requires ElectionOfficials to reconcile totals from HandCount and ManualCount	An ElectionOfficial avoids manual audit by giving excuses (such as MachineCount is more accurate than HandCount), and instructs Auditors to use Totals from the MachineCount.
T	6.6.4	publish bogus audit results	penetrate jurisdiction web site and publish bogus audit results to hide attack	Jones(2005) #62	human-deliberate	canvass	(canvass), (official report), (report results)	lack of publishing system security that leads to obscure results	increase security in both areas - tabulator and publication website	An outsider penetrates into the jurisdiction website and changes the audit results of the election.
O	7	disrupt operations	disrupt operations		human-deliberate, natural, environmental	election system, voting system	voting machines, polling place, voting	exposure to natural or environmental events, fragility of computer equipment, susceptibility of voters to threats and intimidation	disaster planning, contingency planning, physical and environmental protection, incident response, and personnel security	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	7.1	disruption from natural events	voting system failures attributable to natural events	Rackleff 2007	natural	election system, voting system	voting machines, polling place, voting	exposure to natural events	disaster recovery planning; physical and environmental protection policies, incident response with coordination among government entities	
T	7.1.1	natural disaster	polling place hit by tornado, hurricane, tsunami, flood, earthquake, landslide, wildfire, lightening, strike, etc	Rackleff 2007	natural	voting system, election system	voting machines, polling places, displaced voters	exposure to natural or accidental events	disaster recovery planning; hurricane and flood protection; contingency planning; incident response with coordination among government entities	Hurricane Katrina destroyed voting equipment and polling places, displaced voters, and caused elections to be postponed; many of the displaced voters were difficult to find even after basic utilities were restored
T	7.1.2	severe weather	polling place access impaired by severe weather conditions and side effects such as public transportation closure		natural	voting	voting machines, polling place	exposure to severe weather events	contingency planning, such as use of alternate polling places or voting methods	a severe weather threat, including a tornado watch, was forecast for Super Tuesday in 2008; severe weather could have caused power outages or otherwise negatively impacted turnout in several states, including Alabama and Tennessee
O	7.2	disruption from environmental events	disruption from environmental events		environmental	voting	voting machines, polling place	exposure to environment events	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
O	7.2.1	environmental failures	polling place facilities failures including power failure, electrical fire, kitchen fire, burst water pipes		environmental	election system, voting system	voting machines, polling place	exposure to environment events; dependency on power sources	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
T	7.2.1.1	experience a fire	experience a fire that affects the availability of or effective operation of the polling place	Potts (2008)	environmental	voting	voting machines, polling places	exposure to natural or accidental events	All electrical wiring	An election eve fire adjacent to a small Pennsylvania town's only polling place caused a power outage and forced election officials to move the polling place in the middle of the night. Makeshift signs throughout town redirected voters to a new polling place for the November 4, 2008 election. The effect on voter turnout was unknown. (Potts, 2008)
T	7.2.1.2	experience power disruptions	experience unintended power disruptions		environmental	voting	voting machines, rooms needing lighting	lack of control over utility providers	Electric power supply department should be notified and they should insure uninterrupted power supply to the polling place. They should be ready for the emergency services. Alterative arrangements like generators can also be made to run the electronic equipments.	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	7.2.1.3	experience effects of humidity	experience effects of humidity on ballots, including ink bleeding and ballots expanding		environmental	voting system	votable ballots, marked ballots	exposure to humid environments	Marked ballots that have been stored in a high humidity (>90%) environment, and with ink that tends to bleed, are retrieved for recounting, and result in a different result because of bleeding being reinterpreted as stray marks	
T	7.2.2	hazardous accidents	polling place access impaired by nearby hazards including chemical spill, power wire fall, gas main explosion		environmental	election system, voting system	voting machines, polling place, pollworkers, voters	exposure to environment events; exposure to danger	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
O	7.3	disruption from human-created events	disruption from human-created events		human-deliberate, human-unintentional	election system, voting system	voting machine	fragility of computer equipment, mishandling	planning; physical and environmental protection, access control	
O	7.3.1	that damage equipment	directly damage electronic voting equipment	Jones (2005a) #231	human-deliberate, human-unintentional	election system, voting system	voting machine	fragility of computer equipment, mishandling	planning: pollworker rules of behavior, physical and environmental protection: physical access control and monitoring physical access	a voter wearing golf spikes steps on a power strip
T	7.3.1.1	render e-voting equipment inoperable	render electronic voting equipment inoperable		human-deliberate, human-unintentional	election system, voting system	voting machine	fragility of computer equipment, mishandling	physical and environmental protection, access control	
T	7.3.1.2	render removable media not working	render removable media not working		human-deliberate, human-unintentional	election system, voting system	voting machine	fragility of computer equipment, mishandling	physical and environmental protection, access control, media protection policy and procedures; chain of custody of media	
T	7.3.1.3	render paper sensor inoperable	during transportation, the rolls became loose and so the machine registered that it was out of paper when it was not - an attacker could intentionally tamper with rolls in transit or when loading the paper and delay opening of the polls		human-deliberate, human-unintentional, technical	election system, voting system	one voter	Physical attributes of thermal paper roll	physical and environmental protection: physical access control and monitoring physical access; VotingMachine chain of custody procedures	
T	7.3.2	deploy faulty equipment	intentionally or unintentionally deploy faulty voting equipment		human deliberate, human unintentional, technical	election system, voting system	voting machine	poor process of testing and deploying equipment; difficulty in detecting faulty machines	VotingMachine chain of custody procedures; logic and accuracy testing	
T	7.3.3	with environmental effects	intentionally create environmental events to affect voting equipment or polling place operation		human-deliberate	election system, voting system	voting system	exposure to events	physical and environmental protection	
O	7.4	discourage voter participation	discourage voter participation		human-deliberate	election system, voting system	voter	susceptibility of voters to violence, intimidation, fear	awareness and training, planning, contingency planning, incident response, physical and environmental protection	
T	7.4.1	misinform voters	misinformation about polling places or transportation		human-deliberate	election system, voting system	voter	lack of voter awareness of false information	awareness and training: voter education, utilize new media to counteract misinformation campaign	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	7.4.2	threaten personal violence	threaten personal violence, such as in blackmailing a voter to be a no-show or to vote for attacker's candidate; attacker focuses on a particular voter threatens him to vote against his will	Van Acker	human-deliberate	election system, voting system	eligible voter	susceptibility of voters to intimidation; lack of voter privacy	planning, strengthen laws against such crimes; physical and environmental security; voter privacy	a type of voter suppression that involves deliberate acts to cause fear in EligibleVoters, thus deterring them from coming out to vote.
T	7.4.3	threaten mass violence	violence to prevent voting, (i.e., bomb scare, mail contamination scare (do not open mail), perhaps even targeting areas (by zip code)	Foxnews.com (2005)	human-deliberate	election system, voting system	voters	voters' fear for their safety	contingency planning contingency planning, incident response incident response, physical and environmental protection physical and environmental protection	In January, 2005, an Australian polling station for Iraqi exiles voting in their homeland's historic first post-Sadaam election was closed for an hour after a riot broke out and a suspicious bag prompted a bomb scare. The overall turnout was affected, it was thought. Many of Australia's estimated 80,000 Iraqis declined to register for the election, fearing their votes would make relatives in Iraq terrorist targets.
T	7.4.4	commit an act of terror	commit an act of terror		human-deliberate	election system, voting system	voters, election officials, voting equipment	exposure to terrorist acts of violence	physical and environmental protection: arms and ammunitions should not be allowed in the polling area. Unclaimed items should be continuously checked. Regular police patrolling required.	
T	7.4.5	intimidate to suppress turnout	coerce the voter to stay away from polls with threats and intimidation	Van Acker	human-deliberate	election system, voting system	eligible voter	susceptibility of voters to intimidation; lack of voter privacy	awareness and training, strengthen the election law against such crimes	‘Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future.’ (Fund 2004)

4 Central Count Optical Scan

In this tree, we consider threats to voting systems that employ marks sense technology to scan and count committed ballots recorded on a physical medium, such as pre-printed paper ballots. Central-count optical scan (CCOS) is similar to precinct-count optical scan (PCOS) in that physical (paper) ballots are used by voters to cast votes at polling places. In CCOS, marked ballots are committed by being placed in a ballot box at the polling place and are transported to one or more central locations for counting. In contrast, PCOS counting takes place at the precinct and the results are transmitted to the central location; the process of creating control totals at the precinct level provides an additional artifact for auditing which does not exist in CCOS. Additionally, counting all of the ballots a one central location creates the potential for a single point of failure.

From a risk assessment standpoint, there are many similarities between CCOS and PCOS. CCOS has threats associated with the use of computer-based technology, polling places, and paper ballots. The key technologies considered are the CCOS scanning machines that tabulate as well and ballot creation software. The scanning technology used might in some cases be the same type of scanners used in a PCOS system, but often they are larger, faster scanners that can scan a batch of ballots at a time, rather than a single feed at a time. We consider threats that occur at polling places and at central operations, with the different being that the committed ballots are transported and then counted centrally. There are additional threats during transport, and there is another difference: voters do not have the capability to have undervotes and overvotes detected. This voting system includes physical (paper) ballots, and the provisional ballot process is considered as well.

4.1 CCOS Threat Tree

node type - outline number - threat action

O	1	attack voting equipment
A	1.1	attack CCOS scanner
O	1.1.1	gather technical knowledge
T	1.1.1.1	hire existing vendor or testing lab insider
T	1.1.1.2	gain employment as vendor or lab insider
T	1.1.1.3	obtain equipment and reverse engineer
T	1.1.1.4	study a machine in transit
T	1.1.1.5	acquire equipment legally
T	1.1.1.6	find source code
T	1.1.1.7	compromise existing source code escrow
O	1.1.2	avoid detection during inspection
T	1.1.2.1	insert in COTS code
T	1.1.2.2	insert at warehouse
T	1.1.2.3	employ existing vulnerabilities
T	1.1.2.4	employ feature such as total reset card
T	1.1.2.5	insert via viral infestation
T	1.1.2.6	write subtle security flaw in system
O	1.1.3	avoid detection during testing
T	1.1.3.1	supply cryptic knock during testing
T	1.1.3.2	supply cryptic knock during setup
T	1.1.3.3	supply cryptic knock during voting
T	1.1.3.4	disable fraud behavior with using team anti-knock
T	1.1.3.5	use AC power flicker as knock
T	1.1.3.6	detect realistic patterns of voting
T	1.1.3.7	employ calendar/clock method
T	1.1.3.8	obtain cooperation of testers

```
            T   1.1.3.9  deploy cryptic knock in ballot definition files
            T   1.1.3.10 acquire detailed knowledge of testing procedures and scripts
        O   1.1.4   develop and insert malware or misconfiguration
            T   1.1.4.1  modify equipment through supply chain
            T   1.1.4.2  modify configuration file to change votes
            T   1.1.4.3  miscalibrate equipment
            T   1.1.4.4  tamper with ballot creation software
            T   1.1.4.5  tamper with the ballot definition file on scanner
            T   1.1.4.6  inject malicious code
            T   1.1.4.7  change mark sensing threshold of scanner
            T   1.1.4.8  modify basic functionality via replaceable media
            O   1.1.4.9  perform computer-based attacks using ballots
                T   1.1.4.9.1  insert defective ballots into stock
                T   1.1.4.9.2  create substitute ballots to attack ballot rotation
                A   1.1.4.9.3  tamper with ballot design selectively
                    T   1.1.4.9.3.1   select precincts by expected voting pattern
                    T   1.1.4.9.3.2   change font sizes and colors on ballots
                T   1.1.4.9.4  substitute ineffective ballot marking device
                T   1.1.4.9.5  pre-mark ballot using machine readable invisible ink
                T   1.1.4.9.6  pre-mark ballot with subtle visible marks
                T   1.1.4.9.7  perform CCOS overvote/undervote attack
            T   1.1.4.10 jam/interfere with headphone communication
            T   1.1.4.11 create a false close sheet
        O   1.1.5   control/parameterize attack
            T   1.1.5.1  enable attack via a knowing voter
            T   1.1.5.2  enable attack via an unknowing voter
            T   1.1.5.3  enable attack via a technical consultant
            T   1.1.5.4  employ unparameterized attack
            T   1.1.5.5  add steganographic commands to ballot definition file
            T   1.1.5.6  attack wireless communication
        O   1.1.6   adjust recorded data
            T   1.1.6.1  pre-load ballot box with negative and positive votes
            T   1.1.6.2  alter votes at vote time
            T   1.1.6.3  alter vote after vote time but before or at poll closing time
            A   1.1.6.4  add or remove votes
                T   1.1.6.4.1  add or remove CommittedBallots
                T   1.1.6.4.2  defeat BallotBox seals
        T   1.1.7   render routine statistical audit ineffective
O   2   attack with voter impersonation
    A   2.1   impersonate EligibleVoters (simple)
        T   2.1.1   determine number of votes to target
        T   2.1.2   recruit impersonating attackers
        T   2.1.3   select target polling places
        T   2.1.4   create lists of unlikely voters
        T   2.1.5   supply attackers with information about unlikely voters
        T   2.1.6   cast vote as impersonator
    A   2.2   impersonate EligibleVoters (housemate)
        T   2.2.1   determine number of votes to target
        T   2.2.2   recruit sufficient impersonator attackers among loyal followers
        T   2.2.3   select target polling places
        T   2.2.4   each recruit registers out-of-state voters as if they were housemates
        T   2.2.5   attacker has friends vote for the fake housemates
    A   2.3   impersonate EligibleVoters (complex)
```

```
        T   2.3.1   determine number of votes to target
        T   2.3.2   select target polling places
        T   2.3.3   recruit cell captains
        T   2.3.4   educate and motivate cell captains in deniable ways
        T   2.3.5   cell captains recruit impersonating attackers
        T   2.3.6   cell captains create lists of unlikely voters
        T   2.3.7   cell captains supply attackers with information about unlikely voters
        T   2.3.8   cell captains provides all required rewards out of own pocket
        T   2.3.9   impersonators cast votes
A   3   attack with insider access
    O   3.1   subvert separation of duties
        T   3.1.1   staff polling place with attackers
        T   3.1.2   allow rotation of pollworker roles
        T   3.1.3   collude with one or a few other insiders
        T   3.1.4   execute attack as a lone insider
    O   3.2   execute insider attack
        A   3.2.1   perform insider attack at polling place
            O   3.2.1.1   discourage voters from casting ballots
                O   3.2.1.1.1   challenge voters during CheckIn
                    T   3.2.1.1.1.1   falsely reject voter as not registered
                    T   3.2.1.1.1.2   falsely reject voter on identification check
                    T   3.2.1.1.1.3   selectively challenge voters
                    T   3.2.1.1.1.4   falsely record voters as having voted
                    T   3.2.1.1.1.5   creating and use a caging list
                    T   3.2.1.1.1.6   destroy some of the registered cards
                T   3.2.1.1.2   delay opening or close
                O   3.2.1.1.3   create long lines
                    T   3.2.1.1.3.1   stymie voters by intentionally working slowly
                    T   3.2.1.1.3.2   stymie voters by reducing resources
                T   3.2.1.1.4   intentionally stymie voters needing assistance
                T   3.2.1.1.5   mislead voters with phony last-minute ballot change
                T   3.2.1.1.6   mislead voters by announcing that only one party is allowed to vote
                T   3.2.1.1.7   discourage provisional voting
                T   3.2.1.1.8   impede voter access to physical polling place
                T   3.2.1.1.9   fraudulently redirect voters alternate polling place
            A   3.2.1.2   cast votes fraudulently in polling place
                A   3.2.1.2.1   cast fraudulently votes for no-show voters
                    T   3.2.1.2.1.1   create list of unlikely voters
                    T   3.2.1.2.1.2   add no-show voters to pollbook
                    T   3.2.1.2.1.3   commit tampered ballot
                A   3.2.1.2.2   cast fraudulently votes using improperly accessed ballots
                    A   3.2.1.2.2.1   obtain access to MarkedBallot
                        T   3.2.1.2.2.1.1   collect ballots from legitimate voters
                        T   3.2.1.2.2.1.2   tamper with ballots before they are scanned
                A   3.2.1.2.3   cast fraudulently votes using provisional ballots
                    T   3.2.1.2.3.1   compel voter to vote provisional ballot
                    T   3.2.1.2.3.2   tamper with provisional ballots
                T   3.2.1.2.4   fraudulently cast votes of voters needing assistance
        O   3.2.2   perform insider attack at other than polling place
            T   3.2.2.1   subvert ballot decision criteria
            O   3.2.2.2   stuff ballot box after the polls close
                T   3.2.2.2.1   inject ballot box (of physical ballots) during canvass or recount
                T   3.2.2.2.2   manipulate duplicate ballots
```

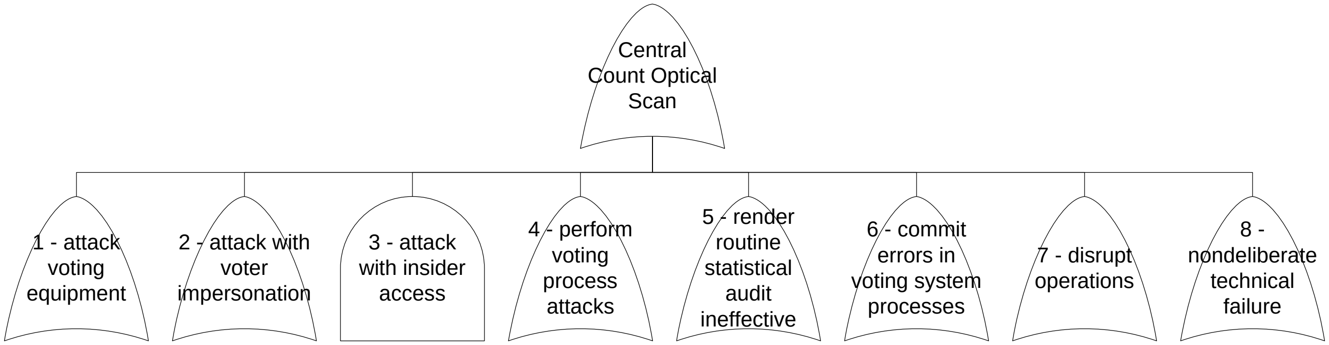
      - O 3.2.2.3 alter or destroy ballots
        - T 3.2.2.3.1 discard or destroy a box of MarkedBallots
        - T 3.2.2.3.2 add, delete, or change ballots during transport
        - T 3.2.2.3.3 tamper with provisional ballot envelope to cause rejection
        - O 3.2.2.3.4 alter ballots
          - T 3.2.2.3.4.1 exploit undervotes or create overvotes
          - T 3.2.2.3.4.2 obscure valid mark on ballot
        - T 3.2.2.3.5 damage ballots
      - O 3.2.2.4 attack results of tabulation process
        - T 3.2.2.4.1 falsely announce tabulation results

- O 4 perform voting process attacks
  - A 4.1 perform chain voting scheme
    - T 4.1.1 gathers sufficient subvertible voters
    - T 4.1.2 entice, persuade, or coerce subvertible voters
    - T 4.1.3 obtain VotableBallot
    - T 4.1.4 vote using premarked ballot
    - T 4.1.5 remove VotableBallot
  - A 4.2 purchase votes
    - O 4.2.1 make purchase
      - T 4.2.1.1 make a direct cash payment
      - T 4.2.1.2 make a non-cash payment
      - T 4.2.1.3 recruit brokers to purchase votes
    - O 4.2.2 verify compliance
      - T 4.2.2.1 self-record during ballot casting
      - T 4.2.2.2 assist voter during vote casting
      - T 4.2.2.3 use stray ballot mark for attribution
  - O 4.3 persuade or coerce voters
    - T 4.3.1 persuade or coerce voters to make selections
    - T 4.3.2 persuade or coerce voters to stay away from polls
  - O 4.4 cast multiple votes
    - T 4.4.1 cast votes via multiple methods
    - T 4.4.2 cast votes in multiple locations
    - T 4.4.3 insert unauthorized ballots into ballot box
  - T 4.5 leverage electoral college design to target attack locations
  - T 4.6 damage electronic voting equipment
- O 5 render routine statistical audit ineffective
  - O 5.1 manipulate audit process
    - T 5.1.1 ignore actual random numbers
    - T 5.1.2 manipulate random number selection
  - T 5.2 alter results by publishing results obscurely
  - T 5.3 substitute fraudulent VotableBallots
  - T 5.4 implement attack code or misconfiguration and substitute fraudulent CommittedBallots
  - T 5.5 instruct auditors fraudulently
  - O 5.6 institute poor auditing practices
    - T 5.6.1 audit insufficient sample
    - T 5.6.2 alter audit unit size
    - T 5.6.3 assume tampered race will not be audited
    - T 5.6.4 manipulate contest audit selection
    - T 5.6.5 manipulate results in unaudited locations or contests
    - T 5.6.6 publish fraudulent results
    - T 5.6.7 offer obscure excuses for audit mismatches
    - T 5.6.8 install malware in auditing device
    - T 5.6.9 impede audit observation with large number of audit teams

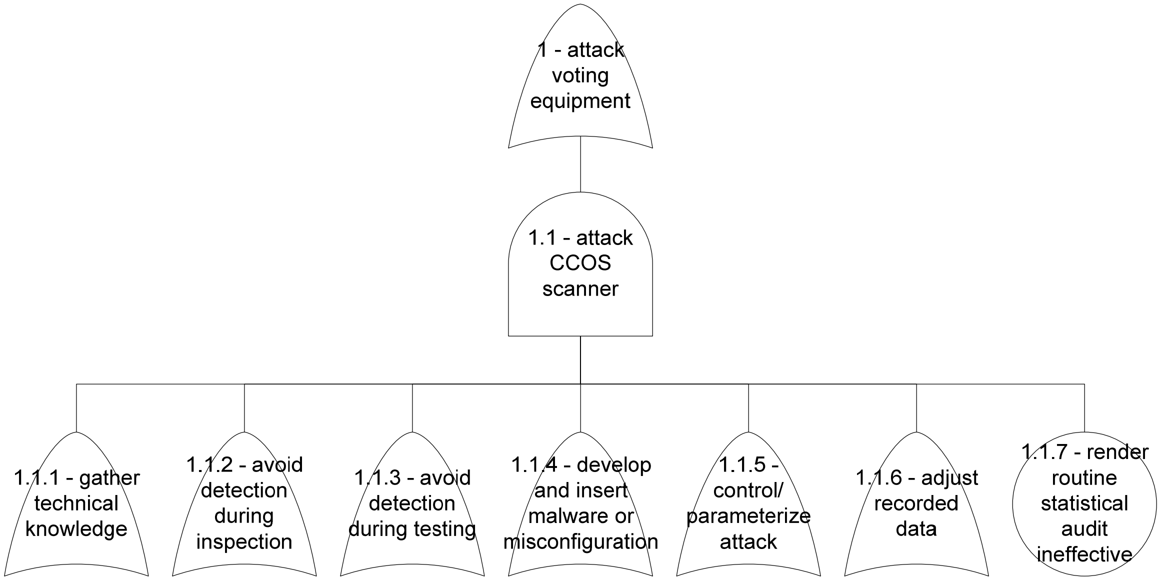
  - T 5.7 misanalyze discrepancies between electronic and paper results
  - T 5.8 destroy CommittedBallots with chemicals
  - T 5.9 substitute fraudulent Paper Tape or rewrite data on RemovableMedia
  - T 5.1 substitute fraudulent Paper Tape and rewrite data on RemovableMedia
  - T 5.11 destroy Paper Tape or RemovableMedia
  - T 5.12 modify pollbooks for audit
  - T 5.13 modify logbooks and log data used in audit
  - T 5.14 attack audit data
  - T 5.15 mislabel batch of audit data
  - T 5.16 manipulate precinct audit selection
- O 6 commit errors in voting system processes
  - T 6.1 experience calibration or date and time setting failures
  - O 6.2 unintentionally discourage the voter from voting
    - T 6.2.1 mistakenly challenge voters during CheckIn
    - T 6.2.2 delay opening or closing polls due to mistakes or slow working
    - T 6.2.3 create long lines by working too slowly
    - T 6.2.4 delay voters by failing to properly assist
    - T 6.2.5 discourage provisional voting by working slowly or incompetently
  - T 6.3 issue marking device incompatible with scanner
  - T 6.4 unintentionally lose voter's vote
  - T 6.5 unintentionally stuff the ballot box
  - O 6.6 confuse voters with poor ballot design
    - T 6.6.1 split candidates for the same office onto different pages or columns
    - T 6.6.2 place response options on both sides of candidate names
    - T 6.6.3 use “complete-the-arrow” instead of “fill-the-oval” response options
    - T 6.6.4 leave columns or rows for disqualified candidates
    - T 6.6.5 inconsistently design ballots in formatting and style
    - T 6.6.6 omit shading to help voters differentiate between voting tasks
    - T 6.6.7 omit bold text to help voters differentiate between voting tasks
    - T 6.6.8 fail to write short, simple instructions
    - T 6.6.9 place Instructions far from related actions
    - T 6.6.10 publish sample ballots different from actual ballots
    - T 6.6.11 fail to inform voters how to correct paper ballots
    - T 6.6.12 force least-objectionable candidate voting
  - O 6.7 make counting (tabulation) errors
    - T 6.7.1 incorrectly accept or reject provisional ballots
    - T 6.7.2 disallow legitimate ballots
    - T 6.7.3 challenge the authenticity of legitimate ballots
    - T 6.7.4 fail to correctly count straight-party voting
    - T 6.7.5 fail to catch machine tabulation error due to excessive variance requirement
  - T 6.8 undervotes and overvotes without warning are allowed
  - T 6.9 input erroneous precinct label on memory card
- O 7 disrupt operations
  - O 7.1 experience failure due to natural events
    - T 7.1.1 flooding at the polling place
    - T 7.1.2 major hurricane
    - T 7.1.3 tornado
    - T 7.1.4 snow storm
    - T 7.1.5 landslide
    - T 7.1.6 earthquake
    - T 7.1.7 tsunami
    - T 7.1.8 lightning strike
    - T 7.1.9 wildfire

  - O 7.2 experience a failure due to environmental events
    - T 7.2.1 fire
    - T 7.2.2 power disruptions
    - T 7.2.3 chemical spill
  - O 7.3 discourage voter participation
    - T 7.3.1 misinform voters
    - T 7.3.2 threaten personal violence
    - T 7.3.3 threaten mass violence
    - T 7.3.4 commit an act of terror
    - T 7.3.5 intimidate to suppress turnout
- O 8 nondeliberate technical failure
  - T 8.1 submit incorrect machine count of ballots
  - T 8.2 calculate machine count of vote total incorrectly
  - T 8.3 mechanical malfunction in the creation of the paper record
  - T 8.4 failure of optical scanners
  - T 8.5 failure of the memory card to store votes
  - T 8.6 faulty ballot creation software

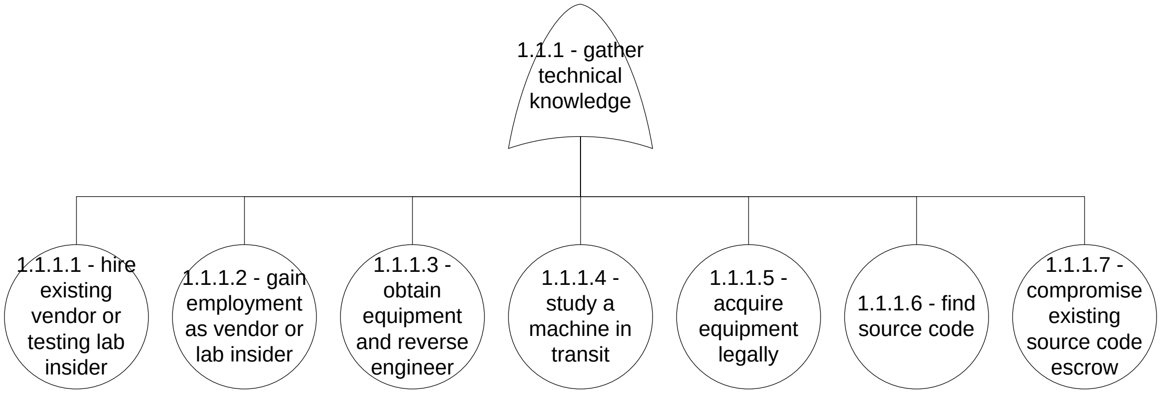
4.2 CCOS Threat Tree – Graphic


Central Count Optical Scan
1 - attack voting equipment
2 - attack with voter impersonation
3 - attack with insider access
4 - perform voting process attacks
5 - render routine statistical audit ineffective
6 - commit errors in voting system processes
7 - disrupt operations
8 - nondeliberate technical failure

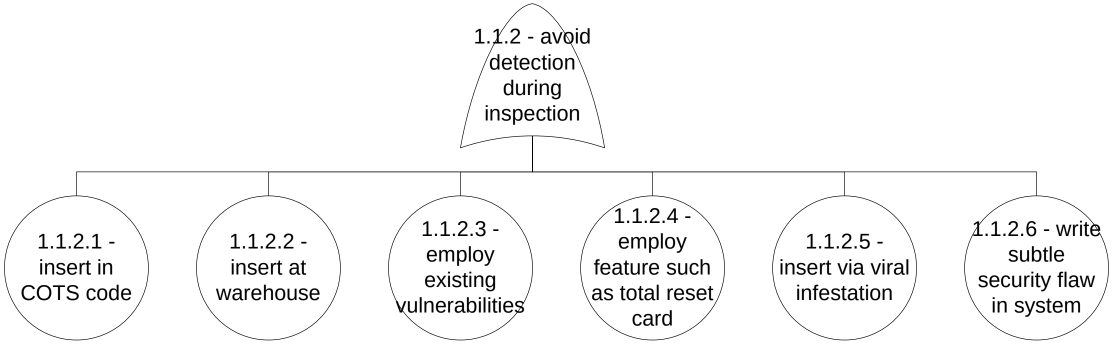
4-1 CCOS Overview


1 - attack voting equipment
1.1 - attack CCOS scanner
1.1.1 - gather technical knowledge
1.1.2 - avoid detection during inspection
1.1.3 - avoid detection during testing
1.1.4 - develop and insert malware or misconfiguration
1.1.5 - control/ parameterize attack
1.1.6 - adjust recorded data
1.1.7 - render routine statistical audit ineffective

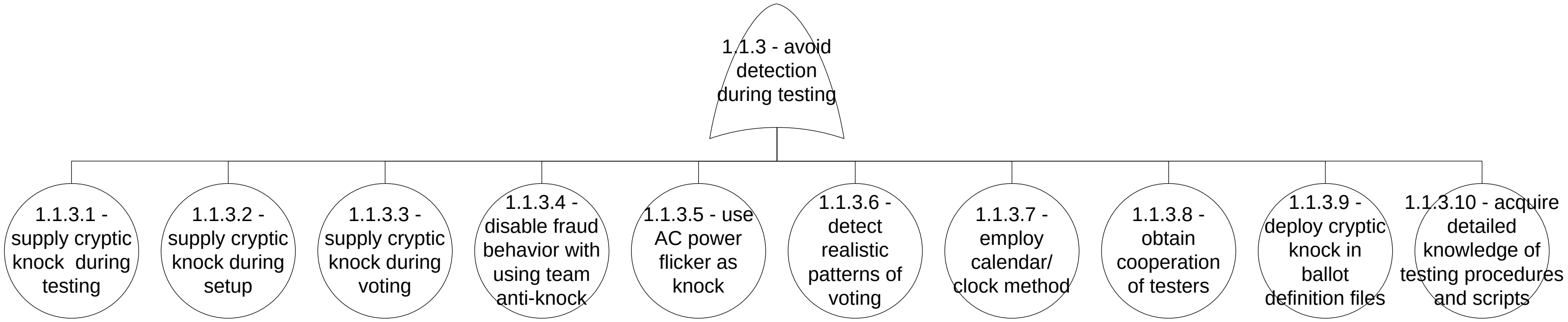
4-2 CCOS Attack Voting Equipment


1.1.1 - gather technical knowledge
1.1.1.1 - hire existing vendor or testing lab insider
1.1.1.2 - gain employment as vendor or lab insider
1.1.1.3 - obtain equipment and reverse engineer
1.1.1.4 - study a machine in transit
1.1.1.5 - acquire equipment legally
1.1.1.6 - find source code
1.1.1.7 - compromise existing source code escrow

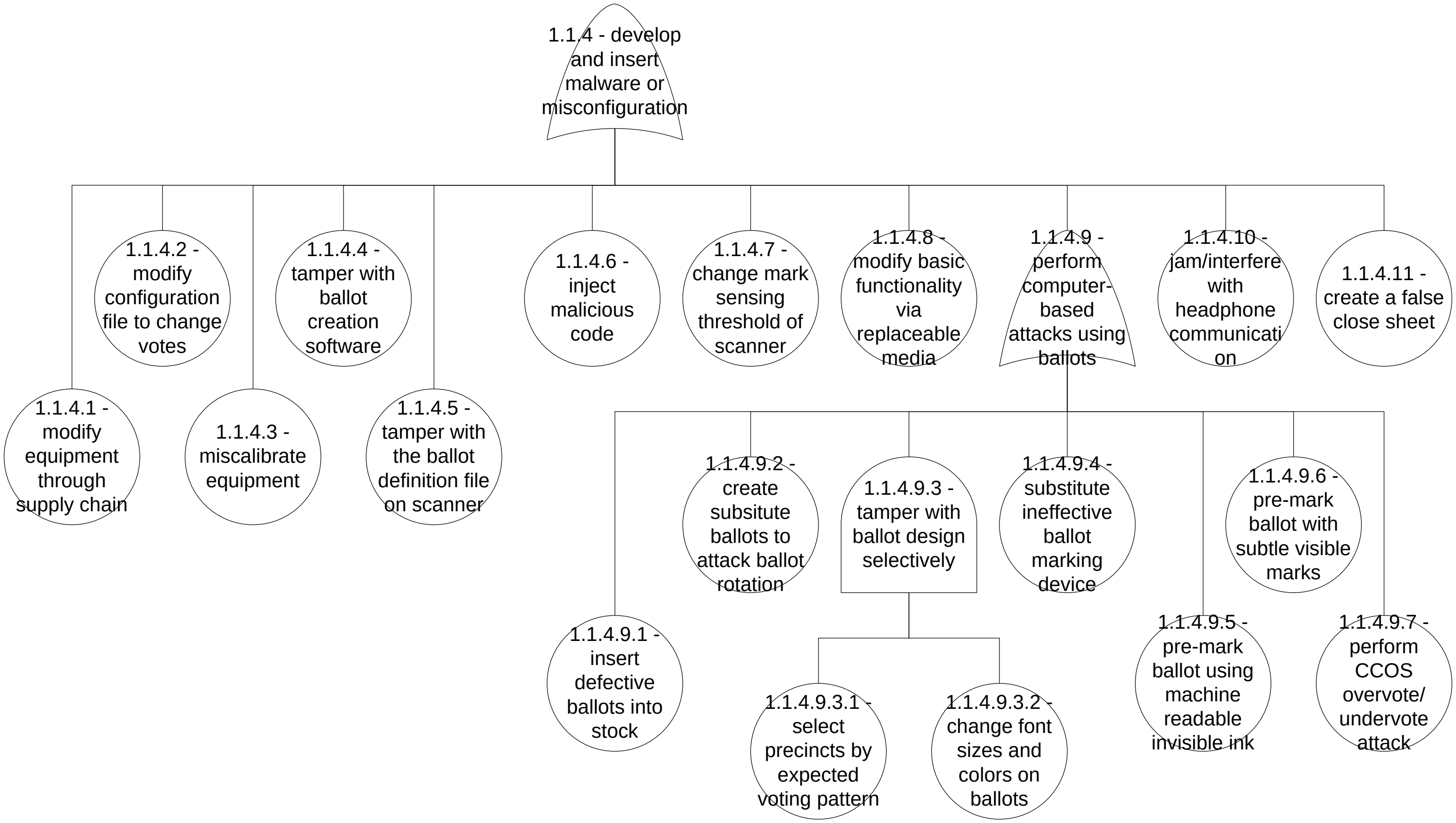
4-3 CCOS Gather Technical Knowledge


1.1.2 - avoid detection during inspection
1.1.2.1 - insert in COTS code
1.1.2.2 - insert at warehouse
1.1.2.3 - employ existing vulnerabilities
1.1.2.4 - employ feature such as total reset card
1.1.2.5 - insert via viral infestation
1.1.2.6 - write subtle security flaw in system

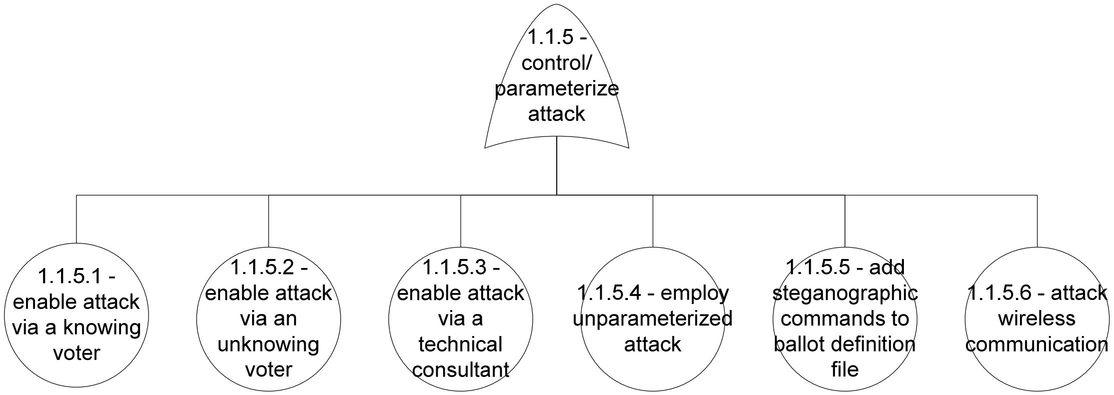
4-4 CCOS Avoid Detection During Inspection


1.1.3 - avoid detection during testing
1.1.3.1 - supply cryptic knock during testing
1.1.3.2 - supply cryptic knock during setup
1.1.3.3 - supply cryptic knock during voting
1.1.3.4 - disable fraud behavior with using team anti-knock
1.1.3.5 - use AC power flicker as knock
1.1.3.6 - detect realistic patterns of voting
1.1.3.7 - employ calendar/ clock method
1.1.3.8 - obtain cooperation of testers
1.1.3.9 - deploy cryptic knock in ballot definition files
1.1.3.10 - acquire detailed knowledge of testing procedures and scripts

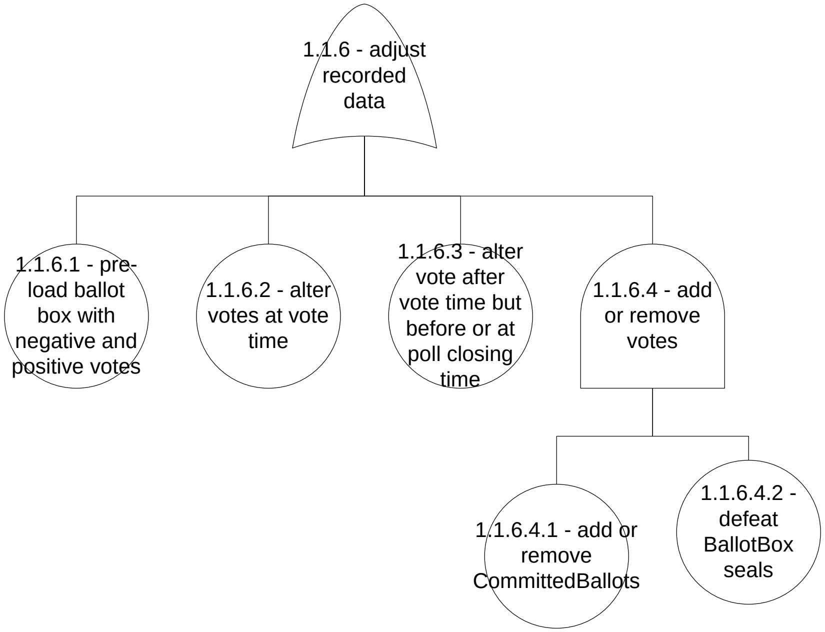
4-5 CCOS Overview


1.1.4 - develop and insert malware or misconfiguration
1.1.4.1 - modify equipment through supply chain
1.1.4.2 - modify configuration file to change votes
1.1.4.3 - miscalibrate equipment
1.1.4.4 - tamper with ballot creation software
1.1.4.5 - tamper with the ballot definition file on scanner
1.1.4.6 - inject malicious code
1.1.4.7 - change mark sensing threshold of scanner
1.1.4.8 - modify basic functionality via replaceable media
1.1.4.9 - perform computer-based attacks using ballots
1.1.4.10 - jam/interfere with headphone communicati on
1.1.4.11 - create a false close sheet
1.1.4.9.1 - insert defective ballots into stock
1.1.4.9.2 - create subsitute ballots to attack ballot rotation
1.1.4.9.3 - tamper with ballot design selectively
1.1.4.9.3.1 - select precincts by expected voting pattern
1.1.4.9.3.2 - change font sizes and colors on ballots
1.1.4.9.4 - substitute ineffective ballot marking device
1.1.4.9.5 - pre-mark ballot using machine readable invisible ink
1.1.4.9.6 - pre-mark ballot with subtle visible marks
1.1.4.9.7 - perform CCOS overvote/ undervote attack

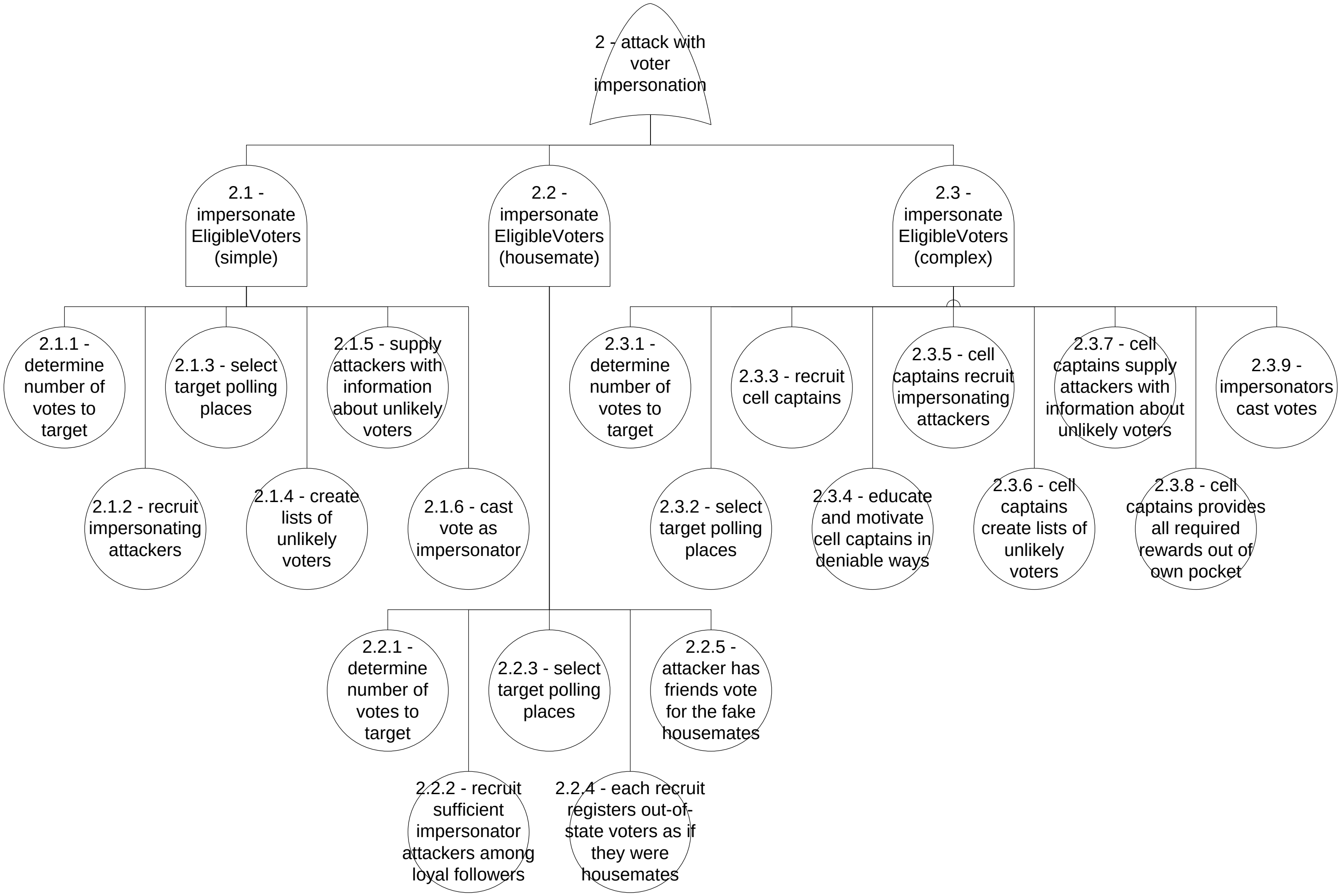
4-6 CCOS Develop and Insert Malware or Misconfiguration


1.1.5 - control/ parameterize attack
1.1.5.1 - enable attack via a knowing voter
1.1.5.2 - enable attack via an unknowing voter
1.1.5.3 - enable attack via a technical consultant
1.1.5.4 - employ unparameterized attack
1.1.5.5 - add steganographic commands to ballot definition file
1.1.5.6 - attack wireless communication

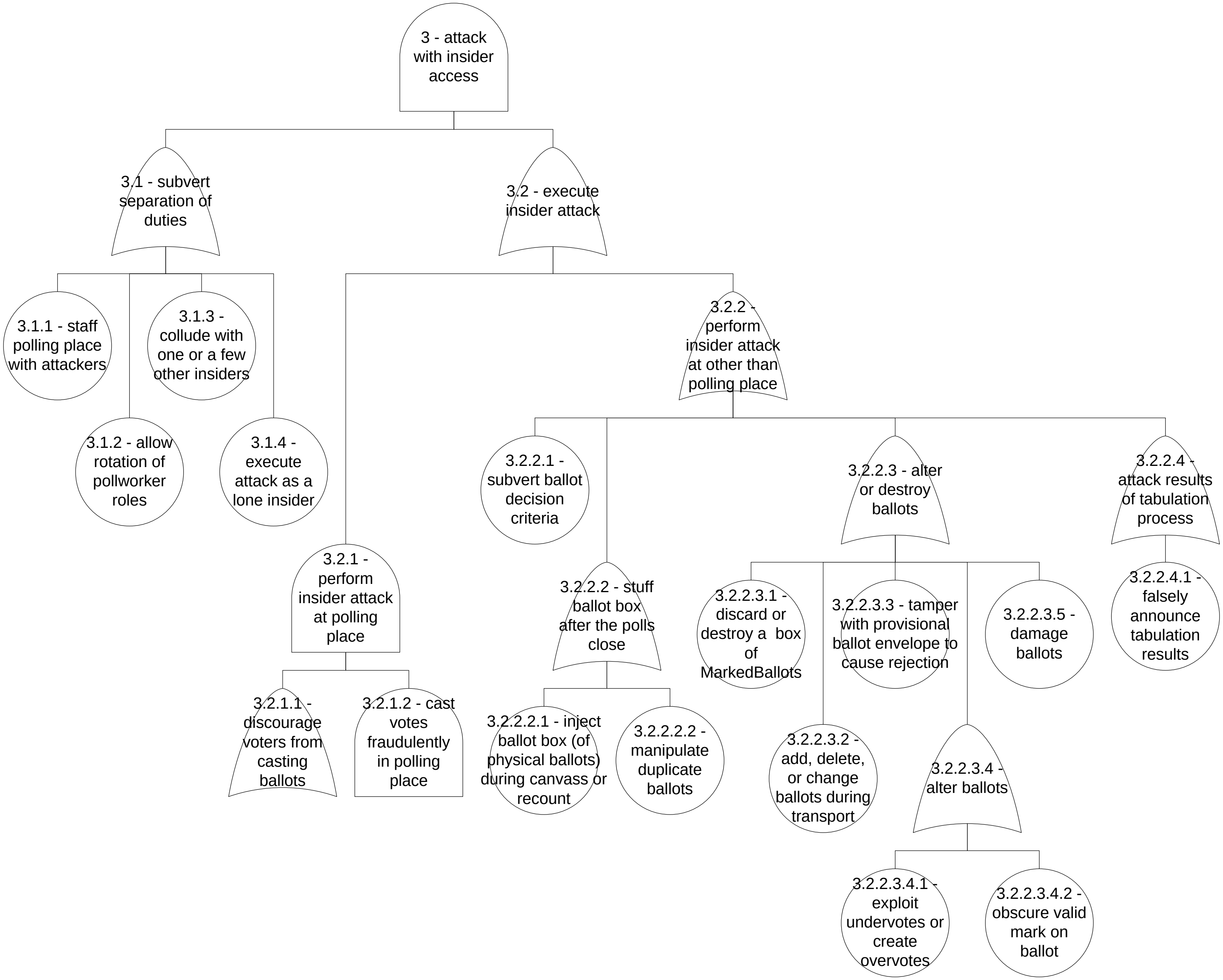
4-7 CCOS Control / Parameterize Attack


1.1.6 - adjust recorded data
1.1.6.1 - pre-load ballot box with negative and positive votes
1.1.6.2 - alter votes at vote time
1.1.6.3 - alter vote after vote time but before or at poll closing time
1.1.6.4 - add or remove votes
1.1.6.4.1 - add or remove CommittedBallots
1.1.6.4.2 - defeat BallotBox seals

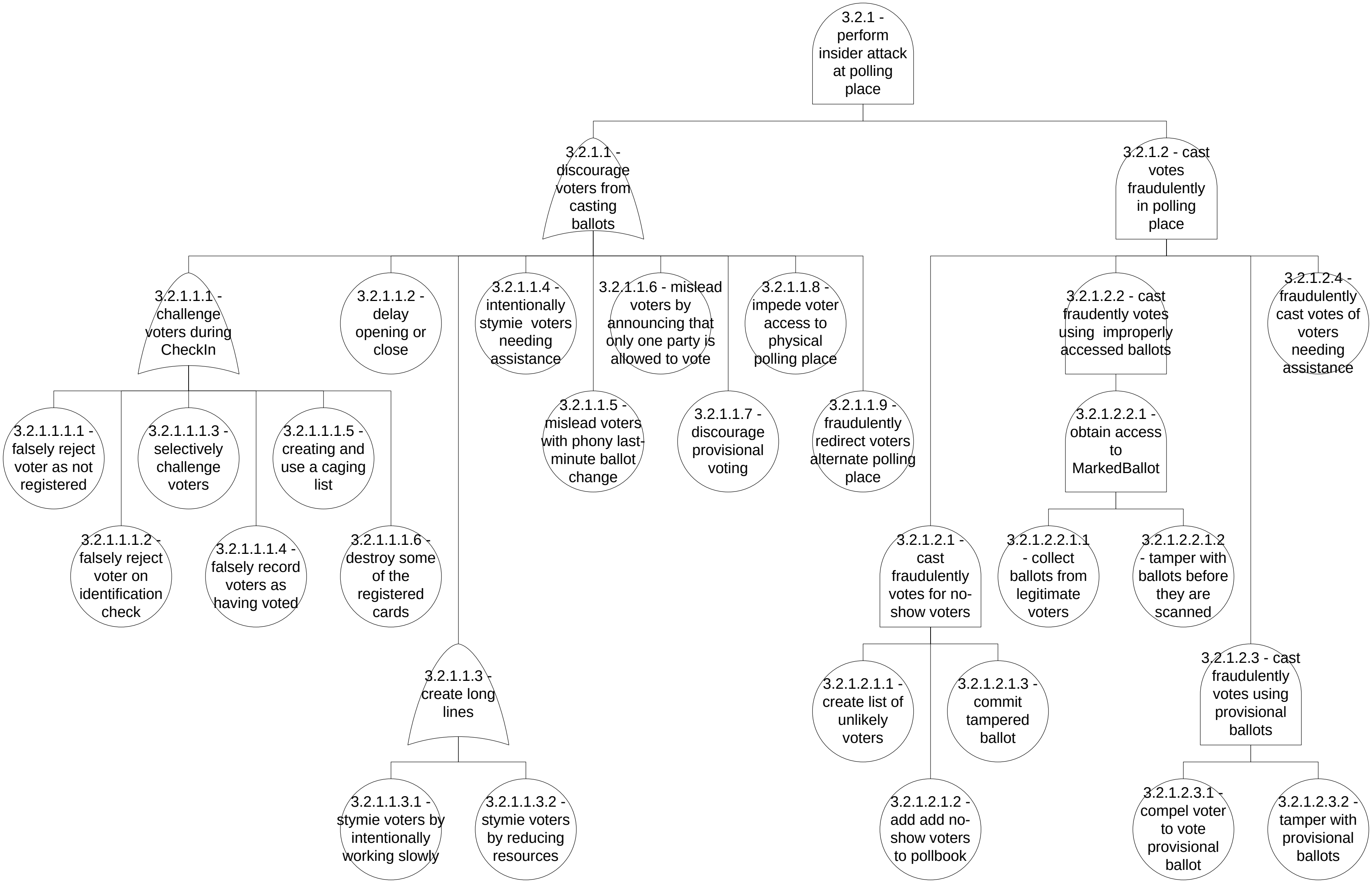
4-8 CCOS Adjust Recorded Data


2 - attack with voter impersonation
2.1 - impersonate EligibleVoters (simple)
2.2 - impersonate EligibleVoters (housemate)
2.3 - impersonate EligibleVoters (complex)
2.1.1 - determine number of votes to target
2.1.2 - recruit impersonating attackers
2.1.3 - select target polling places
2.1.4 - create lists of unlikely voters
2.1.5 - supply attackers with information about unlikely voters
2.1.6 - cast vote as impersonator
2.2.1 - determine number of votes to target
2.2.2 - recruit sufficient impersonator attackers among loyal followers
2.2.3 - select target polling places
2.2.4 - each recruit registers out-of-state voters as if they were housemates
2.2.5 - attacker has friends vote for the fake housemates
2.3.1 - determine number of votes to target
2.3.2 - select target polling places
2.3.3 - recruit cell captains
2.3.4 - educate and motivate cell captains in deniable ways
2.3.5 - cell captains recruit impersonating attackers
2.3.6 - cell captains create lists of unlikely voters
2.3.7 - cell captains supply attackers with information about unlikely voters
2.3.8 - cell captains provides all required rewards out of own pocket
2.3.9 - impersonators cast votes

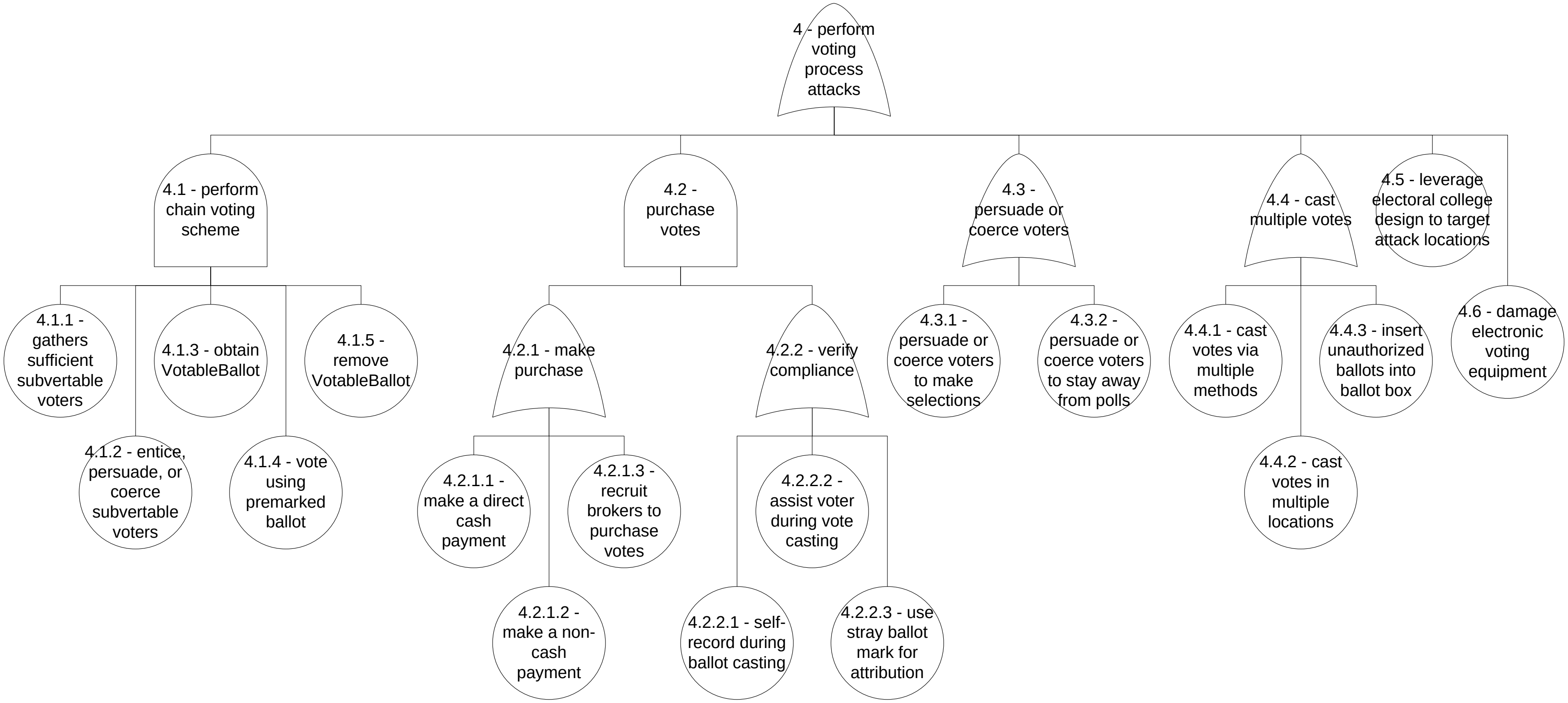
4-9 CCOS Attack with Voter Impersonation


3 - attack with insider access
3.1 - subvert separation of duties
3.2 - execute insider attack
3.1.1 - staff polling place with attackers
3.1.3 - collude with one or a few other insiders
3.1.2 - allow rotation of pollworker roles
3.1.4 - execute attack as a lone insider
3.2.2 - perform insider attack at other than polling place
3.2.2.1 - subvert ballot decision criteria
3.2.2.3 - alter or destroy ballots
3.2.2.4 - attack results of tabulation process
3.2.1 - perform insider attack at polling place
3.2.2.2 - stuff ballot box after the polls close
3.2.2.3.1 - discard or destroy a box of MarkedBallots
3.2.2.3.3 - tamper with provisional ballot envelope to cause rejection
3.2.2.3.5 - damage ballots
3.2.2.4.1 - falsely announce tabulation results
3.2.1.1 - discourage voters from casting ballots
3.2.1.2 - cast votes fraudulently in polling place
3.2.2.2.1 - inject ballot box (of physical ballots) during canvass or recount
3.2.2.2.2 - manipulate duplicate ballots
3.2.2.3.2 - add, delete, or change ballots during transport
3.2.2.3.4 - alter ballots
3.2.2.3.4.1 - exploit undervotes or create overvotes
3.2.2.3.4.2 - obscure valid mark on ballot

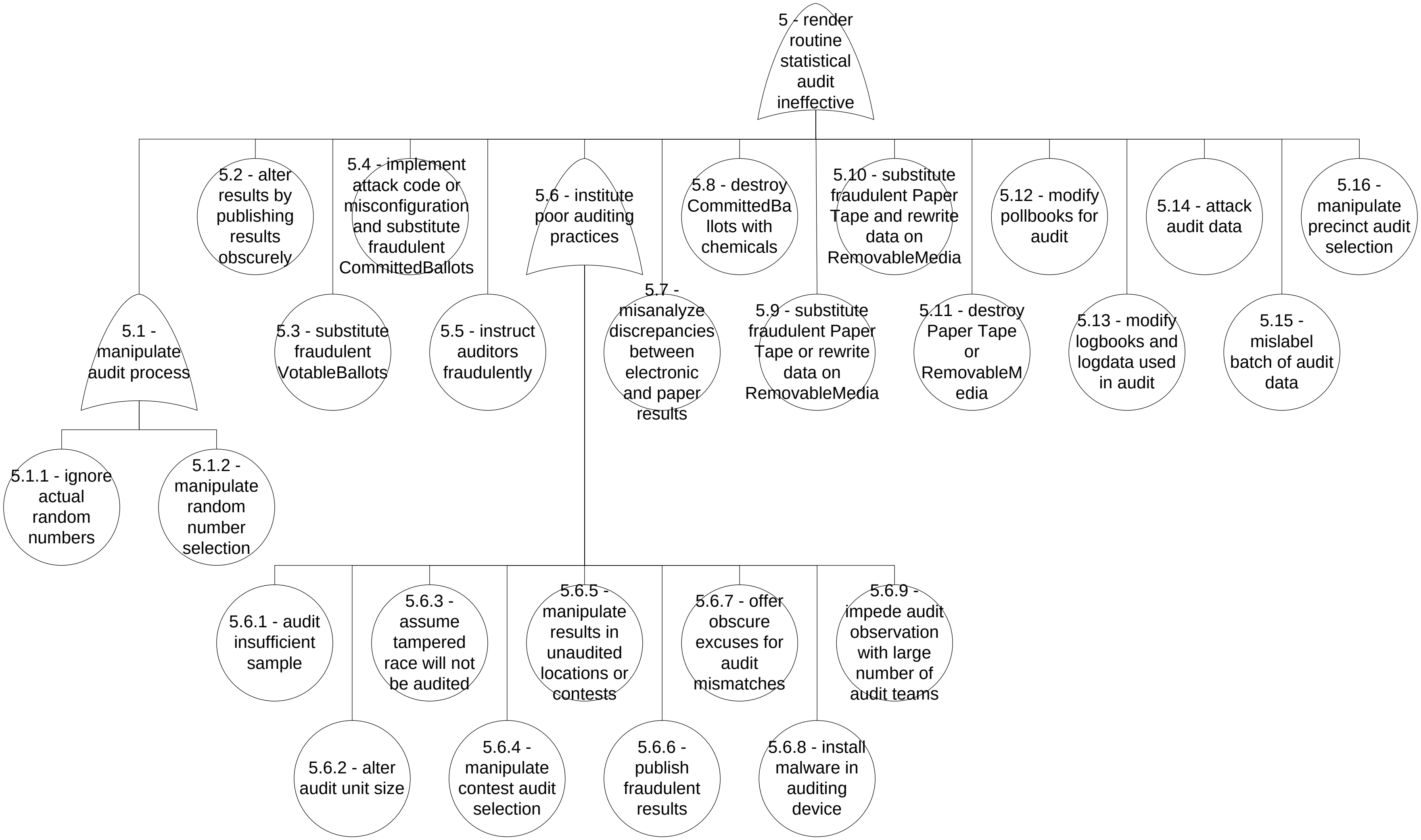
4-10 CCOS Attack with Insider Access


3.2.1 - perform insider attack at polling place
3.2.1.1 - discourage voters from casting ballots
3.2.1.2 - cast votes fraudulently in polling place
3.2.1.1.1 - challenge voters during CheckIn
3.2.1.1.2 - delay opening or close
3.2.1.1.4 - intentionally stymie voters needing assistance
3.2.1.1.6 - mislead voters by announcing that only one party is allowed to vote
3.2.1.1.8 - impede voter access to physical polling place
3.2.1.2.2 - cast fraudently votes using improperly accessed ballots
3.2.1.2.4 - fraudulently cast votes of voters needing assistance
3.2.1.1.1.1 - falsely reject voter as not registered
3.2.1.1.1.3 - selectively challenge voters
3.2.1.1.1.5 - creating and use a caging list
3.2.1.1.5 - mislead voters with phony last-minute ballot change
3.2.1.1.7 - discourage provisional voting
3.2.1.1.9 - fraudulently redirect voters alternate polling place
3.2.1.2.2.1 - obtain access to MarkedBallot
3.2.1.1.1.2 - falsely reject voter on identification check
3.2.1.1.1.4 - falsely record voters as having voted
3.2.1.1.1.6 - destroy some of the registered cards
3.2.1.2.1 - cast fraudulently votes for no-show voters
3.2.1.2.2.1.1 - collect ballots from legitimate voters
3.2.1.2.2.1.2 - tamper with ballots before they are scanned
3.2.1.1.3 - create long lines
3.2.1.2.1.1 - create list of unlikely voters
3.2.1.2.1.3 - commit tampered ballot
3.2.1.2.3 - cast fraudulently votes using provisional ballots
3.2.1.1.3.1 - stymie voters by intentionally working slowly
3.2.1.1.3.2 - stymie voters by reducing resources
3.2.1.2.1.2 - add add no-show voters to pollbook
3.2.1.2.3.1 - compel voter to vote provisional ballot
3.2.1.2.3.2 - tamper with provisional ballots

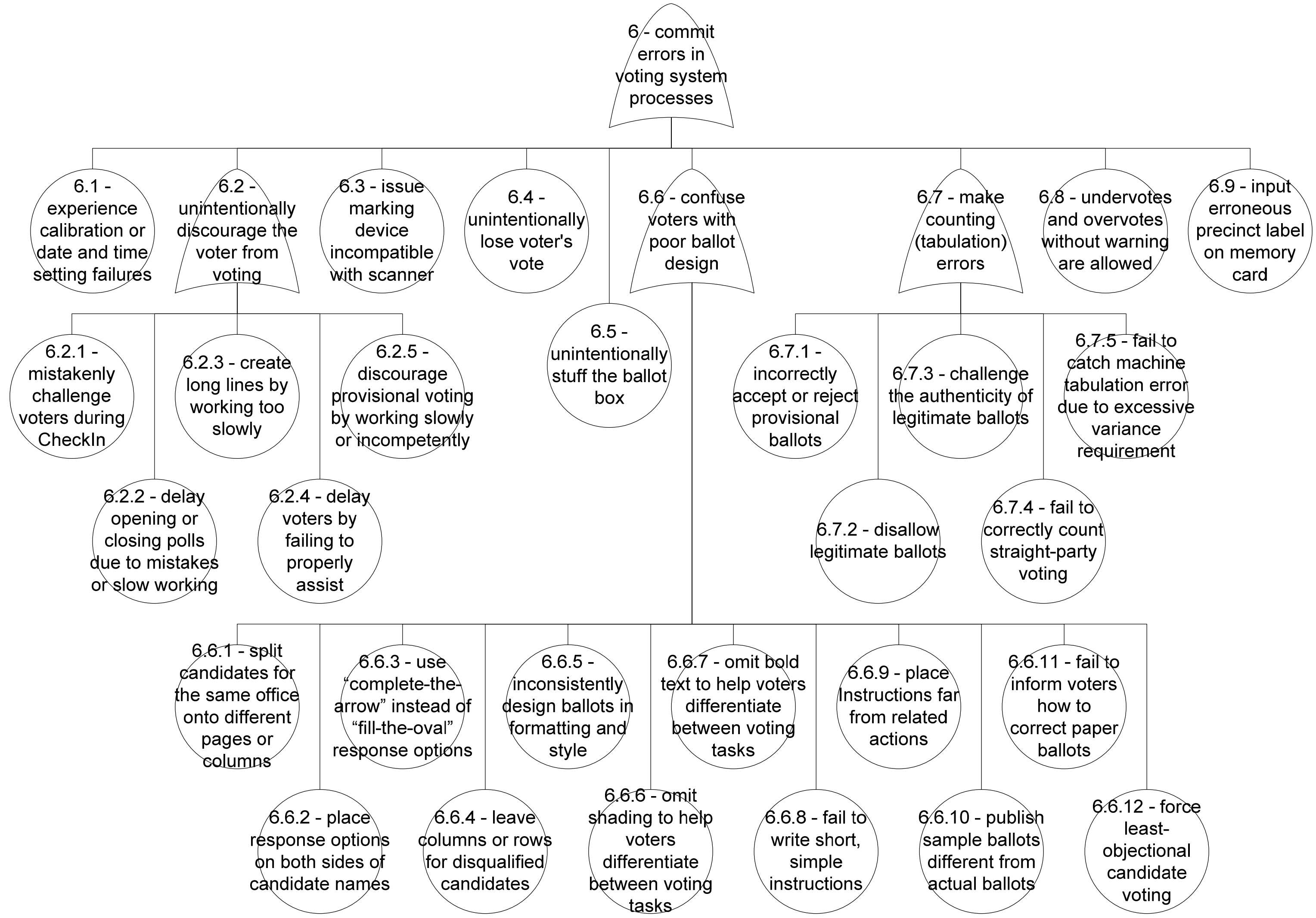
4-11 CCOS Perform Insider Attack at Polling Place


4 - perform voting process attacks
4.1 - perform chain voting scheme
4.2 - purchase votes
4.3 - persuade or coerce voters
4.4 - cast multiple votes
4.5 - leverage electoral college design to target attack locations
4.6 - damage electronic voting equipment
4.1.1 - gathers sufficient subvertable voters
4.1.2 - entice, persuade, or coerce subvertable voters
4.1.3 - obtain VotableBallot
4.1.4 - vote using premarked ballot
4.1.5 - remove VotableBallot
4.2.1 - make purchase
4.2.2 - verify compliance
4.2.1.1 - make a direct cash payment
4.2.1.2 - make a non-cash payment
4.2.1.3 - recruit brokers to purchase votes
4.2.2.1 - self-record during ballot casting
4.2.2.2 - assist voter during vote casting
4.2.2.3 - use stray ballot mark for attribution
4.3.1 - persuade or coerce voters to make selections
4.3.2 - persuade or coerce voters to stay away from polls
4.4.1 - cast votes via multiple methods
4.4.2 - cast votes in multiple locations
4.4.3 - insert unauthorized ballots into ballot box

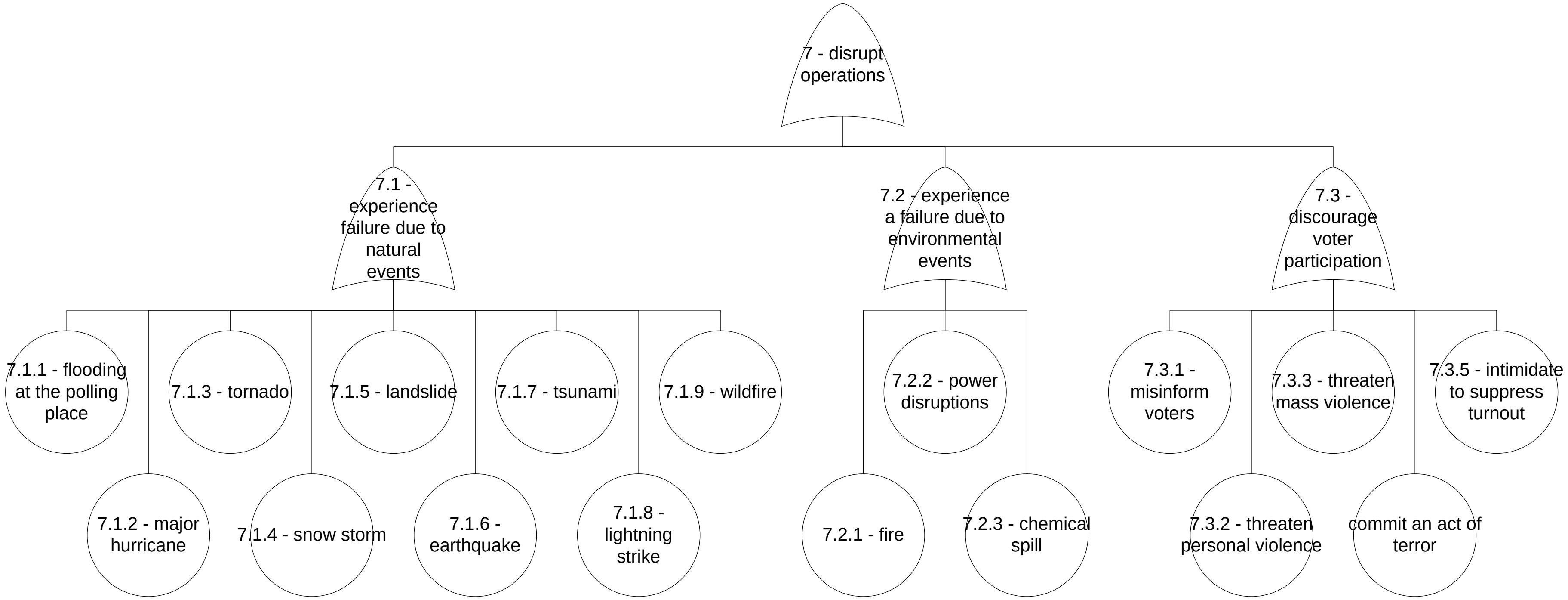
4-12 CCOS Perform Voting Process Attack


5 - render routine statistical audit ineffective
5.1 - manipulate audit process
5.1.1 - ignore actual random numbers
5.1.2 - manipulate random number selection
5.2 - alter results by publishing results obscurely
5.3 - substitute fraudulent VotableBallots
5.4 - implement attack code or misconfiguration and substitute fraudulent CommittedBallots
5.5 - instruct auditors fraudulently
5.6 - institute poor auditing practices
5.6.1 - audit insufficient sample
5.6.2 - alter audit unit size
5.6.3 - assume tampered race will not be audited
5.6.4 - manipulate contest audit selection
5.6.5 - manipulate results in unaudited locations or contests
5.6.6 - publish fraudulent results
5.6.7 - offer obscure excuses for audit mismatches
5.6.8 - install malware in auditing device
5.6.9 - impede audit observation with large number of audit teams
5.7 - misanalyze discrepancies between electronic and paper results
5.8 - destroy CommittedBallots with chemicals
5.9 - substitute fraudulent Paper Tape or rewrite data on RemovableMedia
5.10 - substitute fraudulent Paper Tape and rewrite data on RemovableMedia
5.11 - destroy Paper Tape or RemovableMedia
5.12 - modify pollbooks for audit
5.13 - modify logbooks and logdata used in audit
5.14 - attack audit data
5.15 - mislabel batch of audit data
5.16 - manipulate precinct audit selection

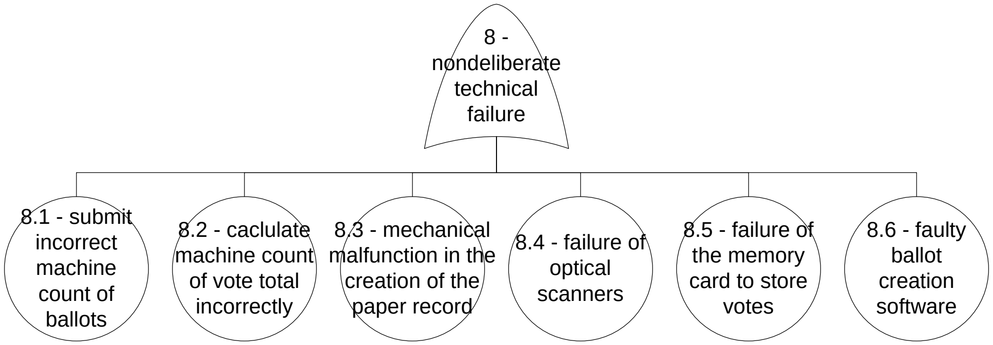
4-13 CCOS Render Routine Statistical Audit Ineffective


6 - commit errors in voting system processes
6.1 - experience calibration or date and time setting failures
6.2 - unintentionally discourage the voter from voting
6.3 - issue marking device incompatible with scanner
6.4 - unintentionally lose voter's vote
6.5 - unintentionally stuff the ballot box
6.6 - confuse voters with poor ballot design
6.7 - make counting (tabulation) errors
6.8 - undervotes and overvotes without warning are allowed
6.9 - input erroneous precinct label on memory card
6.2.1 - mistakenly challenge voters during CheckIn
6.2.3 - create long lines by working too slowly
6.2.5 - discourage provisional voting by working slowly or incompetently
6.2.2 - delay opening or closing polls due to mistakes or slow working
6.2.4 - delay voters by failing to properly assist
6.7.1 - incorrectly accept or reject provisional ballots
6.7.3 - challenge the authenticity of legitimate ballots
6.7.5 - fail to catch machine tabulation error due to excessive variance requirement
6.7.2 - disallow legitimate ballots
6.7.4 - fail to correctly count straight-party voting
6.6.1 - split candidates for the same office onto different pages or columns
6.6.3 - use “complete-the-arrow” instead of “fill-the-oval” response options
6.6.5 - inconsistently design ballots in formatting and style
6.6.7 - omit bold text to help voters differentiate between voting tasks
6.6.9 - place Instructions far from related actions
6.6.11 - fail to inform voters how to correct paper ballots
6.6.2 - place response options on both sides of candidate names
6.6.4 - leave columns or rows for disqualified candidates
6.6.6 - omit shading to help voters differentiate between voting tasks
6.6.8 - fail to write short, simple instructions
6.6.10 - publish sample ballots different from actual ballots
6.6.12 - force least-objectional candidate voting

4-14 CCOS Commit Errors in Voting System Processes


7 - disrupt operations
7.1 - experience failure due to natural events
7.2 - experience a failure due to environmental events
7.3 - discourage voter participation
7.1.1 - flooding at the polling place
7.1.3 - tornado
7.1.5 - landslide
7.1.7 - tsunami
7.1.9 - wildfire
7.1.2 - major hurricane
7.1.4 - snow storm
7.1.6 - earthquake
7.1.8 - lightning strike
7.2.2 - power disruptions
7.2.1 - fire
7.2.3 - chemical spill
7.3.1 - misinform voters
7.3.3 - threaten mass violence
7.3.5 - intimidate to suppress turnout
7.3.2 - threaten personal violence
commit an act of terror

4-15 CCOS Disrupt Operations


8 - nondeliberate technical failure
8.1 - submit incorrect machine count of ballots
8.2 - caclulate machine count of vote total incorrectly
8.3 - mechanical malfunction in the creation of the paper record
8.4 - failure of optical scanners
8.5 - failure of the memory card to store votes
8.6 - faulty ballot creation software

4-16 CCOS Nondeliberate Technical Failure

4.3 CCOS Threat Matrix

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1	attack voting equipment	vandalizing, destroying, or tampering with voting equipment	LTM-USA Delivery 01a	human-deliberate	voting system	Voting System, 3-1,3-2	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	thorough background checks on possible people who may have access to the voting machine	
A	1.1	attack CCOS scanner	tampering with optical scan voting machines		human-deliberate	voting system	Voting System, 3-1,3-2	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	thorough background checks on possible people who may have access to the voting machine	A partisan operative, working on behalf of Congressional candidates in federal elections, bribes a rogue employee of an election systems vendor who manufactures optical scanners for voting systems. The rogue employee, a software developer, injects a Trojan horse into CCOS scanners to be shipped to various states. The Trojan horse, undiscovered during testing, activates itself on election day through a cryptic knock, and proceeds to systematically swap votes in favor of candidates of the operative's political party.
O	1.1.1	gather technical knowledge	hacking system - place Trojan Horse on terminal	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	thorough background checks on possible people who may have access to the voting machine	
T	1.1.1.1	hire existing vendor or testing lab insider	hacking system - place Trojan Horse on terminal	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	susceptibility of insiders to bribery and corruption; access to voting machine	thorough background checks on possible people who may have access to the voting machine	
T	1.1.1.2	gain employment as vendor or lab insider	hacking system - place Trojan Horse on terminal	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	susceptibility of insiders to bribery and corruption; access to voting machine	thorough background checks on possible people who may have access to the voting machine	
T	1.1.1.3	obtain equipment and reverse engineer	steal machines - alter machine - attack machine	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	access to voting machine	thorough background checks on possible people who may have access to the voting machine	
T	1.1.1.4	study a machine in transit	steal machines - alter machine - attack machine	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	access to voting machine	thorough background checks on possible people who may have access to the voting machine	
T	1.1.1.5	acquire equipment legally	Purchase a voting machine on eBay		human-deliberate	voting	3-14 One voter	Voting equipment is not controlled like arms, munitions, secrets etc	Uncontrollable	
T	1.1.1.6	find source code	Find or purchase source code		human-deliberate	voting	3-14 One voter	Code gets out	Uncontrollable	
T	1.1.1.7	compromise existing source code escrow	attacker obtains source code from existing source code escrow source (e.g., State Election Office)		human-deliberate	voting				

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.1.2	avoid detection during inspection	alter machine - attack machine	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	selective / spot tests--lack of testing on all machines	thorough background checks on possible people who may have access to the voting machine	
T	1.1.2.1	insert in COTS code	alter software - chip on hardware from outside source	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	access to COTS, lack of inspection of all machines	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.2.2	insert at warehouse	hacking system - place Trojan Horse on terminal	LTM-USA Delivery 01a	human-deliberate	not modeled	not modeled	lack of inspection of all machines; lack of physical security / monitoring of warehouse	thorough background checks on possible people who may have access to the voting machine; more secure holding place or area for voting machine	
T	1.1.2.3	employ existing vulnerabilities	place Trojan Horse on terminal - ballot box stuffing	LTM-USA Delivery 01a	human-deliberate	voting system or not modeled	not modeled	lack of inspection	run a zero (0) count to test for any 'pre-stuffed' ballots on machine	
T	1.1.2.4	employ feature such as total reset card	ballot box stuffing - reset counts - subtract votes	LTM-USA Delivery 01a	human-deliberate	voting system or not modeled	not modeled	lack of inspection	run a large amount of ballots through and see if the count after is different from the number of ballots in the stack	
T	1.1.2.5	insert via viral infestation	place Trojan Horse on terminal - erase memory	LTM-USA Delivery 01a	human-deliberate	voting system	not modeled	access to machines after inspection	erase any data on memory card prior to voting process	
T	1.1.2.6	write subtle security flaw in system	hacking system - place Trojan Horse on terminal	LTM-USA Delivery 01a	human-deliberate	voting system	not modeled	vendor insider's corruptibility and knowledge of how to avert detection	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
O	1.1.3	avoid detection during testing	hacking system - place Trojan Horse on terminal which is not detected during logic and accuracy testing	LTM-USA Delivery 01a	human-deliberate	voting system	not modeled	inability of normal testing procedures to detect malware	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.1	supply cryptic knock during testing	hacking system - cryptic knocks during logic and accuracy testing	LTM-USA Delivery 01a	human-deliberate	voting system	not modeled	inability to detect the clever insider's infiltration of the L&A test script	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.2	supply cryptic knock during setup	hacking system - cryptic knocks during equipment set up	LTM-USA Delivery 01a	human-deliberate	voting system	Poll Worker setup procedures	routine machine setup procedures of poll workers, when known, can be used to set off cryptic knock unknowingly	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine; review instructions from vendor for machine to check for possible abnormalities	
T	1.1.3.3	supply cryptic knock during voting	hacking system - cryptic knocks	LTM-USA Delivery 01a	human-deliberate	voting system	voting	unlikeliness of tests to produce knock-like behavior	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.4	disable fraud behavior with using team anti-knock	hacking system - anti-cryptic knocks	LTM-USA Delivery 01a	human-deliberate	voting system	testing	election official's control over testing procedures	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.3.5	use AC power flicker as knock	hacking system - cryptic knocks - 'dirty power'	LTM-USA Delivery 01a	human-deliberate	voting system	testing	failure of tests to mimic knock action	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.6	detect realistic patterns of voting	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system	testing	failure to test machines with realistic patterns of voting	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.7	employ calendar/clock method	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system	testing	difficult to detect that the Trojan horse has circumvented the test	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.8	obtain cooperation of testers	Pay or coerce testers to obtain tainted test results	LTM-USA Delivery 01a	human-deliberate	voting system	testing	testers who can be easily induced to assist with an attack	ensure testers follow instructions completely to make sure that everything that you are testing to find is done	
T	1.1.3.9	deploy cryptic knock in ballot definition files	hacking system - cryptic knocks	LTM-USA Delivery 01a	human-deliberate	voting system	testing	failure to use real ballot in testing	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.3.10	acquire detailed knowledge of testing procedures and scripts	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system		access to knowledge of testing procedures	safeguard testing procedures; develop new testing procedures for each election	
O	1.1.4	develop and insert malware or misconfiguration	hacking system - malware onto machines	LTM-USA Delivery 01a	human-deliberate	voting system		access to voting machine software	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.4.1	modify equipment through supply chain	Precinct purchases a machine from a reseller that has introduced malware		human-deliberate	voting	3-14 One voter	Precincts purchase equipment from resellers		
T	1.1.4.2	modify configuration file to change votes	attacker gains access to the configuration file and edit accordingly like as making the scanner credit one candidate with votes intended for another	Jones (2005a) #23232	human deliberate	voting system	Accept Ballot, 3-26	flaws in security design of a system	1.Authentication of Configuration files can prevent against outsider attack. 2. Secure transmission of configuration media. 3.Optical Scan Systems that actually read ballot then looking for marks are possible.	A vendors technician is bribed or forced by the political party workers to manipulate the configuration file of a voting machine in such a way that its scanner credits one candidate even though the vote is intended for another candidate. This can be done prior to the election day.
T	1.1.4.3	miscalibrate equipment	For DRE it is misalignment of touch screen and underlying video. In PCOS it can be misalignment of timing marks relative to circles	Wallach (TBA), Blaze (2008)	human-deliberate, human-unintentional	voting	3-14 One voter	Software and hardware have to be calibrated so that they are synchronized	Testing calibration as part of poll place opening and periodically during polling hours.	A poll worker can surreptitiously re-calibrate the screen in a way that allows most input to behave normally but that denies access to specific regions or a terminal can be maliciously re-calibrated to prevent voting for certain candidates or to cause voter input for one candidate to be recorded for another
T	1.1.4.4	tamper with ballot creation software	Outsider injects malware that changes ballot definition		human-deliberate	Ballot Preparation	3-3 Ballot Preparation	malware can be injected into software	Inspection and careful testing of ballots prior to distributing to precincts	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.4.5	tamper with the ballot definition file on scanner	Many incidents of accidental errors in creating ballot definition files have been recorded. Typically, an error in the ballot layout (or a late change) results in the scanners not recording some valid marks as votes. An intentional attack can be mounted using the same procedure.	Verified Voting for inadvertent cases; anecdotal reports	human-deliberate	Ballot Preparation		Scanner technology requires intermediate programming, typically called ballot definition files that map the physical locations on a scannable ballot to election data.	Strict access controls to ballot definition files and the creation system; extended L&A testing; comprehensive routine post-election audits	An insider with access to the ballot definition system could manipulate ballot definition files in a manner that would improperly record votes. A more subtle approach would be to make small changes that would cause votes made with less than full marks to be uncounted. In other words, if the standard mark recognition would be a field of 100 pixels at a specific location, the attacker might reduce the field size to 50 pixels. Alternatively, the attacker could greatly enlarge the recognition field size such that full marks would fail to meet the minimum percentage to be recognized. A subtle attack might have limited effect, but would be very unlikely to be detected through routine L&A testing. The attack would be fairly easily detected through comprehensive routine audits.
T	1.1.4.6	inject malicious code	Injecting malicious code on a machine could steal votes undetectably, modifying all records , logs and counters to be consistent with the fraudulent vote count it creates.	Feldman (2006),Jones (20051) # 23224	technical	Voting	Voting Machine,3-8 Ballot Possession sequence by voting system (RE(b))	Attacker would be able to disrupt communications by injecting malicious code.	CA7-Continous Monitoring,PL2-System Security Plan,SC7-Boundary Protection,	John is attacker having good knowledge about injecting the malicious code into the system. He gets physical access to a machine or its removable memory card for as little as a minute and could install malicious code. Voters will cast their vote normally. But, the malicious code inserted will steal the votes undetectably , modifying all the records, logs and counters to be consistent with the fraudulent vote counts it creates. He also creates some malicious code that spreads automatically and silently from machine to machine during normal election activities - a voting machine virus

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.4.7	change mark sensing threshold of scanner	a vendor technician changes the threshold value of a mark sensing device of an optical scan voting system	Jones (2005a) #2321	human deliberate	Voting System	Image Created, 2-5	lack of management oversight over technician	Accuracy testing of optical mark-sense scanners should be augmented by a test of scanner calibration.	Shane Bond is an Elections Technician who is care taker of machines provided by a particular vendor. An outsider say Carmel, who is a blind supporter of a particular party Y, may bribe Bond to change the mark sensing threshold of a VotingMachine in a Precinct which is more likely to get votes against the Candidate or likely to get more votes in favor of his party Candidate. This machine may detect UnderVote(s) or OverVote(s) accordingly. Due to this change in the mark sensing threshold machine may reject few Ballot(s) even though they are properly marked. A particular EligibleVoter casts his/her voter and feeds the MarkedBallot into the machine and leaves without verifying that it has been accepted or not. Then a corrupt PollWorker may take advantage of this as he can do anything with this AbandonedBallot.
T	1.1.4.8	modify basic functionality via replaceable media	attacker acquires access to the CCOS memory cards, or is able to change files on the central tabulator before election definitions are loaded into memory cards, or connects to the CCOS machine via telephone line for remote reprogramming of the card to replace unprotected executable	Jones(2005a) #2321	human deliberate			lack of management oversight over technician	1.Avoid interpreted programs. 2.Avoid use of software on replaceable media. 3.Avoiding the use of any software by making all programs into firmware and that is validated via a strong method as in the gaming industry.	
O	1.1.4.9	perform computer-based attacks using ballots								
T	1.1.4.9.1	insert defective ballots into stock	Substitute the stock of VotableBallots with ballots containing unobtrusive defects designed to alter the contest result.	Jones(2005a) # 43	human-deliberate	Voting	Votable Ballot	During the elections , the malicious insider can substitute stock of Votable Ballots with unobtrusive defects like butterfly ballot that has names on both sides and punch holes in the centre designed to change the contest result.	L&A testing, carefully observe ballots by poll workers, match polling data vs. contest results for audit	John is a malicious-insider. He somehow manages to get access to the Votable ballots and substitutes a set of VotableBallots with unobtrusive defected ballots. For example the butterfly ballot that has names on both sides and punch holes in the centre. The voter gets confused and makes a wrong selection. This leads to change in the election result.

node type	**outline number**	**threat action**	**description**	**reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
T	1.1.4.9.2	create substitute ballots to attack ballot rotation	Create Substitute ballots that attack the ballot rotation leading to confusion to the voter while voting	Jones(2005a) # 42	human-deliberate	Voting	Votable Ballot	During the elections , the malicious insider can substitute stock of Votable Ballots with some defective ballots like ballots with the sequence of the nominees altered.	Check the ballots before transferring them to the precinct location	John is a malicious-insider. He somehow manages to get access to the votable ballots. He creates substitute ballots for the (No Suggestions) for example ballots with the sequence of the nominees altered. This creates some kind of confusion for the voters while casting their votes and makes a wrong selection. This leads to change in the election result.
A	1.1.4.9.3	tamper with ballot design selectively	create easy-to-read VotableBallots in favored jurisdictions and hard-to-read VotableBallots in non-favored jurisdictions	NIST (2005)	human deliberate	voting system	Validate Ballot Style, 3-3	weak reviewing process of a ballot design	Pre-election tests of tabulating equipment should include hand-marked ballots as well as machine-printed test ballots.	perpetrator arranges the layout of the mark-sense ballots in such a manner that voters in favored jurisdictions are more likely to have their votes properly counted than voters in non-favored jurisdictions.
T	1.1.4.9.3.1	select precincts by expected voting pattern	Attacker selects a precinct that follows a particular voting pattern making it easier for him to carry out the attack.	NA	human-deliberate	Voting	Polling Place	Increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows.	PS2-Position Categorization,PS3-Personnel Sanctions	John is a poll worker. He selects a precinct of his choice to work on election day. He makes the selection based on the voting pattern the precinct follows. Doing so he can carry out the attacks he can on that particular voting pattern with ease. For example, if he is good at injecting malware into the systems with ease, he would select a precinct that uses internet voting pattern.
T	1.1.4.9.3.2	change font sizes and colors on ballots	change font sizes and colors on ballots to alter potential contest results		human-deliberate	voting system	3-1 Ballot Preparation, 3-3, 3-4	corrupt worker who has access to creating ballots	poll workers and other election officials inspect all ballots prior to polling places opening	There is an insider in the company who makes ballots for a particular precinct's elections. This insider, John Doe, has access to creating the ballot style and ballot format for the ballots. John uses his position to alter the font sizes and color on these ballots to make a particular contest on the ballot difficult for voters to interpret. His motivation in this attack is to deter voters from voting on the specific contest. If John can corrupt the person who is over validating the ballot style, then he is one step closer to accomplishing his task. Now John's final step to accomplishing this task is to create the votable ballot and then get the votable ballot validated. Luckily for John, his brother Johnny, is the person over validating votable ballots and is in cahoots with John in his plan. The votable ballot is now finished and sent to the precinct for voting. John is on the door step of accomplishing his goal. The only thing in the way of John's goal is voters skipping the contest.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.4.9.4	substitute ineffective ballot marking device	Voters told that the pen marks the ballot when it actually does not. (invisible ink, magic pen). Other modalities: poll worker substitutes dry ink pens, voter brings own pen that isn't recognized by machine	http://www.windycitizen.com/2008/02/05/chicago-voting-magic-pen-primary	human-deliberate, human-unintentional	voting	3-14 One voter	gullibility of voters and poll workers		Jim and I went to vote at 7 a.m. We were given Democratic ballots and pens. But when I got to the booth, my pen didn't work -- it was like a felt-tip marker with no ink. So I went back to the desk and was told -- along with several other confused voters trying to swap out their nonfunctional pens -- that these were invisible ink' pens that would not leave marks on the ballot but would absolutely be read by the scanners. Except that they weren't. The optical scanners were spitting out ballots until one of the election judges used a key to override the system and get the ballots into the box. After my ballot was rejected once, I got a confirmation that my vote 'counted' (when the number on the ballot box blipped from 19 to 20), but Jim was given a regular ballpoint to fill in his, and it counted right away.'
T	1.1.4.9.5	pre-mark ballot using machine readable invisible ink	Pre-mark ballot using an IR ink that is not human readable but machine readable	http://www.votersunite.org/article.asp?id=7486	human-deliberate	voting	3-14 One voter	Scanners can recognize both visible and IR wavelengths	Only use scanners that read visible light, randomly inspect ballots with handheld IR reader	
T	1.1.4.9.6	pre-mark ballot with subtle visible marks	tamper with preprinted ballot stock by making faint marks or slightly darkening the lines of 'bubbles' to exploit under votes or create over votes	Merle King; Doug Jones http://www.cs.uiowa.edu/~jones/voting/optical/	human-deliberate	Ballot Preparation, Voting	pre-printed ballots for mark sense scanners	insider access to ballots; lack of oversight / chain of custody of ballots	ballot chain of custody procedures; post-election review of ballots	A single election official or poll worker with access to blank pre-printed ballots. The individual can make slight/partial marks in selected bubbles that may not be obvious to a voter receiving the ballot. Routine L&A testing would not expose this attack but it might be easily detectable by voters. This would typically be a retail level attack although a central office insider could mount a wholesale level attack
T	1.1.4.9.7	perform CCOS over vote/under vote attack	inject malware so that the scanner doesn't recognize the over votes and under votes	Jones (2005a) #232	human-deliberate	canvass, voting, precinct closeout	validate total, precinct closeout	Scanner not rejecting the over votes and under votes	SI 12 Information output handling and retention	Voted ballots will be inserted into the scanner. If there is a over vote or a under vote the scanner doesn't show any warning and simply accepts the spoiled ballot resulting in loss of vote.
T	1.1.4.10	jam/interfere with headphone communication			under attack equipment					
T	1.1.4.11	create a false close sheet	create a false close sheet shutting down the scanner intentionally	Jones(2005a) # 51,Jones(2005a) #63	human-deliberate	precinct closeout	scanner	After the election, during the vote counting process at the central location, the person responsible for counting the votes can shut down the scanner and create a bogus close sheet disregarding the actual vote count	PE 6 Monitoring Physical Access	John is a poll worker and is responsible for the vote counting process at the central location. He using his influence creates a bogus close sheet of the vote counts and shuts the scanner down. Doing so he alters the vote totals.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.1.5	control/parameterize attack	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system		access to voting machine software	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.5.1	enable attack via a knowing voter	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system		extremely unlikely that voting pattern can be detected as a knock	ensure there is no voter impersonation	
T	1.1.5.2	enable attack via an unknowing voter	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system	Legal Voters, campaign (not modeled)	ability of voters to be fooled by false campaign	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.5.3	enable attack via a technical consultant	hacking system - Trojan Horse put on machine	LTM-USA Delivery 01a	human-deliberate	voting system		corrupt consultants to vendors	thorough background checks on possible people who may have access to the voting machine	enable attack via a technical consultant at polling place during health check, repair, setup, or poll close
T	1.1.5.4	employ unparameterized attack	hacking system - Trojan Horse put on machine - vote stealing	LTM-USA Delivery 01a	human-deliberate	voting system		increased difficulty in detecting attacks that do not need to know contest-specific parameters	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	employ unparameterized attack such as party-based attack
T	1.1.5.5	add steganographic commands to ballot definition file	hacking system - steganographic code on ballot definition file	LTM-USA Delivery 01a	human-deliberate	voting system	3-3 Ballot Preparation	corruption of election official; lack of supervision of ballot preparation	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.5.6	attack wireless communication	use wireless communication to trigger attack program, send specific attack codes, access information on how a voter voted, or to help make sure a DRE with VVPAT are synched (page 206)	Norden (2006), pp. 205-207, 215	human-deliberate	Voting System	wireless communication	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect, ability to remotely send / receive wireless signal	SC wireless communication protections, such as encryption; PL planning-banning wireless communications	On Election Day, a LegalVoter executing a machine attack uses a wireless PDA to trigger malicious code on a PCOS scanner to start operating.
O	1.1.6	adjust recorded data	hacking system - vote stealing - ballot box stuffing	LTM-USA Delivery 01a	human-deliberate	voting system		inability of audits to detect wrongdoing or willingness of poll workers to cooperate with attack	run a zero (0) count to test for any 'pre-stuffed' ballots on machine	
T	1.1.6.1	pre-load ballot box with negative and positive votes	hacking system - ballot box stuffing - vote stealing	LTM-USA Delivery 01a	human-deliberate	voting system		lack of audit or difficulty of audit to reconcile	run a zero (0) count to test for any 'pre-stuffed' ballots on machine	
T	1.1.6.2	alter votes at vote time	hacking system - Trojan Horse put on system - vote stealing	LTM-USA Delivery 01a	human-deliberate	voting system		lack of audit or difficulty of audit to reconcile	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	
T	1.1.6.3	alter vote after vote time but before or at poll closing time	hacking system - Trojan Horse put on system - vote stealing	LTM-USA Delivery 01a	human-deliberate	voting system		lack of audit or difficulty of audit to reconcile	thorough testing of voting patterns on voting machines to find possible Trojan horses or cryptic knocks hidden on the voting machine	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	1.1.6.4	add or remove votes	false election results - false voter count - improper poll worker behavior	LTM-USA Delivery 01a	human-deliberate	voting system	3-10 Voter check-in, 3-45 machine accumulation	corrupt poll workers, unsecure poll book, lack of paper vs. memory card reconciliation	thorough background checks of those hired to be poll workers; have election officials watch over poll workers throughout the election	
T	1.1.6.4.1	add or remove CommittedBallots	CommittedBallots are added or removed from BallotBox		human-deliberate	voting system		corrupt poll workers, unsecure poll book, lack of paper vs. memory card reconciliation	BallotBox seals, BallotBox chain of custody procedures	
T	1.1.6.4.2	defeat BallotBox seals			human-deliberate	voting system		corrupt poll workers, unsecure poll book, lack of paper vs. memory card reconciliation		
T	1.1.7	render routine statistical audit ineffective	copy of threat id=4	LTM-USA Delivery 01a	human-deliberate	voting system	Voting System, 3-1,3-2, Precinct Closeout	no separation of duties; control by election officials over audit procedures		
O	2	attack with voter impersonation		LTM-USA Delivery 01a	human-deliberate	voting system	Voting System, 3-1,3-2	accessibility of lists of voters not likely to vote; soft voter authentication process; poll workers don't know voters; corrupt poll workers		Tom is a party worker who has contacts with ElectionsOfficial. Getting EligibleVoters' personal information is an easy task for Tom. He can even prepare a list of EligibleVoters who are unlikely to vote this time through his contacts. After preparing a list, he then prepares fake Id's and bribes a group of loyal followers to impersonate the voters on his list. He sends impersonators to the polling places where PollWorkers are not likely to recognize them.
A	2.1	impersonate EligibleVoters (simple)	a list of voters who are unlikely to vote may be prepared and people may be recruited to vote for that person. A polling place where a poll workers are not likely to know voters may be targeted.	Jones (2005a) #311	human-deliberate	voting system	Authenticate Voter, 3-9, 3-10	access to lists of voters not likely to vote; poll workers don't know voters; corrupt Poll Worker	require Credentials at polling places; conduct precise and careful purges on voter lists to remove duplicate names, people who have moved, died, or are otherwise ineligible.	
T	2.1.1	determine number of votes to target			human-deliberate	not modeled		access to polling data		
T	2.1.2	recruit impersonating attackers	A group of impersonating attackers sufficient to affect the outcome of the targeted contest is recruited. The number of impersonators required will vary based on the predicted margin for the contest.		human-deliberate	not modeled	people being recruited	corruptibility or vulnerability of recruits		
T	2.1.3	select target polling places	target polling places where poll workers are not likely to know voters		human-deliberate	not modeled	poll workers, Authenticate Voter, 3-9, 3-10	poll workers do not know voters		
T	2.1.4	create lists of unlikely voters	create lists of voters very unlikely to vote this election		human-deliberate	not modeled	voter lists	access to voter lists and ability to determine voters not likely to vote		Tom obtains voting participation records from the elections officials. These records are analyzed to identify voting patterns that can be exploited (e.g., infrequent voters, voter who tend not to vote in primaries).

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.1.5	supply attackers with information about unlikely voters	attackers are given names, genders, etc. of unlikely voters		human-deliberate	voting system, not modeled	poll workers, Authenticate Voter, 3-9, 3-10	poll workers fooled by unknown attacker with valid voter information		The list of unlikely voters is matched to other public databases (e.g., driver's license databases) to create fraudulent credentials.
T	2.1.6	cast vote as impersonator	impersonator goes to polling place and votes	Jones(2005a) #311	human-deliberate	voting	voters	susceptibility of insiders to bribery and corruption		
A	2.2	impersonate EligibleVoters (housemate)	Recruit impersonators among loyal followers and register them as housemates of registered voters.	Jones(2005a) #11,12	human-deliberate	Voting System	Authenticate Voter, 3-9, 3-10	soft verification process	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	A party worker may hire non voters from different state, prepare fake IDs and register them as housemates of LegalVoters and ask them to vote for his/her party candidate.
T	2.2.1	determine number of votes to target			human-deliberate	not modeled		access to polling data		
T	2.2.2	recruit sufficient impersonator attackers among loyal followers			human-deliberate	not modeled	people being recruited	corruptibility or vulnerability of recruits		
T	2.2.3	select target polling places	target polling places where poll workers are not likely to know voters		human-deliberate	not modeled	poll workers, Authenticate Voter, 3-9, 3-10	poll workers do not know voters		
T	2.2.4	each recruit registers out-of-state voters as if they were housemates		Jones(2005a) #11,12	human-deliberate	voting system	people being recruited	corruptibility or vulnerability of recruits		
T	2.2.5	attacker has friends vote for the fake housemates		Jones(2005a) #311	human-deliberate	voting system	poll workers, Authenticate Voter, 3-9, 3-10	poll workers fooled by unknown attacker with valid voter information		
A	2.3	impersonate EligibleVoters (complex)	use cell captains to execute deniable impersonation attack	Jones (2005a) #31	human-deliberate	voting system	Authenticate Voter, 3-9, 3-10	political influence / power of political leaders or election officials		
T	2.3.1	determine number of votes to target			human-deliberate	not modeled		access to polling data		
T	2.3.2	select target polling places	target polling places where poll workers are not likely to know voters		human-deliberate	not modeled	poll workers, Authenticate Voter, 3-9, 3-10	poll workers do not know voters		
T	2.3.3	recruit cell captains			human-deliberate	not modeled	people being recruited	corruptibility or vulnerability of political loyalists of political leader		
T	2.3.4	educate and motivate cell captains in deniable ways			human-deliberate	not modeled	people being recruited	insulation of lead attacker from discovery		
T	2.3.5	cell captains recruit impersonating attackers		Jones (2005a) #311	human-deliberate	not modeled	voters	corruptibility of potential impersonators; resources of attackers		
T	2.3.6	cell captains create lists of unlikely voters		Jones (2005a) #311	human-deliberate	voting system, not modeled	voter lists	access to voter lists and ability to determine voters not likely to vote		
T	2.3.7	cell captains supply attackers with information about unlikely voters	attackers are given names, genders, etc. of unlikely voters		human-deliberate	voting system, not modeled	poll workers, Authenticate Voter, 3-9, 3-10	poll workers fooled by unknown attacker with valid voter information		The list of unlikely voters is matched to other public databases (e.g., driver's license databases) to create fraudulent credentials.
T	2.3.8	cell captains provides all required rewards out of own pocket			human-deliberate	not modeled	voters	susceptibility of insiders to bribery and corruption		
T	2.3.9	impersonators cast votes	impersonator goes to polling place and votes	Jones(2005a) #311	human-deliberate	not modeled	voters	susceptibility of insiders to bribery and corruption		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	3	attack with insider access	voter manipulation, ballot manipulation prior to tabulation	LTM-USA Delivery 01a	human-deliberate	voting system	Voting System, 3-1,3-2	access to poll book; corruption of election officials or poll workers; lack of management oversight	improve election day administration and personnel policies	John as a poll worker has the responsibility of recording the voters in the poll book. He uses his position and influence, and fill the polling place with attackers letting them vote for no-show voters.
O	3.1	subvert separation of duties								
T	3.1.1	staff polling place with attackers	voter manipulation-allowing ineligible individuals to vote by staffing polling places with attackers	Jones(2005a) #31	human-deliberate	voting system	3-12 Check Poll Book for Authenticate Voter Activity Diagram	attacker access to polling place and fraudulent checking enabled	improve the administration of voting on the election day	John is a poll worker having access to the poll books and he can verify the voter authentication. He can take advantage of this situation by allowing ineligible voters whose entry is not present in the poll book to vote by providing the votable ballots.
T	3.1.2	allow rotation of poll worker roles	a single person poll worker attacks are more likely when different duties are handled by the same person		human-deliberate	Voting	3-9 ElectionsOfficial / Poll Worker for Voter Check In Activity Diagram	poor election laws / policies / guidelines	AC-5 separation of duties	John, a poll worker colludes with the election-official to subvert separation of duties. He handles the poll book and issues ballots to certain voters
T	3.1.3	collude with one or a few other insiders								
T	3.1.4	execute attack as a lone insider								
O	3.2	execute insider attack								
A	3.2.1	perform insider attack at polling place		LTM-USA Delivery 01a	human-deliberate	Voting System	voters, ballots			
O	3.2.1.1	discourage voters from casting ballots	voter manipulation - improper assistance to voters - improper advantage taken of voters with legitimate need for assistance	Jones(2005a) # 211 Jones(2005a) #332	human-deliberate	Voting System		unwillingness or inability of voters to appeal poll workers' decisions	improved the administration of voting on the election day	Poll workers intentionally refuse to allow the voter to vote even though voters name is present on the county register of voters.
O	3.2.1.1.1	challenge voters during CheckIn								
T	3.2.1.1.1.1	falsely reject voter as not registered			human-deliberate	voting system	3-12 Check Poll Book for Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal poll workers' decisions	provide appeal process for oversight of poll worker	
T	3.2.1.1.1.2	falsely reject voter on identification check			human-deliberate	voting system	3-11 Provide Credential	unwillingness or inability of voters to appeal poll workers' decisions		
T	3.2.1.1.1.3	selectively challenge voters	selective challenges to 'undesirable' voters at polling place	Jones #212	human-deliberate	Voting	Voter CheckIn	ability of poll workers or collusions of poll workers to control voter checking; lack of oversight	improve election day administration and personnel policies	A corrupt poll worker may use race, gender, appearance of age, a person's attire, etc., as a means of 'profiling' a voter, and then selectively challenge a person's voter status based upon the expectation that a person fitting that profile will vote contrary to attacker

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.1.1.1.4	falsely record voters as having voted	in the poll book, fraudulently record voters as having voted thereby preventing them from voting.		human-deliberate	Voting				Robert who works as a poll worker falsely signs in voters in the poll book; when the voter arrives at the poll, he is told that they cannot vote because they have already voted in that election. Rachel who has access to the current electronic poll book and the electronic poll books from previous elections uses the digital signatures captured in previous elections to falsely sign-in voters; when the voters arrive at the polls, it appears that they have already voted and because the signature is an actual digital copy of their signature, it will be difficult to detect and remedy on election day.
T	3.2.1.1.1.5	creating and use a caging list	sends registered mail to addresses of registered voters that they've identified as likely to be unfriendly to their candidate. All mail that is returned as undeliverable is placed on what is called a caging list. Then this list is used to challenge the registration or right to vote of those names on it.	Levitt (2007)	human-deliberate	not modeled	Eligible Voters; Send To Senior PW; 3-12	disclosing information of voters	Avoid unauthorized access to the voters list.	John who works at the central location mails out registered mails to a list of voters that are likely to vote for the opposition Candidate. Once the mails are returned back as undeliverable, he creates a list to prevent those voters from voting.
T	3.2.1.1.1.6	destroy some of the registered cards	a third party working on behalf of voter registration may encourage people to register and after the registration process destroy or discard their cards	Ballotpedia (2008)	human-deliberate	not modeled	registered cards	lack of management oversight over third party	Get the details from third party and mail the voter Id's to the votes instead asking third party to handover the id's.	John volunteers to help register voters before the election. Unknowingly to the officials, he was bribed by the Candidate to destroy voters' cards after the registration process is over.
T	3.2.1.1.2	delay opening or close	create a plausible excuse to delay poll opening or closing	Jones (2005a) #33	human-deliberate	voting system	2.1 Votable Ballot for Ballot State Transition Diagram; 3.9 Authenticate Voter for Voter check In activity diagram; 3-10 Authenticate Voter for Voter Check In Dataflow diagram.	inability to detect that Poll Worker actions are intentional; lack of oversight	improved administration of voting on the election day	
O	3.2.1.1.3	create long lines	discourage voters from voting by creating long queues leading the voters leave the polling place		human-deliberate	Voting	Voters	inability to detect that Poll Worker actions are intentional; lack of oversight		
T	3.2.1.1.3.1	stymie voters by intentionally working slowly	work slowly with plausible excuses		human-deliberate	voting system	Voting process	inability to detect that Poll Worker actions are intentional; lack of oversight		John, a poll worker at a particular precinct, works slowly e.g. he intentionally verifies the voter's authentication details slowly and issues the votable ballots to the voters slowly making the voters form long lines. Due to long waiting time few voters who cannot wait will leave the polling place without casting the vote.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.1.1.3.2	stymie voters by reducing resources	provide insufficient resources in the polling place		human-deliberate	voting system	Voting process			Steve, a local elections officials, allocates fewer resources such as privacy booths to targeted polling places which results in long lines on election day
T	3.2.1.1.4	intentionally stymie voters needing assistance	voter manipulation - improper assistance to voters - improper advantage taken of voters with legitimate need for assistance	Jones (2005a) #332	human-deliberate	voting system	3.26 Feed Attempt for PCOS Activity Diagram. 3.27 Feed Attempt for PCOS Data Flow Diagram.	lack of management oversight over poll workers designated to assist at polls	improve the administration of voting on the election day; let the voters be aware of the rules and regulations prior to the election day; improve the poll worker training	John is a poll worker for a particular precincts election and is responsible for assisting the voter say 'X' needing help while marking the ballot or inserting the marked ballot into the scanner. His main aim in this threat attack is to stymie the voters from voting or vote for the voters who ask for help. If X has trouble inserting the marked ballot into the scanner(assume the scanner rejects the vote showing over votes), John can take advantage of the situation and change the ballot or simply without revising insert the ballot into the scanner resulting in the loss or cancellation of vote.
T	3.2.1.1.5	mislead voters with phony last-minute ballot change	poll worker passes out the ballots to voters and tell them there has been a changed on the ballot.		human-deliberate	voting	Eligible Voter, Signed In Voter	susceptibility of voters to believe what was being informed by the poll worker	PL-4 poll worker rules of behavior, PS-2 position categorization	John, a corrupted poll worker informs voters that Candidate John Smith has withdrawn from the Senate contest
T	3.2.1.1.6	mislead voters by announcing that only one party is allowed to vote	poll worker tells voters that only registered voters of one party is allowed to vote		human-deliberate	voting	Eligible Voter, Signed In Voter	susceptibility of voters to believe what was being informed by the Poll Worker	PL-4 poll worker rules of behavior, PS-2 position categorization	John, a corrupted poll worker informs voters that only registered voters from the Republican party are allowed to vote in this election
T	3.2.1.1.7	discourage provisional voting	poll worker turns voter away by not issuing a provisional ballot		human-deliberate	voting	3-12 Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal poll workers' decisions	PL-4 poll worker rules of behavior, PS-2 position categorization	John, a corrupted poll worker, has access to the poll book and authority to authenticate a voter. John refuses to issue provisional ballots to voters by giving them various excuses, thus resulting in loss of vote.
T	3.2.1.1.8	impede voter access to physical polling place	an attacker selectively prevents voters from some precincts, typically under some kind of color of authority.		human-deliberate	Voting	Voters and Voting	If a voter must be present at a particular location (e.g. precinct) to cast a ballot, it is possible to prevent the voter from voting by physical exclusion.	Physical security at polling places; public education	A sheriff in a rural jurisdiction, unlikely to be observed by media or activists, impedes some voters from getting to the polling place by conducting improper traffic stops outside select precincts
T	3.2.1.1.9	fraudulently redirect voters alternate polling place	an attacker fraudulently redirects voter to an alternate polling place intending to reduce the likelihood that they cast a vote		human-deliberate	Voting				Sharron, a corrupted poll worker, tells voters that they are not at the correct polling location; the voter becomes frustrated when they are unable to vote at the second polling place and does not attempt to vote.
A	3.2.1.2	cast votes fraudulently in polling place		LTM-USA Delivery 01a	human-deliberate	Voting System				
A	3.2.1.2.1	cast fraudulently votes for no-show voters	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones (2005a) #311; Jones (2005a) #312 Wvvotes.com (2008)	human-deliberate	voting system	unsecured poll book; corrupt official who coerces other poll workers		limited/no access to the ballot boxes to the poll workers after the polls close; improve administration of the poll workers on the election day	John as a poll worker has the responsibility of recording the voters in the poll book. He uses his position and influence, and fill the polling place with attackers letting them vote for no-show voters.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.1.2.1.1	create list of unlikely voters			human-deliberate	not modeled	voter registration databases	access to voter lists and ability to determine voters not likely to vote		
T	3.2.1.2.1.2	add no-show voters to poll book			human-deliberate	voting system	Poll book	unsecured poll book; lack of supervision		
T	3.2.1.2.1.3	commit tampered ballot	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones(2005a) #41	human-deliberate	voting system	3-32 [[Absentee]] for Provide Credential (Remote) Activity Diagram	lack of supervision or other monitoring / poll observers	improved administration of voting on the election day; Video recording after the polls close	A Ballot Stuffer will cast votes on behalf of the people who did not show up to the polls ; sometimes , votes will even be cast by those who are long dead or fictitious characters often referred to as impersonation
A	3.2.1.2.2	cast fraudulently votes using improperly accessed ballots								
A	3.2.1.2.2.1	obtain access to MarkedBallot	obtain physical access to MarkedBallots		human-deliberate, human-unintentional	Voting	Marked Ballots, especially prior to counting	Ballots are not scanned in the precinct, so there are no control totals to verify against the tabulation		A poll worker has voters hand her their ballots and does not deposit them right away; a fraudulent ballot box is used to collect ballots in the polling place; ballots are accessed during transportation to the central count location.
T	3.2.1.2.2.1.1	collect ballots from legitimate voters								
T	3.2.1.2.2.1.2	tamper with ballots before they are scanned	tamper with CommittedBallots before the ballot box is sealed							
A	3.2.1.2.3	cast fraudulently votes using provisional ballots	poll worker forces the voter to vote on provisional ballot-vote manipulation	Jones(2005a) #21	human-deliberate	voting system	3-12 Check Poll Book for Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal poll workers' decisions	improved administration of voting on the election day	Irrespective of the valid information provided by the voter , Poll worker forces voter to vote on provisional ballots. Since the provisional ballots are counted after the voter verification is done, the poll worker can tamper with the provisional ballots before turning them in with other election materials.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.1.2.3.1	compel voter to vote provisional ballot	voter manipulation- not allowing the eligible voters to vote as the registration information is not available	Jones (2005a) #3	human-deliberate	voting system	3-12 Check Poll Book for Authenticate Voter Activity Diagram	unwillingness or inability of voters to appeal poll workers' decisions	1) An election official at the polling place shall notify the individual that the individual may cast a provisional ballot in that election. (2) The individual shall be permitted to cast a provisional ballot at that polling place upon the execution of a written affirmation by the individual before an election official at the polling place stating that the individual is-- (A) a registered voter in the jurisdiction in which the individual desires to vote; and (B) eligible to vote in that election. (3) An election official at the polling place shall transmit the ballot cast by the individual or the voter information contained in the written affirmation executed by the individual under paragraph (2) to an appropriate State or local election official for prompt verification under paragraph (4). (4) If the appropriate State or local election official to whom the ballot or voter information is transmitted under paragraph (3) determines that the individual is eligible under State law to vote, the individual's provisional ballot shall be counted as a vote in that election in accordance with State law	John is a poll worker at particular precinct elections. He has the access to the poll book where he can verify the voter's authentication to check the eligibility to vote. If the voters name is not present in the poll book or voters hold on to a voter ID card from many years ago which listed an incorrect precinct, it is John's responsibility to issue a provisional ballot to the voter. John here can take advantage of not issuing the provisional ballot to the voter thus resulting in loss of vote.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.1.2.3.2	tamper with provisional ballots	ballot manipulation - neglect to seal the provisional ballot envelops-not writing the reason on the envelop	Jones(2005a) #33	human-deliberate	voting system	2.1 Ballot State Transition Diagram	no monitoring or checking or observing PollWorker actions	eliminate barriers to voter registration so as to reduce the use of provisional voting; improve the administration of provisional voting on the Election day; Increase the scrutiny and transparency of provisional voting process; Improve the poll worker training by among other things making clear that provisional ballots should be issued as a last resort and only in limited circumstances , providing instruction on assessing precincts, and requiring examination of provisional ballots for completeness; The poll worker should direct the voter to place the provisional ballot inner envelop into the provisional ballot outer envelope and seal the envelope and cross verify if the ballot is sealed properly. The poll worker here can be negligent or intentionally not seal the envelopes so that the vote can be disregarded.	
T	3.2.1.2.4	fraudulently cast votes of voters needing assistance								
O	3.2.2	perform insider attack at other than polling place			human-deliberate	Voting System				
T	3.2.2.1	subvert ballot decision criteria								
O	3.2.2.2	stuff ballot box after the polls close		Jones (2005a) #413						
T	3.2.2.2.1	inject ballot box (of physical ballots) during canvass or recount		2004 Washington Governor Contest	human-deliberate	Canvas, Post Certification Audit	Validate Total, Process Remote Ballots	After the election, during the validate process, ballot boxes may be placed where they will be found in storage rooms, elections officials' cars, etc.	Ballot watermarking, ballot accounting, registration reconciliation	1. During a recount, an elections official places and then 'finds' a box of ballots in a key-controlled storage room and presents these ballots to the canvassing board for inclusion in the count. 2. During a recount, a poll worker places, and then finds, a box of ballots in the trunk of their car and presents these ballots to the canvassing board for inclusion in the count..
T	3.2.2.2.2	manipulate duplicate ballots	alter the ballot to be counted, or mishandle to allow both the original and duplicate to be counted	NA	human-deliberate	Voting, Precinct Close Out, Canvass, State Accumulation, Post Certification Audit	Ballot Box Accounting, Recount, Validate Jurisdiction Results, Ballot Delivery	Marked Ballots cannot be bound to the voter, so detecting multiple votes by / for the same voter is difficult to detect and / or prevent.	Personnel management, Chain of Custody rules	When processing ballots that require duplication, incorrectly mark the duplicate ballot or handle the ballot so that the original is also counted, or is duplicated multiple times.
O	3.2.2.3	alter or destroy ballots		Jones (2005a) #421						

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.2.3.1	discard or destroy a box of MarkedBallots	use private access to discard or destroy a box of MarkedBallots		human-deliberate	State Accumulation, Canvass, PostCertification	Precinct Close Out, Deliver To Jurisdiction, etc. Any activity where one person or a group of collaborating people, can gain private access to a physical ballot box.	For any system based on physical ballots, each ballot is a constrained data item (CDI). It is a well known security principle that the more CDIs there are, the more difficult it is to protect them.	Ballot accounting, chain of custody, personnel screening	1. During precinct closeout, an elections official may remove a box of ballots from the controlled area and discard it, e.g. in a trash bin.
T	3.2.2.3.2	add, delete, or change ballots during transport	Intentionally trying to change the election result by altering the ballots during transport to central location.	Jones(2005a) #413	human-deliberate	precinct closeout	3-35 One voter(Remote) Activity Diagram - Ballot Delivery, 3-36 One Voter(Remote) Data Flow Diagram	failure to take the details of the person transferring the votes to the central location	PE 16 Delivery and Removal, , PS Third Party personnel security	John is a poll worker responsible for tabulating the votes on the election night. This includes all kinds of votes like the absentee ballots, early votes, provisional ballots etc. He can use his influence and try to manipulate the precinct results by ignoring the ballots or by adding counterfeit ballots so as to match the original count of votes since the precinct results will be telephoned to the election department by the inspector prior to transmission.
T	3.2.2.3.3	tamper with provisional ballot envelope to cause rejection	an envelope is altered to change it from an accepted ballot to a rejected ballot	Dallas (2008)	human-deliberate	Voting, Canvass	Committed provisional Ballot	access to / lack of control or custody of Committed Ballot	AC, access controls, AU, auditing and logging	
O	3.2.2.3.4	alter ballots								
T	3.2.2.3.4.1	exploit under votes or create over votes	alter physical ballots by marking selections that either exploit under votes or cause over votes	Jones (2005a) #421	human-deliberate	Voting, Precinct Close Out, Canvass, State Accumulation, Post Certification Audit	Precinct Close Out, Deliver To Jurisdiction, etc. Any activity where one person or a group of collaborating people, can gain private access to physical ballots.	Paper ballots have no 'final form' status. That is, they can be marked after the voter has cast the ballot. For any system based on physical ballots, each ballot is a constrained data item (CDI). It is a well known security principle that the more CDIs there are, the more difficult it is to protect them.	Personnel management, Chain of Custody rules	After the polls close, poll worker(s) remove(s) ballots from the ballot box. If anytime thereafter they, or with a group of collaborators, gain private access to the paper ballots, they may selectively mark ballots to favor one or more candidates by exploiting under votes (marking contests where voters did not make a selection) or to create over votes in contests where voters selected the opponent of a preferred candidate. This could happen at the polling place, between the polling place and the jurisdiction's central site.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.2.3.4.2	obscure valid mark on ballot	To be properly recognized and interpreted by the scanner, mark sense ballots must have clear and unobscured marks. Proper marks can be obscured by applying stickers. White stickers will be effective, but may be easily detected. Some apparently clear stickers might be sufficient to interfere with the scanner but be hard to detect.	TMB, possible in Saltman	human-deliberate	Ballot Preparation, Voting	Marked Ballots, especially prior to counting	insider access to ballots; lack of oversight / chain of custody of ballots	ballot chain of custody procedures; post-election review of ballots	Persons with access to marked ballots can obscure voters marks by applying opaque stickers over the marks. This is possible even if indelible pens are used to mark the ballots (compare to erasure of pencil marks). In CCOS and remote voting environments the stickers could be applied in large numbers before the ballots are scanned the first time and could result in significant vote total changes. In PCOS environments there will be more limited possibilities of applying stickers before the initial scan. Nevertheless, applying stickers after the initial scan could result in audit and recount exceptions that would undermine voter confidence even if the outcome was not changed.
T	3.2.2.3.5	damage ballots	Damage paper/paper roll by pouring chemicals onto paper	CA TTBR	human-deliberate	voting	3-14 One voter	Unobserved physical access to paper	Make physical access harder (DRE)	DUPLICATE with AUDIT step
O	3.2.2.4	attack results of tabulation process		Jones (2005a) #6						
T	3.2.2.4.1	falsely announce tabulation results	announcement of tabulation result ignoring actual ballots	Jones (2005a) #51	human-deliberate	Canvass, State Accumulation	3-48 Unofficial Results, 3-54 Report Results	dependence on key election official(s) with centralized power to announce / certify result	CA use certification policies that prevent threat, AC separation of duties, AU verify announced results against tabulated	
O	4	perform voting process attacks			human-deliberate, operational	voting system, election system	3-1, Voting, 3-2	susceptibility of voters to being bribed or intimidated; lack of polling place security		a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
A	4.1	perform chain voting scheme	chain voting	Jones (2005b)	human deliberate	voting system		susceptibility of voters to being bribed or intimidated; lack of polling place security	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	
T	4.1.1	gathers sufficient subvertible voters	Subvertible voters will be gathered by attacker for increasing the impact of chain voting or a group of attackers carry out chain voting attack	Jones (2005b)	human deliberate	voting system		susceptibility of voters to being bribed or intimidated		
T	4.1.2	entice, persuade, or coerce subvertible voters	attacker uses payment, persuasion, or coercion to enlist the cooperation of subvertible voters	Jones (2005a) #32, Jones(2005b)	human deliberate	Paper ballot systems	Folded Marked Ballot, 3-23	corrupt Poll Worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	
T	4.1.3	obtain VotableBallot	attacker obtains a VotableBallot or uses an absentee ballot for chain voting attack	Jones (2005b)	human deliberate	voting system		lack of polling place security	Tighten the security in election precinct	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.1.4	vote using premarked ballot	privacy of voting allows voters to exchange the ballots privately	Jones (2005b)	human deliberate	voting system		lack of polling place security; voter privacy measures helps attacker conceal ballots	Tighten the security in election precinct	subverted voter takes MarkedBallot to polling place and votes with it
T	4.1.5	remove VotableBallot	voter smuggles VotableBallot out of polling place and takes it to attacker to enable next cycle of chain voting	Jones (2005b)	human deliberate	voting system		lack of polling place security; voter privacy measures helps attacker conceal ballots		
A	4.2	purchase votes		Dekel (2004)	human deliberate	Voting System, Election System	Eligible Voter, Signed In Voter	susceptibility of voters to bribery; breach of voter privacy	maintain voter privacy; limit access to polling place	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
O	4.2.1	make purchase	a voter is paid for giving his vote away to an attacker		human-deliberate	not modeled	Voter	human susceptibility to being bribed		
T	4.2.1.1	make a direct cash payment	attacker promises to bribe voters if they prove the attacker with evidence that they voted to the particular candidate supported by attacker. pay the 'market' rate for a vote in direct cash payment	Fund (2004), Dekel (2004), Campbell (2006) pp. 278, 283	human deliberate	Voting System, Election System	Eligible Voter, Signed In Voter	susceptibility of voters to bribery	Educate the voters about the importance of voting; prosecute voters who sell their vote; throw out illegal votes; maintain ballot secrecy	'Democrats are far more skilled at encouraging poor people — who need money — to participate in shady vote-buying schemes. 'I had no choice. I was hungry that day,' Thomas Felder told the Miami Herald in explaining why he illegally voted in a mayoral election. 'You wanted the money, you were told who to vote for.''(Fund 2004) In a 1987 Kentucky race, the price for a vote reached $200, while in 1996 Dodge County, Georgia, the going rate was $20 per vote (Campbell 2008)
T	4.2.1.2	make a non-cash payment	attacker promises and exchanges drugs or alcohol in exchange for voting for attacker's candidates	Campbell (2006) pp. 144, 282, Estep (2009)	human deliberate	Voting System, Election System	Eligible Voter, Signed In Voter	susceptibility of voters with substance abuse to bribery	maintain ballot secrecy	In 1910, the price of a vote was 'a drink of whiskey' (Campbell 2006, p. 144); in 2002, two Clay County, KY, election officers allegedly used the prescription painkiller OxyContin to buy votes (Estep 2009)
T	4.2.1.3	recruit brokers to purchase votes	attacker recruits loyal followers, giving them cash bills to buy votes on behalf of attacker's choices	Campbell (2006) pp. 278, 282, 337	human deliberate	Voting System, Election System	Eligible Voter, Signed In Voter	attacker's power to acquire significant resources	expand campaign finance reform to cover wholesale vote-buying; prosecute voting conspiracies, including vote haulers and voters; maintain ballot secrecy	A Dodge County, GA, county commissioner used $15,000 in $20 bills, giving $4,000 to one vote 'hauler' to buy votes at the $20 going rate; one county commissioner forced his road department employees to work on the campaign or else lose their jobs (Campbell 2008, p. 282)
O	4.2.2	verify compliance	to ascertain that a bribed voter goes along with the vote fraud, attacker attempts to verify that voter voted for attacker's choices		human-deliberate	Voting System	Voter	inability to prevent voter attribution	prevent voter attribution with ballot secrecy, preventing stray marks, and making sure that voter assistance is legitimately needed	
T	4.2.2.1	self-record during ballot casting	Voter captures video of his ballot casting, produces it to the attacker as evidence.	Dekel (2004)	human deliberate	voting system	Eligible Voter, Signed In Voter	breech of voter privacy in polling place	Tighten the security of voting system	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.2.2.2	assist voter during vote casting	voter requests assistance to earn reward from assistant	Jones (2005a) #333	human-deliberate	Voting, Canvass	3-12 Sign Poll Book, 3-48 Validate Precinct Results	failure to authenticate voter's assistant; failure to detect unusual patterns of assistance (same assistant, higher than normal assistance)	AU audit precinct results and investigate any unusual voting patterns, such as a high percentage of voter assistance or repeated assistance by the same assistant; prevent by asking voter for reason assistance needed	A man wearing dark glasses and appearing to be sight-impaired shows up with an assistant to help him vote. Following the procedures for check-in, the voter and the assistant obtain a VotableBallot, which is then marked and committed with the full knowledge and help of the assistant, who provides a cash payoff afterwards.
T	4.2.2.3	use stray ballot mark for attribution			human-deliberate	Voting	Votable Ballot	ability of voter to mark ballot freely	use ballot marking that prevents stray marks; clear plastic ballot sleeve	voter votes for attacker candidates and then votes for a write-in candidate by writing in a predetermined code word intended for an inside confederate to see and verify the bought vote
O	4.3	persuade or coerce voters	a type of voter suppression that involves deliberate acts to cause fear in EligibleVoters, thus deterring them from coming out to vote.	Fund (2004), Jones(2005a) #21	human deliberate	lack of privacy				'Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future.' (Fund 2004)
T	4.3.1	persuade or coerce voters to make selections	persuade or coerce voter to make selections favored by the attacker; intruding into the voters privacy trying to find out to whom he has vote or persuade him to vote for a particular candidate; blackmail	Van Acker, Jones(2005a) #332	human deliberate	Voting System, ElectionSystem	Eligible Voter, Signed In Voter, Voting Activity	susceptibility of voters to intimidation; lack of voter privacy, lack of decisiveness in the voter, lack of management oversight over poll workers	Strengthen the election law against such crimes. PL4-Rules of Behavior	An incumbent candidate seeking reelection sends a loyal confederate to the polls accompanying the incumbents' employees, who are coerced to vote for the incumbent, once they receive their votable ballots. Poll worker/election official/voter during the day of election try to intrude into personnel privacy of the voter and try to persuade him to cast his vote to someone else or blackmail him for some reason.
T	4.3.2	persuade or coerce voters to stay away from polls	coerce the voter to stay away from polls with threats and intimidation	Van Acker	human deliberate	voting system		susceptibility of voters to intimidation; lack of voter privacy	Strengthen the election law against such crimes	
O	4.4	cast multiple votes	a LegalVoter votes more than once; ballot box stuffing by the voter		human-deliberate	Voting	Voting	inability of voting system to capture duplicate votes by a voter		
T	4.4.1	cast votes via multiple methods	vote early and regular, or absentee and provisional as a form of ballot box stuffing	Jones (2005a) #41, TIRA panel	human-deliberate	Voting	3-33 Authenticate Voter (remote), 3-31 Voter List, Voter Information, Authenticate Voter, AuthenticationRules, Jurisdiction	inability to or failure to cross-check poll books for different voting methods within a single place (jurisdiction)	SI-improve integrity of voter lists, IA-authenticate voters	a voter casts an absentee ballot but then votes again at the polling place on election day

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.4.2	cast votes in multiple locations	vote in two neighboring states or multiple precincts with registrations in more than one place	Jones (2005a) #11, 312	human-deliberate	Voting	3-31 Voter List, Voter Information, Authenticate Voter, AuthenticationRules, Jurisdiction	inability to or failure to cross-check voter lists across multiple jurisdictions	SI-improve integrity of voter lists, IA-authenticate voters	a husband and wife who move from Pensacola, FL to Mobile, AL prior to a federal election registers and votes in Alabama, then drives to Pensacola on same election day, voting in the precinct for their former address
T	4.4.3	insert unauthorized ballots into ballot box		NA	human-deliberate	voting	Commit Ballot	Cannot bind a paper ballot to a voter. For a physical ballot box with a slot, a voter may stack several ballots and insert them at the same time. For a PCOS system, the scanner attendant ,must ensure that voter's only submit one ballot.	Ballot box attendant, probably not particular effective	A voter may acquire ballot copies, pre-mark them, and insert them into a ballot box with their legal ballot.
T	4.5	leverage electoral college design to target attack locations	use winner-take-all electoral college design to tempt a selective attack in a tight presidential race	Campbell (2008), p. 337	human-deliberate	Voting System, Election System	Voting System, Election System	availability of polling data enables careful calculation of the number of votes needed to win, which can be leveraged by the winner-take-all electoral design	recommend that states award electoral votes in proportion to popular vote	Several tight presidential elections (1844, 1876, 1884, 1888, 1960, and 2000) could have been turned by fraud in a few selected areas (Campbell 2008, p. 337)
T	4.6	damage electronic voting equipment	physical destruction of voting equipment	Jones (2005a) #231	human-unintentional	Voting System	Voting Machine	fragility of computer equipment, mishandling	PL-4 poll worker rules of behavior, PE-3 physical access control , PE-6 monitoring physical access	Central count scanner is damaged immediately prior to or during tabulation disrupting operations during that critical time window
O	5	render routine statistical audit ineffective		LTM-USA Delivery 01a	human-deliberate	voting system	Voting System, 3-1,3-2, Precinct Close Out	no separation of duties; control by election officials over audit procedures		A corrupted ElectionOfficial with the help of some auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited items. Then proceed to publish the election results.
O	5.1	manipulate audit process	subvert random selection of items being audited, and ignore random numbers and audit something else	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	lack of basic audit in effect	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	A corrupted Auditor ignores random numbers and audit other ContestArtifacts while the corrupted Observer turns a blind eye.
T	5.1.1	ignore actual random numbers	follow the normal procedure for randomly generating audit selections, but then perform the audit on audit units that will not cause the fraud to be discovered		human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)		implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	A corrupted Auditor ignores random numbers and audit other ContestArtifacts while the corrupted Observer turns a blind eye.
T	5.1.2	manipulate random number selection	manipulate the selection process rendering it not random and select the audit units that will not cause the fraud to be discovered		human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)		implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	A corrupted Auditor ignores random numbers and audit other ContestArtifacts while the corrupted Observer turns a blind eye.
T	5.2	alter results by publishing results obscurely	re-publication attack - change election results via tabulator or jurisdiction website	Jones(2005) #62	human-deliberate	results of the tabulation process	1-1 (Canvass), (Official Report), 3-54 (Report Results)	lack of publishing system security that leads to obscure results	increase security in both areas - tabulator and publication website	An outsider penetrates into the jurisdiction website and changes the results of the election.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.3	substitute fraudulent VotableBallots	replace real VotableBallots with VotableBallots designed to match the electronic and audit in warehouse	Jones(2005) #421	human-deliberate	results of the tabulation process	3-2 (Votable Ballots)	Real Votable Ballots has limited physical security	add more security features to the real VotableBallots to discourage attackers to duplicate VotableBallots, implement chain of custody and strong physical security	After the VotableBallots are printed, an insider who has access to the warehouse replaces the real VotableBallots with tampered VotableBallots.
T	5.4	implement attack code or misconfiguration and substitute fraudulent CommittedBallots	results manipulation - change real CommittedBallots with tampered CommittedBallots to cover the track of the attack on the voting terminal; implement attack code or misconfiguration at voting terminal, and replace real CommittedBallots with fraudulent CommittedBallots	Jones(2005) #611	human-deliberate	voting system	3-1 (Voting) 3-43 (Deliver To Jurisdiction)	lack of management oversight over poll workers during transit and limited physical security on Committed Ballots and voting machine	add more security features to the real CommittedBallots and implement chain of custody and strong physical security on voting terminal and CommittedBallots	Assume there are at least two corrupted PollWorkers. PollWorker A injects malware into the voting terminal just before the election. After the election is over, PollWorker B replaces real CommittedBallots with fraudulent CommittedBallots.
T	5.5	instruct auditors fraudulently	give improper instructions to Auditors to render audit ineffective, and avoid detection	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor policies allows ElectionOfficial to specify their own rules	revise policies to ensure that ElectionOfficial follows the guidelines for auditing process	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors thus resulting in undetected subverted VotingMachines. Note Auditors may or may not be in cahoots with the ElectionOfficial.
O	5.6	institute poor auditing practices	audit manipulation		human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	
T	5.6.1	audit insufficient sample	audit manipulation - audit insufficient of sample to avoid tampered audit unit detected	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors to audit insufficient data thus resulting in undetected tampered audit units. Note Auditors may or may not be in cahoots with ElectionOfficial.
T	5.6.2	alter audit unit size	audit manipulation - random sampling from large variation of audit unit size minimize the risk of detection; create big variation in audit units size so random sampling is unlikely to pick tampered audit units	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors by creating a big variation in audit units size so that tampered audit units will not be selected during random sampling. Note Auditors may or may not be in cahoots with the ElectionOfficial.
T	5.6.3	assume tampered race will not be audited	election law manipulation - select a race randomly - assume audit untampered race only; pick one randomly selected race for audit and assume tampered race will not be audited	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors by picking one randomly selected race for audit so that tampered race will not be selected during random sampling. Note Auditors may or may not be in cahoots with the ElectionOfficial.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.6.4	manipulate contest audit selection	election law manipulation - select a race non-randomly - audit untampered race only	Jones(2005) #612	human-deliberate	results of the tabulation process	3-48 (Validate Precinct Results)	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	A corrupted ElectionOfficial gives improper or unclear instructions to Auditors by picking one randomly selected race for audit so that tampered race will not be selected during non-random sampling. Note Auditors may or may not be in cahoots with the ElectionOfficial.
T	5.6.5	manipulate results in unaudited locations or contests	tabulation manipulation - clean up data automatically based on operator; complete random selection first, and clean data so fraud is moved to unaudited items	Jones(2005) #612	human-deliberate	tabulation server	3-48 (Accumulate Totals) 3-55 (Contest Artifacts), (Contest Audit)	lack of tabulation server security	increase security features of tabulators	A corrupted ElectionOfficial with the help of some Auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited items. Then proceed to publish the election results.
T	5.6.6	publish fraudulent results	election results manipulation - precinct total do not add up to machine total	Jones(2005) #612 Norden(2006) #3	human-deliberate	results of the tabulation process	1-1 (Precinct Accumulation), (Vote Tabulating Machine), 3-43 (Precinct Audit Data), (Machine Accumulation),	poor auditing practices or procedures	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	A corrupted ElectionOfficial releases precinct-level data that reflects the fraudulent results without tampering the MachineCount. Thus, the precinct total does not tally with the machine total.
T	5.6.7	offer obscure excuses for audit mismatches	election results manipulation - give reasons for mismatch - avoid recount, examining voting terminals, and fraud audit items detection	Jones(2005) #612	human-deliberate	results of the tabulation process	3-54 (Validate Jurisdiction Results)	poor election laws / policies / guidelines	implement a policy that requires ElectionOfficial to give non-obscure reasons for result discrepancies and take corrective measures to avoid fraud	During the validation of the Jurisdiction results, a mismatch was found. The corrupted ElectionOfficial tries to offer obscure reasons to hide the actual attack.
T	5.6.8	install malware in auditing device	voting system manipulation - install malware to tamper results through physical access or network access	Jones(2005) # 612 Norden(2006) #2,#3	human-deliberate	voting system / auditing device	3-42 / 3-43 (Ballot Box Accounting), (Machine Accumulation)	corrupt officials using unsecured and non-certified voting system or custom device as audit device	use only certified voting system or secured custom device and implement a policy that requires ElectionOfficials to reconcile totals from HandCount and ManualCount	A corrupted ElectionOfficial avoids manual audit by giving excuses (such as MachineCount is more accurate than HandCount), and instructs Auditors to use Totals from the MachineCount.
T	5.6.9	impede audit observation with large number of audit teams	auditor manipulation - incompetent Auditors ballot manipulation - dishonest audit; employ as many teams as possible including corrupt or incompetent Auditors so Observers won't be able to monitor all of the Auditors	Jones(2005) #5,#6	human-deliberate	ballot tabulation process / results of the tabulation process	3-48 (Validate Precinct Results)	lack of management oversight over Election Officials and Auditors	implement a policy that specifies only certain number of Auditors can be employed so that Observers can perform their duty efficiently	A corrupted ElectionOfficial hires as many incompetent or corrupt Auditors as possible knowing that an Observer can only monitor a limited number of Auditors at a time.
T	5.7	misanalyze discrepancies between electronic and paper results	results discrepancies - totals do not tally - failed to correctly analyze the discrepancies	Jones(2005) #6	human-unintentional	results of the tabulation process	3-42 / 3-43 (Ballot Box Accounting), (Machine Accumulation)	ElectionOfficial has limited knowledge on discrepancies issues	Provide training or courses to equip ElectionOfficial with up-to-date knowledge on election materials, or hire experienced ElectionOfficial	An ElectionOfficial was recently hired to run the PollingPlace at a local Precinct. His experience as ElectionOfficial is somewhat limited as he has just began his job not too long ago. After the election is over, he was being informed that the totals from the paper and electronic do not match. Because of his lack of experience, he misanalyzes and offers ambiguous reasons for discrepancies.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.8	destroy CommittedBallots with chemicals	ballot destruction - destroy or damage CommittedBallots	Jones(2005) #6, Norden(2006) #9	human-deliberate	voting system	3-43 (Deliver To Jurisdiction)	poor security during Contest Artifacts delivery	Implement chain of custody and strong physical security during delivery	A group of terrorists places a bomb in the truck that carries ContestArtifacts to the Jurisdiction. As soon as the engine cranks, the truck was blown apart. All the ContestArtifacts were destroyed.
T	5.9	substitute fraudulent Paper Tape or rewrite data on RemovableMedia	results manipulation - change real Paper Tape with fraudulent Paper Tape [OR] rewrite data on RemovableMedia	Jones (2005) #612 #62	human-deliberate	results of the tabulation process	3-45 (Paper Tape of Machine Totals Printed), (Removable memory card total generated)	lack of management oversight over Poll Worker and Observers	Tally the totals from Paper Tape and RemovableMedia to check for discrepancy. Restrict access to ports with RemovableMedia.	A corrupted PollWorker who has the authority to handle the Paper Tape [OR] RemovableMedia colludes with a corrupted Observer before the initial tallying. The PollWorker replaces the Paper Tape with fraudulent Paper Tape [OR] rewrite data on the RemovableMedia (given that he or she has access to a PC or terminal with ports).
T	5.10	substitute fraudulent Paper Tape and rewrite data on RemovableMedia	results manipulation - change real Paper Tape with fraudulent Paper Tape [AND] rewrite data on RemovableMedia	Jones (2005) #612 #62	human-deliberate	results of the tabulation process	3-45 (Paper Tape of Machine Totals Printed), (Removable memory card total generated), (Paper Tape totals of machine count reconciled to removable memory card total)	lack of management oversight over Poll Worker and Observers	Implement strong physical security and chain of custody. Report the MachineCount and check the number of AcceptedBallots against the number of registered voters. Conduct thorough background checks on PollWorkers, ElectionOfficials, and Observers.	Let's assume there are at least three participants in this attack. PollWorker A rewrites data on the memory card while PollWorker B replaces the Paper Tape with fraudulent tape to cover the tracks of the attack on the RemovableMedia. Let's assume the Observer(s) are in cahoots with the corrupted Poll workers in order to successfully execute the attack with little or no suspicion. Note: Machine Totals reflect the total on the memory card after the attack is performed.
T	5.11	destroy Paper Tape or RemovableMedia	destruction of Paper Tape of Machine Totals [OR] RemovableMedia	Jones (2005) #6	human-deliberate	results of the tabulation process	3-45 (Precinct Data)	poor security during election artifacts delivery	Implement chain of custody and strong physical security during delivery	A corrupted ElectionOfficial or an Outsider steals or destroys Paper Tape [OR] RemovableMedia during delivery of the ContestArtifacts to the central location.
T	5.12	modify poll books for audit	poll worker or election-official changes poll books to avoid fraud detection		human-deliberate	Voting, Precinct Close Out	3-12 Check Poll Book for Authenticate Voter Activity Diagram, 3-43 Poll Worker Logs for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	AU-6 audit monitoring, analysis, and reporting	John, a corrupted poll worker, has access to the poll book and authority to authenticate a voter. John alters the poll books so the number of eligible voters matches the number of CommittedBallots which includes fraud ballots.
T	5.13	modify logbooks and log data used in audit	poll worker or election-official changes logbooks and log data to avoid fraud detection		human-deliberate	Precinct Closeout	3-43 Poll Worker Logs for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	AU-6 audit monitoring, analysis, and reporting	Jane, a corrupted election-official, has access to logbooks and log data. She alters the content in the logbooks and log data so auditors would not be able to detect any fraud.
T	5.14	attack audit data	poll worker changes audit data		human-deliberate	Precinct Closeout	3-43 Precinct Audit Data for Precinct Closeout Data Flow Diagram	lack of management oversight over Poll Worker, election-official, auditor	AU-6 audit monitoring, analysis, and reporting	Jane, a corrupted election-official, has access to audit data and modifies it during delivery to the jurisdiction.
T	5.15	mislabel batch of audit data	poll worker or election-official incorrectly labels batch of audit data		human-deliberate, human-unintentional	Precinct Closeout	3-43 Precinct Audit Data for Precinct Closeout Data Flow Diagram	unintentional - vulnerability to human error due to carelessness; intentional - mislabel batch to cover fraud from being detected	AU-6 audit monitoring, analysis, and reporting	John, a newly hired poll worker, is responsible for labeling batches of audit data. Unfortunately, he mislabeled one of the batches due to his inexperience.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.16	manipulate precinct audit selection	break randomization pattern to leverage voting pattern of a precinct		human-deliberate	Precinct Close Out	Audit Data	poor auditing practices or procedures; failure to follow procedures; lack of management oversight over auditing practices	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines (AU-6,8)	
O	6	commit errors in voting system processes		Brief History	human unintentional, operational	voting system	voting machines, various voting system activities	human / process error vulnerabilities	better training, personnel policies, monitoring, testing procedures	In a 2004 Massachusetts race, 171 ballots were not machine-readable because the wrong kind of lead was used in the marking devices.
T	6.1	experience calibration or date and time setting failures	An important aspect of calibration is the plane in which the voting unit is set during an operation. If the unit is flat versus in a slanted position, the calibration can be done improperly.	King	human unintentional, operational	Voting System	Voting Machine	vulnerability to human error; failure to test / check for correct procedure	Either precinct level persons should be trained for this purpose or vendor ; assistance should be available at precinct level.	
O	6.2	unintentionally discourage the voter from voting			human-unintentional	Voting	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.2.1	mistakenly challenge voters during CheckIn			human-unintentional	Voting	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.2.2	delay opening or closing polls due to mistakes or slow working			human-unintentional	Voting	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.2.3	create long lines by working too slowly			human-unintentional	Voting	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.2.4	delay voters by failing to properly assist			human-unintentional	Voting	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.2.5	discourage provisional voting by working slowly or incompetently			human-unintentional	Voting	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.3	issue marking device incompatible with scanner	The machine failed to read 171 ballots because they were completed with the wrong kind of lead. Recount of the selectman race overturned the election. Because other candidates did not file for a recount in time, the other races cannot legally be recounted. Thus the other races remain in question.	Brief History	human-unintentional, operational	Ballot Preparation, Voter CheckIn, Votable Ballot	failure to understand requirements of scanners or logistical failure in managing supply of marking devices	Marking device specifications should be laid out. Use of BMD's should be encouraged.		
T	6.4	unintentionally lose voter's vote	misplace a box of ballots before they are scanned during counting or recounting		human-unintentional	Voting, Canvass	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.5	unintentionally stuff the ballot box	scan ballots more than once, by accident		human-unintentional	Voting, Canvass	poll workers, voters	poor planning	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
O	6.6	confuse voters with poor ballot design	poor ballot design that confuses or misleads voters during Voting process, or fails to prevent voter errors in marking ballot	Norden (2008)	human-unintentional	Ballot Preparation	Validate Ballot Style, 3-3, CheckedIn Voter	weak reviewing process of a ballot design	use ballot design checklist, implement usability testing, review and amend election laws	(see children)
T	6.6.1	split candidates for the same office onto different pages or columns	poor ballot design	Norden (2008) #1 p. 20	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	* use ballot design checklist, implement usability testing, review and amend design laws (* note the above also applies to thread id # 557 - 568), list all candidates for the same race on the same page in the same column	The 2000 presidential race in Palm Beach county, Florida has high residual vote rate due to confusing ballot design that displayed candidates in separate columns with response options in the center - hence the term 'butterfly ballot'.
T	6.6.2	place response options on both sides of candidate names	poor ballot design	Norden (2008) #3 p. 28	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	place response options (such as fill-in-the-ovals) in a consistent place on the ballot, such as one side of candidate names or ballot or ballot question choices	Response options placed on both sides of the candidate's name caused confusion among Hamilton county voters in Illinois. Voters tend to marked the arrow to the right of the candidate's name when they were supposed to mark the arrows on the left.
T	6.6.3	use 'complete-the-arrow' instead of 'fill-the-oval' response options	poor ballot design	Norden (2008) #4 p. 30	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	use the fill-the-oval response option for selecting a choice in a contest	Polk county, Iowa uses optical scan system that requires voters to 'complete-the-arrow' to cast votes. Unfortunately, voters are more familiar with 'fill-in-the-oval' which has lesser residual vote rate compared to 'complete-the-arrow' response option.
T	6.6.4	leave columns or rows for disqualified candidates	poor ballot design	Norden (2008) #5 p. 32	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	Failure to remove disqualified candidates from ballot; Failure to inform voters of disqualified candidates	remove the entire column or row for any candidate or party that has been withdrawn or disqualified (not just the candidate or party name)	The 2004 Presidential race in Montgomery county, Ohio has a higher over vote rate when the name of Ralph Nader was replaced with the words 'Candidate Removed'

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.6.5	inconsistently design ballots in formatting and style	poor ballot design	Norden (2008) #6 p. 36, Frisina (2008)	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	use consistent format and style for every contest and voting action	The inconsistent use of colors in Sarasota county ballot caused voters to skip the Thirteenth Congressional District race. The second page shows 'State' highlighted in teal which is the same as the first page's 'Congressional' word. Thus, it was easy to overlook the congressional district race.
T	6.6.6	omit shading to help voters differentiate between voting tasks	poor ballot design	Norden (2008) #7 p. 40	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	shade certain text, such as office name to help voters to differentiate between voting tasks	Failure to shade office titles on ballot result in higher residual vote rate in Escambia country, Florida. The affected races were Attorney General and Commissioner of Agriculture.
T	6.6.7	omit bold text to help voters differentiate between voting tasks	poor ballot design	Norden (2008) #8 p. 44	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	bold certain text, such as office name to help voters to differentiate between voting tasks	Misused of bold-faced text on the Franklin county ballot in Illinois made it difficult for voters to differentiate contests within each type. Hence, the residual votes were higher for the Attorney General and the Secretary of State races.
T	6.6.8	fail to write short, simple instructions	poor ballot design	Norden (2008) #9 p. 46	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	write short instructions with simple words	The 2004 presidential race in Kansas experienced high residual vote rate due to the long and confusing instruction on the ballot. For example, they used complicated words such as 'Deface' and 'wrongfully mark' instead of 'make a mistake'.
T	6.6.9	place Instructions far from related actions	poor ballot design	Norden (2008) #10 p. 48	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	place specific instructions and related actions together.	Nonpartisan voters in Los Angeles county, California were told to fill out an oval to indicate their party choice before voting in partisan contests. Failure to do so, votes cast for party contest will not count.
T	6.6.10	publish sample ballots different from actual ballots	poor ballot design	Norden (2008) #13 p. 58	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	publish actual ballots that looks the same as the sample ballots	The actual ballot used on the election day in Sarasota county looked very different from the sample ballot. Almost all voters saw the confusing ballot layout for the first time when they were in the voting booth.
T	6.6.11	fail to inform voters how to correct paper ballots	poor ballot design	Norden (2008) #11 p. 54	human-unintentional	Ballot Preparation	3-3 Validate Ballot Style for Ballot Preparation Activity Diagram	weak reviewing process of a ballot design	include information of how to correct paper ballots if voters make mistakes, as required by HAVA for CCOS	Lincoln county, Tennessee had a high residual vote rate compared to the state's residual vote rate for the 2002 Senate race. The ballots in Lincoln did not have instructions for voters who wished to correct their ballots if mistakes were made.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.6.12	force least-objectionable candidate voting	any ballot without a none-of-above choice leaves voters to either under vote or choose the least-objectionable candidate, and requires that someone will win	VNOTA (2009)	human-deliberate	Ballot Preparation	Votable Ballot	lack of acceptable candidates running for office	SI-9, allow for 'none-of-the above' choices in contests	After incumbent governor Buddy Roemer finished 3rd in the general election, Louisiana voters were faced with a lesser-of-two-evils choice between Edwin Edwards, long dogged by allegations of corruption, and David Duke, the former Ku Klux Klan leader, in the 1991 gubernatorial run-off. Without a none-of-the-above choice, voters could either under vote or choose. Edwins won and eventually went to prison for racketeering.
O	6.7	make counting (tabulation) errors	incorrect counting	Jones (2005a) #53	operational; human-deliberate	Canvass, State Accumulation	various counting activities	flawed counting procedures; tendency for human counting error	AT awareness and training,; PS personnel policies; AU audit and accountability; SI accuracy tests; PL planning	
T	6.7.1	incorrectly accept or reject provisional ballots	threats to the tabulation process	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #5	human-unintentional	Canvass	3-50 Validate Precinct Results, 3-51 Resolve Provisional Ballots, Reconcile Voter Feedback	lack of oversight; human error; lack of voter being informed; inability of voter to protest	AT poll worker training, MP labeling provisional ballots or other distinguishing them from other ballots, AU audit provisional ballot data	In a 2005 Washington governor's race, King County election officials admitted that 348 provisional ballots had been improperly counted before the voters' registration status could be determined.
T	6.7.2	disallow legitimate ballots	challenge the authenticity of legitimate ballots	Jones (2005a) #23	human-deliberate	Canvass, State Accumulation, Post Certification Audit	Validate Total, Recount	Cannot bind a ballot to a voter	see duplicates of this one	An elections official may apply non-existent or hyper-sensitive rules for accepting ballots during hand counting, hand recount, absentee ballot processing, etc.
T	6.7.3	challenge the authenticity of legitimate ballots	Jones #43 applied to recount, CCOS PCOS, and audits	Jones (2005a) #43	human-deliberate	Voting, Canvass, State Accumulation	3-51 Resolve Provisional Ballots, 3-53 Validate Remote Ballot, 3-54 Recount	reliance on one or a few potentially colluding poll workers or officials to make a judgment call; inability to review / correct the decision	AU enable audits of decisions made, and the ability to reverse these decisions	
T	6.7.4	fail to correctly count straight-party voting	incorrect counting	Independent Political Report (2008), Jones #53	human-deliberate and human-unintentional, technical	Voting, Canvass	3-43 Machine Results, and more	design complexity, difficultly in detecting attack	SI testing at the polls, SA testing required of vendors, SI-9 input restrictions--removal of straight-party voting from the ballot	see reference source; break out
T	6.7.5	fail to catch machine tabulation error due to excessive variance requirement	failure to catch the machine tabulation error results in vote loss		technical	Canvass	Validate Total	The tabulation software used to tally votes drops of some ballots from the totals at the precinct.	SI2-Flaw Remediation,SI7-Software and Information Integrity,SI11-Error Handling	Machine uses a tabulation software to tally votes with the precinct total. Flaw in the software can inexplicably delete the ballots without election officials ever knowing. Any unfixed programming error can cause the ballots to be dropped off without providing any indication to officials running the system that it was doing so. Threat unidentified can result in huge loss of votes and change in the election outcome.
T	6.8	under votes and over votes without warning are allowed	unintentional errors and omission of under votes and over votes results in loss of votes	Jones (2005a) #33; Review Panel	human-unintentional	Voting	Voting Machine	failure to assist voter in detecting under votes	SI 12 Information output handling and retention, IR4 Incident handling,IR6 Incident reporting	Voters unaware that they have not voted in a contest that has been under voted or over voted

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	6.9	input erroneous precinct label on memory card	The memory cards that count the votes in optical scanners had the wrong precinct labels, so the cards were sent back to the company to be reprogrammed.	Brief History	human-unintentional, operational	vulnerability to human error; failure to test / check for correct procedure	Improvement in procedures required			
O	7	disrupt operations	disrupt operations		human-deliberate, natural, environmental	election system, voting system	voting machines, polling place, voting	exposure to natural or environmental events, fragility of computer equipment, susceptibility of voters to threats and intimidation	disaster planning, contingency planning, physical and environmental protection, incident response, and personnel security	
O	7.1	experience failure due to natural events	voting system failures attributable to natural events	Rackleff 2007	natural	Voting System	voting machines, polling places, voters	exposure to natural events	disaster recovery planning; physical and environmental protection policies	Hurricane Katrina destroyed voting equipment and polling places, displaced voters, and caused elections to be postponed; many of the displaced voters were difficult to find even after basic utilities were restored
T	7.1.1	flooding at the polling place			natural	Polling Place	voting machines, polling places, displaced voters	exposure to natural or accidental events	Polling places and parking places should not be made in low areas where water clogging is possible	
T	7.1.2	major hurricane	experience a major hurricane strike that devastates election assets, displaces voters	Rackleff 2007	natural	Voting System, Election System	voting machines, polling places, displaced voters	exposure to natural or accidental events	disaster recovery planning; hurricane and flood protection; contingency planning	Hurricane Katrina destroyed voting equipment and polling places, displaced voters, and caused elections to be postponed; many of the displaced voters were difficult to find even after basic utilities were restored
T	7.1.3	tornado								in tornado alley during Super Tuesday
T	7.1.4	snow storm								in Denver or the midwest
T	7.1.5	landslide								or mudslide in Calif.
T	7.1.6	earthquake								in the Western US (like San Francisco quake in Oct 1989)
T	7.1.7	tsunami								on the California coast
T	7.1.8	lightning strike								that causes a power outage at polling place
T	7.1.9	wildfire								San Diego wildfires or paper ballot impacts?
O	7.2	experience a failure due to environmental events	voting system failure attributable to non-technical and non-voting related accidents, such as power failure, fires, chemical leaks, oil spills, transportation disasters, or building or bridge collapse	Rackleff 2007	environmental	Voting System	voting machines, polling places, voters	exposure to accidental events	disaster recovery planning; physical and environmental protection policies	wildfire affected ballot delivery
T	7.2.1	fire	experience a fire that affects the availability of or effective operation of the polling place	Potts (2008)	environmental	Poling Place	voting machines, polling places	exposure to natural or accidental events	All Electrical wiring and appliances should be thoroughly checked. There must not be any chance of sparking. Smoking should not be allowed in 100 ft radius. Lighters, matchsticks and other inflammable materials should not be allowed in and around polling place.	An election eve fire adjacent to a small Pennsylvania town's only polling place caused a power outage and forced election officials to move the polling place in the middle of the night. Makeshift signs throughout town redirected voters to a new polling place for the November 4, 2008 election. The effect on voter turnout was unknown. (Potts, 2008)

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	7.2.2	power disruptions			environmental	Polling Place	Voting Machines, rooms needing lighting	environmental failure	Electric power supply department should be notified and they should insure uninterrupted power supply to the polling place. They should be ready for the emergency services. Alterative arrangements like generators can also be made to run the electronic equipments.	
T	7.2.3	chemical spill			environmental	Polling Place				
O	7.3	discourage voter participation	discourage voter participation		human-deliberate	election system, voting system	voter	susceptibility of voters to violence, intimidation, fear	awareness and training, planning, contingency planning, incident response, physical and environmental protection	
T	7.3.1	misinform voters	misinformation about polling places or transportation		human-deliberate	election system, voting system	voter	lack of voter awareness of false information	awareness and training: voter education, utilize new media to counteract misinformation campaign	
T	7.3.2	threaten personal violence	threaten personal violence, such as in blackmailing a voter to be a no-show or to vote for attacker's candidate; attacker focuses on a particular voter threatens him to vote against his will	Van Acker	human-deliberate	election system, voting system	eligible voter	susceptibility of voters to intimidation; lack of voter privacy	planning, strengthen laws against such crimes; physical and environmental security; voter privacy	a type of voter suppression that involves deliberate acts to cause fear in EligibleVoters, thus deterring them from coming out to vote.
T	7.3.3	threaten mass violence	violence to prevent voting, (i.e., bomb scare, mail contamination scare (do not open mail), perhaps even targeting areas (by zip code)	Foxnews.com (2005)	human-deliberate	election system, voting system	voters	voters' fear for their safety	contingency planning contingency planning, incident response incident response, physical and environmental protection physical and environmental protection	In January, 2005, an Australian polling station for Iraqi exiles voting in their homeland's historic first post-Sadaam election was closed for an hour after a riot broke out and a suspicious bag prompted a bomb scare. The overall turnout was affected, it was thought. Many of Australia's estimated 80,000 Iraqis declined to register for the election, fearing their votes would make relatives in Iraq terrorist targets.
T	7.3.4	commit an act of terror	commit an act of terror		human-deliberate	election system, voting system	voters, election officials, voting equipment	exposure to terrorist acts of violence	physical and environmental protection: arms and ammunitions should not be allowed in the polling area. Unclaimed items should be continuously checked. Regular police patrolling required.	
T	7.3.5	intimidate to suppress turnout	coerce the voter to stay away from polls with threats and intimidation	Van Acker	human-deliberate	election system, voting system	eligible voter	susceptibility of voters to intimidation; lack of voter privacy	awareness and training, strengthen the election law against such crimes	'Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future.' (Fund 2004)

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	8	nondeliberate technical failure	Ballot tabulating machines failed to work properly in 31 of 41 precincts. Local election officials said the problem was the result of a software glitch, and ballots had to be recounted.	Brief History	technical, operational	Voting System	Precinct Close Out, Voting Machine, Poll Worker	technical failure		Election officials in New Mexico's most populous county found that a flaw in the ballot programming caused 67,000 absentee and early-voting ballots to be incorrectly counted following the Nov 2000 presidential election.
T	8.1	submit incorrect machine count of ballots	4/2004 Alameda County, California: A bug in the software caused the machines to count absentee ballots inaccurately. The County must use a workaround. 5/2004 Marblehead, Massachusetts: Machine count showed 1834 to 1836. Manual recount showed 1831 to 1830, overturning the election outcome.	Brief History; Jones (2005a) #53	Technical	Voting Machine	software failure		Continuous development on the software required. Service Packs and Updates required regularly.	ones #53, North Carolina case (Jeremy): machine stopped counting after 500 votes
T	8.2	calculate machine count of vote total incorrectly	For the third time in as many elections, Pima County, Arizona, found errors in the tally. The computers recorded no votes for 24 precincts in the 1998 general election, but voter rolls showed thousands had voted at those polling places.	Brief History; Jones (2005a) #54	technical, operational	Precinct Close Out, Voting Machine, Poll Worker	failure of ballot tabulating machines; flaw in the ballot programming		Quality standards should be improved and accountability should be fixed; Improved technical training to election officials and better vendor support; Votes cast should be reported on hourly basis	
T	8.3	mechanical malfunction in the creation of the paper record	Lack of ink or toner, lack of paper, a paper jam, machine malfunction or the unintended loss or destruction of the paper record	Konopasek	Technical	Voting Machine, Voting	technical failure		Insure availability of adequate quantities of quality ink, toner and paper as and when required. Proven qualities of hardware and software should be used. Calibration and testing should be done by competent persons only. Technical assistance should be available in case of necessity.	
T	8.4	failure of optical scanners	In a notable aberration in the 2003 California recall-election vote totals in the 17 California counties that used Diebold, several minor candidates recorded widely disproportionate vote totals.	Brief History	Technical	technical failure			Stringent checks on quality should be imposed and equipments should be delivered well in time so that election officials have enough time for quality checks.	
T	8.5	failure of the memory card to store votes	A computer error caused a failure of the memory card which stores vote data. 13,000 ballots must be rescanned.	Brief History	Technical	technical failure			Improvement in software and hardware required	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	8.6	faulty ballot creation software			technical	Ballot Preparation	ballots, Election Officials	poor quality practices at vendor labs and poor testing at the election jurisdiction	more and better testing at the vendor labs and election jurisdictions	After upgrading ballot creation software, an election official creates a ballot, not aware that the software misprinted or left candidates off of defined contests

5 Vote by Mail

In this tree, we consider threats to voting systems that pass marked ballots across postal systems for tabulation. Vote By Mail is widely used to support absentee voting and is the voting method of choice for voters covered by the Uniformed and Overseas Citizens Voting Act (UOCAVA).

VBM has several important, inherent security and reliability properties. The first two issues relate to VBM's posture as a remote voting system. The first challenge is that the voter is not physically present to allow strong authentication. This leaves VBM susceptible to masquerade attacks. Second, since VBM ballots are not marked in view of elections officials, VBM voters are susceptible to coercion, vote buying and other vote attribution attacks.

In addition to remote voting attacks, VBM is susceptible to man in the middle attacks because marked ballots are out of the control of both the voter and elections officials once they enter the postal system. Moreover, postal systems are not designed for high assurance delivery, so VBM ballots are susceptible to unpreventable, even undetectable destruction and delay while in the postal system.

VBM voting also has two inherent reliability challenges, again relating to its remote voting posture and to postal system delivery. First, because VBM ballots are marked remotely, voter assistance is limited. Thus, simple mistakes on VBM ballots cannot be easily remedied as they can in a polling place.

Second, delivery of both blank and marked ballots is both uncontrollable and unpredictable. This places a rigid time constraint on VBM voters and many VBM ballots are disallowed in every VBM election due to timing challenges. The time challenges are even more difficult for mobile, military voters whose mail delivery may be delayed well beyond voters with stable residence addresses. There are two primary architectural VBM variations: (1) VBM ballots are collected, processed, and tabulated at the LEO office (2) VBM Ballots are tabulated at their respective precincts.

5.1 Vote by Mail Threat Tree

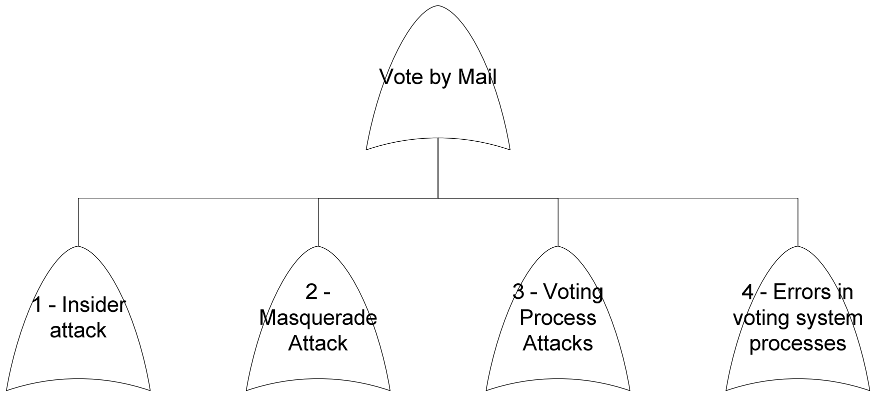
node type - outline number - threat action

O	1	Insider attack
O	1.1	Edit Marked Ballots
O	1.1.1	Edit at Local Elections Office
A	1.1.1.1	Edit During Duplication
T	1.1.1.1.1	Form Collaboration of PWs
T	1.1.1.1.2	Gain Exclusive Access to Ballots
T	1.1.1.1.3	Mark under/overvotes or change votes
T	1.1.1.2	Edit During Counting
T	1.1.1.3	Edit During Other Handling
O	1.1.2	Edit in Transit
T	1.1.2.1	Edit in Post Office
T	1.1.2.2	Edit in intermediate mail room
O	1.2	Discard Marked Ballot
O	1.2.1	Challenge Committed Ballot
O	1.2.1.1	Errant Challenge
T	1.2.1.1.1	Judge misinterprets rule
T	1.2.1.1.2	Errant Failed Signature
O	1.2.1.2	Malicious Challenge
T	1.2.1.2.1	Challenge signature
T	1.2.1.2.2	Challenge postmark

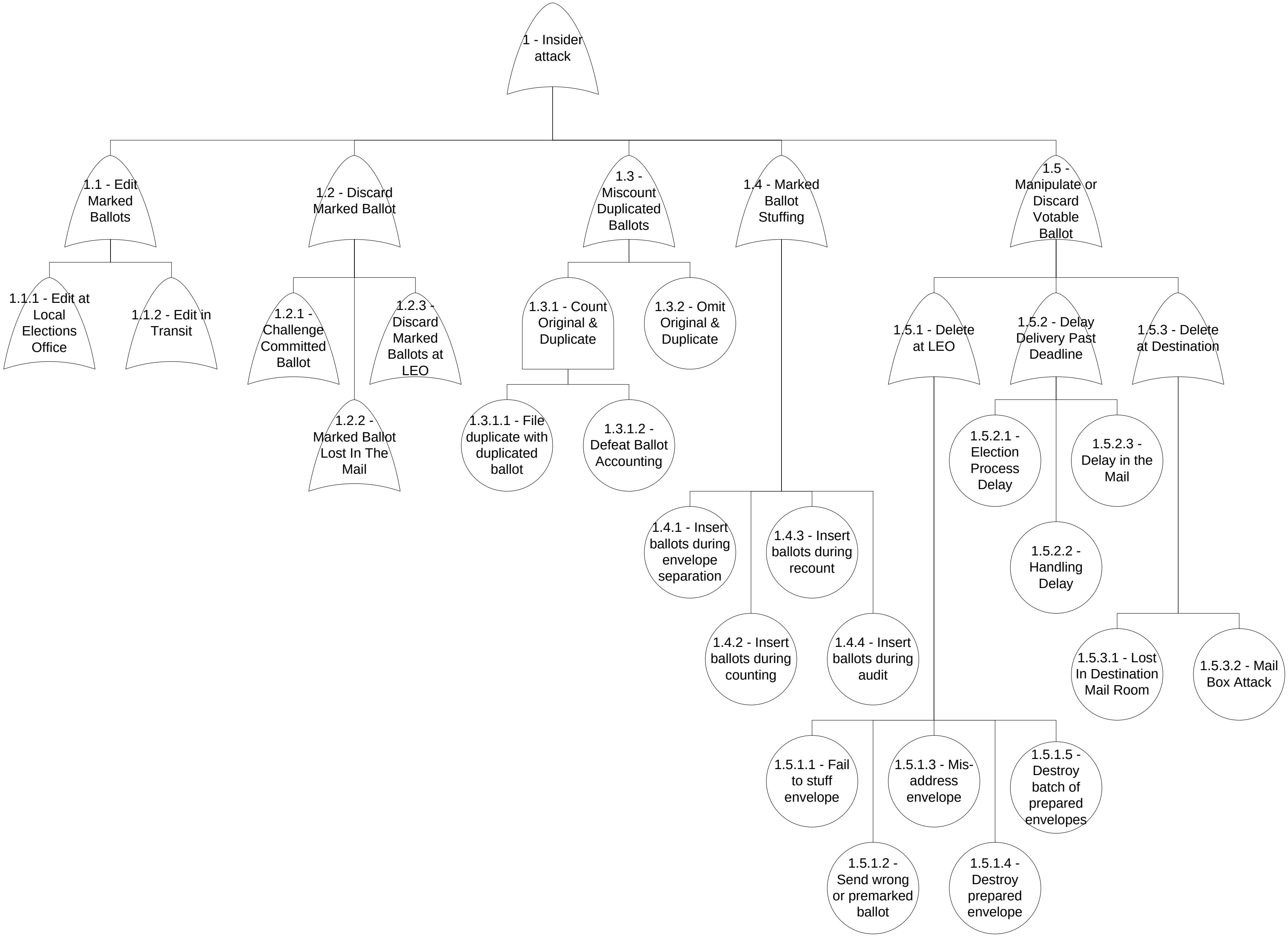
- T 1.2.1.2.3 Challenge intent
- O 1.2.2 Marked Ballot Lost In The Mail
- T 1.2.2.1 Malicious Loss
- T 1.2.2.2 Accidental Loss
- O 1.2.3 Discard Marked Ballots at LEO
- A 1.2.3.1 Delete During Duplication
- T 1.2.3.1.1 Form Collaboration of PWs
- T 1.2.3.1.2 Gain Exclusive Access to Ballots
- T 1.2.3.1.3 Overcome Controls
- T 1.2.3.2 Remove During Counting
- T 1.2.3.3 Mark registration system to reflect duplicate
- T 1.2.3.4 Remove During Other Handling
- O 1.3 Miscount Duplicated Ballots
- A 1.3.1 Count Original & Duplicate
- T 1.3.1.1 File duplicate with duplicated ballot
- T 1.3.1.2 Defeat Ballot Accounting
- T 1.3.2 Omit Original & Duplicate
- O 1.4 Marked Ballot Stuffing
- T 1.4.1 Insert ballots during envelope separation
- T 1.4.2 Insert ballots during counting
- T 1.4.3 Insert ballots during recount
- T 1.4.4 Insert ballots during audit
- O 1.5 Manipulate or Discard Votable Ballot
- O 1.5.1 Delete at LEO
- T 1.5.1.1 Fail to stuff envelope
- T 1.5.1.2 Send wrong or premarked ballot
- T 1.5.1.3 Mis-address envelope
- T 1.5.1.4 Destroy prepared envelope
- T 1.5.1.5 Destroy batch of prepared envelopes
- O 1.5.2 Delay Delivery Past Deadline
- T 1.5.2.1 Election Process Delay
- T 1.5.2.2 Handling Delay
- T 1.5.2.3 Delay in the Mail
- O 1.5.3 Delete at Destination
- T 1.5.3.1 Lost In Destination Mail Room
- T 1.5.3.2 Mail Box Attack
- O 2 Masquerade Attack
- A 2.1 Deceased Voters
- T 2.1.1 Identify target deceased voters
- T 2.1.2 Register them to an accessible address
- T 2.1.3 Receive, mark, return their ballot
- T 2.1.4 Defeat Signature Check
- T 2.2 Family Members
- A 2.3 Central Housing
- T 2.3.1 Identify target residents
- T 2.3.2 Register them
- T 2.3.3 Intercept, mark, and return their ballot
- O 2.3.4 Defeat Signature Check
- T 2.3.4.1 Register as the Voter
- T 2.3.4.2 Forge the Signature
- A 2.4 Mail Box Attack
- T 2.4.1 Identify Target
- T 2.4.2 Steal Blank Ballot from Mailbox

- T 2.4.3 Receive, mark, return their ballots
- O 2.4.4 Defeat Signature Check
  - T 2.4.4.1 Register as the Voter
  - T 2.4.4.2 Forge the Signature
- T 2.5 Malicious "Messenger Ballots"
- O 3 Voting Process Attacks
  - O 3.1 Vote Buying
    - T 3.1.1 Bookie Model
    - A 3.1.2 Internet Vote Buying Attack
      - O 3.1.2.1 Attract voters
        - T 3.1.2.1.1 Attract voters with Internet adds
        - T 3.1.2.1.2 Identify prospective vote sellers from voter rolls
      - T 3.1.2.2 Receive, mark, return their ballots
      - T 3.1.2.3 Pay the voters via the Internet
    - T 3.1.3 Pay voters not to vote
  - O 3.2 Organizer Coercion Attack
    - T 3.2.1 Attribution Threats
    - T 3.2.2 Debate and Vote Parties
  - T 3.3 Employer Coercion Attack
  - T 3.4 Family Member Coercion Attack
  - T 3.5 Distribute false ballots
- O 4 Errors in voting system processes
  - O 4.1 Administrative Error
    - T 4.1.1 Failure to sign correctly
    - T 4.1.2 Signature mismatch
    - T 4.1.3 Failure to bundle correctly
    - T 4.1.4 Failure to meet time requirements
    - T 4.1.5 Confusion with FWAB
  - O 4.2 Selection Error
    - T 4.2.1 Human error mis-mark
    - T 4.2.2 Ballot Design Flaw
    - T 4.2.3 Correction mistake
    - T 4.2.4 Candidate name confusion

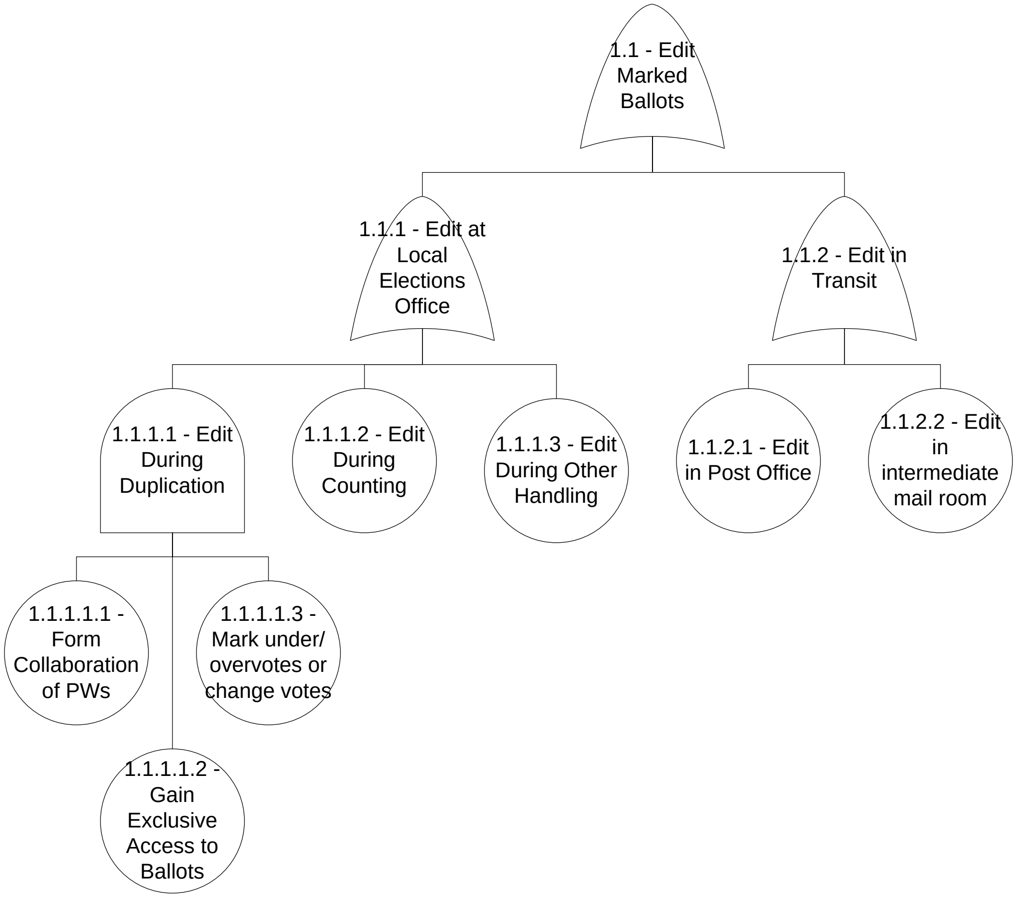
5.2 Vote by Mail Threat Tree – Graphic


Vote by Mail
1 - Insider attack
2 - Masquerade Attack
3 - Voting Process Attacks
4 - Errors in voting system processes

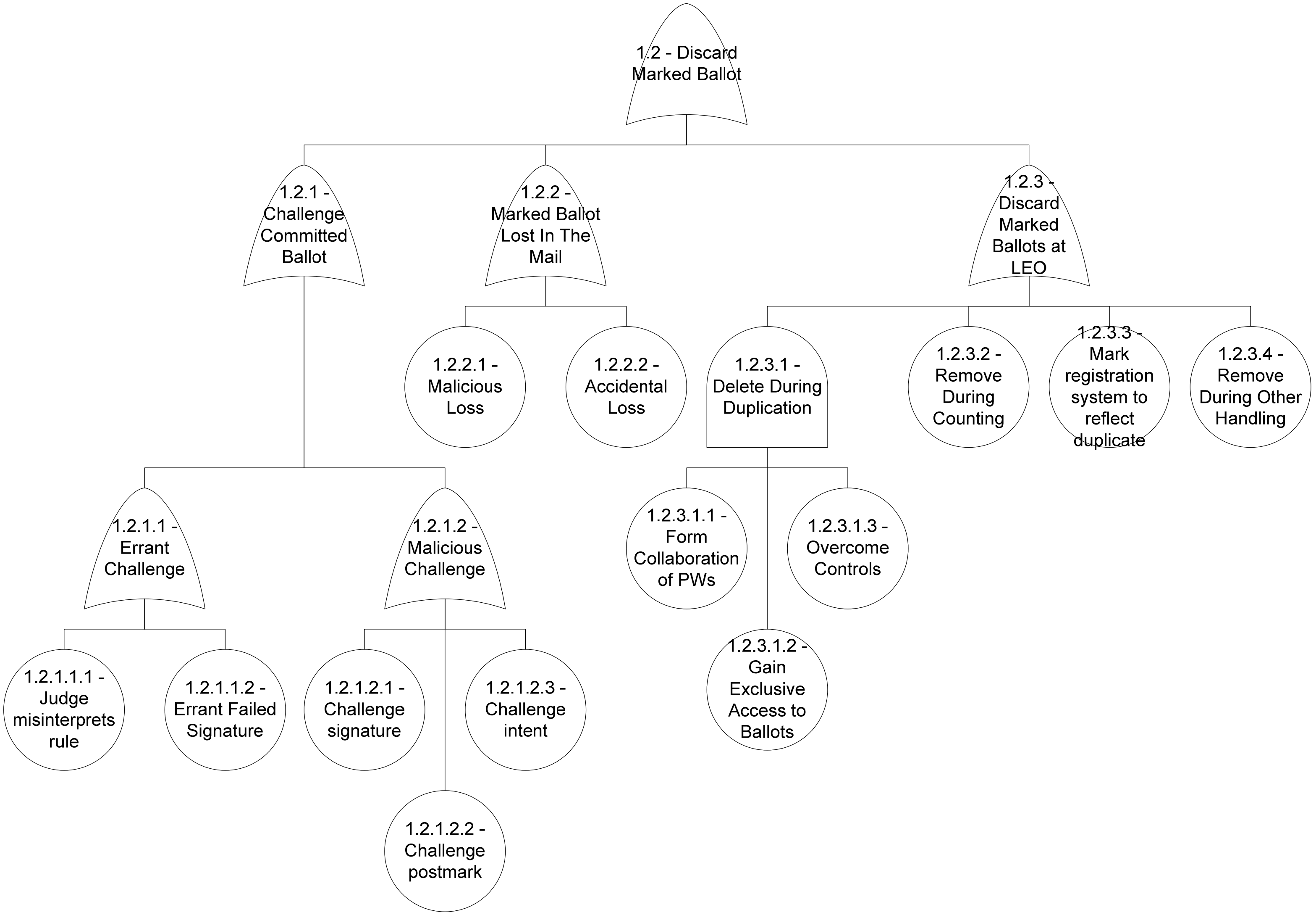
5-1 Vote by Mail Overview


1 - Insider attack
1.1 - Edit Marked Ballots
1.2 - Discard Marked Ballot
1.3 - Miscount Duplicated Ballots
1.4 - Marked Ballot Stuffing
1.5 - Manipulate or Discard Votable Ballot
1.1.1 - Edit at Local Elections Office
1.1.2 - Edit in Transit
1.2.1 - Challenge Committed Ballot
1.2.3 - Discard Marked Ballots at LEO
1.2.2 - Marked Ballot Lost In The Mail
1.3.1 - Count Original & Duplicate
1.3.2 - Omit Original & Duplicate
1.3.1.1 - File duplicate with duplicated ballot
1.3.1.2 - Defeat Ballot Accounting
1.5.1 - Delete at LEO
1.5.2 - Delay Delivery Past Deadline
1.5.3 - Delete at Destination
1.5.2.1 - Election Process Delay
1.5.2.3 - Delay in the Mail
1.5.2.2 - Handling Delay
1.4.1 - Insert ballots during envelope separation
1.4.3 - Insert ballots during recount
1.4.2 - Insert ballots during counting
1.4.4 - Insert ballots during audit
1.5.3.1 - Lost In Destination Mail Room
1.5.3.2 - Mail Box Attack
1.5.1.1 - Fail to stuff envelope
1.5.1.3 - Mis-address envelope
1.5.1.5 - Destroy batch of prepared envelopes
1.5.1.2 - Send wrong or premarked ballot
1.5.1.4 - Destroy prepared envelope

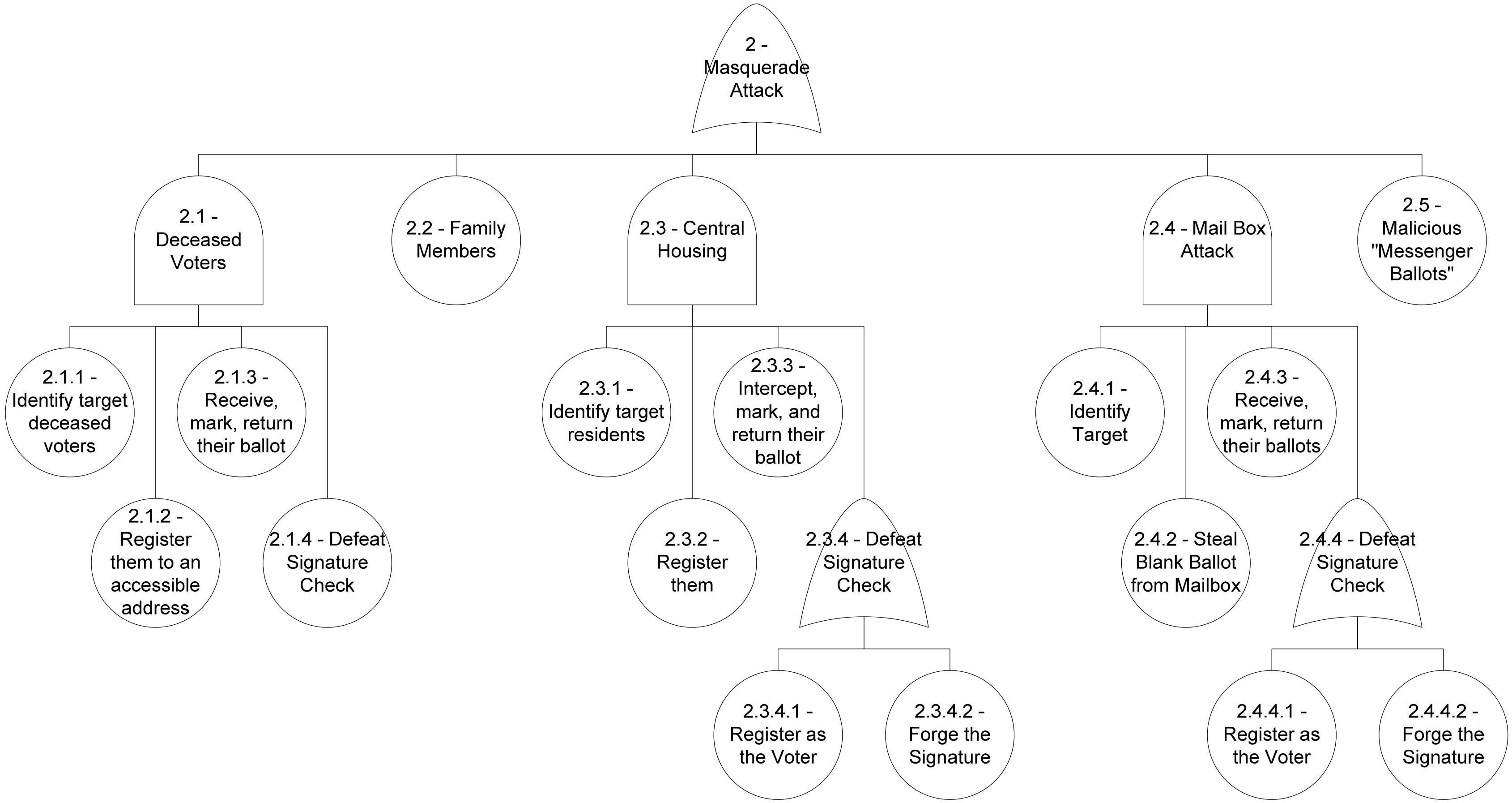
5-2 Vote by Mail Insider Attack


1.1 - Edit Marked Ballots
1.1.1 - Edit at Local Elections Office
1.1.2 - Edit in Transit
1.1.1.1 - Edit During Duplication
1.1.1.2 - Edit During Counting
1.1.1.3 - Edit During Other Handling
1.1.2.1 - Edit in Post Office
1.1.2.2 - Edit in intermediate mail room
1.1.1.1.1 - Form Collaboration of PWs
1.1.1.1.3 - Mark under/ overvotes or change votes
1.1.1.1.2 - Gain Exclusive Access to Ballots

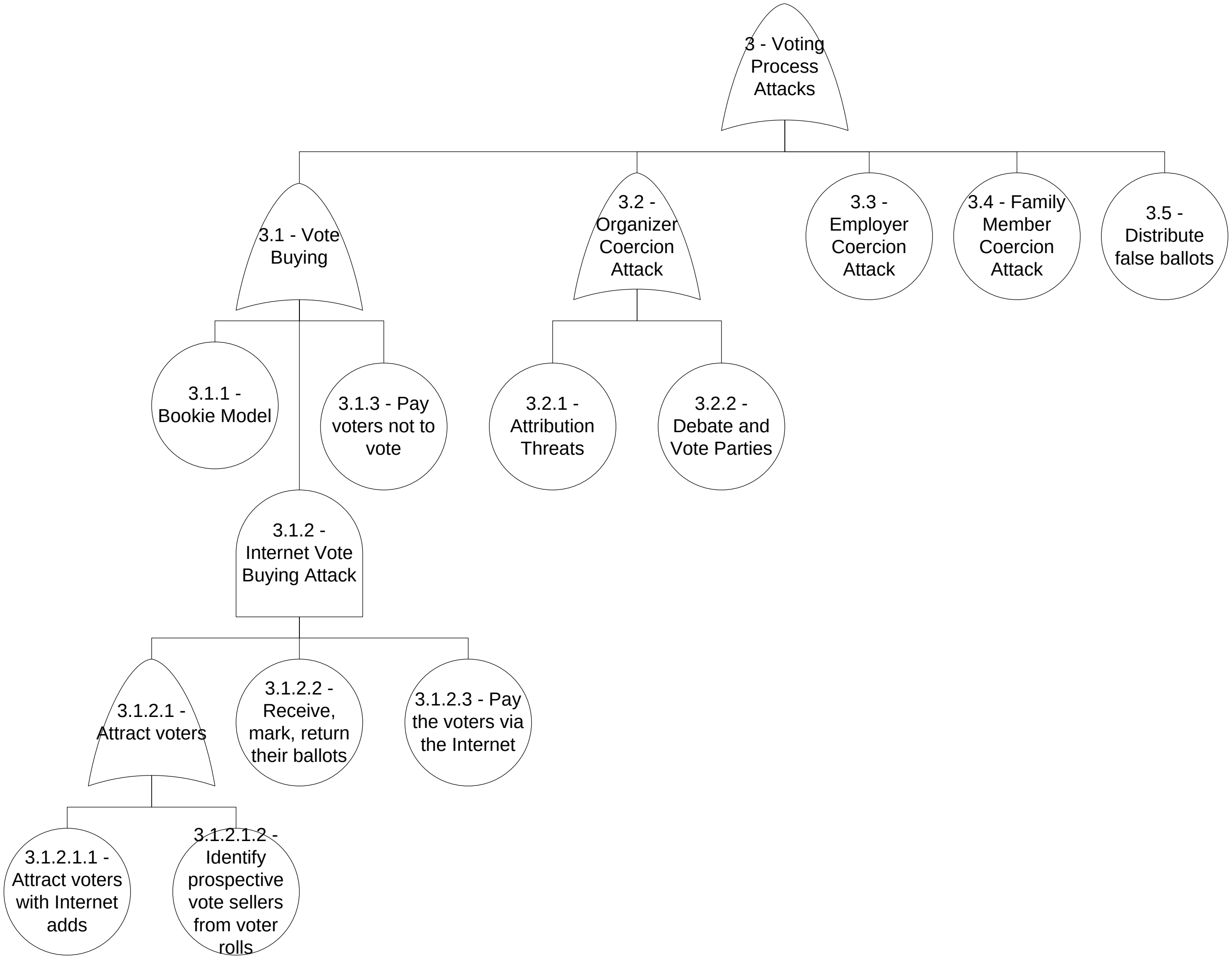
5-3 Vote by Mail Edit Marked Ballots


1.2 - Discard Marked Ballot
1.2.1 - Challenge Committed Ballot
1.2.2 - Marked Ballot Lost In The Mail
1.2.3 - Discard Marked Ballots at LEO
1.2.2.1 - Malicious Loss
1.2.2.2 - Accidental Loss
1.2.3.1 - Delete During Duplication
1.2.3.2 - Remove During Counting
1.2.3.3 - Mark registration system to reflect duplicate
1.2.3.4 - Remove During Other Handling
1.2.1.1 - Errant Challenge
1.2.1.2 - Malicious Challenge
1.2.3.1.1 - Form Collaboration of PWs
1.2.3.1.3 - Overcome Controls
1.2.3.1.2 - Gain Exclusive Access to Ballots
1.2.1.1.1 - Judge misinterprets rule
1.2.1.1.2 - Errant Failed Signature
1.2.1.2.1 - Challenge signature
1.2.1.2.3 - Challenge intent
1.2.1.2.2 - Challenge postmark

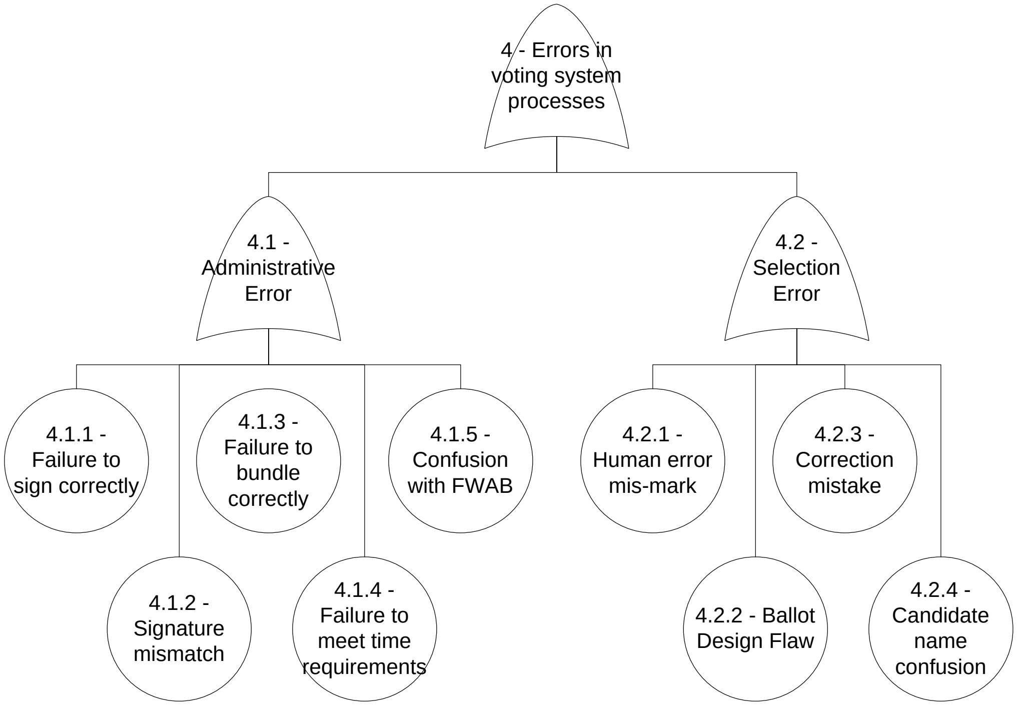
5-4 Vote by Mail Discard Marked Ballot


2 - Masquerade Attack
2.1 - Deceased Voters
2.2 - Family Members
2.3 - Central Housing
2.4 - Mail Box Attack
2.5 - Malicious "Messenger Ballots"
2.1.1 - Identify target deceased voters
2.1.2 - Register them to an accessible address
2.1.3 - Receive, mark, return their ballot
2.1.4 - Defeat Signature Check
2.3.1 - Identify target residents
2.3.2 - Register them
2.3.3 - Intercept, mark, and return their ballot
2.3.4 - Defeat Signature Check
2.3.4.1 - Register as the Voter
2.3.4.2 - Forge the Signature
2.4.1 - Identify Target
2.4.2 - Steal Blank Ballot from Mailbox
2.4.3 - Receive, mark, return their ballots
2.4.4 - Defeat Signature Check
2.4.4.1 - Register as the Voter
2.4.4.2 - Forge the Signature

5-5 Vote by Mail Masquerade Attack


3 - Voting Process Attacks
3.1 - Vote Buying
3.2 - Organizer Coercion Attack
3.3 - Employer Coercion Attack
3.4 - Family Member Coercion Attack
3.5 - Distribute false ballots
3.1.1 - Bookie Model
3.1.3 - Pay voters not to vote
3.2.1 - Attribution Threats
3.2.2 - Debate and Vote Parties
3.1.2 - Internet Vote Buying Attack
3.1.2.1 - Attract voters
3.1.2.2 - Receive, mark, return their ballots
3.1.2.3 - Pay the voters via the Internet
3.1.2.1.1 - Attract voters with Internet adds
3.1.2.1.2 - Identify prospective vote sellers from voter rolls

5-6 Vote by Mail Voting Process Attacks


4 - Errors in voting system processes
4.1 - Administrative Error
4.2 - Selection Error
4.1.1 - Failure to sign correctly
4.1.2 - Signature mismatch
4.1.3 - Failure to bundle correctly
4.1.4 - Failure to meet time requirements
4.1.5 - Confusion with FWAB
4.2.1 - Human error mis-mark
4.2.2 - Ballot Design Flaw
4.2.3 - Correction mistake
4.2.4 - Candidate name confusion

5-7 Vote by Mail Errors in Voting System Processes

5.3 Vote by Mail Threat Matrix

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1	Insider attack	Attack accomplished by an elections official or poll worker	Sherman	human-deliberate insider	Voting System	Voting System		(1) Two-person integrity rules (2) Background checks for all trusted parties.	
O	1.1	Edit Marked Ballots	Make or delete a mark on a marked ballot.		human-deliberate insider	Voting System	Marked Ballot	insider's access to ballots		
O	1.1.1	Edit at Local Elections Office	Edit during one of the VBM processing steps at the LEO		human-deliberate insider	Voting, Canvass	Marked Ballot	insider's access to ballots		
A	1.1.1.1	Edit During Duplication	Edit during the VBM ballots duplication process at the LEO.		human-deliberate insider	Process Remote Ballots	Marked Ballot	insider's access to ballots	(1) Two person integrity (2) Require independent oversight (3) Videotape duplication process (4) PW whistleblower program	
T	1.1.1.1.1	Form Collaboration of PWs	Form an alliance of PWs that will collude to edit ballots at the LEO.		human-deliberate insider	Election System	Poll worker	susceptibility to bribery and coercion	(1) Background check (2) Require worker-signed honesty statement (3) PW whistleblower program	
T	1.1.1.1.2	Gain Exclusive Access to Ballots	Isolate VBM ballots so that only colluding PWs are able to observe VBM ballots at the LEO.		human-deliberate insider	Process Remote Ballots	Marked Ballot	gaps in the chain of ballot custody procedures	(1) Two-person integrity rules (2) Rigorous protection procedures/facilities for marked ballots.	
T	1.1.1.1.3	Mark under/overvotes or change votes	Make selections in races that were not marked, or in races that were marked to create an overvote, or change votes if possible.		human-deliberate insider	Process Remote Ballots	Marked Ballot	access to ballots; inability to bind MarkedBallot to Voter	(1) Two person integrity (2) Require independent oversight (3) Videotape duplication process (4) PW whistleblower program	
T	1.1.1.2	Edit During Counting	Edit VBM ballots during the counting process at the LEO		human-deliberate insider	Process Remote Ballots	Marked Ballot	poor oversight, lack of transparency of counting process	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) PW whistleblower program	
T	1.1.1.3	Edit During Other Handling	Edit VBM ballots during other handling processes that are unique to VBM ballots at the LEO		human-deliberate insider	Voting System	Marked Ballot	lack of transparency, oversight; broken chain of ballot custody	(1) Two person integrity (2) Require independent oversight (3) Videotape handling process	
O	1.1.2	Edit in Transit	Edit VBM ballots in the mail or other delivery process.	NIST	human-deliberate insider	Ballot Delivery	Marked Ballot, Envelope	lack of physical protection/control of ballots	(1) Tamper-resistant envelopes (2) Legal deterrence	
T	1.1.2.1	Edit in Post Office	Edit VBM ballots at a Post Office where the ballot passes in transit from the voter to the LEO.	NIST	human-deliberate insider	Ballot Delivery	Marked Ballot, Envelope	lack of physical protection/control of ballots	(1) Tamper-resistant envelopes (2) Two person integrity for envelopes at the post office	
T	1.1.2.2	Edit in intermediate mail room	Edit VBM ballots at an intermediate mail room where the ballot passes in transit from the voter to the LEO.	NIST	human-deliberate insider	Ballot Delivery	Marked Ballot, Envelope	lack of physical protection/control of ballots	(1) Tamper-resistant envelopes	
O	1.2	Discard Marked Ballot	Steal, destroy, or otherwise preclude VBM ballots from tabulation.		human-deliberate insider	Process Remote Ballots	Marked Ballot	faulty validation process; personnel training or integrity issues; delivery failures	(1) Rigorous audit procedures for detection/deterrence	
O	1.2.1	Challenge Committed Ballot	Challenge a VBM ballot in order to prevent its tabulation		human-deliberate insider	Process Remote Ballots	Validate Remote Ballot	faulty validation process		
O	1.2.1.1	Errant Challenge	Accidently file an erroneous VBM ballot challenge		human-unintentional insider	Process Remote Ballots	Validate Remote Ballot	faulty validation process	(1) Clear challenge rules (2) Challenge rule training	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.1.1	Judge misinterprets rule	A judge challenges a VBM ballot in error because she misunderstands a rule		human-unintentional insider	Process Remote Ballots	Validate Remote Ballot	faulty validation process	(1) Clear challenge rules (2) Challenge rule training (3) Responsive escalation process	
T	1.2.1.1.2	Errant Failed Signature	A signature judge wrongly adjudicates that a ballot signature does not match the registration signature and prevents the ballot from being tabulated.		human-unintentional insider	Process Remote Ballots	Validate Remote Ballot	faulty validation process; poorly trained election officials	(1) Signature recognition training (2) Two person signature verification integrity (3) Escalation process for signature rejection	
O	1.2.1.2	Malicious Challenge	An attempt to prevent ballot tabulation by claiming that the voter/ballot violates an elections rule.		human-deliberate insider	Process Remote Ballots	Validate Remote Ballot	lack of integrity of election official	(1) Legal deterrence	
T	1.2.1.2.1	Challenge signature	Challenge a ballot because the voter's signature does not match the registration signature.		human-deliberate insider	Process Remote Ballots	Validate Remote Ballot	lack of integrity of election official	(1) Two person signature verification integrity (2) Escalation process for signature rejection	
T	1.2.1.2.2	Challenge postmark	Challenge a ballot because the postmark date does not satisfy the date requirement for the election.		human-deliberate insider	Process Remote Ballots	Validate Remote Ballot	lack of integrity of election official	(1) Two person postmark verification integrity (2) Escalation process for postmark rejection	
T	1.2.1.2.3	Challenge intent	Challenge a ballot because one or more marks do not satisfy the published mark standard.		human-deliberate insider	Process Remote Ballots	Validate Remote Ballot	lack of integrity of election official	(1) Use machine marking (2) Use marking template (3) Ignore unofficial marks	
O	1.2.2	Marked Ballot Lost In The Mail	A VBM ballot is destroyed or misplaced in the mail system.	Hackett	human-deliberate insider, human-unintentional insider	Ballot Delivery	Marked Ballot	lack of control over delivery process; inability to recover lost ballots	(1) Dual submit electronically (2) Utilize an independent tracking process. (3) Receipt-based courier	
T	1.2.2.1	Malicious Loss	A VBM ballot is intentionally destroyed or misplaced in the mail system.	NIST	human-deliberate insider	Ballot Delivery	Marked Ballot	lack of control over delivery process; inability to recover lost ballots	(1) Dual submit electronically (2) Utilize an independent tracking process. (3) Receipt-based courier with chain of custody	
T	1.2.2.2	Accidental Loss	A VBM ballot is unintentionally destroyed or misplaced in the mail system.	NIST	human-unintentional insider	Ballot Delivery	Marked Ballot	lack of control over delivery process; inability to recover lost ballots	(1) Dual submit electronically (2) Utilize an independent tracking process. (3) Receipt-based courier with chain of custody	
O	1.2.3	Discard Marked Ballots at LEO	A marked ballot is lost, destroyed, or disposed of at the LEO.		human-deliberate insider	Process Remote Ballots	Marked Ballot	insider's access to ballots	(1) Two person integrity (2) Use rigorous chain of custody protection	
A	1.2.3.1	Delete During Duplication	A marked ballot is destroyed or disposed of during the ballot duplication process.	Yasinsac	human-deliberate insider	Process Remote Ballots	Marked Ballot	insider's access to ballots	(1) Two person integrity (2) Use rigorous chain of custody protection (3) Require independent oversight (3) video tape duplication	
T	1.2.3.1.1	Form Collaboration of PWs	Form an alliance of PWs that will collude to edit ballots at the LEO.		human-deliberate insider	Election System	Poll worker	susceptibility to bribery and coercion	(1) Background check (2) Require worker-signed honesty statement.	
T	1.2.3.1.2	Gain Exclusive Access to Ballots	Isolate ballots so that only colluding PWs are able to observe VBM ballots at the LEO.		human-deliberate insider	Process Remote Ballots	Marked Ballot	gaps in the chain of ballot custody procedures	(1) Two-person integrity rules (2) Rigorous protection procedures/facilities for marked ballots.	
T	1.2.3.1.3	Overcome Controls	Implement procedures to overcome chain of custody or other controls.		human-deliberate insider	Process Remote Ballots	Marked Ballot	gaps in the chain of ballot custody procedures		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.3.2	Remove During Counting	Remove ballots during the counting process at the LEO		human-deliberate insider	Process Remote Ballots	Marked Ballot	poor oversight, lack of transparency of counting process	(1) Chain of custody (2) Two person integrity (3) Rigorous oversight	
T	1.2.3.3	Mark registration system to reflect duplicate	Attacker manipulates the registration system to reflect that the voter cast another, overriding ballot.		human-deliberate insider	Process Remote Ballots	Marked Ballot	Weak registration system protection	(1) Strong security protection for registration system	
T	1.2.3.4	Remove During Other Handling	Remove ballots during other handling processes at the LEO	Yasinsac	human-deliberate insider	Voting System	Marked Ballot	lack of transparency, oversight; broken chain of ballot custody	(1) Chain of custody (2) Two person integrity (3) Rigorous oversight	
O	1.3	Miscount Duplicated Ballots	Cause duplicated ballots to be incorrectly tabulated.		human-deliberate insider	Process Remote Ballots	Precinct Data	lack of transparency, oversight	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process	
A	1.3.1	Count Original & Duplicate	Cause both duplicate and duplicated ballots to be tabulated.	Yasinsac	human-deliberate insider	Process Remote Ballots	Precinct Data	lack of transparency, oversight	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) Audit via ballot accounting	
T	1.3.1.1	File duplicate with duplicated ballot	Cause both duplicate and duplicated ballots to be stored as counted ballots.	Yasinsac	human-deliberate insider	Process Remote Ballots	Precinct Data	lack of transparency, oversight	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) Audit via ballot accounting	
T	1.3.1.2	Defeat Ballot Accounting	Cause confusion or inconsistencies in ballot accounting procedures.		human-deliberate insider	Ballot Box Accounting	Precinct Data	lack of transparency, oversight	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process	
T	1.3.2	Omit Original & Duplicate	Cause both duplicate and duplicated ballots to be stored as spoiled ballots.		human-deliberate insider	Process Remote Ballots	Duplicated Ballot, Duplicate Ballot	lack of transparency, oversight; inability to detect or recover	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) Audit via ballot accounting	
O	1.4	Marked Ballot Stuffing	Insert illegitimate ballots into tabulation.	Sherman	human-deliberate insider	Process Remote Ballots	Precinct Data	lack of transparency, oversight; inability to detect or recover	(1) Two person integrity (2) Require independent oversight (3) Audit via ballot accounting	
T	1.4.1	Insert ballots during envelope separation	During envelope separation, workers may be able to insert pre-marked ballots into tabulation unnoticed.		human-deliberate insider	Process Remote Ballots	Precinct Data	lack of transparency, oversight; inability to detect or recover	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	
T	1.4.2	Insert ballots during counting	During VBM counting, workers may be able to insert pre-marked ballots into tabulation unnoticed.		human-deliberate insider	Process Remote Ballots	Precinct Data	lack of transparency, oversight; inability to detect or recover	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	
T	1.4.3	Insert ballots during recount	During a recount, workers may be able to insert pre-marked ballots into tabulation unnoticed.		human-deliberate insider	Recount	Jurisdiction Results	lack of transparency, oversight; inability to detect or recover	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	
T	1.4.4	Insert ballots during audit	During an audit workers may be able to insert pre-marked ballots into tabulation unnoticed.		human-deliberate insider	Contest Audit	Audit Results	lack of transparency, oversight; inability to detect or recover	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	
O	1.5	Manipulate or Discard Votable Ballot	Prevent distribution of a votable ballot to a valid VBM voter.	Hackett	human-deliberate insider	Process Remote Ballots	Votable Ballot	faulty validation process; personnel training or integrity issues; delivery failures	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.5.1	Delete at LEO	Take action at the LEO that prevents a votable ballot from being distributed to a legitimate VBM voter.		human-deliberate insider	Ballot Preparation	Votable Ballot	faulty validation process; personnel training or integrity issues; delivery failures	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	
T	1.5.1.1	Fail to stuff envelope	During VBM envelope preparation, prepare an envelope for mailing without inserting a votable ballot.		human-deliberate insider	Create Votable Ballots	Votable Ballot	faulty validation process; personnel training or integrity issues; delivery failures	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	
T	1.5.1.2	Send wrong or premarked ballot	During VBM envelope preparation, prepare an envelope for mailing with a votable ballot that for other than the voter's precinct.		human-deliberate insider	Create Votable Ballots	Votable Ballot	faulty validation process; personnel training or integrity issues; delivery failures	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	
T	1.5.1.3	Mis-address envelope	During VBM envelope preparation, prepare an envelope for mailing with an errant address.		human-deliberate insider	Create Votable Ballots	Votable Ballot	faulty validation process; personnel training or integrity issues	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	
T	1.5.1.4	Destroy prepared envelope	During VBM envelope preparation, destroy or dispose of a previously prepared envelope.		human-deliberate insider	Voting, Issue Ballot (R)	Votable Ballot	faulty validation process; personnel training or integrity issues	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation (4) Chain of custody	
T	1.5.1.5	Destroy batch of prepared envelopes	During VBM envelope preparation, destroy or dispose of a batch of previously prepared envelopes.		human-deliberate insider	Voting, Issue Ballot (R)	Votable Ballot	faulty validation process; personnel training or integrity issues	(1) Two person integrity (2) Require independent oversight (3) Chain of custody	
O	1.5.2	Delay Delivery Past Deadline	Delay delivery of prepared VBM envelopes to the post office.		operational	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures		
T	1.5.2.1	Election Process Delay	Cause election events that delay VBM ballot preparation.		operational	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures		
T	1.5.2.2	Handling Delay	VBM ballot handling problem that delays envelope delivery.	Pew	operational	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures		
T	1.5.2.3	Delay in the Mail	Mail event that delays delivery of prepared VBM envelopes to valid voters.	Pew	operational	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures		
O	1.5.3	Delete at Destination	Delete or destroy VBM ballots after they reach their postal destination.	NIST	human-deliberate insider	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures	(1) Remote ballot status process	
T	1.5.3.1	Lost In Destination Mail Room	VBM ballot/envelope misplaced or destroyed at an intermediate mail room after deliver from the postal system.	NIST	human-unintentional insider	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures	(1) Remote ballot status process	
T	1.5.3.2	Mail Box Attack	Remove VBM ballot/ envelope from the voter's mailbox.	NIST	human-deliberate	Voting, Issue Ballot (R)	Votable Ballot	personnel training or integrity issues; delivery failures	(1) Remote ballot status process (2) Strong ballot fraud legal deterrence	
O	2	Masquerade Attack	Vote for a legitimate voter other than yourself.	Sherman	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong vote attribution procedures	
A	2.1	Deceased Voters	Cast a VBM ballot using a deceased voter's identity.	Estep	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Accurate voter rolls (2) Strong vote attribution procedures	
T	2.1.1	Identify target deceased voters	Match voter rolls against online obituary entries or identify deceased voters for whom they can register.		human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Accurate voter rolls	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.1.2	Register them to an accessible address	Register the identified deceased voter to an address where the attacker can easily retrieve the delivered VBM votable ballot.		human-deliberate	Request Ballot ®	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong voter authentication	
T	2.1.3	Receive, mark, return their ballot			human-deliberate	Provide Credentials (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong legal deterrence	
T	2.1.4	Defeat Signature Check	The primary mechanism used to verify identity is a signature check. Overcoming that control allows successful masquerade.		human-deliberate	Authenticate Voter (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Signature match training	
T	2.2	Family Members	Cast a VBM ballot using a family member's identity or alter a family member's ballot.		human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong vote attribution procedures	
A	2.3	Central Housing	Cast a VBM ballot using a cohabitant of a central housing facility's identity.	Sherman	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong vote attribution procedures	
T	2.3.1	Identify target residents	Identify residents that are legitimate voters that are unlikely to vote, and from whom you can acquire their VBM materials.	Sherman	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong legal deterrence	
T	2.3.2	Register them	Represent yourself as a cohabiting voter by filing registration forms in their name.	Sherman	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong voter authentication	
T	2.3.3	Intercept, mark, and return their ballot	Intercept, mark, and return their ballot	Yasinsac	human-deliberate	Provide Credentials (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong vote attribution procedures	
O	2.3.4	Defeat Signature Check	The primary mechanism used to verify identity is a signature check. Overcoming that control allows successful masquerade.	Yasinsac	human-deliberate	Authenticate Voter (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Signature match training	
T	2.3.4.1	Register as the Voter	Represent yourself as a cohabiting voter by filing registration forms in their name.	Sherman	human-deliberate	Request Ballot (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong voter authentication	
T	2.3.4.2	Forge the Signature	Forge the Signature	Yasinsac	human-deliberate	Provide Credentials (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong voter authentication, (2) Signature match training	
A	2.4	Mail Box Attack	Remove VBM ballot/ envelope from the voter's mailbox.		human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Remote ballot status process (2) Strong ballot fraud legal deterrence	
T	2.4.1	Identify Target	Identify residents that are legitimate voters that are unlikely to vote, and from whom you can acquire their VBM materials.	Estep	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	None	
T	2.4.2	Steal Blank Ballot from Mailbox	Steal Blank Ballot from Mailbox	Yasinsac	human-deliberate	Voter checking (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong legal deterrence	
T	2.4.3	Receive, mark, return their ballots	Receive, mark, return their ballots	Yasinsac	human-deliberate	Provide Credentials (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong voter authentication, (2) Signature match training	
O	2.4.4	Defeat Signature Check	The primary mechanism used to verify identity is a signature check. Overcoming that control allows successful masquerade.		human-deliberate	Authenticate Voter (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong legal deterrence	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.4.4.1	Register as the Voter	Represent yourself as a cohabiting voter by filing registration forms in their name.	Sherman	human-deliberate	Request Ballot (R)	Remote voter	personnel training or integrity issues; faulty authentication	(1) Strong legal deterrence	
T	2.4.4.2	Forge the Signature	Forge the Signature	Yasinsac	human-deliberate	Provide Credentials (R)	Remote voter	personnel training or integrity issues; faulty authentication	(1) Strong legal deterrence	
T	2.5	Malicious Messenger Ballots	Messenger ballots allow voters to designate another voter to pick transport votable and marked ballots in their name. Attacker may [illegally] solicit applications for ballots from others and designate themselves as the authorized messenger, but vote the ballot them self.	Sherman	human-deliberate	Provide Credentials (R)	Remote voter	weak voter authentication	Strong voter authentication	
O	3	Voting Process Attacks			human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
O	3.1	Vote Buying	Attacker pays a voter to make a particular selection. Requires vote attribution.	Estep	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	
T	3.1.1	Bookie Model	Attacker attracts vote sellers via word of mouth and conducts transactions individually. VBM ballots are viewed by attacker, who seals and mails envelope.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	
A	3.1.2	Internet Vote Buying Attack	Attacker uses Internet capabilities to reach masses and to overcome legal deterrence.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	
O	3.1.2.1	Attract voters	Vote buyers must find eligible voters that are willing to sell their vote.	Estep	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	3.1.2.1.1	Attract voters with Internet adds	Attacker attracts vote sellers through blogs, message boards, Internet ads, etc.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	3.1.2.1.2	Identify prospective vote sellers from voter rolls	Attacker utilizes voter rolls to identify prospective vote sellers.	Estep	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	3.1.2.2	Receive, mark, return their ballots	Attacker marks or verifies marked ballots and ensures that they are mailed.		human-deliberate	Voting	Remote voter	susceptibility to bribery and coercion	(1) Strong voter authentication, (2) Signature match training	
T	3.1.2.3	Pay the voters via the Internet	Voters may be paid via any of several Internet payment companies.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	3.1.3	Pay voters not to vote	An attacker may gain advantage on a particular contest by incentivizing some voters not to vote.	Hasen	human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
O	3.2	Organizer Coercion Attack	An organizer may be a government organization or public group.	Hester	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	
T	3.2.1	Attribution Threats	An organizer may intimidate voters by claiming that they can identity voter selections.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting process (2) Strong legal deterrence	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.2.2	Debate and Vote Parties	Groups may encourage members to bring their blank VBM ballots to parties and apply peer pressure to influence their selections.	Johnson	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting process (2) Strong legal deterrence	
T	3.3	Employer Coercion Attack	Employer Coercion Attack		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting process (2) Strong legal deterrence	
T	3.4	Family Member Coercion Attack	Voter is coerced by a family member to make selections other than their own intent.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting process (2) Strong legal deterrence	
T	3.5	Distribute false ballots	Attacker sends fake ballots to targeted voters as a denial of service.		human-deliberate	Election System	Remote voter	Limited two-way authentication	(1) Voter education (2) Strong branding (3) Legal deterrence	
O	4	Errors in voting system processes		Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Simple, rigorously tested user interface	
O	4.1	Administrative Error	Many VBM ballots are disqualified for administrative errors, preventing otherwise legitimate VBM ballots from being tabulated.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Clear rules (2) Simple procedures (3) Explicit instructions	
T	4.1.1	Failure to sign correctly	Since signature matching is the primary VBM authentication method, rules may be precisely enforced, so even minor deviations may disqualify an otherwise legitimate VBM ballot.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Clear rules (2) Simple procedures (3) Explicit instructions	
T	4.1.2	Signature mismatch	Signature deviations and errors by officials can cause erroneous mismatch disqualifications that prevent legitimate VBM ballots from being tabulated.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Signature match training (2) Signature mis-match escalation procedure	
T	4.1.3	Failure to bundle correctly	Instructions for what must be returned and how it must be packaged may be confusing and may be precisely enforced, preventing otherwise legitimate VBM ballots from being tabulated.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Clear rules (2) Simple procedures (3) Explicit instructions	
T	4.1.4	Failure to meet time requirements	VBM voters may not be able to meet VBM ballot receipt deadlines due to circumstances beyond their control, thus preventing legitimate VBM ballots from being tabulated	Pew	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Early preparation (2) Status check process (3) Minimized the number of steps (4) Minimize duration of each step	
T	4.1.5	Confusion with FWAB	Voters may misunderstand confusing FWAB instructions, preventing legitimate VBM ballots from being tabulated.	Pew	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Voter education (2) Simplify FWAB	
O	4.2	Selection Error	Voter selection does not match their intent.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Simple, rigorously tested user interface	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.2.1	Human error mis-mark	Voter marks the wrong selection indicator, i.e. does not properly match the selection indicator to their preferred choice.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Simple, rigorously tested user interface	
T	4.2.2	Ballot Design Flaw	The ballot structure or presentation causes voters to make selection errors.		human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Simple, rigorously tested ballot design	
T	4.2.3	Correction mistake	If a VBM voter fails to follow instructions when making a correction, the ballot may be rejected.	Yasinsac	human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Clear rules (2) Simple procedures (3) Explicit instructions	
T	4.2.4	Candidate name confusion	A VBM voter may confuse candidate names on long ballots.		human-unintentional	Voting System	Remote voter	faulty validation process; poorly trained election officials	(1) Voter Education	

6 Vote by Phone

Vote by Phone is a VotingSystem that utilizes the telephone system to deliver a VotableBallot to the voter and to capture voter selections. While Vote by Phone may be used for remote voting, its primary deployment today is as a polling place voting system to support disabled voter access.

Vote By Phone's distinctive properties are that:

(1) It delivers the VotableBallot to the voter via recorded voice,

(2) It captures the voter's selections through the voter's telephone operation, i.e. either key pad operation or voice response, and

(3) It constructs the electronic MarkedBallot on the voting server.

As an inherently electronic voting system, Vote y Phone is prospectively susceptible to the full spectrum of electronic voting system threats.

6.1 Vote by Phone Threat Tree

node type - outline number - threat action

O	1	Attack on Voting Equipment
A	1.1	Phone Device Malware
A	1.1.1	Create the Malware
O	1.1.1.1	Design the Attack
T	1.1.1.1.1	Flip Votes
T	1.1.1.1.2	Create Undervote
O	1.1.1.1.3	Deny Service
T	1.1.1.1.3.1	
T	1.1.1.1.3.2	
T	1.1.1.1.3.3	
T	1.1.1.2	Gain Necessary Knowledge
A	1.1.1.3	Test the Malware
T	1.1.1.3.1	Replicate the Environment
T	1.1.1.3.2	Simulate System Load
O	1.1.2	Install the Malware
T	1.1.2.1	Removable Media
T	1.1.2.2	Vendor Installed
T	1.1.2.3	During L&A
O	1.1.3	Trigger the Malware
T	1.1.3.1	Time Trigger
T	1.1.3.2	Event Trigger
O	1.2	Network Attack
O	1.2.1	Denial of Service
T	1.2.1.1	Flood Voting Device
T	1.2.1.2	Flood voting server
T	1.2.1.3	Flood Supporting Network
T	1.2.1.4	Destroy Voting Component
A	1.2.2	Man in the Middle / Pharming
T	1.2.2.1	Design the Attack
T	1.2.2.2	Compromise Network Device
T	1.2.2.3	Intercept Voter Transaction

- T 1.2.2.4 Insert Manipulated Transaction
- O 1.3 Voting Server Attack
  - T 1.3.1 Malicious Admin Account
  - T 1.3.2 Denial of Service
  - A 1.3.3 Voting Server Malware
    - O 1.3.3.1 Install the Malware
      - T 1.3.3.1.1 Removable Media
      - T 1.3.3.1.2 Botnet
      - T 1.3.3.1.3 Vendor Installed
      - T 1.3.3.1.4 During L&A
    - O 1.3.3.2 Trigger the Malware
- T 1.4 Alter Ballot Creation Software
- O 2 Voting Process Attack
  - A 2.1 Phishing Attack
    - T 2.1.1 Attract the Voter
    - T 2.1.2 Alter the Voting Session
  - O 2.2 Voter Impersonation Attack
    - T 2.2.1 Steal Voters' Passwords
    - A 2.2.3 Automate Voting
      - 2.2.3.1 Identify an automatable voter authentication attack.
      - T 2.2.3.2 Develop the Attack Software
      - T 2.2.3.3 Identify Unlikely Voters
      - T 2.2.3.4 Steal Voters' Credentials
      - T 2.2.4.5 Implement the Attack
      - T 2.2.4.6 Trigger the Attack
  - O 2.3 Vote Attribution Attack
    - A 2.3.1 Vote Buying
      - T 2.3.1.1 Recruit Brokers
      - T 2.3.1.2 Identify Prospective Sellers
      - T 2.3.1.3 Send Instructions
      - O 2.3.1.4 Verify the Vote
        - T 2.3.1.4.1 Eavesdrop on the Phone Line
        - T 2.3.1.4.2 Eavesdrop at Voting Server
      - T 2.3.1.5 Make the Payment
    - T 2.3.2 Voter Coercion
    - T 2.3.3 Pay Voter Not to Vote
  - T 2.4 Exhaust Authentication Threshold
  - A 2.5 Cast Multiple Ballots
    - T 2.5.1 Defeat Phone Authorization
    - T 2.5.2 Use Credential Multiple Times
- O 3 Insider Attacks
  - O 3.1 Install Malware
    - T 3.1.1 During Development
    - A 3.1.2 During Install / Test
      - T 3.1.2.1 Gain Necessary Knowledge
      - T 3.1.2.2 Hire Inside Collaborator
      - T 3.1.2.3 Acquire Artifacts for Study
    - T 3.1.3 During Voting Period
    - T 3.1.4 After Voting Period
  - O 3.2 Non-malware attacks
    - T 3.2.1 Manipulate Ballot Definition
    - T 3.2.2 Denial of Service
    - T 3.2.3 Manipulate Voted Ballots

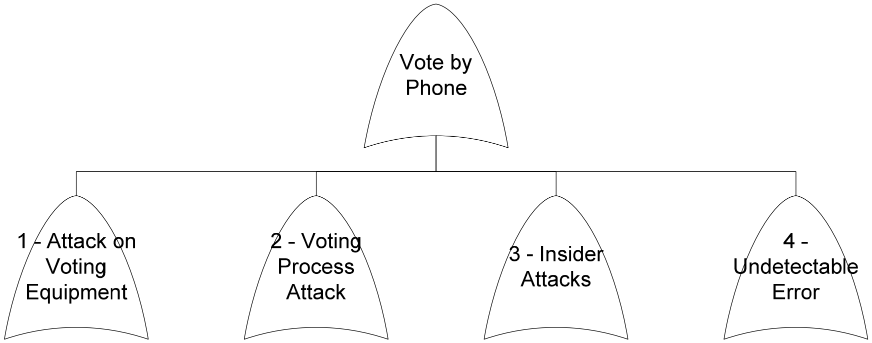
- T 3.2.4 Flip Votes
- T 3.2.5 Create Undervote
- T 3.2.6 Delete Contests/Candidates
- T 3.2.7 Manipulate Accumulation Data
- T 3.2.8 Manipulate Audit Data

T 3.3 Manipulate Randomization

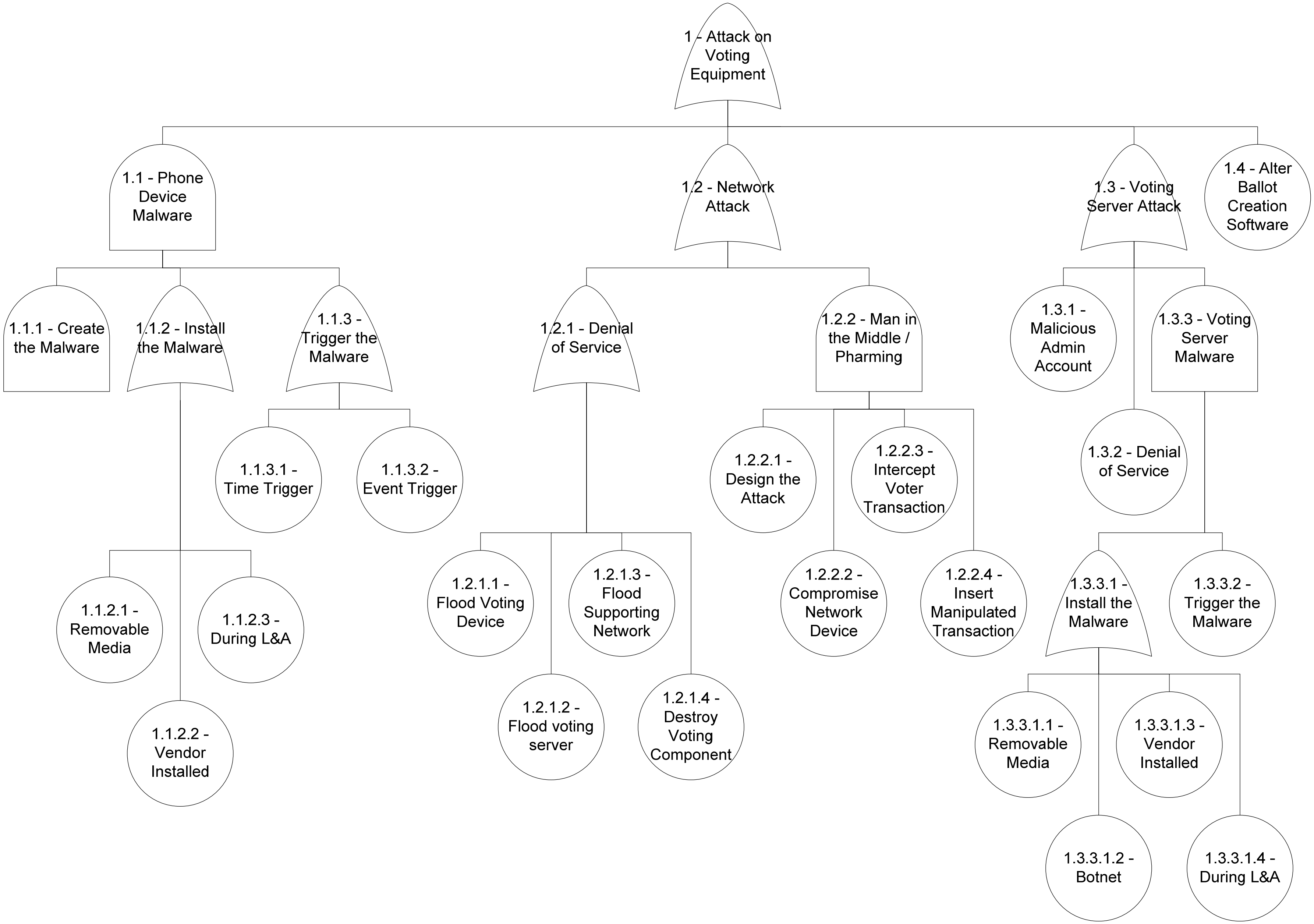
O 4 Undetectable Error

- T 4.1 Human Error Mis-selection
- T 4.2 Ballot Design Flaw
- T 4.3 Name Confusion

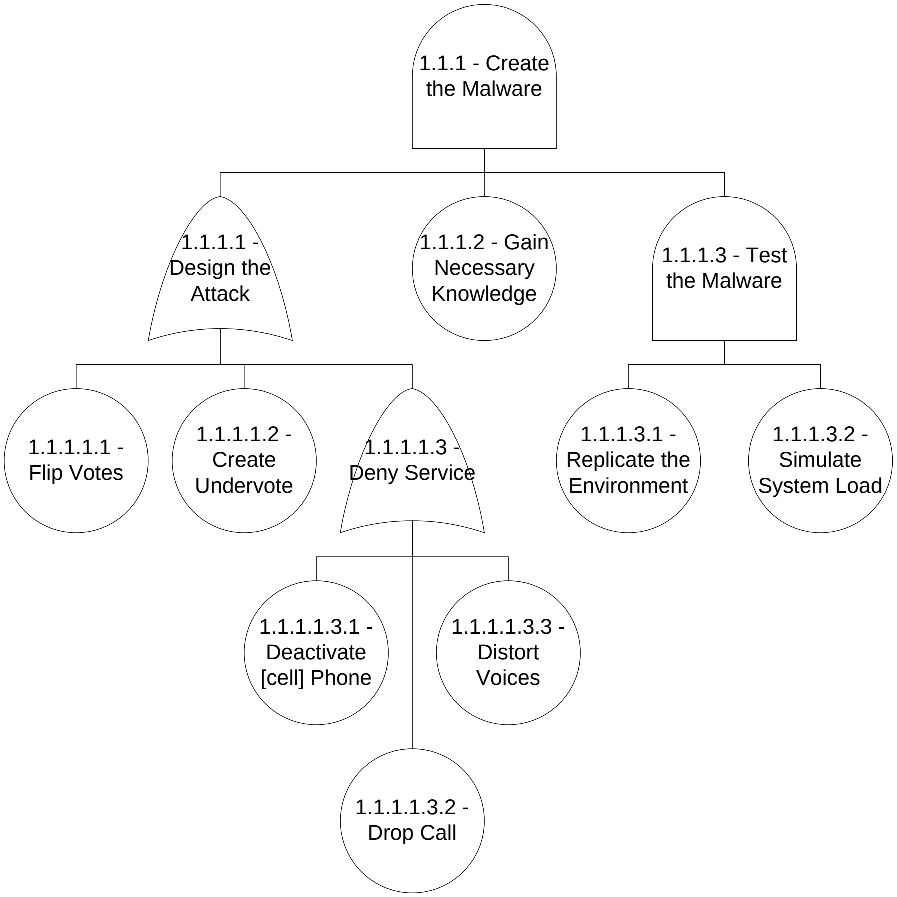
6.2 Vote by Phone Threat Tree – Graphic



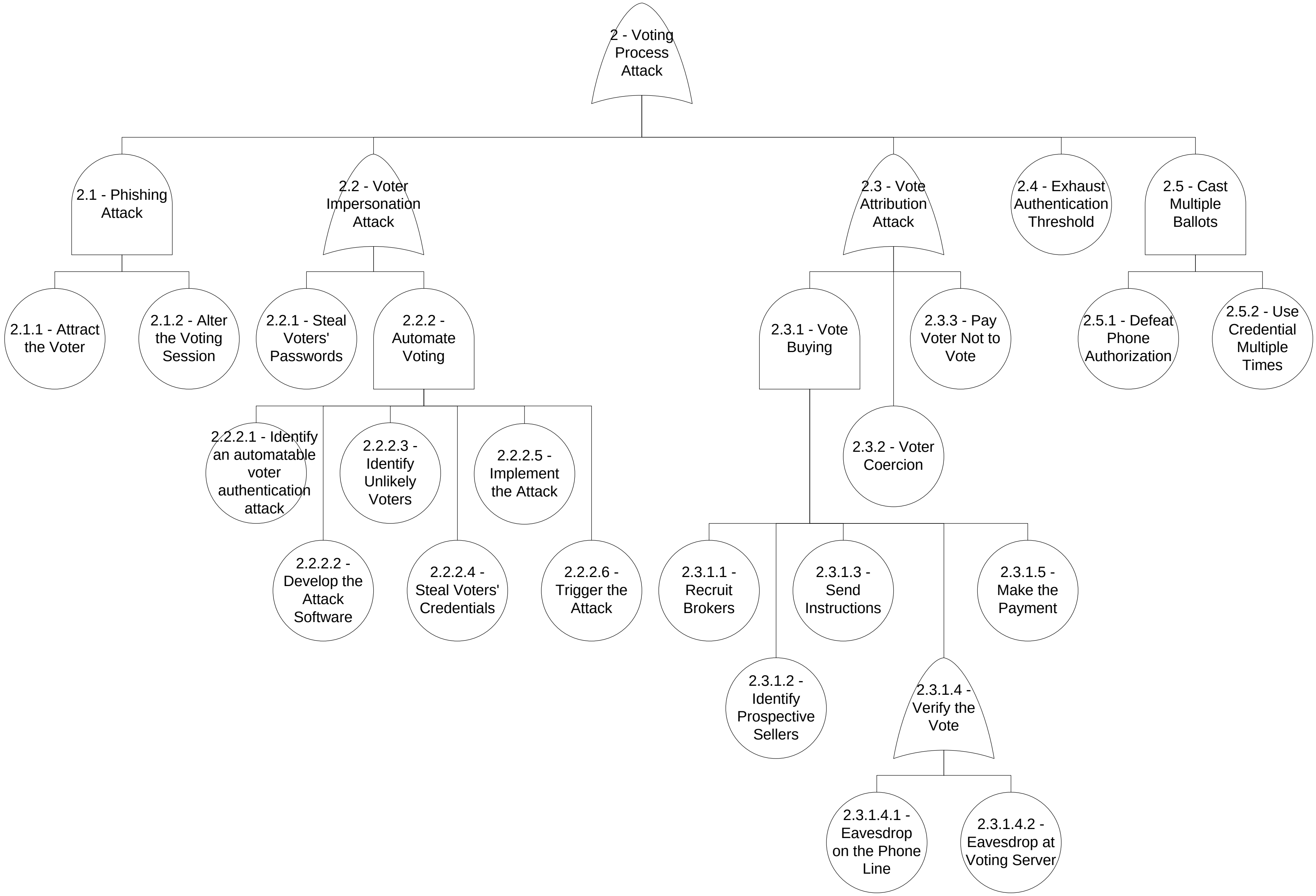
6-1 Vote by Phone Overview


1 - Attack on Voting Equipment
1.1 - Phone Device Malware
1.2 - Network Attack
1.3 - Voting Server Attack
1.4 - Alter Ballot Creation Software
1.1.1 - Create the Malware
1.1.2 - Install the Malware
1.1.3 - Trigger the Malware
1.2.1 - Denial of Service
1.2.2 - Man in the Middle / Pharming
1.3.1 - Malicious Admin Account
1.3.3 - Voting Server Malware
1.1.3.1 - Time Trigger
1.1.3.2 - Event Trigger
1.2.2.1 - Design the Attack
1.2.2.3 - Intercept Voter Transaction
1.3.2 - Denial of Service
1.2.1.1 - Flood Voting Device
1.2.1.3 - Flood Supporting Network
1.2.2.2 - Compromise Network Device
1.2.2.4 - Insert Manipulated Transaction
1.3.3.1 - Install the Malware
1.3.3.2 - Trigger the Malware
1.1.2.1 - Removable Media
1.1.2.3 - During L&A
1.2.1.2 - Flood voting server
1.2.1.4 - Destroy Voting Component
1.3.3.1.1 - Removable Media
1.3.3.1.3 - Vendor Installed
1.1.2.2 - Vendor Installed
1.3.3.1.2 - Botnet
1.3.3.1.4 - During L&A

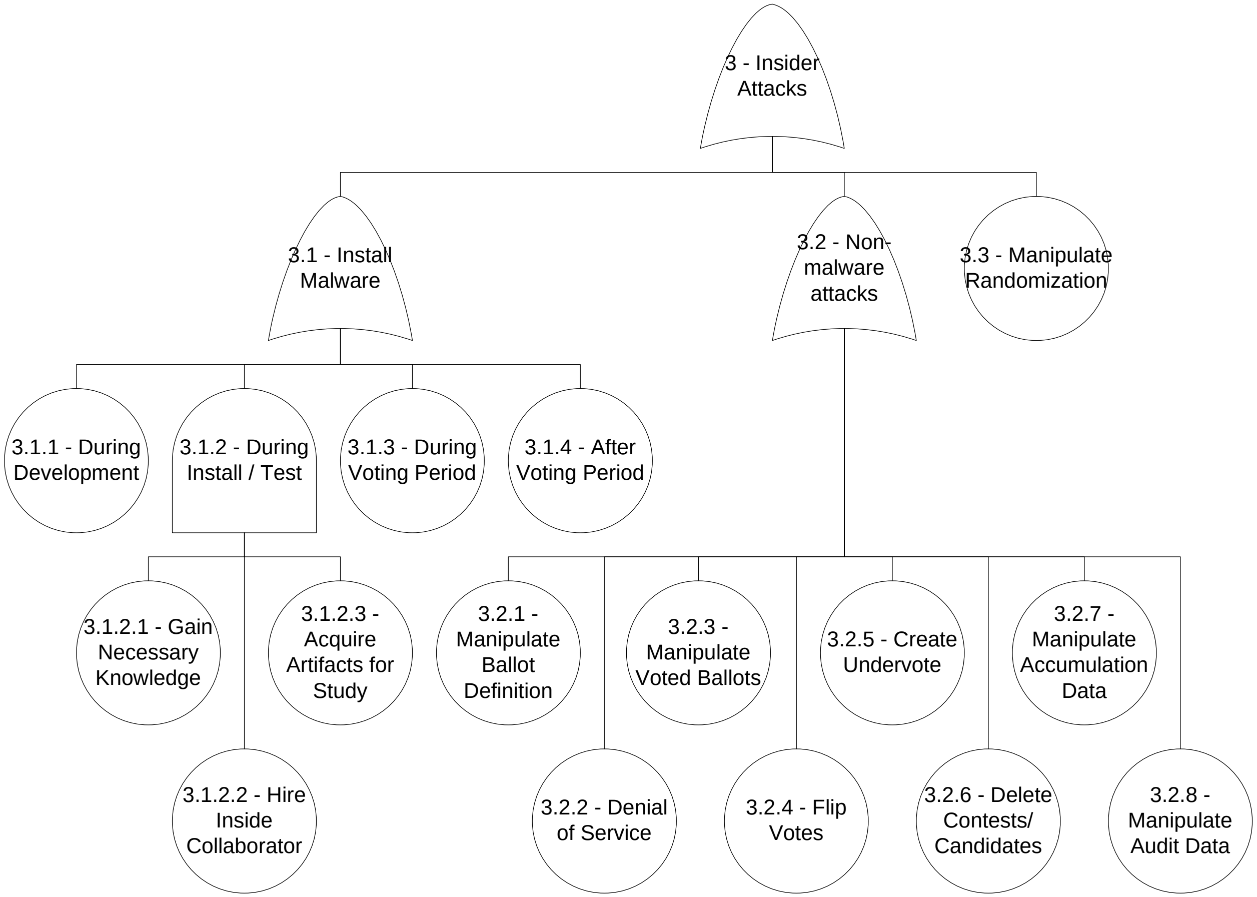
6-2 Vote by Phone Attack on Voting Equipment


1.1.1 - Create the Malware
1.1.1.1 - Design the Attack
1.1.1.2 - Gain Necessary Knowledge
1.1.1.3 - Test the Malware
1.1.1.1.1 - Flip Votes
1.1.1.1.2 - Create Undervote
1.1.1.1.3 - Deny Service
1.1.1.3.1 - Replicate the Environment
1.1.1.3.2 - Simulate System Load
1.1.1.1.3.1 - Deactivate [cell] Phone
1.1.1.1.3.3 - Distort Voices
1.1.1.1.3.2 - Drop Call

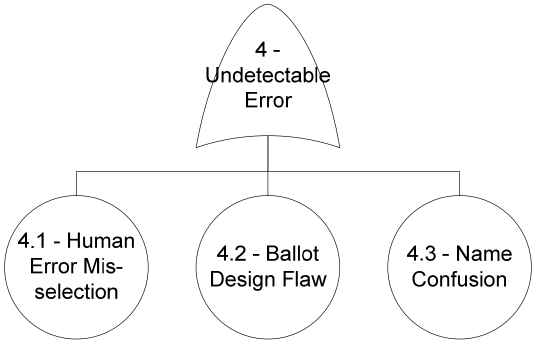
6-3 Vote by Phone Create Malware


2 - Voting Process Attack
2.1 - Phishing Attack
2.1.1 - Attract the Voter
2.1.2 - Alter the Voting Session
2.2 - Voter Impersonation Attack
2.2.1 - Steal Voters' Passwords
2.2.2 - Automate Voting
2.2.2.1 - Identify an automatable voter authentication attack
2.2.2.2 - Develop the Attack Software
2.2.2.3 - Identify Unlikely Voters
2.2.2.4 - Steal Voters' Credentials
2.2.2.5 - Implement the Attack
2.2.2.6 - Trigger the Attack
2.3 - Vote Attribution Attack
2.3.1 - Vote Buying
2.3.1.1 - Recruit Brokers
2.3.1.2 - Identify Prospective Sellers
2.3.1.3 - Send Instructions
2.3.1.4 - Verify the Vote
2.3.1.4.1 - Eavesdrop on the Phone Line
2.3.1.4.2 - Eavesdrop at Voting Server
2.3.1.5 - Make the Payment
2.3.2 - Voter Coercion
2.3.3 - Pay Voter Not to Vote
2.4 - Exhaust Authentication Threshold
2.5 - Cast Multiple Ballots
2.5.1 - Defeat Phone Authorization
2.5.2 - Use Credential Multiple Times

6-4 Vote by Phone Voting Process Attacks


3 - Insider Attacks
3.1 - Install Malware
3.2 - Non-malware attacks
3.3 - Manipulate Randomization
3.1.1 - During Development
3.1.2 - During Install / Test
3.1.3 - During Voting Period
3.1.4 - After Voting Period
3.1.2.1 - Gain Necessary Knowledge
3.1.2.3 - Acquire Artifacts for Study
3.1.2.2 - Hire Inside Collaborator
3.2.1 - Manipulate Ballot Definition
3.2.3 - Manipulate Voted Ballots
3.2.5 - Create Undervote
3.2.7 - Manipulate Accumulation Data
3.2.2 - Denial of Service
3.2.4 - Flip Votes
3.2.6 - Delete Contests/ Candidates
3.2.8 - Manipulate Audit Data

6-5 Vote by Phone Insider Attacks



6-6 Vote by Phone Undetectable Error

6.3 Vote by Phone Threat Matrix

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1	Attack on Voting Equipment			human-deliberate	Election System	Voting System	access to VotingSystem;		
A	1.1	Phone Device Malware	Install malicious software on a device so that it can later execute on that device.		human-deliberate	Election System	Voting Machine	access to VotingSystem;	(1) High assurance software	
A	1.1.1	Create the Malware	Design, code, and test the software artifact that will be used to attack the voting system.	Gardner	human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption		
O	1.1.1.1	Design the Attack	Identify requirements and construct the architecture for the malicious software.	Gardner/ Yasinsac07	human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	(1) High assurance software	
T	1.1.1.1.1	Flip Votes	Create software that will record a vote that is different from the voter's selection.	Jones (2005a) #23232	human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	(1) High assurance software (2) Physical vote record	
T	1.1.1.1.2	Create Undervote	Create software that records a vote in a race with no voter selection.		human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	(1) High assurance software (2) Physical vote record	
O	1.1.1.1.3	Deny Service	Preventing or slowing the voting process.	Rubin/ NIST	human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	(1) Redundant systems and/or mechanisms	
T	1.1.1.1.3.1	Deactivate [cell] Phone	Utilize wireless phone capability to turn the device power off		human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption		
T	1.1.1.1.3.2	Drop Call	Cause the call to be abnormally interrupted by the voting device or the voting server.		human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption		
T	1.1.1.1.3.3	Distort Voices	Inject noise into the communication circuit to distort directions to the voter or responses from the voter.		human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.1.2	Gain Necessary Knowledge	Attackers must acquire information that allows them to implement and exercise a malware attack.	Gardner	human-deliberate	Election System	Voting Machine, Sensitive Tech Data, Tech Insiders	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	NA	
A	1.1.1.3	Test the Malware	Attackers must be able to test the software that they will use in a voting system attack. This may require acquisition of proprietary software and/or hardware.	Gardner	human-deliberate	Election System	Voting Machine, Sensitive Tech Data, Tech Insiders	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	NA	
T	1.1.1.3.1	Replicate the Environment	In order to test malware, the attacker must be able to create an software/hardware environment that is consistent with the target environment.		human-deliberate	Election System	Voting Machine, Sensitive Tech Data, Tech Insiders	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	NA	
T	1.1.1.3.2	Simulate System Load	An essential element of testing is to simulate transaction volume.		human-deliberate	Election System	Voting Machine, Sensitive Tech Data, Tech Insiders	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	NA	
O	1.1.2	Install the Malware	The attacker install malware on the target device in order to execute the software to achieve the desired impact.	Gardner/ Yasinsac07	human-deliberate	Voting System	Telephony Devices, Server	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Strong legal deterrence	
T	1.1.2.1	Removable Media	Malware installed from removable media that contracted a virus or other regenerating malware.	Gardner/ Yasinsac07	human-deliberate	Ballot Preparation, Voting	Telephony Devices, Server	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2)Strong media authentication	
T	1.1.2.2	Vendor Installed	Malicious software may be installed by a member of the vendor's development team.	Gardner/ Yasinsac07	human-deliberate	Election System	Not Modeled	out of scope	(1) High assurance software (2) Strong legal deterrence (3) Employee background checks	
T	1.1.2.3	During L&A	Malicious software may be installed by a member of the logic and accuracy test team.	Gardner/ Yasinsac07	human-deliberate	Canvass	Telephony Devices, Server	inability to detect the clever insider's infiltration of the L&A test script	(1) High assurance software (2) Software chain of custody (3) Employee background checks (4) Strong legal deterrence	
O	1.1.3	Trigger the Malware	Cause the installed malware to be executed on the target device.	Gardner/ Yasinsac07	human-deliberate	Voting	Telephony Devices, server	Poor security of voting equipment	(1) Strong legal deterrence	
T	1.1.3.1	Time Trigger	Utilize a timing trigger to start malware execution.	Gardner/ Yasinsac07	human-deliberate	Voting	Telephony Devices, Server	Poor security of voting equipment	(1) High assurance software (2) Strong legal deterrence (3) Locked equipment cages for sleepover	
T	1.1.3.2	Event Trigger	Create the code to wait for a specific action to trigger its full operation.	Gardner/ Yasinsac07	human-deliberate	Voting	Telephony Devices, Server	Poor security of voting equipment	(1) High assurance software (2) Strong legal deterrence	
O	1.2	Network Attack	Malicious act targeting the network that supports the voting system.		human-deliberate	Voting System	Telephony Devices, Servers, PC, Terminal, Network Device	Poor network and telephony security, poor security configuration by admin	(1) Strong network security (2) Legal deterrence	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.2.1	Denial of Service	Attempt to prevent voting system operation.	Rubin	human-deliberate	Voting System	Telephony Devices, Servers, PC, Terminal, Network Device	Poor network and telephony security, poor security configuration by admin	Redundant systems and/or resources	
T	1.2.1.1	Flood Voting Device	Creating a high volume of traffic to prevent legitimate information from flowing to/from the voting terminal..	Rubin	human-deliberate	Voting System	Telephony Devices, Servers, PC, Terminal, Network Device	Poor network and telephony security, poor security configuration by admin	(1) Filters (2) Redundancy (3) Distribution	
T	1.2.1.2	Flood voting server	Creating a high volume of traffic to prevent legitimate information from flowing to/from the voting server..	Rubin	human-deliberate	Voting System	Telephony Devices, Servers, PC, Terminal, Network Device	Poor network and telephony security, poor security configuration by admin	(1) Filters (2) Redundancy (3) Distribution	
T	1.2.1.3	Flood Supporting Network	Creating a high volume of traffic to prevent legitimate information from flowing across the supporting network.	Rubin	human-deliberate	Election System	Telephony Devices, Servers, PC, Terminal, Network Device	Poor network and telephony security, poor security configuration by admin	(1) Filters (2) Redundancy (3) Distribution	
T	1.2.1.4	Destroy Voting Component	Destroy or otherwise disable a critical voting system component to stop or slow voting in targeted areas.	Jones (2005a) #231; 232	human-deliberate	Voting System	Telephony Devices, Servers, PC, Terminal, Network Device	Poor network and telephony security, poor security configuration by admin	(1) Strong Physical security	
A	1.2.2	Man in the Middle / Pharming	Attacker masquerades concurrently as a client and server, using information from each session to accomplish objectives in the other session.	Rubin	human-deliberate	Voting System			(1) Strong network security (2) Strong legal deterrence	
T	1.2.2.1	Design the Attack	Attacker conceptualizes the attack and devises an attack strategy and protocol.	Gardner/ Yasinsac07	human-deliberate	Election System	Not Modeled	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery/corruption	NA	
T	1.2.2.2	Compromise Network Device	Attacker exploits a vulnerability that allows her to control or alter communication on a network device.	Rubin	human-deliberate	Ballot Delivery (R)	Network Device	Poor network security, poor security configuration by admin	(1) Strong network security	
T	1.2.2.3	Intercept Voter Transaction	Attack on a network device allows attacker to intercept traffic during a voting session.	Rubin	human-deliberate	Ballot Delivery (R)	Network Device	Poor network security, poor security configuration by admin	(1) Strong network security (2) Strong legal deterrence	
T	1.2.2.4	Insert Manipulated Transaction	Attack on a network device allows attacker to insert a manipulated message into a voting session.	Rubin	human-deliberate	Ballot Delivery (R)	Network Device	Poor network security, poor security configuration by admin	(1) Strong network security (2) Strong legal deterrence	
O	1.3	Voting Server Attack	Attack on a network device allows attacker to insert a manipulated message into a voting session.	Rubin	human-deliberate	Voting System	Network Server	Poor network security, poor security configuration by admin	(1) Strong network security (2) Strong legal deterrence	
T	1.3.1	Malicious Admin Account	Attacker compromises voting server security by establishing an admin account.	Gardner	human-deliberate	Voting System	Network Server	Admin susceptibility to bribery and coercion	(1) Strong network security (2) Strong legal deterrence (3) Employee background checks	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.2	Denial of Service	Preventing or slowing the voting process.	Jefferson D	human-deliberate	Voting System	Network Server	Poor network security, poor security configuration by admin	Redundant systems and/or resources	
A	1.3.3	Voting Server Malware	An attacker may install malicious software on the voting server to manipulate voting sessions or to alter tabulation or other stored data.	Rubin	human-deliberate	Voting System	Network Server	Poor network security, poor security configuration by admin	(1) High assurance software	
O	1.3.3.1	Install the Malware	The attacker install malware on the target device in order to execute the software to achieve the desired impact.	Rubin	human-deliberate	Voting System	Network Server	poor security during election artifacts delivery, insecure voter technology	(1) Strong Network security (2) Strong physical security	
T	1.3.3.1.1	Removable Media	Malware installed from removable media that contracted a virus or other regenerating malware.	Gardner/ Yasinsac07	human-deliberate	Ballot Preparation, Voting	Network Server	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2)Strong media authentication	
T	1.3.3.1.2	Botnet	Coordinated effort to install malware across a network on a large number of voting terminals.		human-deliberate	Voting	Network Server	Poor network security	(1) High assurance software (2) Strong network security	
T	1.3.3.1.3	Vendor Installed	Malicious software may be installed by a member of the vendor's development team.	Gardner/ Yasinsac07	human-deliberate	Election System	Network Server	out of scope	(1) High assurance software (2) Software chain of custody (3) Employee background checks (4) Strong legal deterrence	
T	1.3.3.1.4	During L&A	Malicious software may be installed by a member of the logic and accuracy test team.	Gardner/ Yasinsac07	human-deliberate	Canvass	Network Server	inability to detect the clever insider's infiltration of the L&A test script	(1) High assurance software (2) Strong legal deterrence	
T	1.3.3.2	Trigger the Malware	Cause the installed malware to be executed on the target device.	Gardner/ Yasinsac07	human-deliberate	Voting	Network Server	Poor security of voting equipment	(1) Strong legal deterrence	
T	1.4	Alter Ballot Creation Software	Attacker alters the system used to generate ballot formats, either causing malformed ballots or to allow external control for ballot faults.		human-deliberate	Ballot Preparation	Network Server	poor security during election artifacts delivery, insecure voter technology		
O	2	Voting Process Attack			human-deliberate	Election System	Eligible Voter	susceptibility to bribery, coercion, and deception		
A	2.1	Phishing Attack	Attracting a voter to a malicious voting web site.	Rubin/ NIST	human-deliberate	Voting System	Eligible Voter	susceptibility to bribery, coercion, and deception	(1) Strong legal deterrence (2) Voter education	
T	2.1.1	Attract the Voter	Attacker tricks voters to visit the malicious web site.	Rubin	human-deliberate	Voting System	Eligible Voter	susceptibility to bribery, coercion, and deception	(1) Voter education	
T	2.1.2	Alter the Voting Session	Attacker alters the voter's interaction to accomplish their election fault.	Jefferson D	human-deliberate	Mark Ballot	Eligible Voter	susceptibility to bribery, coercion, and deception		
O	2.2	Voter Impersonation Attack	Attacker assumes the identity of a legitimate voter.		human-deliberate	Voter checkin (R)	Eligible Voter	personnel training or integrity issues; faulty authentication	(1) Strong mutual authentication	
T	2.2.1	Steal Voters' Passwords	Attacker steals a legitimate voter's credential	Jones(2005a) # 311	human-deliberate	Voter checkin (R)	Eligible Voter	Weak passwords and susceptibility to bribery, coercion, and deception		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	2.2.2	Automate Voting	An attacker than can connect to the voting server and can masquerade as a legitimate voting device, could automate the voting process if they can systematically defeat the voter authentication process.	Rubin	human-deliberate	Voting	Network Server	Poor network security, poor security configuration by admin	(1) Strong legal deterrence (2) High assurance software (3) Strong application security	
T	2.2.2.1	Identify an automatable voter authentication attack	Defeat the session control protocol to allow multiple ballots to be cast from a single session.		human-deliberate	Election System	Voting Server	Poor application security	(1) Strong legal deterrence (2) High assurance software (3) Strong application security	
T	2.2.2.2	Develop the Attack Software	Design, code, and test the software artifact that will be used to attack the voting system.	Gardner	human-deliberate	Election System	Voting Machine	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) Strong legal deterrence (2) High assurance software (3) Strong application security	
T	2.2.2.3	Identify Unlikely Voters	1. Cross-check phone book with voter participation information 2. Many other methods to identify unlikely voters.	Estep	human-deliberate	Election System	Eligible Voter	Public voter information	NA	
T	2.2.2.4	Steal Voters' Credentials	Illegitimately acquire multiple voter credentials using the method identified in step 2.2.3.1.		human-deliberate	Voting System	Eligible Voter	access to machines/information, application software	(1) Strong application security	
T	2.2.2.5	Implement the Attack	Put the software and trigger mechanisms in place.	Gardner/ Yasinsac07	human-deliberate	Voting	Telephony Devices, Servers, PC, Terminal	Poor security of voting equipment	(1) Strong physical security (2) Strong network security	
T	2.2.2.6	Trigger the Attack	Cause the installed malware to be executed on the target device.	Gardner/ Yasinsac07	human-deliberate	Voting	Telephony Devices, Servers, PC, Terminal	Poor security of voting equipment	(1) Strong physical security (2) Strong network security	
O	2.3	Vote Attribution Attack	Attack enabled by a voter being able to prove how they vote.		human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Receipt-free voting system	
A	2.3.1	Vote Buying	Attacker pays a voter.	Hasen, Jones(2005a) # 311	human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Receipt-free voting system (2) Strong legal deterrence	
T	2.3.1.1	Recruit Brokers	Attacker recruits brokers to reach move voters and to protect themself from legal ramifications.		human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	2.3.1.2	Identify Prospective Sellers	Attacker engages voters that are willing to sell their votes.	Estep	human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	2.3.1.3	Send Instructions	Attacker communicates the actions that the vote sellers take to accomplish the transaction.		human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
O	2.3.1.4	Verify the Vote	Attacker confirms that the vote seller accomplished the agreed action.	Estep	human-deliberate	Voting	Eligible Voter	susceptibility to bribery and coercion	(1) Receipt-free voting system	
T	2.3.1.4.1	Eavesdrop on the Phone Line	Physically tap the phone line, or capture electronic emanations		human-deliberate	Voting	Telephony Devices, Servers, PC, terminal	Poor security of voting equipment	(1) Strong physical security (2) Tempest security	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.3.1.4.2	Eavesdrop at Voting Server	Install malicious software on the voting server that will transmit or capture voter interactions.		human-deliberate	Voting	Telephony Devices, Servers, PC, Terminal	Poor security of voting equipment	(1) Strong legal deterrence (2) Strong network security	
T	2.3.1.5	Make the Payment	Attacker transfers payment to the vote seller.		human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	2.3.2	Voter Coercion	Attacker influences voter via threat or intimidation.	Jones(2005a) #332	human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Voter training (2) Receipt-free voting system (3) Strong legal deterrence	
T	2.3.3	Pay Voter Not to Vote	Attacker pays a voter to NOT cast a ballot at all.	Hasen	human-deliberate	Election System	Eligible Voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	2.4	Exhaust Authentication Threshold	Often, authentication system limit the number of errors that a user can make during authentication. Intentionally making multiple errors could cause an account to lock, thus disenfranchising, or discouraging targeted user.		human-deliberate	Voting	Telephony Devices, Servers, PC, Terminal	Poor security of voting equipment	Effective authentication system	
A	2.5	Cast Multiple Ballots	The user that has control of the phone may cast multiple ballots, for example, by stealing or fraudulently acquiring other voter's credentials.	Estep	human-deliberate	Voting	Telephony Devices, Servers, PC, Terminal	Poor security of voting equipment	(1) Effective audit process (2) Strong legal deterrence (3) Dedicated poll worker	
T	2.5.1	Defeat Phone Authorization	Steal or fraudulently acquire other voter's credentials.	Gardner	human-deliberate	Provide Credentials (R), Commit Ballot (R)	Eligible Voter	Poor security of voting equipment	(1) Strong voter authentication (2) Strong legal deterrence	
T	2.5.2	Use Credential Multiple Times	Defeat the session control protocol to allow multiple ballots to be cast from a single session.		human-deliberate	Provide Credentials (R), Commit Ballot (R)	Eligible Voter	Poor security of voting equipment	(1) Strong voter authentication (2) Strong legal deterrence	
O	3	Insider Attacks	Attacks by elections officials or poll workers.	Gardner/ Yasinsac07	human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices	(1) Strong legal deterrence (2) Employee background checks (3) Effective audit process	
O	3.1	Install Malware	Install malicious software on a device so that it can later execute on that device.	Rubin Gardner	human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices	(1) Strong legal deterrence (2) Physical security (3) Employee background checks	
T	3.1.1	During Development	Malicious software may be installed by a member of the vendor's development team.	Gardner/ Yasinsac07	human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices	(1) Strong legal deterrence (2) Employee background checks	
A	3.1.2	During Install / Test	Malicious software may be installed by a member of the logic and accuracy test team.	Gardner/ Yasinsac07	human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices	(1) Strong legal deterrence (2) Employee background checks (3) High assurance software	
T	3.1.2.1	Gain Necessary Knowledge	Attackers must acquire information that allows them to implement and exercise a malware attack.	Gardner	human-deliberate insider	Election System	Voting Machine, Sensitive Tech Data, Tech Insiders	access to machines/information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.1.2.2	Hire Inside Collaborator	Attackers may acquire information that allows them to implement and exercise a malware attack by hiring an insider that has that information.		human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices	(1) Strong legal deterrence (2) Employee background checks	
T	3.1.2.3	Acquire Artifacts for Study	Many voting system components are not off the shelf hardware, so must be acquired illegally or through complex legal channels.	Gardner	human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices		
T	3.1.3	During Voting Period	Malicious software may be installed by a voter, a member of the elections staff, or by malicious pollworkers while the machines are operational.	Gardner	human-deliberate insider	Voting	Votable Ballot	Insider's access to telephony devices	(1) Strong physical security (2) Two person integrity (3) High Assurance Software	
T	3.1.4	After Voting Period	Malicious software may be installed by a member of the elections staff or by malicious pollworkers during closeout, between closeout and audit, or during any audit.		human-deliberate insider	Canvass	Marked Ballot	(1) Relaxed security after the election is over (2) Ability of the attacker to know exactly how many votes are needed to alter the result.	(1) Employee background checks (2) Two person integrity	
O	3.2	Non-malware attacks	Attack the voting system by using insider physical equipment access.	Gardner	human-deliberate insider	Voting System	Marked Ballot	Insider's access to telephony devices or the voting server	(1) Employee background checks (2) Two person integrity	
T	3.2.1	Manipulate Ballot Definition	Alter the structure or content of the ballot presentation format.	Gardner	human-deliberate insider	Create Ballot Style	Votable Ballot	Insider's access to voting server or telephony devices	(1) Employee background checks (2) Two person integrity	
T	3.2.2	Denial of Service	Disrupt voting system operation to prevent or delay the voting process.	Rubin	human-deliberate insider	Voting System	Telephony Devices	Insider's access to telephony devices	Redundant systems	
T	3.2.3	Manipulate Voted Ballots	Alter the content of a MarkedBallot	Gardner/ Yasinsac07	human-deliberate insider	Voting	Marked Ballot	Insider's access to voting server or telephony devices	(1) Strong physical security (2) Two person integrity	
T	3.2.4	Flip Votes	Record a vote that is different from the voter's selection.	Gardner/ Yasinsac07	human-deliberate insider	Voting	Marked Ballot	Insider's access to voting server or telephony devices	(1) Strong physical security (2) Two person integrity	
T	3.2.5	Create Undervote	Records a vote in a race where the voter elected to make no selection.		human-deliberate insider	Voting	Marked Ballot	Insider's access to voting server or telephony devices	(1) Strong physical security (2) Two person integrity	
T	3.2.6	Delete Contests/Candidates	Deletes contests or candidates from the ballot that is presented to the voter.		human-deliberate insider	Voting	Marked Ballot	Insider's access to voting server or telephony devices	(1) Strong physical security (2) Two person integrity	
T	3.2.7	Manipulate Accumulation Data	Create software that alters the machine's vote tabulation.	Yasinsac07	human-deliberate insider	Canvass	Votable Ballot	faulty validation process; personnel training or integrity issues	(1) Strong legal deterrence (2) Strong application security (3) Effective audit process	
T	3.2.8	Manipulate Audit Data	Alter or delete data that is intended for use in verifying the voting system's proper operation.	Yasinsac07	human-deliberate insider	Contest Audit	Audit Results	lack of transparency, oversight; inability to detect or recover	(1) Strong legal deterrence (2) Strong application security (3) Employee background checks	
T	3.3	Manipulate Randomization	Influence randomization process to allow attacker to predict values.	Gardner	human-deliberate insider	Contest Audit	Audit Results	lack of transparency, oversight; inability to detect or recover	(1) Rigorously engineered randomness approach	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	4	Undetectable Error	Errors for which there is no reliable detection mechanism.	Yasinsac	technical	Voting	Eligible Voter	Voting machine interface	(1) Interactive voter interface (2) Under/over vote check	
T	4.1	Human Error Mis-selection	Voter inadvertently makes a selection that they did not intend to make.	Yasinsac	human-unintentional	Mark Ballot	Eligible Voter	Voting machine interface	(1) Effective user interface	
T	4.2	Ballot Design Flaw	The ballot structure or presentation causes voters to make selection errors.	Yasinsac07	human-unintentional	Create Ballot Style	Votable Ballot	faulty testing process; personnel training or integrity issues	(1) Rigorous ballot design testing	
T	4.3	Name Confusion	A voter may confuse candidate names due to poor sound quality, pronunciation, local noise, etc.		human-unintentional	Mark Ballot	Eligible Voter	Voting machine interface		

7 Internet Voting

In this tree, we consider threats to voting systems that pass marked ballots across the Internet for tabulation. The most pure form of Internet voting is for voters to cast an official electronic ballot across the Internet from a personal computer.

There are many architectural Internet voting variations. Some consider voting by email to be a form of Internet voting. Others argue that since most faxed ballots travel on Internet circuits at some point, vote by fax is also an Internet voting scheme. We take no position on those arguments. Rather, we focus our efforts on the widely accepted Internet voting variety and contend that many of these threats also apply to many other varieties of Internet voting.

We have also been asked to distinguish between the different voting platform arrangements in Internet voting, for example, to distinguish between voting from a private computer and voting on a centrally controlled terminal, which often referred to as the kiosk model. We consider the kiosk model to be a control, or mitigating architectural adjustment, to counter voting terminal malware. Similarly, we do not consider encryption as a fundamental election mechanism, but rather consider its application as an attempt to mitigate communication threats. Please note that we do not address cryptography-based, end-to-end, voting systems in any way.

7.1 Internet Voting Threat Tree

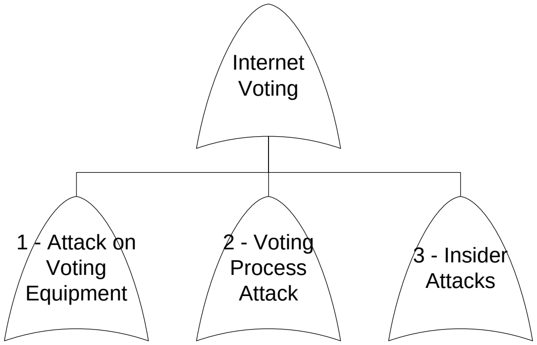
node type - outline number - threat action

O	1	Attack on Voting Equipment
A	1.1	Inject Malware
A	1.1.1	Create the Malware
O	1.1.1.1	Design the Attack
T	1.1.1.1.1	Flip votes
T	1.1.1.1.2	Create undervote
T	1.1.1.1.3	Alter results
T	1.1.1.1.4	Delete contest/candidate
T	1.1.1.1.5	Manipulate Audit Data
T	1.1.1.2	Gain necessary knowledge
A	1.1.1.3	Test the malware
T	1.1.1.3.1	Replicate environment
T	1.1.1.3.2	Simulate the volume
O	1.1.2	Install the Malware
T	1.1.2.1	Removable Media
T	1.1.2.2	Botnet or systematic virus infection
T	1.1.2.3	Vendor Installed
T	1.1.2.4	During L&A
T	1.1.2.5	During Sleepover
O	1.1.3	Trigger the Malware
T	1.1.3.1	Automatic
T	1.1.3.2	Cryptic Knock
T	1.1.3.3	Timing
O	1.2	Network Attack
O	1.2.1	Denial of Service
T	1.2.1.1	Flood voting terminal
T	1.2.1.2	Flood voting server
T	1.2.1.3	Flood supporting network
T	1.2.1.4	Disable voting component
T	1.2.1.5	Routing attack

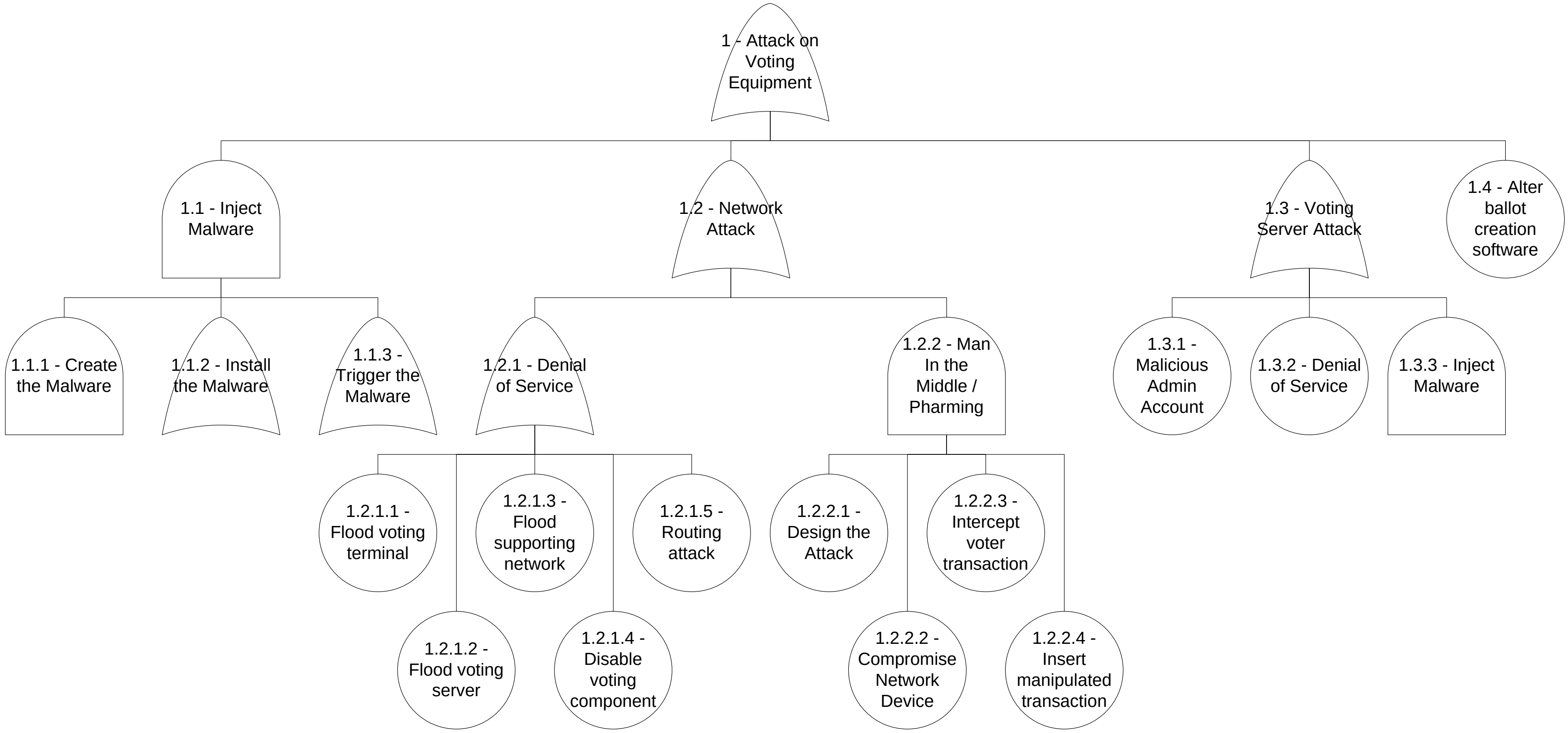
- A 1.2.2 Man In the Middle / Pharming
- T 1.2.2.1 Design the Attack
- T 1.2.2.2 Compromise Network Device
- T 1.2.2.3 Intercept voter transaction
- T 1.2.2.4 Insert manipulated transaction
- O 1.3 Voting Server Attack
- T 1.3.1 Malicious Admin Account
- T 1.3.2 Denial of Service
- A 1.3.3 Inject Malware
- A 1.3.3.1 Create the Malware
- O 1.3.3.1.1 Design the Attack
- T 1.3.3.1.1.1 Flip votes
- T 1.3.3.1.1.2 Create undervote
- T 1.3.3.1.1.3 Alter results
- T 1.3.3.1.1.4 Delete races
- T 1.3.3.1.2 Gain necessary knowledge
- A 1.3.3.1.3 Test the malware
- T 1.3.3.1.3.1 Replicate environment
- T 1.3.3.1.3.2 Simulate the volume
- O 1.3.3.2 Install the Malware
- T 1.3.3.2.1 Removable Media
- T 1.3.3.2.2 Botnet
- T 1.3.3.2.3 Vendor Installed
- T 1.3.3.3.4 During L&A
- O 1.3.3.3 Trigger the Malware
- T 1.4 Alter ballot creation software
- O 2 Voting Process Attack
- A 2.1 Phishing Attack
- T 2.1.1 Attract the Voter
- O 2.1.2 Alter the Voting Session
- T 2.1.2.1 Discard the ballot
- T 2.1.2.2 Alter the ballot
- T 2.1.2.3 Collect voter information
- O 2.2 Voter Impersonation Attack
- T 2.2.1 Steal voters' password
- T 2.2.2 Vote For Relative
- A 2.2.3 Vote for Deceased Voters
- T 2.2.3.1 Identify target deceased voters
- T 2.2.3.2 Register for them
- T 2.2.3.3 Receive, mark, return their ballot
- T 2.2.4 Other Systematic Selection
- O 2.3 Vote Attribution Attack
- A 2.3.1 Vote Buying
- T 2.3.1.1 Recruit brokers
- T 2.3.1.2 Identify prospective sellers
- T 2.3.1.3 Send instructions
- T 2.3.1.4 Verify the vote
- T 2.3.1.5 Make the payment
- T 2.3.2 Voter Coercion
- T 2.3.3 Pay Voter Not to Vote
- O 2.4 Attack Cryptography
- T 2.4.1 Compromise key management
- T 2.4.2 Compromise randomness

- T 2.4.3 Other protocol compromise
- T 2.4.4 Cryptanalysis
- T 2.4.5 Exploit weak password
- O 3 Insider Attacks
  - O 3.1 Inject Malware
    - A 3.1.1 Create the Malware
      - O 3.1.1.1 Design the Attack
        - T 3.1.1.1.1 Flip votes
        - T 3.1.1.1.2 Create undervote
        - T 3.1.1.1.3 Alter results
        - T 3.1.1.1.4 Delete races
      - T 3.1.1.2 Gain necessary knowledge
      - A 3.1.1.3 Test the malware
        - T 3.1.1.3.1 Replicate environment
        - T 3.1.1.3.2 Simulate the volume
      - O 3.1.1.4 Install the Malware
        - T 3.1.1.4.1 Removable Media
        - T 3.1.1.4.2 Botnet
        - T 3.1.1.4.3 Vendor Installed
        - T 3.1.1.4.4 During L&A
        - T 3.1.1.4.5 During Sleepover
      - O 3.1.1.5 Trigger the Malware
        - T 3.1.1.5.1 Automatic
        - T 3.1.1.5.2 Cryptic Knock
        - T 3.1.1.5.3 Timing
  - T 3.2 Manipulate ballot definition
  - T 3.3 Denial of Service
  - T 3.4 Manipulate voted ballots
  - T 3.5 Manipulate accumulation data
  - T 3.6 Manipulate audit data
  - T 3.7 Manipulate randomization
    - O 3.8. Undetectable voter error
    - T 3.8.1 Human error mis-mark
    - T 3.8.2 Ballot Design Flaw
    - T 3.8.3 Correction mistake
    - T 3.8.4 Candidate name confusion

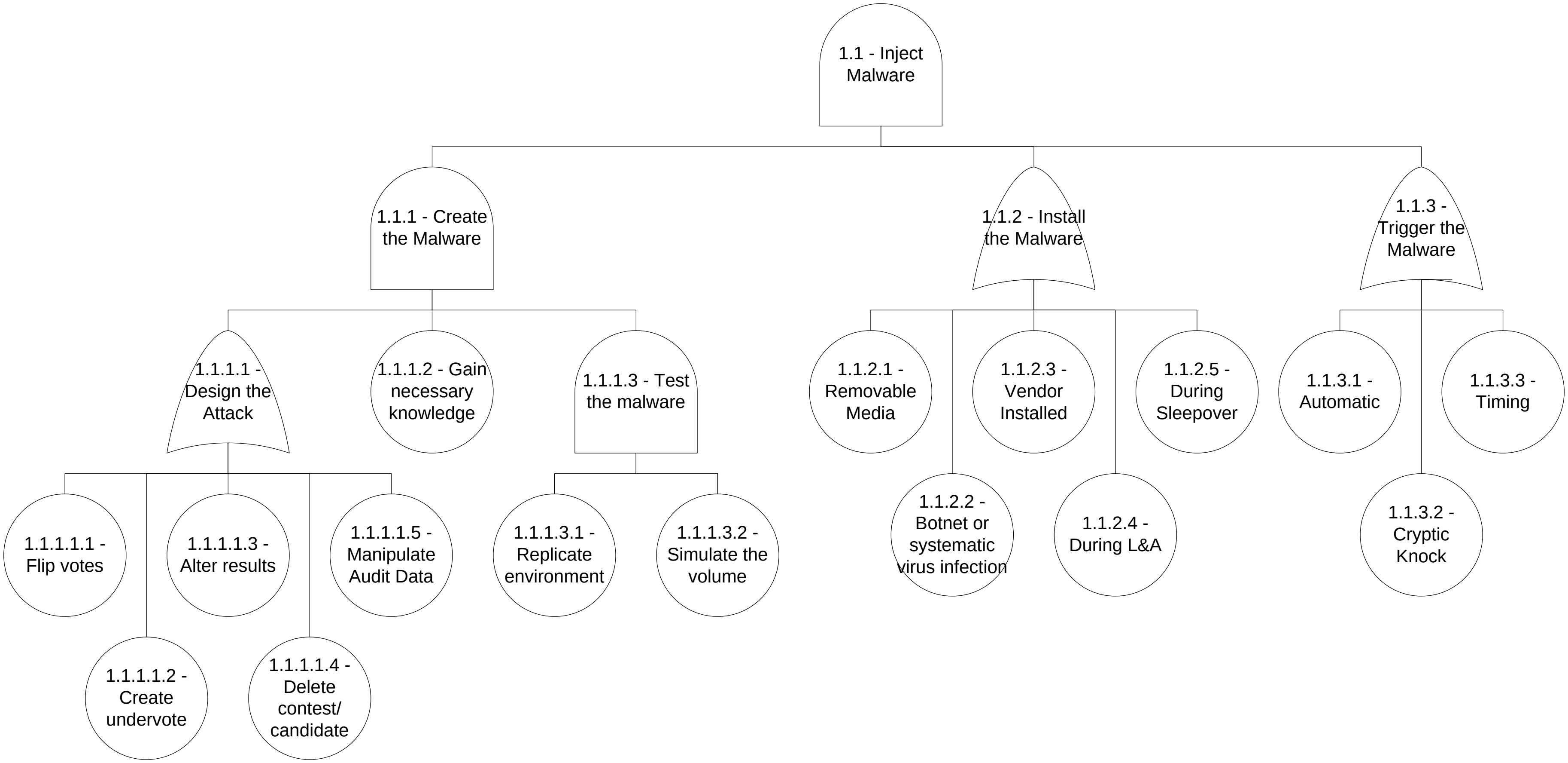
7.2 Internet Voting Threat Tree – Graphic



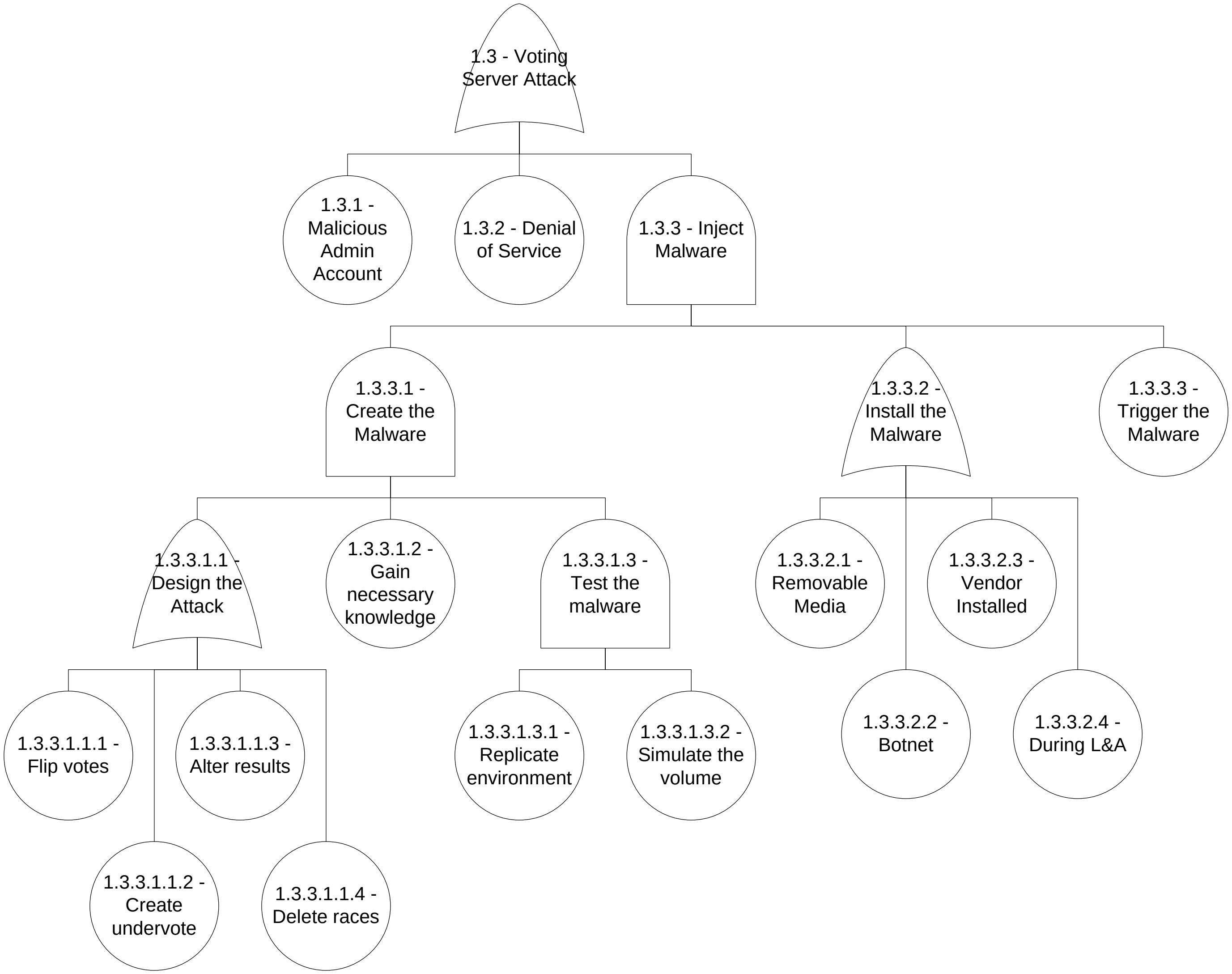
7-1 Internet Voting Overview


1 - Attack on Voting Equipment
1.1 - Inject Malware
1.2 - Network Attack
1.3 - Voting Server Attack
1.4 - Alter ballot creation software
1.1.1 - Create the Malware
1.1.2 - Install the Malware
1.1.3 - Trigger the Malware
1.2.1 - Denial of Service
1.2.2 - Man In the Middle / Pharming
1.3.1 - Malicious Admin Account
1.3.2 - Denial of Service
1.3.3 - Inject Malware
1.2.1.1 - Flood voting terminal
1.2.1.2 - Flood voting server
1.2.1.3 - Flood supporting network
1.2.1.4 - Disable voting component
1.2.1.5 - Routing attack
1.2.2.1 - Design the Attack
1.2.2.2 - Compromise Network Device
1.2.2.3 - Intercept voter transaction
1.2.2.4 - Insert manipulated transaction

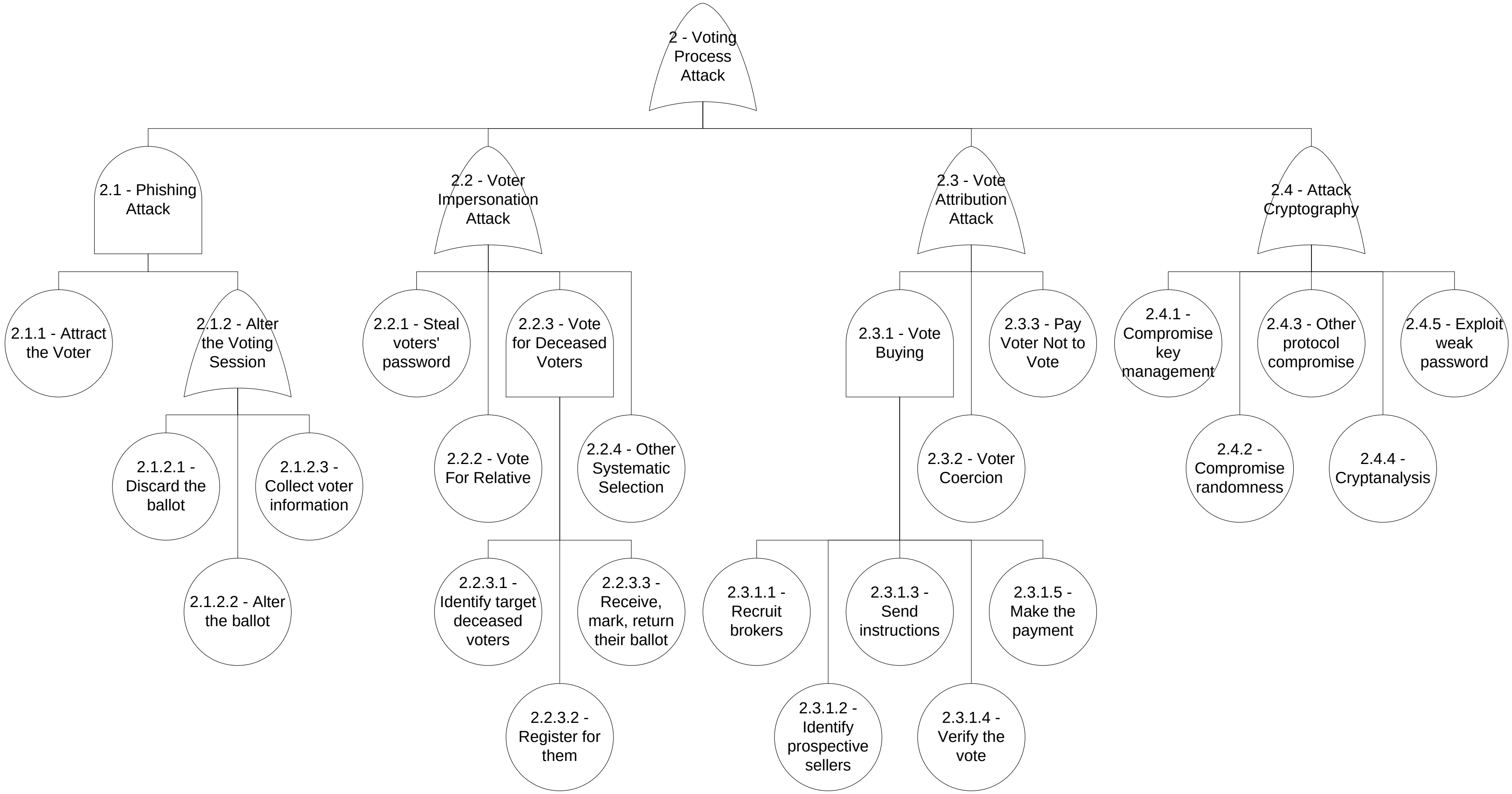
7-2 Internet Voting Attack on Voting Equipment


1.1 - Inject Malware
1.1.1 - Create the Malware
1.1.2 - Install the Malware
1.1.3 - Trigger the Malware
1.1.1.1 - Design the Attack
1.1.1.2 - Gain necessary knowledge
1.1.1.3 - Test the malware
1.1.2.1 - Removable Media
1.1.2.3 - Vendor Installed
1.1.2.5 - During Sleepover
1.1.3.1 - Automatic
1.1.3.3 - Timing
1.1.1.1.1 - Flip votes
1.1.1.1.3 - Alter results
1.1.1.1.5 - Manipulate Audit Data
1.1.1.3.1 - Replicate environment
1.1.1.3.2 - Simulate the volume
1.1.2.2 - Botnet or systematic virus infection
1.1.2.4 - During L&A
1.1.3.2 - Cryptic Knock
1.1.1.1.2 - Create undervote
1.1.1.1.4 - Delete contest/ candidate

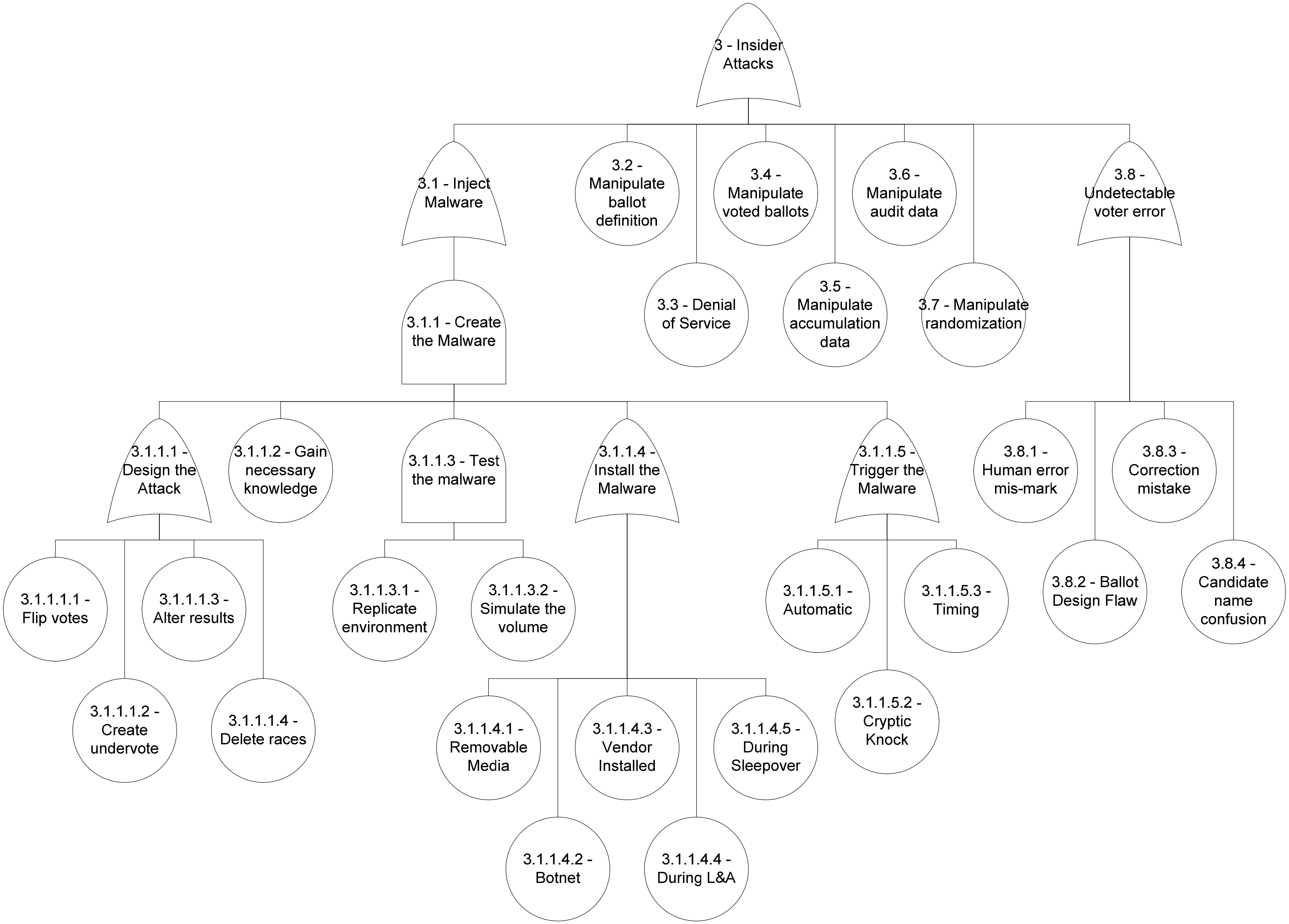
7-3 Internet Voting Inject Malware


1.3 - Voting Server Attack
1.3.1 - Malicious Admin Account
1.3.2 - Denial of Service
1.3.3 - Inject Malware
1.3.3.1 - Create the Malware
1.3.3.2 - Install the Malware
1.3.3.3 - Trigger the Malware
1.3.3.1.1 - Design the Attack
1.3.3.1.2 - Gain necessary knowledge
1.3.3.1.3 - Test the malware
1.3.3.2.1 - Removable Media
1.3.3.2.3 - Vendor Installed
1.3.3.1.1.1 - Flip votes
1.3.3.1.1.3 - Alter results
1.3.3.1.3.1 - Replicate environment
1.3.3.1.3.2 - Simulate the volume
1.3.3.2.2 - Botnet
1.3.3.2.4 - During L&A
1.3.3.1.1.2 - Create undervote
1.3.3.1.1.4 - Delete races

7-4 Internet Voting Voting Server Attack


2 - Voting Process Attack
2.1 - Phishing Attack
2.1.1 - Attract the Voter
2.1.2 - Alter the Voting Session
2.1.2.1 - Discard the ballot
2.1.2.2 - Alter the ballot
2.1.2.3 - Collect voter information
2.2 - Voter Impersonation Attack
2.2.1 - Steal voters' password
2.2.2 - Vote For Relative
2.2.3 - Vote for Deceased Voters
2.2.3.1 - Identify target deceased voters
2.2.3.2 - Register for them
2.2.3.3 - Receive, mark, return their ballot
2.2.4 - Other Systematic Selection
2.3 - Vote Attribution Attack
2.3.1 - Vote Buying
2.3.1.1 - Recruit brokers
2.3.1.2 - Identify prospective sellers
2.3.1.3 - Send instructions
2.3.1.4 - Verify the vote
2.3.1.5 - Make the payment
2.3.2 - Voter Coercion
2.3.3 - Pay Voter Not to Vote
2.4 - Attack Cryptography
2.4.1 - Compromise key management
2.4.2 - Compromise randomness
2.4.3 - Other protocol compromise
2.4.4 - Cryptanalysis
2.4.5 - Exploit weak password

7-5 Internet Voting Voting Process Attack


3 - Insider Attacks
3.1 - Inject Malware
3.2 - Manipulate ballot definition
3.3 - Denial of Service
3.4 - Manipulate voted ballots
3.5 - Manipulate accumulation data
3.6 - Manipulate audit data
3.7 - Manipulate randomization
3.8 - Undetectable voter error
3.1.1 - Create the Malware
3.1.1.1 - Design the Attack
3.1.1.2 - Gain necessary knowledge
3.1.1.3 - Test the malware
3.1.1.4 - Install the Malware
3.1.1.5 - Trigger the Malware
3.8.1 - Human error mis-mark
3.8.2 - Ballot Design Flaw
3.8.3 - Correction mistake
3.8.4 - Candidate name confusion
3.1.1.1.1 - Flip votes
3.1.1.1.2 - Create undervote
3.1.1.1.3 - Alter results
3.1.1.1.4 - Delete races
3.1.1.3.1 - Replicate environment
3.1.1.3.2 - Simulate the volume
3.1.1.4.1 - Removable Media
3.1.1.4.2 - Botnet
3.1.1.4.3 - Vendor Installed
3.1.1.4.4 - During L&A
3.1.1.4.5 - During Sleepover
3.1.1.5.1 - Automatic
3.1.1.5.2 - Cryptic Knock
3.1.1.5.3 - Timing

7-6 Internet Voting Insider Attacks

7.3 Internet Voting Threat Matrix

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1	Attack on Voting Equipment	attack on Internet voting system	Rubin/ NIST/ Mote	human-deliberate	Voting System	Voting System	remote access to VotingSystem; voter attribution	(1) Only attestable voting platforms	
A	1.1	Inject Malware	Install malicious software on a device so that it can later execute on that device.	Rubin/ NIST /Mote	human-deliberate	Voting	One voter (R)	malware can be injected into software	(1) Chain of custody (2) Two person integrity (3) High Assurance Software (4) Rigorous testing	
A	1.1.1	Create the Malware	Design, code, and test the software artifact that will be used to attack the voting system.	Gardner	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
O	1.1.1.1	Design the Attack	Identify requirements and construct the architecture for the malicious software.	Jefferson-04	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software	
T	1.1.1.1.1	Flip votes	Create software that will record a vote that is different from the voter's selection.	Rubin	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software (2) Physical vote record	
T	1.1.1.1.2	Create undervote	Create software that records a vote in a race with no voter selection.	Gardner/ Yasinsac07	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software (2) Physical vote record	
T	1.1.1.1.3	Alter results	Create software that alters the machine's vote tabulation.	Gardner/ Yasinsac07	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software (2) Physical vote records	
T	1.1.1.1.4	Delete contest/candidate	Create software that deletes contests or candidates from the ballot that is presented to the voter.	Gardner/ Yasinsac07	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption+M30	(1) High assurance software	
T	1.1.1.1.5	Manipulate Audit Data	Create software that alters or deletes data that is intended for use in verifying the voting system's proper operation.	Gardner/ Yasinsac07	human-deliberate	Election System	Voting System	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption+M30	(1) High assurance software	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.1.1.2	Gain necessary knowledge	Attackers must acquire information that allows them to implement and exercise a malware attack.	Gardner/ Yasinsac07	human-deliberate	Election System	Voting Machine, sensitive tech data, tech insiders	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
A	1.1.1.3	Test the malware	Attackers must be able to test the software that they will use in a voting system attack. This may require acquisition of proprietary software and/or hardware.	Gardner/ Yasinsac07	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
T	1.1.1.3.1	Replicate environment	In order to test malware, the attacker must be able to create an software/hardware environment that is consistent with the target environment.	Gardner/ Yasinsac07	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
T	1.1.1.3.2	Simulate the volume	An essential element of testing is to simulate transaction volume.		human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
O	1.1.2	Install the Malware	The attacker install malware on the target device in order to execute the software to achieve the desired impact.	Rubin	human-deliberate	Voting System	Servers, PC, terminal	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Dedicated use terminal	
T	1.1.2.1	Removable Media	Malware installed from removable media that contracted a virus or other regenerating malware.	Gardner/ Yasinsac07	human-deliberate	Ballot Preparation, Voting	Servers, PC, terminal	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Equipment/media chain of custody (3) Equipment/media two person integrity (4) Strong media authentication	
T	1.1.2.2	Botnet or systematic virus infection	Coordinated effort to install malware across a network on a large number of voting terminals.	Jefferson-04	human-deliberate	Voting	Network	Poor network security	(1) Voting terminal not network connected (2) Voting server not network connected (3) Strong network security	
T	1.1.2.3	Vendor Installed	Malicious software may be installed by a member of the vendor's development team.	Gardner	human-deliberate	Election System	not modeled	out of scope	(1) High assurance software (2) Software chain of custody (3) Employee background checks (4) Strong legal deterrence	
T	1.1.2.4	During L&A	Malicious software may be installed by a member of the logic and accuracy test team.	Gardner/ Yasinsac07	human-deliberate	Canvass	Servers, PC, terminal	inability to detect the clever insider's infiltration of the L&A test script	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Election official background checks (5) Strong legal deterrence	
T	1.1.2.5	During Sleepover	Malicious software installed by a pollworker or elections official that has exclusive control of the terminal after L&A and before the election.	Gardner/ Yasinsac07	human-deliberate	Ballot Preparation, Voting	Precinct Kiosk	poor security during election artifacts delivery	(1) High assurance software (2) Strong legal deterrence (3) Locked equipment cages for sleepover	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.1.3	Trigger the Malware	Cause the installed malware to be executed on the target device.	Gardner/ Yasinsac07	human-deliberate	Voting	Servers, PC, terminal	Poor security of voting equipment	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	
T	1.1.3.1	Automatic	Create the code that execution is automatic.	Gardner/ Yasinsac07	human-deliberate	Voting	Servers, PC, terminal	Poor security of voting equipment		
T	1.1.3.2	Cryptic Knock	Create the code to wait for a specific action to trigger its full operation.	Gardner/ Yasinsac07	human-deliberate	Voting	Servers, PC, terminal	overcoming the defense against cryptic knocks	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	
T	1.1.3.3	Timing	Utilize a timing trigger to start malware execution.	Gardner/ Yasinsac07	human-deliberate	Voting	Servers, PC, terminal	Poor security of voting equipment		
O	1.2	Network Attack	Malicious act targeting the network that supports the voting system.	Rubin	human-deliberate	Voting System	Servers, PC, terminal, network device	Poor network security, poor security configuration by admin		
O	1.2.1	Denial of Service	Attempt to prevent voting system operation.	Rubin/ NIST Mote	human-deliberate	Voting System	Servers, PC, terminal, network device	Poor network security, poor security configuration by admin	(1) Service redundancy (2) Strong network security	
T	1.2.1.1	Flood voting terminal	Creating a high volume of traffic to prevent legitimate information from flowing to/from the voting terminal..	Rubin	human-deliberate	Voting	Servers, PC, terminal, network device	Poor network security, poor security configuration by admin	(1) Redundancy (2) Strong network security	
T	1.2.1.2	Flood voting server	Creating a high volume of traffic to prevent legitimate information from flowing to/from the voting server..	Rubin	human-deliberate	Voting	Servers, PC, terminal, network device	Poor network security, poor security configuration by admin	(1) Redundancy (2) Strong network security	
T	1.2.1.3	Flood supporting network	Creating a high volume of traffic to prevent legitimate information from flowing across the supporting network.	Rubin	human-deliberate	Election System	Servers, PC, terminal, network device	Poor network security, poor security configuration by admin	(1) Strong network security	
T	1.2.1.4	Disable voting component	Destroy or otherwise disable a critical voting system component to stop or slow voting in targeted areas.	Rubin	human-deliberate	Voting	Servers, PC, terminal, network device	Poor network security, poor security configuration by admin	(1) Strong physical security	
T	1.2.1.5	Routing attack	Manipulate the network routing infrastructure to disrupt communications in the voting system.	Rubin/ NIST Mote	human-deliberate	Voting	PC Terminal	Network routing infrastructure	(1) Strong physical security	
A	1.2.2	Man In the Middle / Pharming	Attacker masquerades concurrently as a client and server, using information from each session to accomplish objectives in the other session.	Jefferson-04 Mote	human-deliberate	Voting System			(1) Strong network security	
T	1.2.2.1	Design the Attack	Attacker conceptualizes the attack and devises an attack strategy and protocol.	Jefferson-04	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.2.2	Compromise Network Device	Attacker exploits a vulnerability that allows her to control or alter communication on a network device.	Rubin	human-deliberate	Ballot Delivery (R)	Network device	Poor network security, poor security configuration by admin	(1) Strong network security	
T	1.2.2.3	Intercept voter transaction	Attack on a network device allows attacker to intercept traffic during a voting session.	Rubin	human-deliberate	Ballot Delivery (R)	Network device	Poor network security, poor security configuration by admin	(1) Strong network security	
T	1.2.2.4	Insert manipulated transaction	Attack on a network device allows attacker to insert a manipulated message into a voting session.	Jefferson-04	human-deliberate	Ballot Delivery (R)	Network device	Poor network security, poor security configuration by admin	(1) Strong network security	
O	1.3	Voting Server Attack	Attack on a network device allows attacker to insert a manipulated message into a voting session.	Jefferson-04	human-deliberate	Voting System	Network Server	Poor network security, poor security configuration by admin		
T	1.3.1	Malicious Admin Account	Attacker compromises voting server security by establishing an admin account.	Rubin	human-deliberate	Voting	Network Server	Admin susceptibility to bribery and coercion	(1) Strong network security (2) Strong legal deterrence	
T	1.3.2	Denial of Service	Preventing or slowing the voting process.	Rubin	human-deliberate	Voting	Network Server	Poor network security, poor security configuration by admin	(1) Redundant services (2) Strong legal deterrence	
A	1.3.3	Inject Malware	Install malicious software on a device so that it can later execute on that device.	Rubin	human-deliberate	Voting	Network Server	Poor network security, poor security configuration by admin	(1) High Assurance software (2) Two person integrity (3) Strong network security (4) Strong legal deterrence	
A	1.3.3.1	Create the Malware	Design, code, and test the software artifact that will be used to attack the voting system.	Rubin, Jefferson-04	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
O	1.3.3.1.1	Design the Attack	Identify requirements and construct the architecture for the malicious software.	Jefferson-04	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High Assurance Software	
T	1.3.3.1.1.1	Flip votes	Create software that will record a vote that is different from the voter's selection.	Rubin	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High Assurance Software (2) Effective auditing	
T	1.3.3.1.1.2	Create undervote	Create software that records a vote in a race with no voter selection.	Gardner	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High Assurance Software (2) Effective auditing	
T	1.3.3.1.1.3	Alter results	Create software that alters the machine's vote tabulation.	Gardner	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High Assurance Software (2) Effective auditing	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.3.1.1.4	Delete races	Create software that deletes contests from the ballot that is presented to the voter.	Gardner	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High Assurance Software (2) Effective auditing	
T	1.3.3.1.2	Gain necessary knowledge	Attackers must acquire information that allows them to implement and exercise a malware attack.	Rubin	human-deliberate	Election System	Voting Machine, sensitive tech data, tech insiders	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
A	1.3.3.1.3	Test the malware	Attackers must be able to test the software that they will use in a voting system attack. This may require acquisition of proprietary software and/or hardware.	Gardner	human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
T	1.3.3.1.3.1	Replicate environment	In order to test malware, the attacker must be able to create an software/hardware environment that is consistent with the target environment.		human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
T	1.3.3.1.3.2	Simulate the volume	An essential element of testing is to simulate transaction volume.		human-deliberate	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
O	1.3.3.2	Install the Malware	The attacker install malware on the target device in order to execute the software to achieve the desired impact.	Rubin	human-deliberate	Voting System	Network Server	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity	
T	1.3.3.2.1	Removable Media	Malware installed from removable media that contracted a virus or other regenerating malware.	Gardner/ Yasinsac07	human-deliberate	Ballot Preparation, Voting	Network Server	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Equipment/media chain of custody (3) Equipment/media two person integrity (4) Strong media authentication	
T	1.3.3.2.2	Botnet	Coordinated effort to install malware across a network on a large number of voting terminals.	Jefferson-04	human-deliberate	Voting	Network Server	Poor network security	(1) Voting terminal not network connected (2) Voting server not continuously network connected (3) Strong network security	
T	1.3.3.2.3	Vendor Installed	Malicious software may be installed by a member of the vendor's development team.	Gardner	human-deliberate	Election System	not modeled	out of scope	(1) High assurance software (2) Software chain of custody (3) Employee background checks (4) Strong legal deterrence	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.3.3.2.4	During L&A	Malicious software installed by a pollworker or elections official that has exclusive control of the terminal after L&A and before the election.	Gardner	human-deliberate	Canvass	Network Server	inability to detect the clever insider's infiltration of the L&A test script	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Election official background checks (5) Strong legal deterrence	
T	1.3.3.3	Trigger the Malware	Cause the malware to begin execution.	Jefferson-04	human-deliberate	Voting	Network Server	Poor security of voting equipment	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Election official background checks (5) Strong legal deterrence	
T	1.4	Alter ballot creation software	Attacker alters the system used to generate ballot formats, either causing malformed ballots or to allow external control for ballot faults.	Gardner	human-deliberate	Ballot Preparation	Network Server	poor security during election artifacts delivery, insecure voter technology	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	
O	2	Voting Process Attack			human-deliberate	Election System	Remote voter	susceptibility to bribery, coercion, and deception		
A	2.1	Phishing Attack	Attracting a voter to a malicious voting web site.	Rubin NIST	human-deliberate	Voting System	Remote voter	susceptibility to bribery, coercion, and deception	(1) Voter training (2) Strong legal deterrence	
T	2.1.1	Attract the Voter	Attacker tricks voters to visit the malicious web site.	Rubin	human-deliberate	Voting System	Remote voter	susceptibility to bribery, coercion, and deception	(1) Voter training (2) Strong legal deterrence	
O	2.1.2	Alter the Voting Session	Attacker alters the voter's interaction to accomplish their election fault.	Rubin	human-deliberate	Mark Ballot	Remote voter	susceptibility to bribery, coercion, and deception	(1) High assurance software	
T	2.1.2.1	Discard the ballot	Attacker terminates the session, convincing the voter that the ballot was cast, but without casting the ballot.	Rubin	human-deliberate	Spoil Ballot	Remote voter	susceptibility to bribery, coercion, and deception	(1) High assurance software	
T	2.1.2.2	Alter the ballot	Attacker reports other than the voter's selections for tabulation.		human-deliberate	Commit Ballot	Remote voter	susceptibility to bribery, coercion, and deception	(1) High assurance software	
T	2.1.2.3	Collect voter information	Attacker collects voter information for later malicious election related use.		human-deliberate	Election System	not modeled	susceptibility to bribery, coercion, and deception	(1) High assurance software	
O	2.2	Voter Impersonation Attack	Attacker assumes the identity of a legitimate voter.	Jefferson-04	human-deliberate	Voter checkin (R)	Remote voter	personnel training or integrity issues; faulty authentication	(1) Strong voter authentication (2) Strong legal deterrence	
T	2.2.1	Steal voters' password	Attacker steals a legitimate voter's password.		human-deliberate	Voter checkin (R)	Remote voter	Weak passwords and susceptibility to bribery, coercion, and deception		
T	2.2.2	Vote For Relative	Attacker masquerades as a family member or coercively submits a relative's ballot.		human-deliberate	Voter checkin (R)	Remote voter	personnel training or integrity issues; faulty authentication		
A	2.2.3	Vote for Deceased Voters	Cast a VBM ballot using a deceased voter's identity.	Estep	human-deliberate	Voter checkin (R)	Remote voter	personnel training or integrity issues; faulty authentication	(1) Accurate voter rolls	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.3.1	Identify target deceased voters	Match voter rolls against online obituary entries or identify deceased voters for whom they can register.	Estep	human-deliberate	Voter checkin (R)	Remote voter	personnel training or integrity issues; faulty authentication		
T	2.2.3.2	Register for them	Register the identified deceased voter to an address where the attacker can easily retrieve the delivered VBM votable ballot.		human-deliberate	Request Ballot (R)	Remote voter	personnel training or integrity issues; faulty authentication	(1) Accurate voter rolls	
T	2.2.3.3	Receive, mark, return their ballot			human-deliberate	Provide Credentials (R), Commit Ballot (R)	Remote voter	personnel training or integrity issues; faulty authentication		
T	2.2.4	Other Systematic Selection	Attacker identifies prospective targets that maximize their masquerade success.		human-deliberate	Provide Credentials (R), Commit Ballot (R)	Remote voter	personnel training or integrity issues; faulty authentication		
O	2.3	Vote Attribution Attack	Attack enabled by a voter being able to prove how they vote.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting system	
A	2.3.1	Vote Buying	Attacker pays a voter.	Jefferson-04 Mote	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting system (2) Strong legal deterrence	
T	2.3.1.1	Recruit brokers	Attacker recruits brokers to reach move voters and to protect themself from legal ramifications.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	2.3.1.2	Identify prospective sellers	Attacker engages voters that are willing to sell their votes.	Estep	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
T	2.3.1.3	Send instructions	Attacker communicates the actions that the vote sellers take to accomplish the transaction.		human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Legal deterrence	
T	2.3.1.4	Verify the vote	Attacker confirms that the vote seller accomplished the agreed action.	Jefferson-04	human-deliberate	Voting	Remote voter	susceptibility to bribery and coercion	(1) Receipt-free voting system	
T	2.3.1.5	Make the payment	Attacker transfers payment to the vote seller.	Estep	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion		
T	2.3.2	Voter Coercion	Attacker influences voter via threat or intimidation.	Jefferson-04 Mote	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Voter training (2) Receipt-free voting system (3) Strong legal deterrence	
T	2.3.3	Pay Voter Not to Vote	Attacker pays a voter to NOT cast a ballot at all.	Hasen	human-deliberate	Election System	Remote voter	susceptibility to bribery and coercion	(1) Strong legal deterrence	
O	2.4	Attack Cryptography	Identify and exploit weaknesses in the system's cryptography implementation.	Gardner	human-deliberate	Voting System	Network Device, Server, PC	Attacker access to tools, techniques, and information	(1) High assurance software	
T	2.4.1	Compromise key management	Identify and exploit weaknesses in the system's key management process.	Gardner	human-deliberate	Voting System	Network Device, Server, PC	Attacker access to tools, techniques, and information	(1) High assurance software	
T	2.4.2	Compromise randomness	Identify and exploit weaknesses in the system's random number generation.	Gardner	human-deliberate	Voting System	Network Device, Server, PC	Attacker access to tools, techniques, and information	(1) High assurance software	
T	2.4.3	Other protocol compromise	Identify and exploit weaknesses in other security protocols.	Gardner	human-deliberate	Voting System	Network Device, Server, PC	Attacker access to tools, techniques, and information	(1) High assurance software	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.4.4	Cryptanalysis	Attack the system's encryption algorithm	Gardner	human-deliberate	Voting System	Network Device, Server, PC	Attacker access to tools, techniques, and information	(1) High assurance software	
T	2.4.5	Exploit weak password	Expose poorly chosen/protected password.	Gardner/ Yasinsac07	human-deliberate	Voting System	Network Device, Server, PC	Attacker access to tools, techniques, and information	(1) Effective password selection/protection process	
O	3	Insider Attacks	Attacks by elections officials or poll workers.	Gardner/ Yasinsac07	human-deliberate insider	Voting System	Voting System	susceptibility to bribery and coercion	(1) Election official background checks (2) PW background checks (3) Strong legal deterrence (4) Two person integrity	
O	3.1	Inject Malware	Install malicious software on a device so that it can later execute on that device.	Rubin Gardner	human-deliberate insider	Voting	Network Server	PW access to Server and software	(1) Chain of custody (2) Two person integrity (3) High Assurance Software (4) Rigorous testing	
A	3.1.1	Create the Malware	Design, code, and test the software artifact that will be used to attack the voting system.	Rubin/ Gardner	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	None	
O	3.1.1.1	Design the Attack	Identify requirements and construct the architecture for the malicious software.	Gardner	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software	
T	3.1.1.1.1	Flip votes	Create software that will record a vote that is different from the voter's selection.	Gardner/ Yasinsac07	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software (2) Physical vote record	
T	3.1.1.1.2	Create undervote	Create software that records a vote in a race with no voter selection.		human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software (2) Physical vote record	
T	3.1.1.1.3	Alter results	Create software that alters the machine's vote tabulation.	Yasinsac07	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software (2) Physical vote records	
T	3.1.1.1.4	Delete races	Create software that deletes contests from the ballot that is presented to the voter.	Gardner/ Yasinsac07	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	(1) High assurance software	
T	3.1.1.2	Gain necessary knowledge	Attackers must acquire information that allows them to implement and exercise a malware attack.	Gardner	human-deliberate insider	Election System	Voting Machine, sensitive tech data, tech insiders	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	3.1.1.3	Test the malware	Attackers must be able to test the software that they will use in a voting system attack. This may require acquisition of proprietary software and/or hardware.	Garener	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
T	3.1.1.3.1	Replicate environment	In order to test malware, the attacker must be able to create an software/hardware environment that is consistent with the target environment.	Gardner	human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
T	3.1.1.3.2	Simulate the volume	An essential element of testing is to simulate transaction volume.		human-deliberate insider	Election System	not modeled	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption		
O	3.1.1.4	Install the Malware	The attacker install malware on the target device in order to execute the software to achieve the desired impact.	Gardner/Yasinsac07	human-deliberate insider	Voting System	Servers, PC, terminal	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity	
T	3.1.1.4.1	Removable Media	Malware installed from removable media that contracted a virus or other regenerating malware.	Yasinsac07	human-deliberate insider	Ballot Preparation, Voting	Servers, PC, terminal	poor security during election artifacts delivery, insecure voter technology	(1) High assurance software (2) Equipment/media chain of custody (3) Equipment/media two person integrity (4) Strong media authentication	
T	3.1.1.4.2	Botnet	Coordinated effort to install malware across a network on a large number of voting terminals.	Yasinsac07	human-deliberate insider	Voting	Network	Poor network security	(1) Voting terminal not network connected (2) Voting server not network connected (3) Strong network security	
T	3.1.1.4.3	Vendor Installed	Malicious software may be installed by a member of the vendor's development team.	Gardner	human-deliberate insider	Election System	not modeled	out of scope	(1) High assurance software (2) Software chain of custody (3) Employee background checks (4) Strong legal deterrence	
T	3.1.1.4.4	During L&A	Malicious software may be installed by a member of the logic and accuracy test team.	Gardner/Yasinsac07	human-deliberate insider	Canvass	Servers, PC, terminal	inability to detect the clever insider's infiltration of the L&A test script	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Election official background checks (5) Strong legal deterrence	
T	3.1.1.4.5	During Sleepover	Malicious software installed by a pollworker or elections official that has exclusive control of the terminal after L&A and before the election.	Gardner	human-deliberate insider	Ballot Preparation, Voting	Precinct Kiosk	poor security during election artifacts delivery	(1) High assurance software (2) Strong legal deterrence (3) Locked equipment cages for sleepover	
O	3.1.1.5	Trigger the Malware	Create the code so that execution is automatic.	Gardner	human-deliberate insider	Voting	Servers, PC, terminal	Poor security of voting equipment	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.1.1.5.1	Automatic	Create the code to wait for a specific action to trigger its full operation.	Yasinsac07	human-deliberate insider	Voting	Servers, PC, terminal	Poor security of voting equipment		
T	3.1.1.5.2	Cryptic Knock	Attacker utilizes a timing trigger to start malware execution.	Yasinsac07	human-deliberate insider	Voting	Servers, PC, terminal	overcoming the defense against cryptic knocks	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	
T	3.1.1.5.3	Timing	Attacker utilizes a timing trigger to start malware execution.	Gardner	human-deliberate insider	Voting	Servers, PC, terminal	Poor security of voting equipment		
T	3.2	Manipulate ballot definition	Attacker alters the ballot definition to manipulate voter selections.	NIST	human-deliberate insider	Create Ballot Style	Votable Ballot	faulty validation process; personnel training or integrity issues	(1) High assurance software (2) Legal deterrence	
T	3.3	Denial of Service	Attempt to prevent voting system operation.	Rubin	human-deliberate insider	Voting System	Servers, PC, terminal	Poor network security, poor security configuration by admin	(1) High assurance software (2) Legal deterrence	
T	3.4	Manipulate voted ballots	Attacker changes selections on voted ballots.	Yasinsac07	human-deliberate insider	Ballot Delivery (R)	Marked Ballot	faulty validation process; personnel training or integrity issues	(1) High assurance software (2) Legal deterrence	
T	3.5	Manipulate accumulation data	Attacker alters tabulation data.	Yasinsac07	human-deliberate insider	Precinct Closeout	Machine Accumulation	faulty validation process; personnel training or integrity issues	(1) High assurance software (2) Legal deterrence	
T	3.6	Manipulate audit data	Attacker alters data that is retained for audit use.	Yasinsac07	human-deliberate insider	Contest Audit	Audit Results	lack of transparency, oversight; inability to detect or recover	(1) High assurance software (2) Legal deterrence	
T	3.7	Manipulate randomization	Attacker compromises randomization algorithm to alter votes or tabulation.	Gardner	human-deliberate insider	Contest Audit	Audit Results	lack of transparency, oversight; inability to detect or recover	(1) High assurance software (2) Legal deterrence	
O	3.8	Undetectable voter error		Yasinsac	human-unintentional	Voting	Eligible Voter	Voting machine interface	(1) Interactive voter interface (2) Under/over vote check	
T	3.8.1	Human error mis-mark	Voter marks the wrong selection indicator, i.e. does not properly match the selection indicator to their preferred choice.	Yasinsac	human-unintentional	Mark Ballot	Eligible Voter	Voting machine interface	(1) Voter training	
T	3.8.2	Ballot Design Flaw	The ballot structure or presentation causes voters to make selection errors.	Gardner/ Yasinsac07	human-unintentional	Create Ballot Style	Votable Ballot	faulty testing process; personnel training or integrity issues	(1) Rigorous ballot design testing	
T	3.8.3	Correction mistake	Voter fails to follow instructions when making a correction, the ballot may be rejected.		human-unintentional	Mark Ballot	Eligible Voter	Voting machine interface	(1) Interactive voter interface	
T	3.8.4	Candidate name confusion	Voter may confuse candidate names on long ballots.		human-unintentional	Mark Ballot	Eligible Voter	Voting machine interface	(1) Voter training	

8 Hand Counted Paper Ballots

In this tree, we consider threats to voting systems where voters use physical ballots are used to mark votes and machines are not used to accumulate contest totals. Hand-counted paper ballots (HCPB) are the only one of seven voting systems considered that do not use computer-based technology. HCPB is one of four systems that use physical (paper) ballots, including PCOS, CCOS, and Vote by Mail.

From a risk assessment standpoint, HCPB has an absence of threats associated with the use of computer-based technology. Because voting is assumed to take place at precinct-based polling places, the HCPB trees incorporate polling place threats. HCPB trees model threats involving the use of paper ballots. Paper ballots in HCPB can be designed for hand-counting, or they may be the mark sense ballots designed for machine counting, but that might need to be hand-counted in certain circumstances. Hand-counting can take place at polling places or at central operations, and election officials associated with our project say that polling place counting is more predominant, and that it is a less risky approach to election operations. Counting might even take place before polls close, and might need to occur for efficiency and fatigue reasons.

8.1 Hand Counted Paper Ballots Threat Tree

node type	outline number	threat action
A	1	perform insider attack
O	1.1	form inside attack team
T	1.1.1	infiltrate as volunteer poll worker
T	1.1.2	infiltrate as observer
T	1.1.3	staff with attackers
T	1.1.4	collude with other insiders
O	1.2	execute insider attack
O	1.2.1	attack at polling place
O	1.2.1.1	discourage voters
O	1.2.1.1.1	challenge at CheckIn
T	1.2.1.1.1.1	falsely reject voter registration
T	1.2.1.1.1.2	falsely reject id check
T	1.2.1.1.1.3	selectively challenge voters
T	1.2.1.1.1.4	falsely challenge voters on target list
T	1.2.1.1.1.5	destroy registered cards
T	1.2.1.1.2	delay open/close with excuses
O	1.2.1.1.3	create long lines
T	1.2.1.1.3.1	work slowly to stymie
T	1.2.1.1.4	stymie voters needing assistance
T	1.2.1.1.5	issue incorrect ballot style
T	1.2.1.1.6	mislead w/phony ballot change
T	1.2.1.1.7	mislead w/one party only ruse
T	1.2.1.1.8	discourage provisional voting
T	1.2.1.1.9	impede voter access
T	1.2.1.1.10	persuade voter selections
A	1.2.1.2	alter voter's vote
A	1.2.1.2.1	access ballots to alter votes
T	1.2.1.2.1.1	obtain VotableBallot
A	1.2.1.2.1.2	obtain MarkedBallot
T	1.2.1.2.1.2.1	mislead about committing ballot
T	1.2.1.2.1.2.2	collect ballots from voters

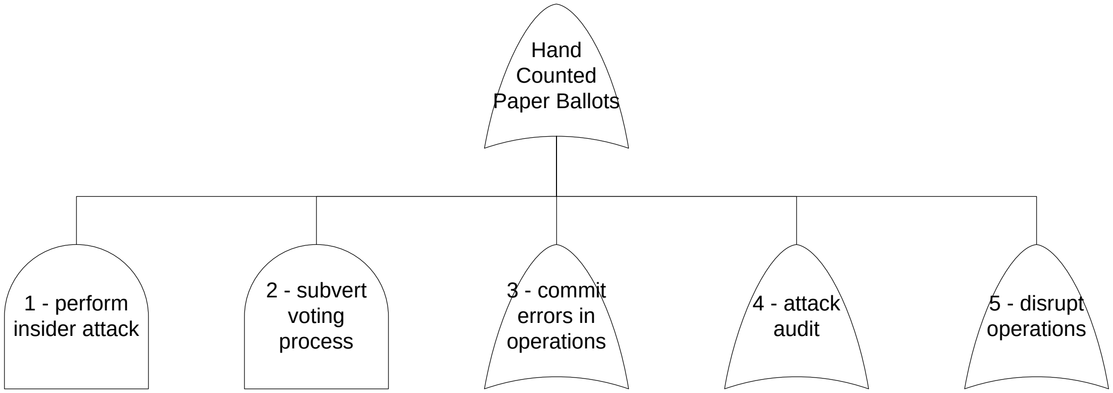
```
                  A     1.2.1.2.1.3       steal provisional ballot
                        T     1.2.1.2.1.3.1       force provisional vote
                        T     1.2.1.2.1.3.2       obtain provisional ballot
                  T     1.2.1.2.1.4       obtain ballot of assisted voter
            O     1.2.1.2.2   tamper with ballots
                  A     1.2.1.2.2.1       subvert no-show vote
                        O     1.2.1.2.2.1.1       conceal poll book tampering
                              T     1.2.1.2.2.1.1.1
                              T     1.2.1.2.2.1.1.2
                              T     1.2.1.2.2.1.1.3
                        T     1.2.1.2.2.1.2       mark VotableBallot
                        T     1.2.1.2.2.1.3       tamper with poll book
                  O     1.2.1.2.2.2       subvert MarkedBallot of voter
                        T     1.2.1.2.2.2.1       mark undervote to create vote
                        T     1.2.1.2.2.2.2       mark vote to create overvote
                        T     1.2.1.2.2.2.3       swap ballot with new MarkedBallot
            T     1.2.1.2.3   commit subverted ballot
      A     1.2.1.3     subvert tabulation
            O     1.2.1.3.1   subvert counting process
                  T     1.2.1.3.1.1       by intentionally miscounting
                  T     1.2.1.3.1.2       by subverting straight-party vote
                  T     1.2.1.3.1.3       by omitting tallies from totals
                  T     1.2.1.3.1.4       by adding tallies multiple times
                  T     1.2.1.3.1.5       by losing a batch of ballots
                  T     1.2.1.3.1.6       by mislabeling a batch of ballots
                  O     1.2.1.3.1.7       by subverting ballot adjudication
                        T     1.2.1.3.1.7.1       incorrectly accept provisional ballots
                        T     1.2.1.3.1.7.2       incorrectly reject provisional ballots
                        T     1.2.1.3.1.7.3       disallow legitimate ballots
                        T     1.2.1.3.1.7.4       incorrectly accept ballots
                        O     1.2.1.3.1.7.5       subvert rules for determining voter intent
                              T     1.2.1.3.1.7.5.1
                              T     1.2.1.3.1.7.5.2
            T     1.2.1.3.2   subvert validation process
O     1.2.2 attack other than polls
      A     1.2.2.1     attack ballots
            T     1.2.2.1.1   access ballots
            O     1.2.2.1.2   tamper with ballots
                  T     1.2.2.1.2.1       by subverting ballot rotation
                  T     1.2.2.1.2.2       by marking ballot
                  T     1.2.2.1.2.3       with invalidating marks
                  T     1.2.2.1.2.4       by undoing voter marks
                  T     1.2.2.1.2.5       by subverting provisional envelope
                  T     1.2.2.1.2.6       with physical damage
            O     1.2.2.1.3   replace ballots
                  T     1.2.2.1.3.1       switch valid ballots with tampered ones
                  T     1.2.2.1.3.2       switch box during transport
                  T     1.2.2.1.3.3       discard / destroy MarkedBallots
      T     1.2.2.2     stuff ballots after closing
      T     1.2.2.3     stuff during canvass or recount
      O     1.2.2.4     attack tabulated results
            T     1.2.2.4.1   subvert reported results
            T     1.2.2.4.2   falsely announce results
```

```
                    T     1.2.2.4.3   alter results transmission
A  2  subvert voting process
   O  2.1  target polling places
      T    2.1.1  by expected voting pattern
      T    2.1.2  where PollWorkers not likely to know Voters
      T    2.1.3  that exploit electoral college rules
      T    2.1.4  that exploit leaked results
      T    2.1.5  where PollWorkers can be co-opted
      T    2.1.6  with lax enforcement of procedures
   O  2.2  form attack team
      A    2.2.1  use cell captains to execute deniable impersonation attack
           T      2.2.1.1  recruit cell captains
           T      2.2.1.2  motivate cell captains
           T      2.2.1.3  recruit attackers
      T    2.2.2  recruit attackers among LegalVoters
      T    2.2.3  recruit brokers
   O  2.3  commit vote fraud attack
      A    2.3.1  perform chain vote
           T      2.3.1.1  acquire VotableBallot
           T      2.3.1.2  vote with pre-marked ballot
           T      2.3.1.3  smuggle VotableBallot out
      O    2.3.2  perform impersonation attack
           O      2.3.2.1  create fraudulent voter registrations
                  T     2.3.2.1.1   register as an housemate
                  T     2.3.2.1.2   register as a dead person
                  T     2.3.2.1.3   register an ineligible person
                  T     2.3.2.1.4   register as a fictitious person
           O      2.3.2.2  create target list of voters to impersonate
                  T     2.3.2.2.1   fraudulent registrations
                  T     2.3.2.2.2   unlikely voters
                  T     2.3.2.2.3   voters likely to vote late in the day
           A      2.3.2.3  execute impersonated voting
                  T     2.3.2.3.1   assign impersonator to voter
                  T     2.3.2.3.2   go to target voter's polling place
                  T     2.3.2.3.3   check in as the impersonated voter
                  T     2.3.2.3.4   vote in place of voter
                  T     2.3.2.3.5   supply rewards
      A    2.3.3  buy or coerce vote
           O      2.3.3.1  motivate voter
                  O     2.3.3.1.1   pay
                        O      2.3.3.1.1.1      pay for candidate support
                               T      2.3.3.1.1.1.1      use drugs, alcohol as payment
                               T      2.3.3.1.1.1.2      pay voters cash
                        T      2.3.3.1.1.2      promise to pay
                  O     2.3.3.1.2   coerce
                        T      2.3.3.1.2.1      promise to punish
                        T      2.3.3.1.2.2      punish and promise more
                        T      2.3.3.1.2.3      punish and promise repair
           O      2.3.3.2  direct voter to make specific votes
                  T     2.3.3.2.1   to make specific votes
                  T     2.3.3.2.2   to not make specific votes
           O      2.3.3.3  verify bought vote
                  T     2.3.3.3.1   by self-recorded casting
```

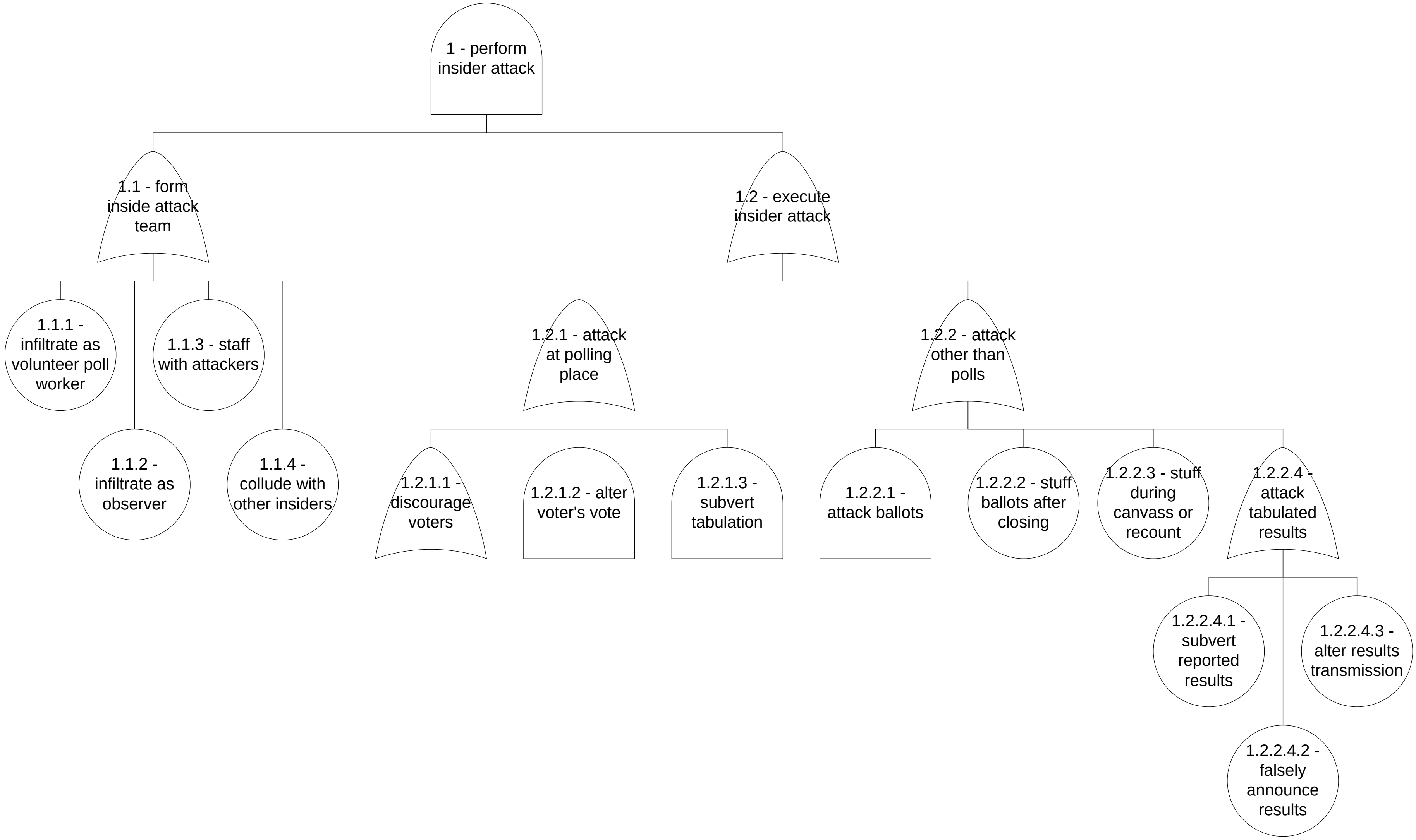
T 2.3.3.3.2 with phony voter assistant
T 2.3.3.3.3 with encoded stray marks
T 2.3.3.3.4 through PollWorker ballot chaining
T 2.3.3.4 supply rewards or punishment
O 2.3.4 vote more than once
T 2.3.4.1 vote using more than one method
T 2.3.4.2 vote in more than one place
T 2.3.4.3 insert unauthorized physical ballots into the ballot box
O 3 commit errors in operations
O 3.1 unintentionally discourage voting
T 3.1.1 create long lines by working slowly
T 3.1.2 mistakenly challenge voters at CheckIn
T 3.1.3 delay opening or closing
T 3.1.4 delay voters with poor assistance
T 3.1.5 send voter to wrong place
T 3.1.6 require provisional by mistake
O 3.2 misinform about overvoting / undervoting
T 3.2.1 allow undervotes without help
T 3.2.2 allow overvotes without help
T 3.2.3 encourage voter override
O 3.3 issue erroneous VotableBallot
T 3.3.1 of the incorrect ballot style
T 3.3.2 with errors in contests or candidates
T 3.3.3 with errors in selection rules
O 3.4 confuse voters with poor ballot design
T 3.4.1 by splitting contests up
T 3.4.2 by spreading response options
T 3.4.3 by keeping disqualified candidates
T 3.4.4 with inconsistent formats
T 3.4.5 by omitting useful shading
T 3.4.6 by omitting use of bold
T 3.4.7 with complex instructions
T 3.4.8 with distant instructions
T 3.4.9 with no correction guidance
T 3.4.10 force least-objectionable choice
T 3.4.11 publish invalid sample ballots
O 3.5 mishandle ballots
T 3.5.1 lose ballots by accident
T 3.5.2 abuse ballots by accident
T 3.5.3 stuff, swap, or lose the ballot box
T 3.5.4 run out of ballots
O 3.6 commit hand tabulation errors
T 3.6.1 by making counting mistakes
T 3.6.2 in straight-party vote tabulation
T 3.6.3 due to improper tabulation technique
T 3.6.4 by omitting tallies from totals
T 3.6.5 by adding tallies multiple times
T 3.6.6 by losing a batch of ballots
T 3.6.7 by mislabeling a batch of ballots
T 3.6.8 due to language differences
O 3.7 make mistakes in ballot adjudication
T 3.7.1 incorrectly accept provisional ballots
T 3.7.2 incorrectly reject provisional ballots

    - T 3.7.3 disallow legitimate ballots
    - T 3.7.4 incorrectly accept ballots
    - T 3.7.5 by misapplying rules for determining voter intent
- O 4 attack audit
  - O 4.1 attack election evidence
    - T 4.1.1 destroy ElectionArtifacts
    - T 4.1.2 mishandle ElectionArtifacts
    - T 4.1.3 add new fraudulent evidence
    - T 4.1.4 modify ElectionArtifacts
  - O 4.2 improperly select audit samples
    - T 4.2.1 select audit units before election
    - T 4.2.2 select non-randomly
    - T 4.2.3 use subverted selection method
    - T 4.2.4 ignore proper selections
  - O 4.3 use poor audit process
    - T 4.3.1 misguide auditors
    - T 4.3.2 audit insufficient sample
    - T 4.3.3 exploit variation in batch sizes
    - T 4.3.4 establish single contest audit rule
    - T 4.3.5 arrange contest audit
    - T 4.3.6 select audited items before commit
    - T 4.3.7 tamper with audit totals
    - T 4.3.8 avoid correction
    - T 4.3.9 overwhelm audit observers
  - T 4.4 commit auditing error
  - T 4.5 compromise auditors
  - O 4.6 attack audit results
    - T 4.6.1 mishandle audit batch
    - T 4.6.2 add fraudulent result data
    - O 4.6.3 attack audit data
      - T 4.6.3.1 modify deliberately
      - T 4.6.3.2 modify unintentionally
    - T 4.6.4 publish bogus audit results
- O 5 disrupt operations
  - O 5.1 disruption from natural events
    - T 5.1.1 natural disaster
    - T 5.1.2 severe weather
  - O 5.2 disruption from environment events
    - O 5.2.1 environmental failures
      - T 5.2.1.1 experience a fire
      - T 5.2.1.2 experience power disruptions
      - T 5.2.1.3 experience effects of humidity
    - T 5.2.2 hazardous accidents
  - T 5.3 disruption from human-created events
  - O 5.4 discourage voter participation
    - T 5.4.1 misinform voters
    - T 5.4.2 threaten personal violence
    - T 5.4.3 threaten mass violence
    - T 5.4.4 commit an act of terror
    - T 5.4.5 intimidate to suppress turnout

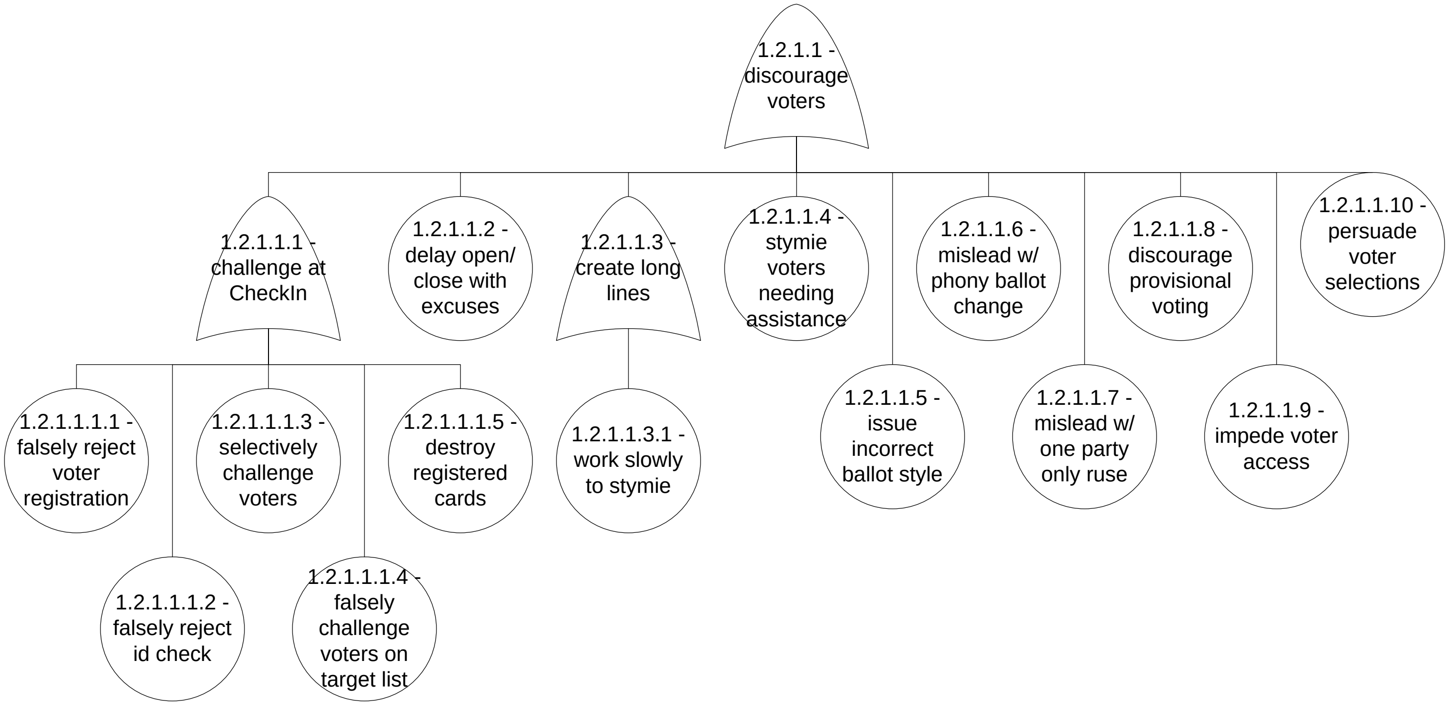
8.2 Hand Counted Paper Ballots Threat Tree –Graphic


Hand Counted Paper Ballots
1 - perform insider attack
2 - subvert voting process
3 - commit errors in operations
4 - attack audit
5 - disrupt operations

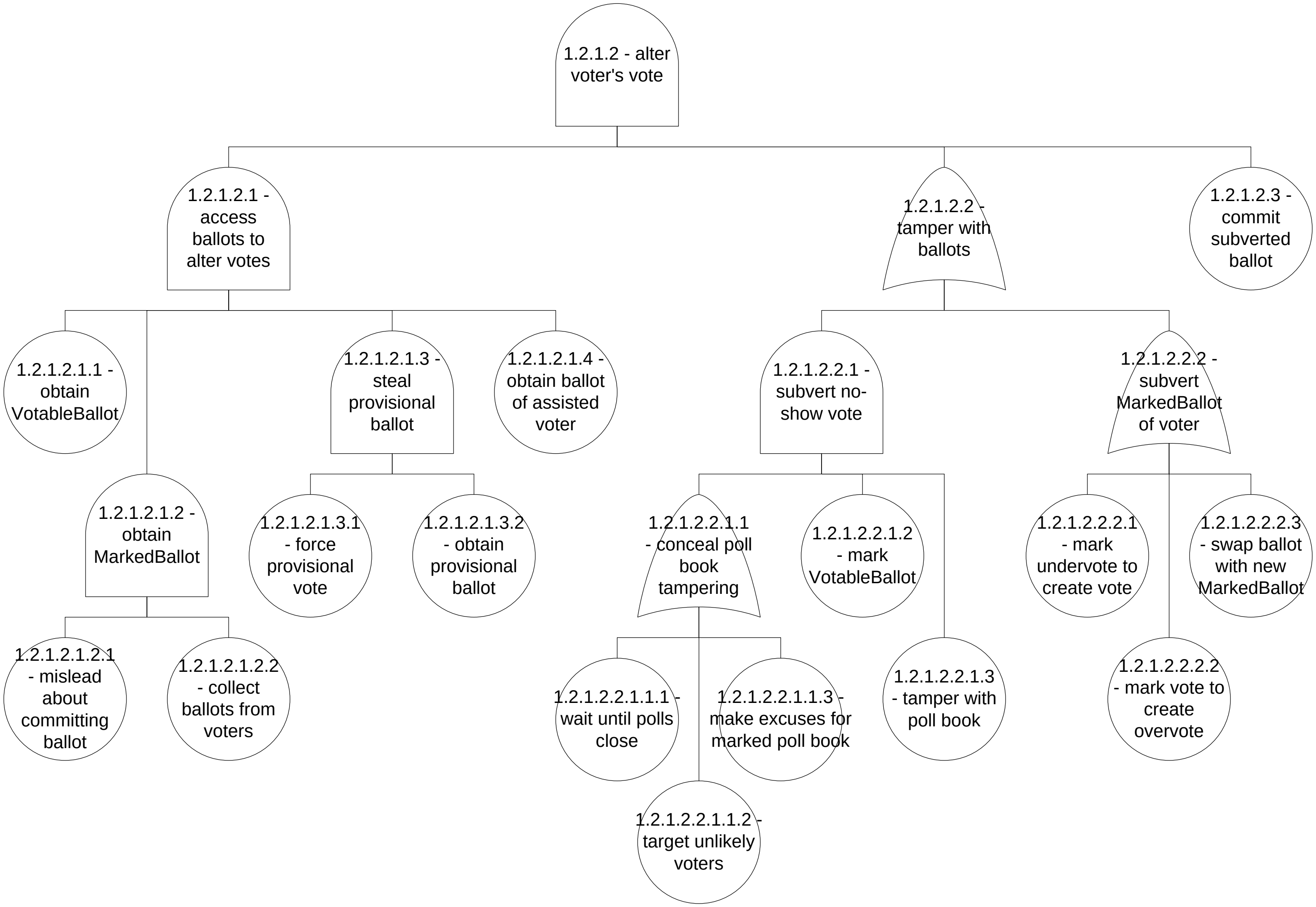
8-1 HCPB Overview


1 - perform insider attack
1.1 - form inside attack team
1.2 - execute insider attack
1.1.1 - infiltrate as volunteer poll worker
1.1.3 - staff with attackers
1.1.2 - infiltrate as observer
1.1.4 - collude with other insiders
1.2.1 - attack at polling place
1.2.2 - attack other than polls
1.2.1.1 - discourage voters
1.2.1.2 - alter voter's vote
1.2.1.3 - subvert tabulation
1.2.2.1 - attack ballots
1.2.2.2 - stuff ballots after closing
1.2.2.3 - stuff during canvass or recount
1.2.2.4 - attack tabulated results
1.2.2.4.1 - subvert reported results
1.2.2.4.3 - alter results transmission
1.2.2.4.2 - falsely announce results

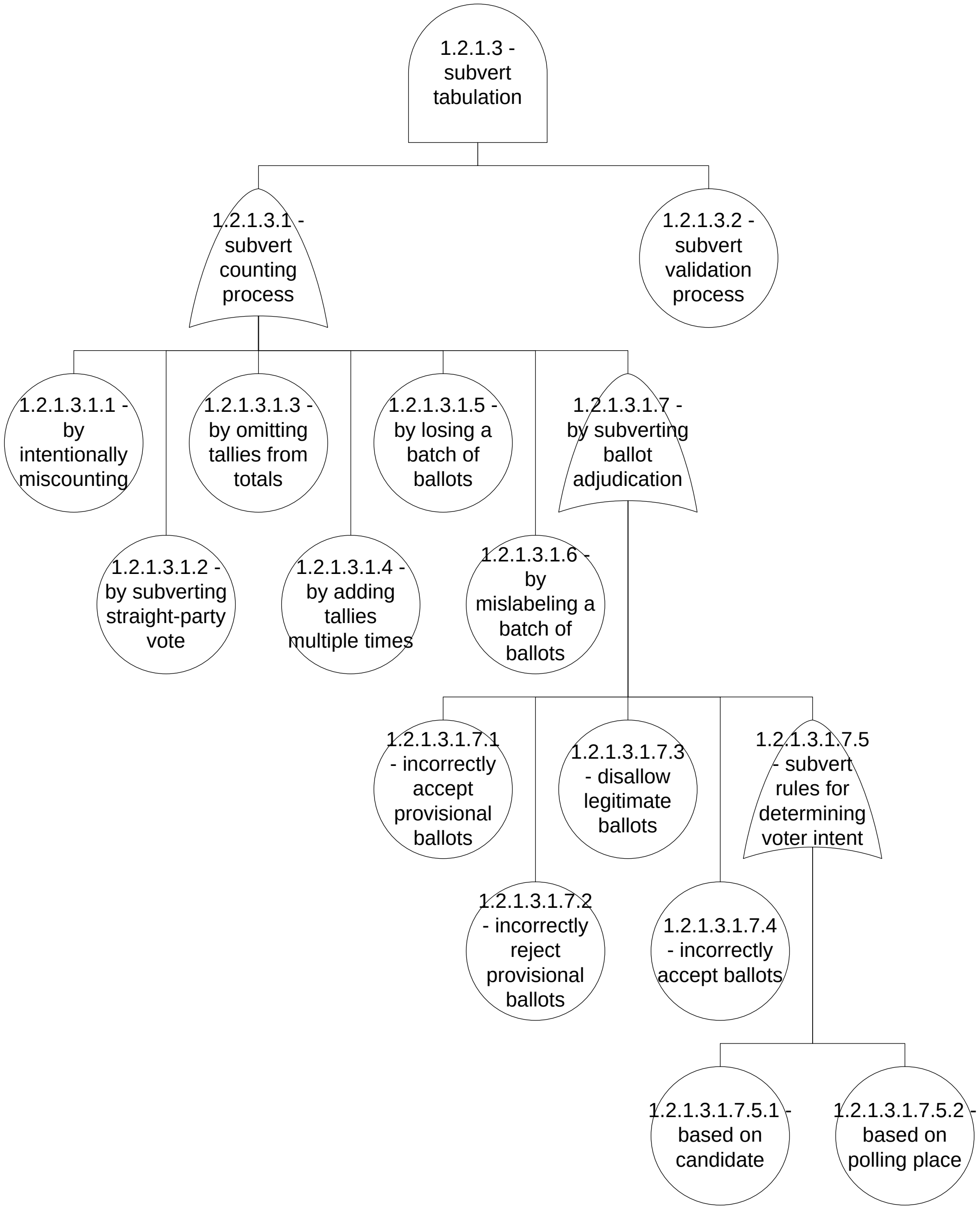
8-2 HCPB Perform Insider Attack


1.2.1.1 - discourage voters
1.2.1.1.1 - challenge at CheckIn
1.2.1.1.2 - delay open/ close with excuses
1.2.1.1.3 - create long lines
1.2.1.1.4 - stymie voters needing assistance
1.2.1.1.5 - issue incorrect ballot style
1.2.1.1.6 - mislead w/ phony ballot change
1.2.1.1.7 - mislead w/ one party only ruse
1.2.1.1.8 - discourage provisional voting
1.2.1.1.9 - impede voter access
1.2.1.1.10 - persuade voter selections
1.2.1.1.1.1 - falsely reject voter registration
1.2.1.1.1.2 - falsely reject id check
1.2.1.1.1.3 - selectively challenge voters
1.2.1.1.1.4 - falsely challenge voters on target list
1.2.1.1.1.5 - destroy registered cards
1.2.1.1.3.1 - work slowly to stymie

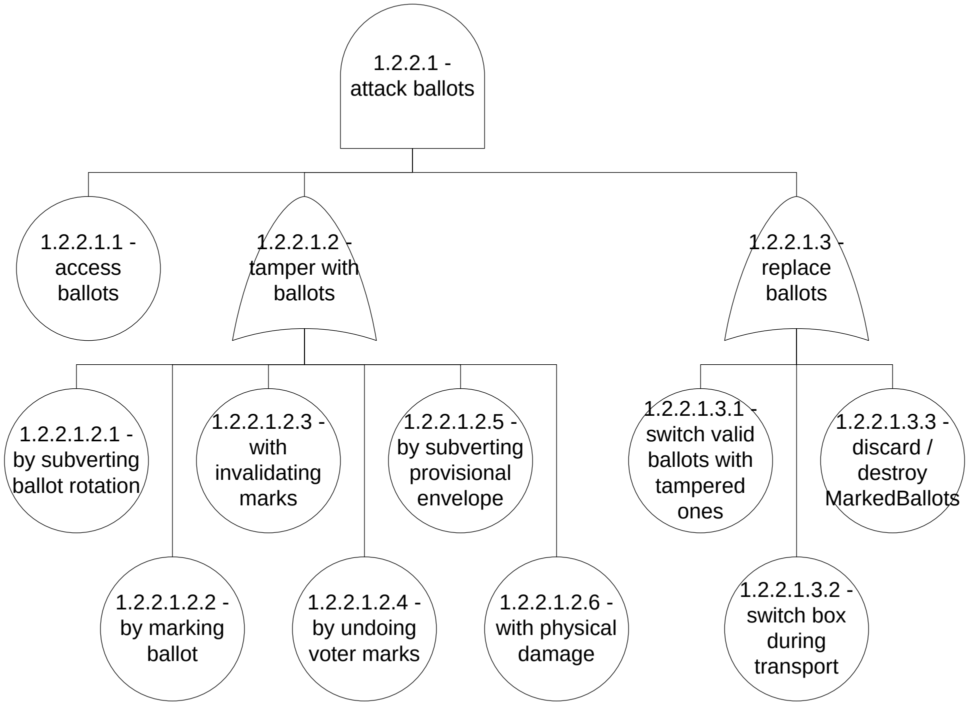
8-3 HCPB Discourage Voters


1.2.1.2 - alter voter's vote
1.2.1.2.1 - access ballots to alter votes
1.2.1.2.2 - tamper with ballots
1.2.1.2.3 - commit subverted ballot
1.2.1.2.1.1 - obtain VotableBallot
1.2.1.2.1.2 - obtain MarkedBallot
1.2.1.2.1.3 - steal provisional ballot
1.2.1.2.1.4 - obtain ballot of assisted voter
1.2.1.2.2.1 - subvert no-show vote
1.2.1.2.2.2 - subvert MarkedBallot of voter
1.2.1.2.1.3.1 - force provisional vote
1.2.1.2.1.3.2 - obtain provisional ballot
1.2.1.2.2.1.1 - conceal poll book tampering
1.2.1.2.2.1.2 - mark VotableBallot
1.2.1.2.2.2.1 - mark undervote to create vote
1.2.1.2.2.2.3 - swap ballot with new MarkedBallot
1.2.1.2.1.2.1 - mislead about committing ballot
1.2.1.2.1.2.2 - collect ballots from voters
1.2.1.2.2.1.1.1 - wait until polls close
1.2.1.2.2.1.1.3 - make excuses for marked poll book
1.2.1.2.2.1.3 - tamper with poll book
1.2.1.2.2.2.2 - mark vote to create overvote
1.2.1.2.2.1.1.2 - target unlikely voters

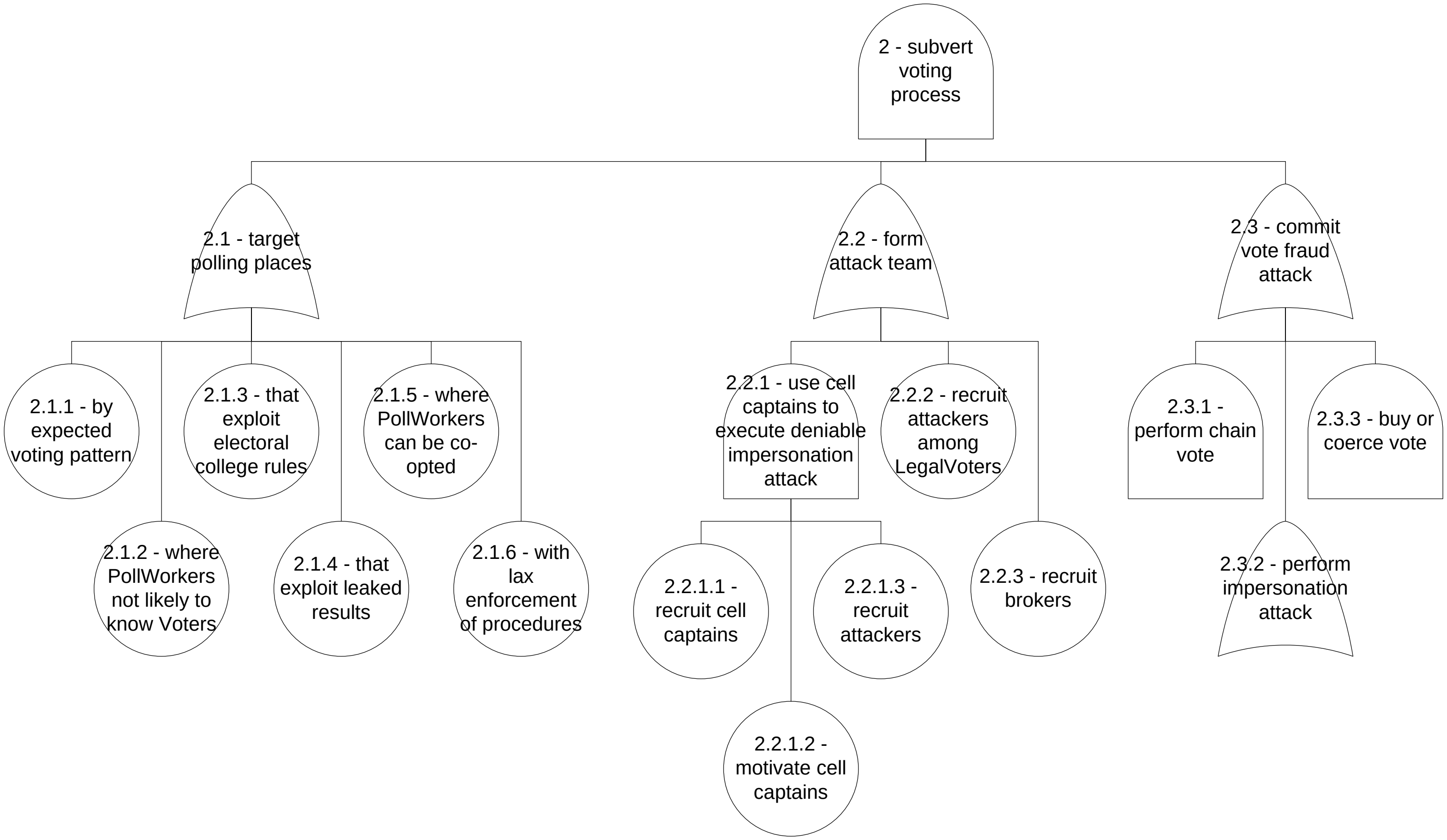
8-4 HCPB Alter Voter's Vote


1.2.1.3 - subvert tabulation
1.2.1.3.1 - subvert counting process
1.2.1.3.2 - subvert validation process
1.2.1.3.1.1 - by intentionally miscounting
1.2.1.3.1.2 - by subverting straight-party vote
1.2.1.3.1.3 - by omitting tallies from totals
1.2.1.3.1.4 - by adding tallies multiple times
1.2.1.3.1.5 - by losing a batch of ballots
1.2.1.3.1.6 - by mislabeling a batch of ballots
1.2.1.3.1.7 - by subverting ballot adjudication
1.2.1.3.1.7.1 - incorrectly accept provisional ballots
1.2.1.3.1.7.2 - incorrectly reject provisional ballots
1.2.1.3.1.7.3 - disallow legitimate ballots
1.2.1.3.1.7.4 - incorrectly accept ballots
1.2.1.3.1.7.5 - subvert rules for determining voter intent
1.2.1.3.1.7.5.1 - based on candidate
1.2.1.3.1.7.5.2 - based on polling place

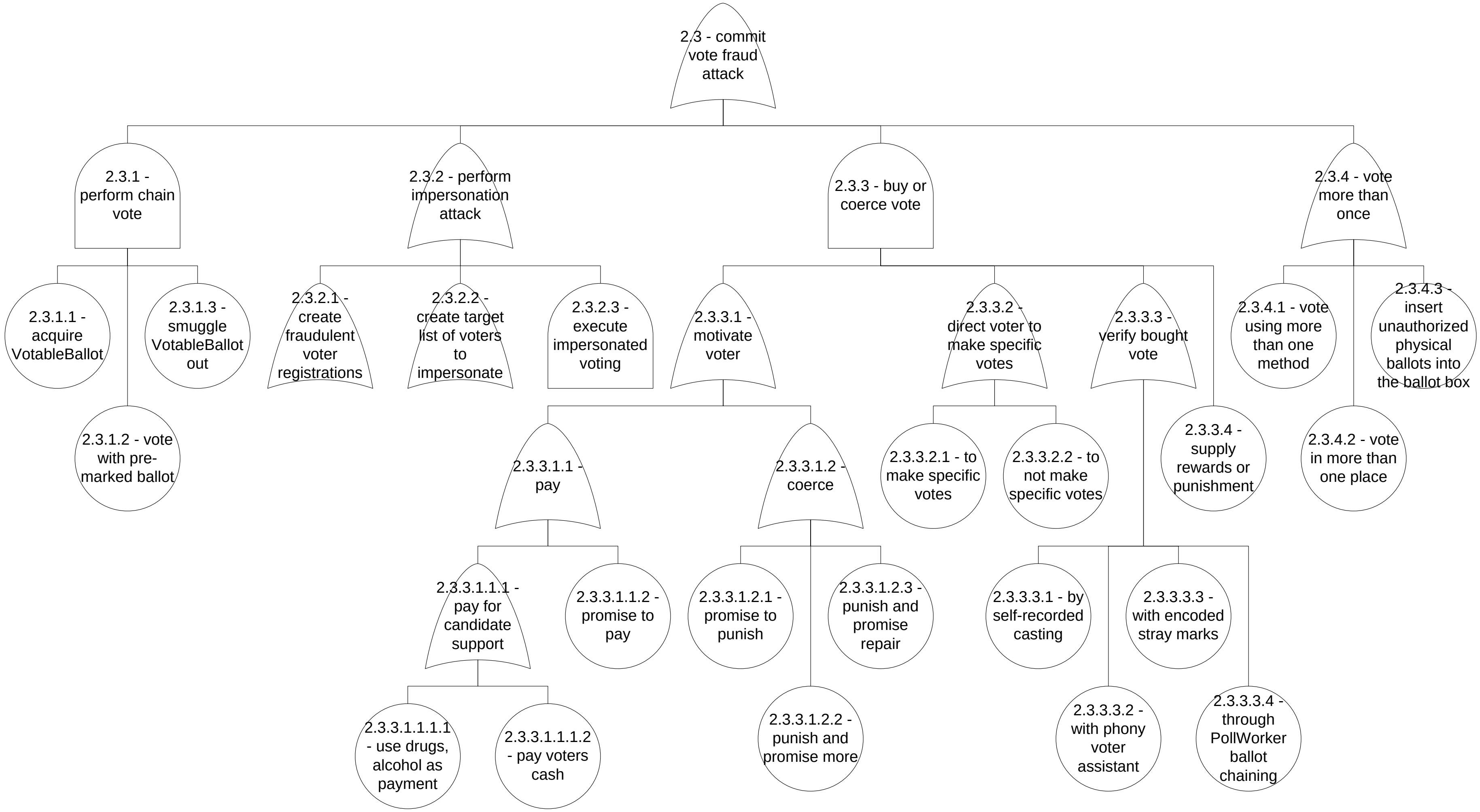
8-5 HCPB Subvert Tabulation


1.2.2.1 - attack ballots
1.2.2.1.1 - access ballots
1.2.2.1.2 - tamper with ballots
1.2.2.1.3 - replace ballots
1.2.2.1.2.1 - by subverting ballot rotation
1.2.2.1.2.2 - by marking ballot
1.2.2.1.2.3 - with invalidating marks
1.2.2.1.2.4 - by undoing voter marks
1.2.2.1.2.5 - by subverting provisional envelope
1.2.2.1.2.6 - with physical damage
1.2.2.1.3.1 - switch valid ballots with tampered ones
1.2.2.1.3.2 - switch box during transport
1.2.2.1.3.3 - discard / destroy MarkedBallots

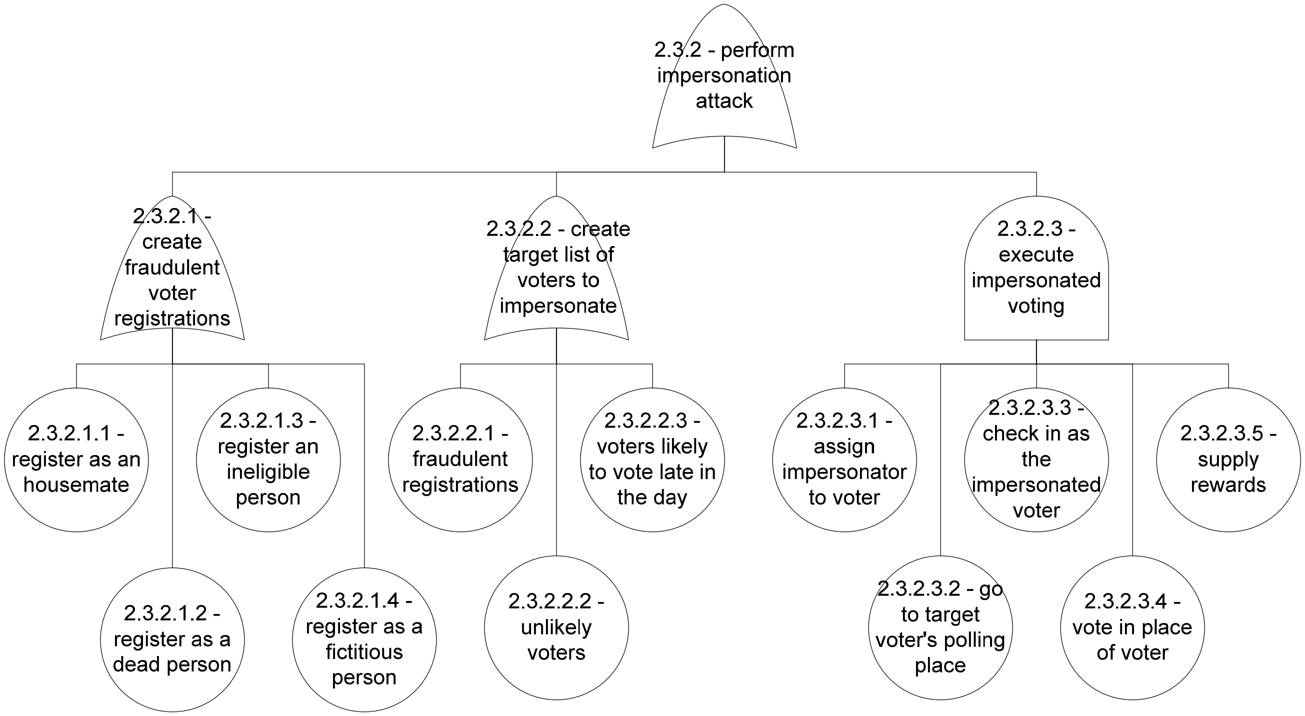
8-6 HCPB Attack Ballots


2 - subvert voting process
2.1 - target polling places
2.2 - form attack team
2.3 - commit vote fraud attack
2.1.1 - by expected voting pattern
2.1.2 - where PollWorkers not likely to know Voters
2.1.3 - that exploit electoral college rules
2.1.4 - that exploit leaked results
2.1.5 - where PollWorkers can be co-opted
2.1.6 - with lax enforcement of procedures
2.2.1 - use cell captains to execute deniable impersonation attack
2.2.2 - recruit attackers among LegalVoters
2.2.3 - recruit brokers
2.2.1.1 - recruit cell captains
2.2.1.2 - motivate cell captains
2.2.1.3 - recruit attackers
2.3.1 - perform chain vote
2.3.2 - perform impersonation attack
2.3.3 - buy or coerce vote

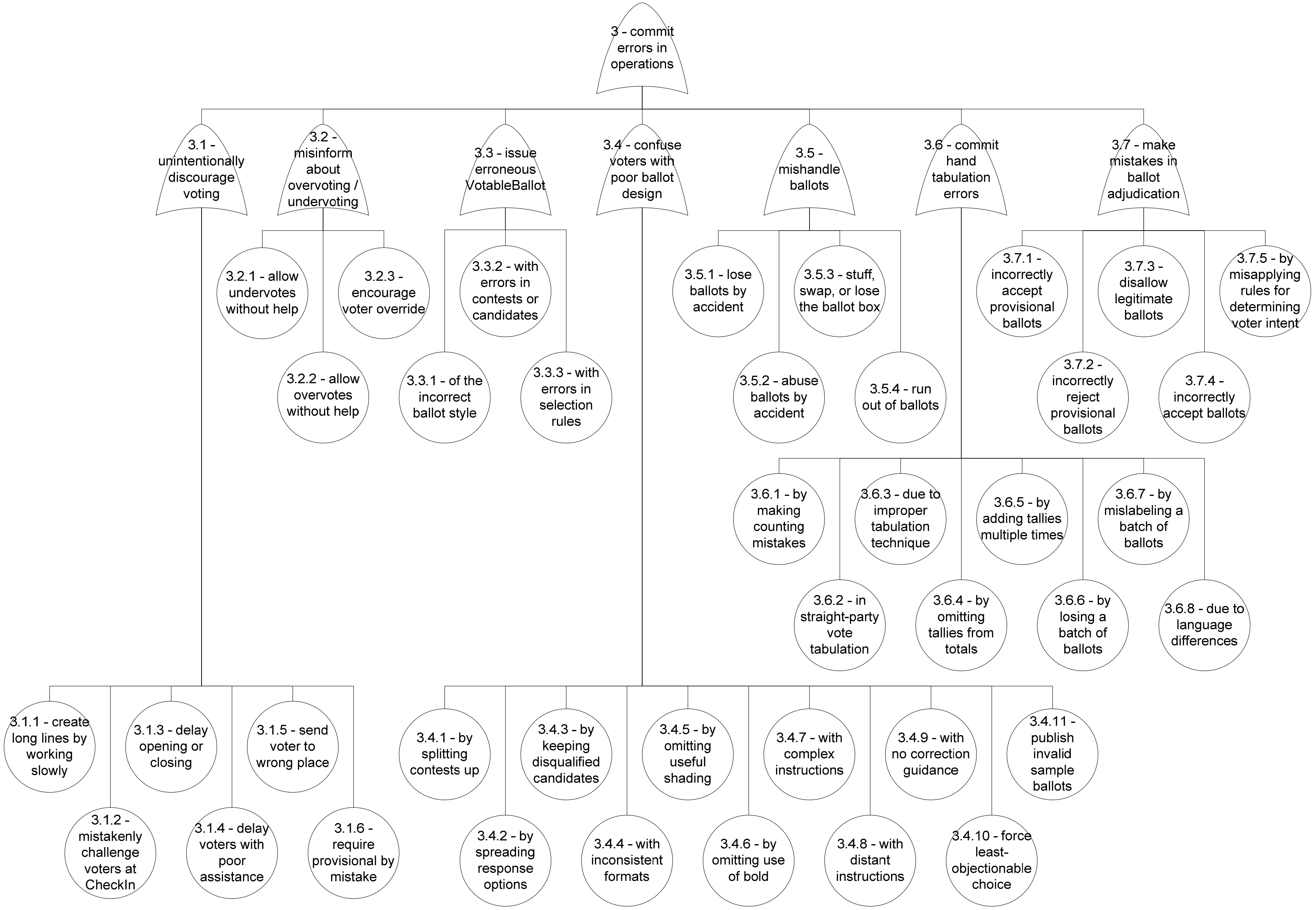
8-7 HCPB Subvert Voting Process


2.3 - commit vote fraud attack
2.3.1 - perform chain vote
2.3.2 - perform impersonation attack
2.3.3 - buy or coerce vote
2.3.4 - vote more than once
2.3.1.1 - acquire VotableBallot
2.3.1.3 - smuggle VotableBallot out
2.3.1.2 - vote with pre-marked ballot
2.3.2.1 - create fraudulent voter registrations
2.3.2.2 - create target list of voters to impersonate
2.3.2.3 - execute impersonated voting
2.3.3.1 - motivate voter
2.3.3.2 - direct voter to make specific votes
2.3.3.3 - verify bought vote
2.3.3.4 - supply rewards or punishment
2.3.4.1 - vote using more than one method
2.3.4.3 - insert unauthorized physical ballots into the ballot box
2.3.4.2 - vote in more than one place
2.3.3.1.1 - pay
2.3.3.1.2 - coerce
2.3.3.2.1 - to make specific votes
2.3.3.2.2 - to not make specific votes
2.3.3.1.1.1 - pay for candidate support
2.3.3.1.1.2 - promise to pay
2.3.3.1.2.1 - promise to punish
2.3.3.1.2.3 - punish and promise repair
2.3.3.3.1 - by self-recorded casting
2.3.3.3.3 - with encoded stray marks
2.3.3.1.1.1.1 - use drugs, alcohol as payment
2.3.3.1.1.1.2 - pay voters cash
2.3.3.1.2.2 - punish and promise more
2.3.3.3.2 - with phony voter assistant
2.3.3.3.4 - through PollWorker ballot chaining

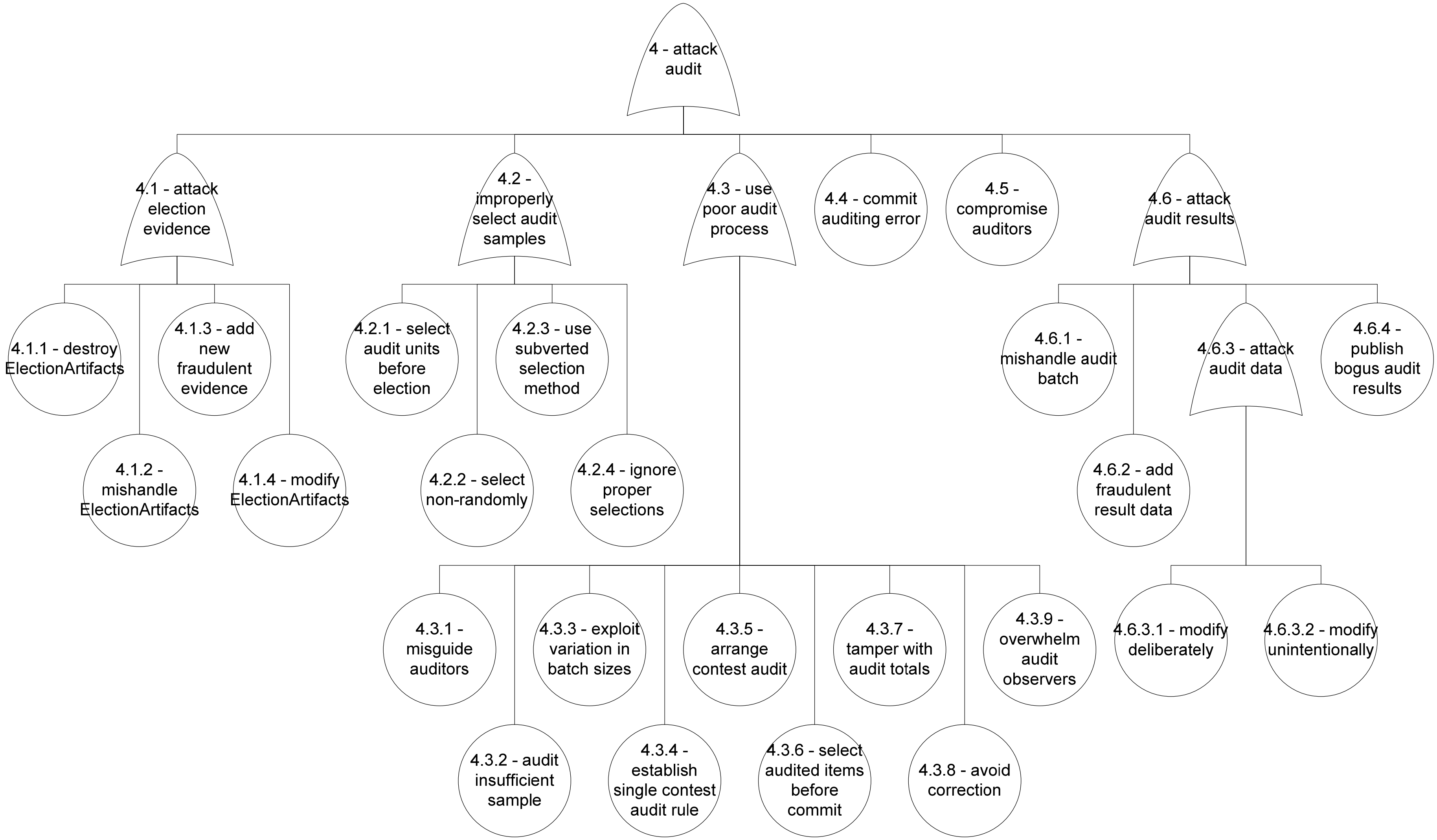
8-8 HCPB Commit Vote Fraud Attack


2.3.2 - perform impersonation attack
2.3.2.1 - create fraudulent voter registrations
2.3.2.2 - create target list of voters to impersonate
2.3.2.3 - execute impersonated voting
2.3.2.1.1 - register as an housemate
2.3.2.1.2 - register as a dead person
2.3.2.1.3 - register an ineligible person
2.3.2.1.4 - register as a fictitious person
2.3.2.2.1 - fraudulent registrations
2.3.2.2.2 - unlikely voters
2.3.2.2.3 - voters likely to vote late in the day
2.3.2.3.1 - assign impersonator to voter
2.3.2.3.2 - go to target voter's polling place
2.3.2.3.3 - check in as the impersonated voter
2.3.2.3.4 - vote in place of voter
2.3.2.3.5 - supply rewards

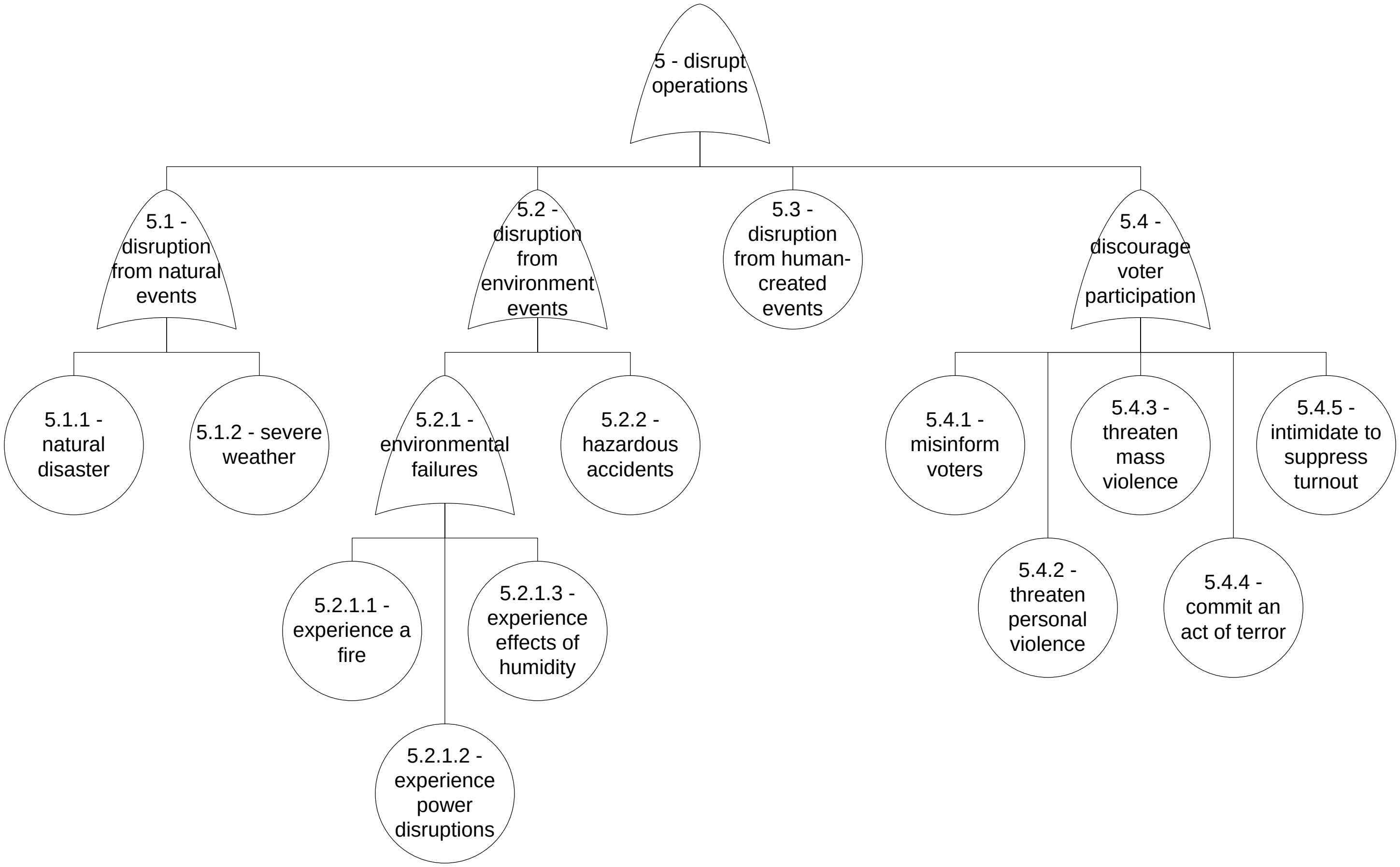
8-9 HCPB Perform Impersonation Attack


3 - commit errors in operations
3.1 - unintentionally discourage voting
3.2 - misinform about overvoting / undervoting
3.3 - issue erroneous VotableBallot
3.4 - confuse voters with poor ballot design
3.5 - mishandle ballots
3.6 - commit hand tabulation errors
3.7 - make mistakes in ballot adjudication
3.2.1 - allow undervotes without help
3.2.2 - allow overvotes without help
3.2.3 - encourage voter override
3.3.1 - of the incorrect ballot style
3.3.2 - with errors in contests or candidates
3.3.3 - with errors in selection rules
3.5.1 - lose ballots by accident
3.5.2 - abuse ballots by accident
3.5.3 - stuff, swap, or lose the ballot box
3.5.4 - run out of ballots
3.7.1 - incorrectly accept provisional ballots
3.7.2 - incorrectly reject provisional ballots
3.7.3 - disallow legitimate ballots
3.7.4 - incorrectly accept ballots
3.7.5 - by misapplying rules for determining voter intent
3.6.1 - by making counting mistakes
3.6.2 - in straight-party vote tabulation
3.6.3 - due to improper tabulation technique
3.6.4 - by omitting tallies from totals
3.6.5 - by adding tallies multiple times
3.6.6 - by losing a batch of ballots
3.6.7 - by mislabeling a batch of ballots
3.6.8 - due to language differences
3.1.1 - create long lines by working slowly
3.1.2 - mistakenly challenge voters at CheckIn
3.1.3 - delay opening or closing
3.1.4 - delay voters with poor assistance
3.1.5 - send voter to wrong place
3.1.6 - require provisional by mistake
3.4.1 - by splitting contests up
3.4.2 - by spreading response options
3.4.3 - by keeping disqualified candidates
3.4.4 - with inconsistent formats
3.4.5 - by omitting useful shading
3.4.6 - by omitting use of bold
3.4.7 - with complex instructions
3.4.8 - with distant instructions
3.4.9 - with no correction guidance
3.4.10 - force least-objectionable choice
3.4.11 - publish invalid sample ballots

8-10 HCPB Commit Errors in Operations


4 - attack audit
4.1 - attack election evidence
4.1.1 - destroy ElectionArtifacts
4.1.2 - mishandle ElectionArtifacts
4.1.3 - add new fraudulent evidence
4.1.4 - modify ElectionArtifacts
4.2 - improperly select audit samples
4.2.1 - select audit units before election
4.2.2 - select non-randomly
4.2.3 - use subverted selection method
4.2.4 - ignore proper selections
4.3 - use poor audit process
4.3.1 - misguide auditors
4.3.2 - audit insufficient sample
4.3.3 - exploit variation in batch sizes
4.3.4 - establish single contest audit rule
4.3.5 - arrange contest audit
4.3.6 - select audited items before commit
4.3.7 - tamper with audit totals
4.3.8 - avoid correction
4.3.9 - overwhelm audit observers
4.4 - commit auditing error
4.5 - compromise auditors
4.6 - attack audit results
4.6.1 - mishandle audit batch
4.6.2 - add fraudulent result data
4.6.3 - attack audit data
4.6.3.1 - modify deliberately
4.6.3.2 - modify unintentionally
4.6.4 - publish bogus audit results

8-11 HCPB Attack Audit


5 - disrupt operations
5.1 - disruption from natural events
5.2 - disruption from environment events
5.3 - disruption from human-created events
5.4 - discourage voter participation
5.1.1 - natural disaster
5.1.2 - severe weather
5.2.1 - environmental failures
5.2.2 - hazardous accidents
5.4.1 - misinform voters
5.4.3 - threaten mass violence
5.4.5 - intimidate to suppress turnout
5.2.1.1 - experience a fire
5.2.1.3 - experience effects of humidity
5.4.2 - threaten personal violence
5.4.4 - commit an act of terror
5.2.1.2 - experience power disruptions

8-12 HCPB Disrupt Operations

8.3 Hand Counted Paper Ballots Threat Matrix

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	1	perform insider attack	intentional abuse of insider access and privileges		human-deliberate insider	voting system	voting system, election artifacts, voters	insider access, availability and willingness of insiders, difficulty in detection	more transparency of the entire elections process, laws governing the bipartisan appointment of precinct officials and the distribution of duties within a polling place, laws dictating the configuration of a polling place and access to it, laws criminalizing voter intimidation, caging and the abuse of the challenge process, training programs for election officials at the national, state and local levels, including enhanced training of precinct officials and more aggressive prosecution of violations; effective audits of elections and the ability to respond to attacks by investigating, prosecuting and correcting abuses after the fact	
O	1.1	form inside attack team	form attack team of one or more attackers with insider privileges		human-deliberate insider	election system, voting system	voting system	insider access, availability and willingness of insiders, difficulty in detection	personnel security, awareness and training, incident response, physical and environmental protection	
T	1.1.1	infiltrate as volunteer poll worker	a lone attacker gains insider privilege by signing up as a poll worker		human-deliberate insider	election system, voting system	election officials	difficulty in discovering infiltrators	personnel security, awareness and training, incident response, physical and environmental protection	
T	1.1.2	infiltrate as observer	gain 'insider' access as a poll observer, either by volunteering, or by qualifying, depending on state laws		human-deliberate insider	election system, voting system	election officials	difficulty in discovering infiltrators	personnel security, awareness and training, incident response, physical and environmental protection	
T	1.1.3	staff with attackers	use insider privilege of ElectionOfficial to staff polling place or post-polling operations with attackers	Jones(2005a) #31	human-deliberate insider	voting system	poll workers	power of election official over polling place operations	transparency of polling place activities, presence of observers	
T	1.1.4	collude with other insiders	collude with one or a few other insiders, possibly using bribery or coercion; either at the polling place, central operations, or between both		human-deliberate insider	election system	election officials	removal of potential means of detection	personnel security, awareness and training, incident response, physical and environmental protection	an ElectionOfficial forms a collusive arrangement between a polling place and central operations, for the purpose of having either party overlook the potential abuses being committed by the other party

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.2	execute insider attack	execute insider attack	execute insider attack	human-deliberate insider	voting system	voting system, election artifacts	insider access, availability and willingness of insiders, difficulty in detection	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	1.2.1	attack at polling place	perform insider attack at polling place	LTM-USA Delivery 01a	human-deliberate insider	voting system	voters, ballots, voting system	power and control of insiders over elections operations	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	1.2.1.1	discourage voters	intentionally discourage voters from voting	Jones(2005a) # 211; Jones(2005a) #332	human-deliberate insider	voting system	checking, check poll book, authenticate voter	unwillingness or inability of voters to appeal poll workers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Poll workers intentionally refuse to allow the voter to vote even though voters name is present on the county register of voters.
O	1.2.1.1.1	challenge at CheckIn	challenge voters during CheckIn		human-deliberate insider	checking	checking	unwillingness or inability of voters to appeal poll workers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.1.1.1	falsely reject voter registration	falsely reject voter claiming they are not registered		human-deliberate insider	voting system	checking, check poll book, authenticate voter	unwillingness or inability of voters to appeal poll workers' decisions	provide appeal process for oversight of poll worker	
T	1.2.1.1.1.2	falsely reject id check	falsely reject voter on identification check		human-deliberate insider	voting system	provide credential	unwillingness or inability of voters to appeal poll workers' decisions	provide appeal process for oversight of poll worker	
T	1.2.1.1.1.3	selectively challenge voters	selectively challenge voters, such as 'undesirable' voters in polling place	Jones #212	human-deliberate insider	voting	voter check in	ability of poll workers or collusions of poll workers to control voter checking; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A corrupt poll worker may use race, gender, appearance of age, a person's attire, etc., as a means of 'profiling' a voter, and then selectively challenge a person's voter status based upon the expectation that a person fitting that profile will vote contrary to attacker

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.1.1.4	falsely challenge voters on target list	creating a target list of voters to challenge and falsely question voters' right to vote	Levitt (2007)	human-deliberate insider	voting	eligible voters; (No Suggestions)	disclosing information of voters	chain of custody for voter lists, including access control policies	The attacker sends registered mail to addresses of registered voters that they've identified as likely to be unfriendly to their candidate. All mail that is returned as undeliverable is placed on what is called a caging list. Then this list is used to challenge the registration or right to vote of those names on it.
T	1.2.1.1.1.5	destroy registered cards	a third party working on behalf of voter registration encourages people to register and after the registration process destroy or discard their cards	Ballotpedia (2008)	human-deliberate insider	election system	registered cards	lack of management oversight over third party	Get the details from third party and mail the voter Id's to the votes instead asking third party to handover the id's.	John volunteers to help register voters before the election. Unknowingly to the officials, he was bribed by the Candidate to destroy voters' cards after the registration process is over.
T	1.2.1.1.2	delay open/close with excuses	delay opening or close with plausible excuses; preventing the voters from voting by making long queues and working slowly leading the voters leave the polling place	Jones (2005a) #33	human-deliberate insider	voting system	votable ballot; authenticate voter; authenticate voter	inability to detect that poll worker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	A poll worker at a precinct works slowly e.g. he intentionally verifies the voter's authentication details slowly making the voters form long lines. Due to long waiting time few voters who cannot wait leave without voting.
O	1.2.1.1.3	create long lines	create long lines		human-deliberate insider	voting	voters	inability to detect that poll worker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.1.3.1	work slowly to stymie	intentionally stymie voters by working slowly		human-deliberate insider	voting system	voting process	inability to detect that poll worker actions are intentional; lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.1.4	stymie voters needing assistance	intentionally stymie voters needing assistance; voter manipulation - improper assistance to voters - improper advantage taken of voters with legitimate need for assistance	Jones (2005a) #332	human-deliberate insider	voting system	feed attempt, feed attempt	lack of management oversight over poll workers designated to assist at polls	improve the administration of voting on the election day; let the voters be aware of the rules and regulations prior to the election day improve the poll worker; training	John is a poll worker for a particular precincts election and is responsible for assisting the voter say 'X' needing help while marking the ballot. His main aim in this threat attack is to stymie the voters from voting or vote for the voters who ask for help. If X has trouble marking the ballot, John can take advantage of the situation and change the ballot or simply without revising submit the ballot resulting in the loss or cancellation of vote.
T	1.2.1.1.5	issue incorrect ballot style	issue voter an incorrect ballot style		human-deliberate insider	voter checking	voter	possibility that threat will go undetected by voter	personnel security, voter education	
T	1.2.1.1.6	mislead w/phony ballot change	mislead voters by announcing phony last-minute ballot change		human-deliberate insider	voting	eligible voter, signed in voter	susceptibility of voters to believe what was being informed by the poll worker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker passes out the ballots to voters and tell them there has been a changed on the ballot.
T	1.2.1.1.7	mislead w/one party only ruse	mislead voters by announcing that only one party is allowed to vote		human-deliberate insider	voting	eligible voter, signed in voter	susceptibility of voters to believe what was being informed by the poll worker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker tells voters that only registered voters of one party is allowed to vote
T	1.2.1.1.8	discourage provisional voting	discourage provisional voting		human-deliberate insider	voting	authenticate voter	unwillingness or inability of voters to appeal poll workers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	poll worker turns voter away by not issuing a provisional ballot
T	1.2.1.1.9	impede voter access	impede voter access to physical polling place; an attacker selectively prevents voters from some precincts, typically under some kind of color of authority.		human-deliberate insider	voting	voters and voting	if a voter must be present at a particular location (e.g. precinct) to cast a ballot, it is possible to prevent the voter from voting by physical exclusion.	Physical security at polling places; public education	A sheriff in a rural jurisdiction, unlikely to be observed by media or activists, impedes some voters from getting to the polling place by conducting improper traffic stops outside select precincts

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.1.10	persuade voter selections	persuade the voter to vote a certain way	Jones(2005a) #332	human-deliberate insider	voting	voting activity	lack of decisiveness in the voter, lack of management oversight over poll workers	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Poll worker/election official/voter during the day of election intrudes into personnel privacy of the voter and tries to persuade him to cast his vote a certain way with suggestive, though non-threatening remarks
A	1.2.1.2	alter voter's vote	alter voter's vote in polling place	LTM-USA Delivery 01a	human-deliberate insider	voting system	voter, one voter	poll worker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
A	1.2.1.2.1	access ballots to alter votes	access ballots, either Marked, Provisional, or assisted, to steal votes		human-deliberate insider	election system, voting system	one voter	poll worker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	steal votes through improperly accessed ballots
T	1.2.1.2.1.1	obtain VotableBallot	obtain VotableBallot		human-deliberate insider	election system	one voter	poll worker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
A	1.2.1.2.1.2	obtain MarkedBallot	create plausible reason to obtain MarkedBallot		human-deliberate insider	voting	one voter	poll worker discretion to instruct voter; voter's lack of understanding	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.2.1.2.1	mislead about committing ballot	mislead voters about correct commitment of ballot	http://www.lex18.com/Global/story.asp?S=10037216&nav=menu203_2	human-deliberate insider	voting	one voter	poll workers have discretion to instruct voters and voters do not tend to read informative signs	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	The poll workers told the voters to walk away after the first confirmation. After which, poll workers changed their votes.
T	1.2.1.2.1.2.2	collect ballots from voters	collect ballots from legitimate voters		human-deliberate insider	voting	one voter	poll workers have discretion to instruct voters and voters do not tend to read informative signs	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
A	1.2.1.2.1.3	steal provisional ballot	poll worker forces the voter to vote on provisional ballot-vote manipulation	Jones(2005a) #21	human-deliberate insider	voting system	check poll book for authenticate voter	unwillingness or inability of voters to appeal poll workers' decisions	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Irrespective of the valid information provided by the voter , Poll worker forces voter to vote on provisional ballots. Since the provisional ballots are counted after the voter verification is done, the poll worker can tamper with the provisional ballots before turning them in with other election materials.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.2.1.3.1	force provisional vote	force voter to vote on provisional ballot; voter manipulation- not allowing the eligible voters to vote as the registration information is not available	Jones (2005a) #3	human-deliberate insider	voting	check poll book for authenticate voter	unwillingness or inability of voters to appeal poll workers' decisions	1) An election official at the polling place shall notify the individual that the individual may cast a provisional ballot in that election. (2) The individual shall be permitted to cast a provisional ballot at that polling place upon the execution of a written affirmation by the individual before an election official at the polling place stating that the individual is-- (A) a registered voter in the jurisdiction in which the individual desires to vote; and (B) eligible to vote in that election. (3) An election official at the polling place shall transmit the ballot cast by the individual or the voter information contained in the written affirmation executed by the individual under paragraph (2) to an appropriate State or local election official for prompt verification under paragraph (4). (4) If the appropriate State or local election official to whom the ballot or voter information is transmitted under paragraph (3) determines that the individual is eligible under State law to vote, the individual's provisional ballot shall be counted as a vote in that election in accordance with State law	John is a poll worker at particular precinct elections. He has the access to the poll book where he can verify the voter's authentication to check the eligibility to vote. If the voters name is not present in the poll book or voters hold on to a voter ID card from many years ago which listed an incorrect precinct, it is John's responsibility to issue a provisional ballot to the voter. John here can take advantage of not issuing the provisional ballot to the voter thus resulting in loss of vote.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.2.1.3.2	obtain provisional ballot	tamper with provisional ballots; ballot manipulation - neglect to seal the provisional ballot envelops-not writing the reason on the envelop	Jones(2005a) #33	human-deliberate insider	voting system	ballot	no monitoring or checking or observing PollWorker actions	eliminate barriers to voter registration so as to reduce the use of provisional voting; improve the administration of provisional voting on the Election day; Increase the scrutiny and transparency of provisional voting process; Improve the poll worker training by among other things making clear that provisional ballots should be issued as a last resort and only in limited circumstances , providing instruction on assessing precincts, and requiring examination of provisional ballots for completeness; The poll worker should direct the voter to place the provisional ballot inner envelop into the provisional ballot outer envelope and seal the envelope and cross verify if the ballot is sealed properly. The poll worker here can be negligent or intentionally not seal the envelopes so that the vote can be disregarded.	
T	1.2.1.2.1.4	obtain ballot of assisted voter	steal votes of voters needing assistance		human-deliberate insider	voting	votable or marked ballot	vulnerability of voter in need of assistance to the abuses of malicious poll worker	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	1.2.1.2.2	tamper with ballots	tamper with ballots before they are collected		human-deliberate insider	voting	votable or marked ballot	lack of oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
A	1.2.1.2.2.1	subvert no-show vote	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones (2005a) #311; Jones (2005a) #312 Wvvotes.com (2008)	human-deliberate insider	voting system	check poll book for authenticate voter	unsecured poll book; corrupt official who coerces other poll workers	limited/no access to the ballot boxes to the poll workers after the polls close; improve administration of the poll workers on the election day	John as a poll worker has the responsibility of recording the voters in the poll book. He uses his position and influence, and fill the polling place with attackers letting them vote for no-show voters.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	1.2.1.2.2.1.1	conceal poll book tampering	conceal poll book tampering to reduce the risk of detection		human-deliberate insider	voting, precinct closeout	poll book	lack of access controls on poll book	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.1.1.1	wait until polls close	wait until polls close to tamper with poll book		human-deliberate insider	voting, precinct closeout	poll book	lack of access controls on poll book	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.1.1.2	target unlikely voters	make list of unlikely voters		human-deliberate insider	election system	voter registration databases	access to voter lists and ability to determine voters not likely to vote	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.1.1.3	make excuses for marked poll book	make excuses in case voters show up, and the poll book is pre-signed		human-deliberate insider	voter checking	election official	difficulty in determining the truth when poll workers are lying	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.1.2	mark VotableBallot	mark VotableBallot		human-deliberate insider	voting, precinct closeout	voter	inability to verify voters vote due to lack of voter attribution	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.2.2.1.3	tamper with poll book	tamper with poll book to add no-show voters		human-deliberate insider	voting, precinct closeout	poll book	unsecured poll book; lack of supervision	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
O	1.2.1.2.2.2	subvert MarkedBallot of voter	subvert MarkedBallot of CheckedIn Voter at polls		human-deliberate insider	voting, precinct closeout	voter, marked ballot	inability to verify vote with voter, lack of management oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.2.1	mark undervote to create vote	mark undervote to create vote		human-deliberate insider	voting, precinct closeout	voter	inability to verify voters vote due to lack of voter attribution	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.2.2	mark vote to create overvote	mark vote to create overvote		human-deliberate insider	voting, precinct closeout	voter	inability to verify voters vote due to lack of voter attribution	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.2.2.3	swap ballot with new MarkedBallot	swap ballot with new MarkedBallot		human-deliberate insider	voting, precinct closeout	marked ballot	lack of management oversight	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	
T	1.2.1.2.3	commit subverted ballot	ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Jones(2005a) #41	human-deliberate insider	voting, precinct closeout	provide credential	lack of supervision or other monitoring / poll observers	improved administration of voting on the election day; Video recording after the polls close	A Ballot Stuffer will cast votes on behalf of the people who did not show up to the polls ;sometimes, votes will even be cast by those who are long dead or fictitious characters often referred to as impersonation

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
A	1.2.1.3	subvert tabulation	intentionally commit errors in tabulation (i.e., counting)		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	poor counting and verification processes, lack of transparency	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
O	1.2.1.3.1	subvert counting process	subvert counting process		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	poor counting and verification processes, lack of transparency	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.1.3.1.1	by intentionally miscounting	subvert counting process by intentionally miscounting		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	poor counting and verification processes, lack of transparency	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.1.3.1.2	by subverting straight-party vote	subvert counting process by subverting straight-party vote		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	poor counting and verification processes, lack of transparency	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.1.3.1.3	by omitting tallies from totals	subvert counting process by omitting tallies from totals		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	poor counting and verification processes	multi-person controls to verify correctness of human decisions	
T	1.2.1.3.1.4	by adding tallies multiple times	subvert counting process by adding tallies multiple times		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	poor counting and verification processes, lack of transparency	multi-person controls to verify correctness of human decisions	
T	1.2.1.3.1.5	by losing a batch of ballots	subvert counting process by losing a batch of ballots		human-deliberate insider	precinct closeout, canvass, state accumulation	ballots, contest results	poor ballot accounting processes	personnel security personnel policies; audit and accountability audit and accountability; system and information integrity accuracy tests; planning	
T	1.2.1.3.1.6	by mislabeling a batch of ballots	subvert counting process by mislabeling a batch of ballots		human-deliberate insider	precinct closeout, canvass, state accumulation	ballots, contest results	lack of management oversight	personnel security personnel policies; audit and accountability audit and accountability; system and information integrity accuracy tests; planning	
O	1.2.1.3.1.7	by subverting ballot adjudication	subvert counting process by subverting ballot adjudication		human-deliberate insider	precinct closeout, canvass, state accumulation	contest results	dependence on key election official(s) with centralized power to announce / certify result	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	
T	1.2.1.3.1.7.1	incorrectly accept provisional ballots	incorrectly accept provisional ballots enclosed in envelopes with disqualifying information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #5	human-deliberate insider	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	lack of oversight; lack of voter being informed; inability of voter to protest	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	In King County, Washington in 2005, it was alleged that election officials were counting provisional ballots in parallel with absentee ballots, which could have resulted in accepting provisional ballots for voters who had already voted absentee
T	1.2.1.3.1.7.2	incorrectly reject provisional ballots	incorrectly reject provisional ballots in envelopes with fully compliant information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #6	human-deliberate insider	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	lack of oversight; lack of voter being informed; inability of voter to protest	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	In a 2005 Washington governor's race, King County election officials admitted that 348 provisional ballots had been improperly counted before the voters' registration status could be determined.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.1.3.1.7.3	disallow legitimate ballots	challenge the authenticity of legitimate ballots, including erroneous authenticity challenges, disqualifying marks, etc.	Jones (2005a) #23	human-deliberate insider	canvass, precinct closeout, state accumulation, post certification audit	validate precinct results, resolve provisional ballots, reconcile voter feedback	cannot bind a ballot to a voter	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	An elections official may apply non-existent or hyper-sensitive rules for accepting ballots during hand counting, hand recount, absentee ballot processing, etc.
T	1.2.1.3.1.7.4	incorrectly accept ballots	incorrectly accept ballots with non-legal marks		human-deliberate insider	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	lack of oversight	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	
O	1.2.1.3.1.7.5	subvert rules for determining voter intent	subvert rules for determining voter intent		human-deliberate insider	voting, precinct closeout, canvass	contest results, candidate, political parties	lack of transparency, poor verification process	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.1.3.1.7.5.1	based on candidate	inconsistently apply rules for determining voter intent based for different candidates	Jones (2005a) #521	human-deliberate insider	voting, precinct closeout, canvass	contest results, candidate, political parties	lack of transparency, poor verification process	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.1.3.1.7.5.2	based on polling place	inconsistently apply rules for determining voter intent, depending on which polling place	Jones (2005a) #522	human-deliberate insider	voting, precinct closeout, canvass	contest results, candidate, political parties	lack of transparency, poor verification process	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.1.3.2	subvert validation process	subvert validation process		human-deliberate insider	voting system	BallotBoxAccounting, validate precinct results, validate jurisdiction results	lack of transparency, poor verification process	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
O	1.2.2	attack other than polls	perform insider attack at other than polling place		human-deliberate insider	voting system	contest artifacts	insider access to contest artifacts	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
A	1.2.2.1	attack ballots	perform attacks on VotableBallots or MarkedBallots	Jones (2005a) #421	human-deliberate insider	voting system	votable ballots	access to ballots, difficulty of detection	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.2.1.1	access ballots	access ballots as an insider		human-deliberate insider	voting system	votable ballots	access to ballots	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
O	1.2.2.1.2	tamper with ballots	alter or destroy ballots obtained		human-deliberate insider	voting system	votable ballots	access to ballots	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	1.2.2.1.2.1	by subverting ballot rotation	tamper with ballot design so that ballot rotation is subverted		human-deliberate insider	ballot preparation	votable ballots	failure of tests to detect all anomalies	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	1.2.2.1.2.2	by marking ballot	alter MarkedBallots by marking selections that either exploit undervotes or cause overvotes	Jones (2005a) #421	human-deliberate insider	voting system	precinct close out, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to physical ballots.	paper ballots have no 'final form' status. that is, they can be marked after the voter has cast the ballot. for any system based on physical ballots, each ballot is a constrained data item (cdi). it is a well known security principle that the more cdis there are, the more difficult it is to protect them.	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	After the polls close, poll worker(s) remove(s) ballots from the ballot box. If anytime thereafter they, or with a group of collaborators, gain private access to the paper ballots, they may selectively mark ballots to favor one or more candidates by exploiting undervotes (marking contests where voters did not make a selection) or to create overvotes in contests where voters selected the opponent of a preferred candidate. This could happen at the polling place, between the polling place and the jurisdiction's central site.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.2.1.2.3	with invalidating marks	alter physical ballots by making illegal marks that will invalidate ballots during hand count or hand recount.	Jones (2005a) #421	human-deliberate insider	voting system	precinct close out, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to physical ballots.	paper ballots have no 'final form' status. that is, they can be marked after the voter has cast the ballot. for any system based on physical ballots, each ballot is a constrained data item (cdi). it is a well known security principle that the more cdis there are, the more difficult it is to protect them.	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	After the polls close, poll worker(s) remove(s) ballots from the ballot box. If anytime thereafter they, or with a group of collaborators, gain private access to the paper ballots, they may selectively apply stray or identifying marks to ballots that are marked in support of the opponent of a preferred candidate. This could happen at the polling place, between the polling place and the jurisdiction's central site, etc.
T	1.2.2.1.2.4	by undoing voter marks	Erase or otherwise undo voter's mark on ballot	TMB, possible in Saltman	human-deliberate insider	ballot preparation, voting	marked ballots, especially prior to counting	insider access to ballots; lack of oversight / chain of custody of ballots	ballot chain of custody procedures; post-election review of ballots	Persons with access to marked ballots can obscure voters marks by erasing them or applying opaque stickers over the marks. This is possible even if indelible pens are used to mark the ballots (compare to erasure of pencil marks).
T	1.2.2.1.2.5	by subverting provisional envelope	tamper with provisional ballot envelope to cause rejection; an envelope is altered to change it from an accepted ballot to a rejected ballot	Dallas (2008)	human-deliberate insider	voting, canvass	committed provisional ballot	access to / lack of control or custody of committed ballot	access controls, auditing and logging	
T	1.2.2.1.2.6	with physical damage	tamper with ballots by doing physical damage	CA TTBR	human-deliberate insider	voting	one voter	unobserved physical access to paper	physical access controls	Damage ballots by pouring chemicals onto paper
O	1.2.2.1.3	replace ballots	switch legitimate ballots with tampered ballots		human-deliberate insider	voting system	ballots	access to ballots; lack of management oversight	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	
T	1.2.2.1.3.1	switch valid ballots with tampered ones	switch a set of valid ballots with the ones the tampered ballots		human-deliberate insider	voting system	ballots	access to ballots; lack of management oversight	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	1.2.2.1.3.2	switch box during transport	substitute ballot box (add, discard, change ballots) during transport to central location	Jones(2005a) #413	human-deliberate insider	precinct closeout	one voter, ballot delivery	failure to take the details of the person transferring the votes to the central location	physical and environmental protection-Delivery and Removal, , personnel security-Third Party personnel security	John is a poll worker responsible for tabulating the votes on the election night. This includes all kinds of votes like the absentee ballots, early votes, provisional ballots etc. He can use his influence and try to manipulate the precinct results by ignoring the ballots or by adding counterfeit ballots so as to match the original count of votes since the precinct results will be telephoned to the election department by the inspector prior to transmission.
T	1.2.2.1.3.3	discard / destroy MarkedBallots	use private access to discard or destroy a box of MarkedBallots (fail to replace)		human-deliberate insider	state accumulation, canvass, post certification	precinct close out, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to a physical ballot box.	for any system based on physical ballots, each ballot is a constrained data item (cdi). it is a well known security principle that the more cdis there are, the more difficult it is to protect them.	Ballot accounting, chain of custody, personnel screening	During precinct closeout, an elections official may remove a box of ballots from the controlled area and discard it, e.g. in a trash bin.
T	1.2.2.2	stuff ballots after closing	stuff ballot box after the polls close	Jones (2005a) #413	human-deliberate insider	voting, precinct closeout	ballots, ballot box	access to ballots, ballot box; lack of management oversight	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	
T	1.2.2.3	stuff during canvass or recount	inject ballot box (of physical ballots) during canvass or recount	2004 Washington Governor Contest	human-deliberate insider	canvas, post certification audit	validate total, process remote ballots	after the election, during the validate process, ballot boxes may be placed where they will be found in storage rooms, elections officials' cars, etc.	Ballot watermarking, ballot accounting, registration reconciliation	1. During a recount, an elections official places and then 'finds' a box of ballots in a key-controlled storage room and presents these ballots to the canvassing board for inclusion in the count. 2. During a recount, a poll worker places, and then finds, a box of ballots in the trunk of their car and presents these ballots to the canvassing board for inclusion in the count..
O	1.2.2.4	attack tabulated results	attack results of tabulation process	Jones (2005a) #6	human-deliberate insider	precinct closeout, canvass, state accumulation	election artifacts	dependence on key election official(s) with centralized power to announce / certify result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	

node type	**outline number**	**threat action**	**description**	**reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
T	1.2.2.4.1	subvert reported results	impersonate poll worker reporting preliminary precinct results; malicious outsider threatens the poll worker to disclose false results to the jurisdiction so as to change the election outcome.	Jones(2005a) #51	human-deliberate insider	precinct closeout, canvass, state accumulation	get precinct results flow chart	poll worker impersonation to alter the precinct result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	John is a malicious outsider. He tries to threaten the poll worker who is responsible for reporting the preliminary precinct results to the jurisdiction. Being threatened by the attacker the poll worker announces false results by not considering few ballots like provisional ballots, absentee ballots changing the outcome of the election.
T	1.2.2.4.2	falsely announce results	falsely announce tabulation results; announcement of tabulation result ignoring actual ballots	Jones (2005a) #51	human-deliberate insider	canvass, state accumulation	unofficial results, report results	dependence on key election official(s) with centralized power to announce / certify result	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, separation of duties, physical access controls, auditing and accountability, such as verifying results against tabulated; incident monitoring and reporting; making whole process more transparent to media and public	
T	1.2.2.4.3	alter results transmission	Results will be transmitted to county elections department on the election night. There are chances that the precinct results might be altered before transmitting them to the elections department.	Jones(2005a) #611	human-deliberate insider	precinct closeout	precinct result	attacker can alter the transmission of precinct results by adding a counterfeit ballot box, ignoring the provisional votes etc.,.	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	John is a poll worker responsible for tabulating the votes on the election night. This includes all kinds of votes like the absentee ballots, early votes, provisional ballots etc. He can use his influence and try to manipulate the precinct results by ignoring the ballots or by adding counterfeit ballots so as to match the original count of votes since the precinct results will be telephoned to the election department by the inspector prior to transmission.
A	2	subvert voting process	subvert polling place voting process		human-deliberate, operational	voting system, election system	voting, voters, ballots, poll workers, polling places	susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	planning, risk assessment, awareness and training, incident response, media protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication, system and communications protection	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
O	2.1	target polling places	target polling places		human-deliberate	voting system, election system	poll workers, polling places	availability of information to aid attack strategy	risk assessment, incident response, personnel security	

node type	**outline number**	**threat action**	**description**	**reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
T	2.1.1	by expected voting pattern	select a precinct that follows a particular voting pattern making it easier to carry out the attack	NA	human-deliberate	voting	polling place	increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows	personnel security, including Position Categorization and Personnel Sanctions	John is a poll worker. He selects a precinct of his choice to work on election day. He makes the selection based on the voting pattern the precinct follows. Doing so he can carry out the attacks he can on that particular voting pattern with ease.
T	2.1.2	where PollWorkers not likely to know Voters	target polling places where poll workers are not likely to know voters		human-deliberate	voting	poll workers, authenticate voter, ,	poll workers do not know voters	risk assessment, incident response	
T	2.1.3	that exploit electoral college rules	use winner-take-all electoral college design to tempt a selective attack in a tight presidential race	Campbell (2008), p. 337	human-deliberate	voting system, election system	voting system, election system	availability of polling data enables careful calculation of the number of votes needed to win, which can be leveraged by the winner-take-all electoral design	recommend that states award electoral votes in proportion to popular vote	Several tight presidential elections (1844, 1876, 1884, 1888, 1960, and 2000) could have been turned by fraud in a few selected areas (Campbell 2008, p. 337)
T	2.1.4	that exploit leaked results	target polling places that exploit leaked partial results of hand count before the polls close		human-deliberate	voting system	election artifacts	difficulty controlling insiders with knowledge of partial results	implement personnel policies and sanctions to prevent disclosure; monitor personnel doing the recount	
T	2.1.5	where PollWorkers can be co-opted	target polling places where PollWorkers can be co-opted		human-deliberate	voting	polling place, election official	susceptibility to exploitation by attackers	risk assessment, incident response	
T	2.1.6	with lax enforcement of procedures	target polling places with lax enforcement of procedures		human-deliberate	voting	polling place, election official	susceptibility to exploitation by attackers	risk assessment, incident response	
O	2.2	form attack team	recruit sufficient impersonating attackers		human-deliberate	election system	potential recruits, eligible voters	availability and willingness of recruits	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
A	2.2.1	use cell captains to execute deniable impersonation attack	use cell captains to execute deniable impersonation attack	Jones (2005a) #31	human-deliberate	voting system	authenticate voter, ,	political influence / power of political leaders or election officials	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	2.2.1.1	recruit cell captains	recruit cell captains		human-deliberate	election system	people being recruited	corruptibility or vulnerability of political loyalists of political leader	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	2.2.1.2	motivate cell captains	educate and motivate cell captains in deniable ways		human-deliberate	election system	people being recruited	insulation of lead attacker from discovery	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.2.1.3	recruit attackers	cell captains recruit more attackers	Jones (2005a) #311	human-deliberate	election system	voters	corruptibility of potential impersonators; resources of attackers	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	2.2.2	recruit attackers among LegalVoters	subvertible voters are gathered to increase the impact of chain voting or a group of attackers carry out chain voting attack	Jones (2005b)	human-deliberate	voting system	legal voters	susceptibility of voters to being bribed or intimidated	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	
T	2.2.3	recruit brokers	recruit brokers to buy voters; attacker recruits loyal followers, giving them cash bills to buy votes on behalf of attacker's choices	Campbell (2006) pp. 278, 282, 337	human-deliberate	voting system, election system	eligible voter, signed in voter	attacker's power to acquire significant resources	expand campaign finance reform to cover wholesale vote-buying; prosecute voting conspiracies, including vote haulers and voters; maintain ballot secrecy	A Dodge County, GA, county commissioner used $15,000 in $20 bills, giving $4,000 to one vote 'hauler' to buy votes at the $20 'market' rate; one county commissioner forced his road department employees to work on the campaign or else lose their jobs (Campbell 2008, p. 282)
O	2.3	commit vote fraud attack	commit vote fraud attack		human-deliberate	voting system, election system	voting, voters, ballots, poll workers, polling places	susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	chain of custody controls on ballots, polling place security, multi-party observers	
A	2.3.1	perform chain vote	perform chain voting scheme	Jones (2005b)	human-deliberate	voting system	poll workers, election officials	susceptibility of voters to being bribed or intimidated; lack of polling place security	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	
T	2.3.1.1	acquire VotableBallot	an outside attacker smuggles a VotableBallot or an election insider takes an absentee ballot and uses it for chain voting	Jones (2005b)	human-deliberate	voting system	ballot stock	lack of polling place security	chain of ballot custody procedures, polling place security, including observers	
T	2.3.1.2	vote with pre-marked ballot	subverted voter takes MarkedBallot to polling place and votes with it, while also legally obtaining VotableBallot	Jones (2005b)	human-deliberate	voting system	commit ballot	lack of polling place security; voter privacy measures helps attacker conceal ballots	chain of ballot custody procedures, polling place security, including observers	
T	2.3.1.3	smuggle VotableBallot out	voter smuggles VotableBallot out of polling place and takes it to attacker to enable next cycle of chain voting	Jones (2005b)	human-deliberate	voting system	ballot stock	lack of polling place security; voter privacy measures helps attacker conceal ballots	chain of ballot custody procedures, polling place security, including observers	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.3.2	perform impersonation attack	perform voter impersonation attack	LTM-USA Delivery 01a	human-deliberate	voting system	voting system, ,	accessibility of lists of voters not likely to vote; soft voter authentication process; poll workers don't know voters; willingness of poll workers to engage in fraud	media protection policy and procedures, personnel security, access control, audit and accountability, identification and authentication	Tom is a party worker who has contacts with ElectionsOfficial. Getting EligibleVoters' personal information is an easy task for Tom. He can even prepare a list of EligibleVoters who are unlikely to vote this time through his contacts. After preparing a list, he then prepares fake Id's and bribes a group of loyal followers to impersonate the voters on his list. He sends impersonators to the polling places where PollWorkers are not likely to recognize them.
O	2.3.2.1	create fraudulent voter registrations	create fraudulent voter registrations	Jones(2005a) #1	human-deliberate	election system	election system	poor vetting process, lack of resources, legal constraints on voter registration process	strengthen the controls in the ElectionSystem	
T	2.3.2.1.1	register as an housemate	recruit registers impersonators as housemates / roommates	Jones(2005a) #11, 12	human-deliberate	voting system	people being recruited	corruptibility or vulnerability of recruits	strengthen the controls in the ElectionSystem	A party worker may hire non voters from different state, prepare fake IDs and register them as housemates of LegalVoters and ask them to vote for his/her party candidate.
T	2.3.2.1.2	register as a dead person	register as a deceased or incapacitated person	Jones(2005a) #12	human-deliberate	election system	election system	lack of records management	strengthen the controls in the ElectionSystem	
T	2.3.2.1.3	register an ineligible person	register as an unregistered but ineligible person (e.g., non-citizens, felons)	Jones(2005a) #1	human-deliberate	election system	election system	lack of records management	strengthen the controls in the ElectionSystem	
T	2.3.2.1.4	register as a fictitious person	use a fake Id to register as a fictitious voter	Jones(2005a) #11,12	human-deliberate	voting system	authenticate voter	soft verification process	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	
O	2.3.2.2	create target list of voters to impersonate	create target list of voters to impersonate		human-deliberate	election system	voter lists	access to voter lists	chain of custody controls on voter registration lists, if not public information	
T	2.3.2.2.1	fraudulent registrations	fraudulent registrations		human-deliberate	election system	voters lists	access to voter lists	chain of custody controls on voter registration lists, if not public information	
T	2.3.2.2.2	unlikely voters	make lists of voters very unlikely to vote this election	Jones (2005a) #311	human-deliberate	election system	voter lists	access to voter lists and ability to determine voters not likely to vote	chain of custody controls on voter registration lists, if not public information	Unlikely voters for an election might include infrequent voters, or voters that are absent or overseas
T	2.3.2.2.3	voters likely to vote late in the day	make lists of voters likely to vote late in the day		human-deliberate	election system	voter lists	access to voter lists and ability to identify target voters	chain of custody controls on voter registration lists, if not public information	
A	2.3.2.3	execute impersonated voting	execute impersonated voting		human-deliberate	voting	authenticate voter	failure of election day administration to foil attack	physical and environmental protection, audit and accountability, identification and authentication	
T	2.3.2.3.1	assign impersonator to voter	supply attackers with information about unlikely voter (e.g., name and gender)		human-deliberate	voting system	poll workers, authenticate voter	poll workers fooled by unknown attacker with valid voter information	physical and environmental protection, audit and accountability, identification and authentication	
T	2.3.2.3.2	go to target voter's polling place	impersonator goes to polling place of target voter	Jones(2005a) #311	human-deliberate	voting	voters	susceptibility of insiders to bribery and corruption	physical and environmental protection, including patrolling polling places, looking for suspicious activity	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.3.2.3.3	check in as the impersonated voter	attacker has friends vote for the fake housemates	Jones(2005a) #311	human-deliberate	voter checking	poll workers, authenticate voter	poll workers fooled by unknown attacker with valid voter information	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	
T	2.3.2.3.4	vote in place of voter	impersonate and vote in the place of an EligibleVoter; a list of voters who are unlikely to vote may be prepared and people may be recruited to vote for that person. A polling place where a poll workers are not likely to know voters may be targeted.	Jones (2005a) #311	human-deliberate	voting	authenticate voter	access to lists of voters not likely to vote; poll workers don't know voters; corrupt poll worker	require Credentials at polling places; conduct precise and careful purges on voter lists to remove duplicate names, people who have moved, died, or are otherwise ineligible.	
T	2.3.2.3.5	supply rewards	cell captain provides all required rewards out of own pocket		human-deliberate	election system	voters	susceptibility of insiders to bribery and corruption	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers, physical and environmental protection, limiting access to polling place and providing polling place patrols	
A	2.3.3	buy or coerce vote	motivate voters to either (a) stay away from polls or (b) vote in compliance with attacker demands	Dekel (2004), Fund (2004), Jones(2005a) #21	human-deliberate outsider	voting system, election system	eligible voter, signed in voter	susceptibility of voters to buying and coercion; breach of voter privacy; ability to attribute vote	maintain voter privacy; limit access to polling place	a candidate's confederate goes to the polls with voters willing to sell their vote; and they vote together after legally obtaining their VotableBallots
O	2.3.3.1	motivate voter	motivate voter with bribes or threats		human-deliberate	voting system	voter	human susceptibility to being bribed or coerced	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers, physical and environmental protection, limiting access to polling place and providing polling place patrols	'Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future.' (Fund 2004)
O	2.3.3.1.1	pay	motivate voter with pay		human-deliberate	election system	voter	human susceptibility to being bribed	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.3.3.1.1.1	pay for candidate support	make a direct payment to voters to support a particular candidate; attacker promises to bribe voters if they prove the attacker with evidence that they voted to the particular candidate supported by attacker.	Fund (2004), Dekel (2004)	human-deliberate	voting system	eligible voter, signed in voter	susceptibility of voters to bribery	Educate the voters about the importance of voting	'Democrats are far more skilled at encouraging poor people — who need money — to participate in shady vote-buying schemes. 'I had no choice. I was hungry that day,' Thomas Felder told the Miami Herald in explaining why he illegally voted in a mayoral election. 'You wanted the money, you were told who to vote for."(Fund 2004)
T	2.3.3.1.1.1.1	use drugs, alcohol as payment	use drugs or alcohol as payment for votes; attacker promises and exchanges drugs or alcohol in exchange for voting for attacker's candidates	Campbell (2006) pp. 144, 282, Estep (2009)	human-deliberate	voting system, election system	eligible voter, signed in voter	susceptibility of voters with substance abuse to bribery	maintain ballot secrecy	In 1910, the price of a vote was 'a drink of whiskey' (Campbell 2006, p. 144); in 2002, two Clay County, KY, election officers allegedly used the prescription painkiller OxyContin to buy votes (Estep 2009)
T	2.3.3.1.1.1.2	pay voters cash	pay the 'market' rate for a vote in direct cash payment	Campbell (2006) pp. 278, 283	human-deliberate	voting system, election system	eligible voter, signed in voter	susceptibility of voters to bribery	prosecute voters who sell their vote; throw out illegal votes; maintain ballot secrecy	In a 1987 Kentucky race, the price for a vote reached $200, while in 1996 Dodge County, Georgia, the market rate was $20 per vote (Campbell 2008)
T	2.3.3.1.1.2	promise to pay	promise payment later or promise payment based on subsequent verifiability of voter's carry out attacker's voting demands	Jones(2005a) #311	human-deliberate	voting	voters	susceptibility of voters to bribery	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	
O	2.3.3.1.2	coerce	coerce the voter to vote for the attacker's candidate(s)		human-deliberate	election system	voters	human susceptibility to being coerced	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	
T	2.3.3.1.2.1	promise to punish	promise some form of punishment in order to coerce voter	Van Acker	human-deliberate	election system	eligible voter, signed in voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	An incumbent candidate seeking reelection sends a loyal confederate to the polls accompanying the incumbents' employees, who are coerced to vote for the incumbent, once they receive their votable ballots
T	2.3.3.1.2.2	punish and promise more	provide a real punishment, and then promise more punishment of not compliant		human-deliberate	election system	eligible voter, signed in voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	
T	2.3.3.1.2.3	punish and promise repair	provide a real punishment, and then promise a repair of punishment		human-deliberate	election system	eligible voter, signed in voter	susceptibility of voters to intimidation; lack of voter privacy	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	2.3.3.2	direct voter to make specific votes	direct voter to make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	paper ballot systems	folded marked ballot,	corrupt poll worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
T	2.3.3.2.1	to make specific votes	direct voter to make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	paper ballot systems	folded marked ballot,	corrupt poll worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
T	2.3.3.2.2	to not make specific votes	direct voter to not make specific votes according to attacker's demands	Jones (2005a) #32, Jones(2005b)	human-deliberate	voting	eligible voter	corrupt poll worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
O	2.3.3.3	verify bought vote	assess voter compliance with direction		human-deliberate	voting system	voter	inability to prevent voter attribution	prevent voter attribution with ballot secrecy, preventing stray marks, and making sure that voter assistance is legitimately needed	to ascertain that a bribed voter goes along with the vote fraud, attacker attempts to verify that voter voted for attacker's choices
T	2.3.3.3.1	by self-recorded casting	use a secret camera to self-record voter's ballot casting	Dekel (2004)	human-deliberate	voting system	eligible voter, signed in voter	breech of voter privacy in polling place	Tighten the security of voting system	Voter manages to capture video of his ballot casting, produces it to the attacker as evidence.
T	2.3.3.3.2	with phony voter assistant	assist voter at precinct to verify bought vote; voter requests assistance in order to earn reward from assistant	Jones (2005a) #333	human-deliberate	voting, canvass	sign poll book, validate precinct results	failure to authenticate voter's assistant; failure to detect unusual patterns of assistance (same assistant, higher than normal assistance)	audit and accountability audit precinct results and investigate any unusual voting patterns, such as a high percentage of voter assistance or repeated assistance by the same assistant; prevent by asking voter for reason assistance needed	A man wearing dark glasses and appearing to be sight-impaired shows up with an assistant to help him vote. Following the procedures for check-in, the voter and the assistant obtain a VotableBallot, which is then marked and committed with the full knowledge and help of the assistant, who provides a cash payoff afterwards.
T	2.3.3.3.3	with encoded stray marks	make stray ballot mark for voter attribution		human-deliberate	voting	votable ballot	ability of voter to mark ballot freely	use ballot marking that prevents stray marks; clear plastic ballot sleeve	voter votes for attacker candidates and then votes for a write-in candidate by writing in a predetermined code word intended for an inside confederate to see and verify the bought vote

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	2.3.3.3.4	through PollWorker ballot chaining	voter commits the MarkedBallot into the ballot box and returns the empty VotableBallot to the attacker	Jones (2005a) #32, Jones(2005b)	human-deliberate	paper ballot systems	folded marked ballot,	corrupt poll worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	A political party worker may intimidate EligibleVoters or bribe them to commit a pre MarkedBallot and hand over the unmarked VotableBallot to him. Then this empty VotableBallot is marked by this worker and given to another EligibleVoter who has been bribed or intimidated and the process is repeated.
T	2.3.3.4	supply rewards or punishment	provide promised rewards or punishments based on voter compliance		human-deliberate	election system	post certification audit	difficulty in tracing payments	personnel security, including sanctions against violators	
O	2.3.4	vote more than once	a LegalVoter votes more than once; ballot box stuffing by the voter		human-deliberate	voting	voting	inability of voting system to capture duplicate votes by a voter	system and information integrity, identification and authentication	
T	2.3.4.1	vote using more than one method	vote early and regular, or absentee and provisional as a form of ballot box stuffing	Jones (2005a) #41, TIRA panel	human-deliberate	voting	authenticate voter remote, voter list, voter information, authenticate voter, authentication rules, jurisdiction	inability to or failure to cross-check poll books for different voting methods within a single place (jurisdiction)	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	a voter casts an absentee ballot but then votes again at the polling place on election day
T	2.3.4.2	vote in more than one place	vote in two neighboring states or multiple precincts with registrations in more than one place	Jones (2005a) #11, 312	human-deliberate	voting	voter list, voter information, authenticate voter, authentication rules, jurisdiction	inability to or failure to cross-check voter lists across multiple jurisdictions	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	a husband and wife who move from Pensacola, FL to Mobile, AL prior to a federal election registers and votes in Alabama, then drives to Pensacola on same election day, voting in the precinct for their former address
T	2.3.4.3	insert unauthorized physical ballots into the ballot box	insert unauthorized physical ballots into the ballot box	NA	human-deliberate	voting	commit ballot	cannot bind a paper ballot to a voter. for a physical ballot box with a slot, a voter may stack several ballots and insert them at the same time.	Ballot box attendant, probably not particular effective	A voter may acquire ballot copies, pre-mark them, and insert them into a ballot box with their legal ballot.
O	3	commit errors in operations	commit unintentional errors in polling place operations		human-unintentional	voting system	poll workers, voters, ballots, voting system activities	poor working conditions (fatigue), inadequate training, flawed processes	certification, accreditation, and security assessments, planning, system and services acquisition, awareness and training, contingency planning, incident response, media protection policy and procedures, personnel security	
O	3.1	unintentionally discourage voting	unintentionally discourage the voter from voting		human-unintentional	voting	voter	poor election administration	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
T	3.1.1	create long lines by working slowly	create long lines by working too slowly		human-unintentional	voting	voter	inadequate poll worker training, staffing levels, voter constraints on time, impatience	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.1.2	mistakenly challenge voters at CheckIn	mistakenly challenge voters during CheckIn		human-unintentional	voting	voter	poor poll worker performance; lack of oversight	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
T	3.1.3	delay opening or closing	delay opening or closing polls due to mistakes or slow working		human-unintentional	voting	voter	poor election administration	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
T	3.1.4	delay voters with poor assistance	delay voters by failing to properly assist		human-unintentional	voting	voter	poor poll worker performance; lack of oversight	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
T	3.1.5	send voter to wrong place	erroneously send voter to other polling place		human-unintentional	voting	voter	poor poll worker performance; lack of oversight	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
T	3.1.6	require provisional by mistake	erroneously require a voter to vote provisionally		human-unintentional	voting	voter	poor poll worker performance; lack of oversight	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
O	3.2	misinform about overvoting / undervoting	provide incorrect information about overvotes and undervotes		human-unintentional	voting	voter	poor poll worker performance; lack of oversight	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
T	3.2.1	allow undervotes without help	allow undervotes without help		human-unintentional	voting	voter	failure to assist voter in detecting undervotes	voter education and training; clear ballot instructions that warn users about undervoting	
T	3.2.2	allow overvotes without help	allow overvotes without help		human-unintentional	voting	voter	failure to assist voter in detecting overvotes	voter education and training; clear ballot instructions that warn users about overvoting	
T	3.2.3	encourage voter override	encourage voter override of over/under-votes		human-unintentional	perform override	voter	poor poll worker performance; lack of oversight	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	
O	3.3	issue erroneous VotableBallot	issue an erroneous VotableBallot to the voter		human-unintentional	issue ballot	voter	possibility that voter will not catch error	personnel sanctions	
T	3.3.1	of the incorrect ballot style	issue an incorrect ballot style, that is, a ballot for a different precinct		human-unintentional	issue ballot	voter	possibility that voter will not catch error	poll worker awareness and training	voter gets the ballot for voters of a different precinct, and consequently votes on incorrect set of contests
T	3.3.2	with errors in contests or candidates	issue ballot with mistakes in the contests or candidates		human-unintentional	issue ballot	voter	possibility that voter will not catch error	pre-election ballot validation	ballot designer leaves off a contest or a candidate, or includes a disqualified candidate on the ballot
T	3.3.3	with errors in selection rules	issue ballots with errors in selection rules		human-unintentional	issue ballot	voter	possibility that voter will not catch error	pre-election ballot validation	election official mistakenly designs ballot with incorrect counting rules, such as choosing to vote for no more than 4 votes when the real rule is no more than three

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	3.4	confuse voters with poor ballot design	poor ballot design that confuses or misleads voters during Voting process, or fails to prevent voter errors in marking ballot	Norden (2008)	human-unintentional	ballot preparation	validate ballot style, checked in voter	weak reviewing process of a ballot design	use ballot design checklist, implement usability testing, review and amend election laws	
T	3.4.1	by splitting contests up	split candidates for the same office onto different pages or columns	Norden (2008) #1 p. 20	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	* use ballot design checklist, implement usability testing, review and amend election laws (* note the above also applies to thread id # 557 - 568), list all candidates for the same race on the same page in the same column	The 2000 presidential race in Palm Beach county, Florida has high residual vote rate due to confusing ballot design that displayed candidates in separate columns with response options in the center - hence the term 'butterfly ballot'.
T	3.4.2	by spreading response options	place response options on both sides of candidate names	Norden (2008) #3 p. 28	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	place response options (such as fill-in-the-ovals) in a consistent place on the ballot, such as one side of candidate names or ballot or ballot question choices	Response options placed on both sides of the candidate's name caused confusion among Hamilton county voters in Illinois. Voters tend to marked the arrow to the right of the candidate's name when they were supposed to mark the arrows on the left.
T	3.4.3	by keeping disqualified candidates	leave columns or rows for disqualified candidates	Norden (2008) #5 p. 32	human-unintentional	ballot preparation	validate ballot style	failure to remove disqualified candidates from ballot; failure to inform voters of disqualified candidates	remove the entire column or row for any candidate or party that has been withdrawn or disqualified (not just the candidate or party name)	The 2004 Presidential race in Montgomery county, Ohio has a higher overvote rate when the name of Ralph Nader was replaced with the words 'Candidate Removed'
T	3.4.4	with inconsistent formats	inconsistently design ballots in formatting and style	Norden (2008) #6 p. 36, Frisina (2008)	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	use consistent format and style for every contest and voting action	The inconsistent use of colors in Sarasota county ballot caused voters to skip the Thirteenth Congressional District race. The second page shows 'State' highlighted in teal which is the same as the first page's 'Congressional' word. Thus, it was easy to overlook the congressional district race.
T	3.4.5	by omitting useful shading	omit shading to help voters differentiate between voting tasks	Norden (2008) #7 p. 40	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	shade certain text, such as office name to help voters to differentiate between voting tasks	Failure to shade office titles on ballot result in higher residual vote rate in Escambia county, Florida. The affected races were Attorney General and Commissioner of Agriculture.
T	3.4.6	by omitting use of bold	omit bold text to help voters differentiate between voting tasks	Norden (2008) #8 p. 44	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	bold certain text, such as office name to help voters to differentiate between voting tasks	Misused of bold-faced text on the Franklin county ballot in Illinois made it difficult for voters to differentiate contests within each type. Hence, the residual votes were higher for the Attorney General and the Secretary of State races.
T	3.4.7	with complex instructions	fail to write short, simple instructions	Norden (2008) #9 p. 46	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	write short instructions with simple words	The 2004 presidential race in Kansas experienced high residual vote rate due to the long and confusing instruction on the ballot. For example, they used complicated words such as 'Deface' and 'wrongfully mark' instead of 'make a mistake'.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.4.8	with distant instructions	place Instructions far from related actions	Norden (2008) #10 p. 48	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	place specific instructions and related actions together.	Nonpartisan voters in Los Angeles county, California were told to fill out an oval to indicate their party choice before voting in partisan contests. Failure to do so, votes cast for party contest will not count.
T	3.4.9	with no correction guidance	fail to inform voters how to correct paper ballots	Norden (2008) #11 p. 54	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	include information of how to correct paper ballots if voters make mistakes	Lincoln county, Tennessee had a high residual vote rate compared to the state's residual vote rate for the 2002 Senate race. The ballots in Lincoln did not have instructions for voters who wished to correct their ballots if mistakes were made.
T	3.4.10	force least-objectionable choice	force least-objectionable candidate voting	VNOTA (2009)	operational	ballot preparation	votable ballot	lack of acceptable candidates running for office	system and information integrity-9, allow for 'none-of-the above' choices in contests	After incumbent governor Buddy Roemer finished 3rd in the general election, Louisiana voters were faced with a lesser-of-two-evils choice between Edwin Edwards, long dogged by allegations of corruption, and David Duke, the former Ku Klux Klan leader, in the 1991 gubernatorial run-off. Without a none-of-the-above choice, voters could either undervote or choose. Edwards won and eventually went to prison for racketeering.
T	3.4.11	publish invalid sample ballots	publish sample ballots different from actual ballots	Norden (2008) #13 p. 58	human-unintentional	ballot preparation	validate ballot style	weak reviewing process of a ballot design	publish actual ballots that looks the same as the sample ballots	The actual ballot used on the election day in Sarasota county looked very different from the sample ballot. Almost all voters saw the confusing ballot layout for the first time when they were in the voting booth.
O	3.5	mishandle ballots	mishandle ballots		human-unintentional	voting, canvass	ballots	poor planning	physical and environmental protection, media protection policy and procedures, personnel security, awareness and training, ballot accounting / reconciliation	
T	3.5.1	lose ballots by accident	unintentionally lose or misplace ballots, including close-polls filing errors		human-unintentional	voting system	ballots	poor poll worker performance; lack of oversight	awareness and training awareness and training,; personnel security personnel policies; audit and accountability audit and accountability; information integrity accuracy tests; planning	misplace a box of ballots before they are scanned during counting or recounting
T	3.5.2	abuse ballots by accident	unintentionally tamper with, mark, abuse ballots, including during close-polls operations		human-unintentional	voting, canvass	voting	poor planning	physical and environmental protection, media protection policy and procedures, personnel security, awareness and training	
T	3.5.3	stuff, swap, or lose the ballot box	Count ballots/batches of ballots more than once, by accident		human-unintentional, operational	voting, canvass	poll workers, voters	poor planning	awareness and training awareness and training,; personnel security personnel policies; audit and accountability audit and accountability; information integrity accuracy tests; planning	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.5.4	run out of ballots	run out of Votable Ballot stock		human-unintentional	ballot preparation, voting	votable ballot stock	poor planning; process whereby ballots must be preprinted	plan well and print plenty of ballots; fewer ballot styles; ballot on demand	
O	3.6	commit hand tabulation errors	experience un-detected tabulation errors	Jones (2005a) #5	human-unintentional, technical, operational	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fatigue, unclear counting rules, misinterpret counting rules	start counting well before polls close; use dedicated counting team; have new hires work under trainers; take breaks after each hour of counting; use techniques not prone to error; checking	
T	3.6.1	by making counting mistakes	make counting mistakes when accumulating totals by hand		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fatigue, unclear counting rules, misinterpret counting rules	start counting well before polls close; use dedicated counting team; have new hires work under trainers; take breaks after each hour of counting; use techniques not prone to error; checking	
T	3.6.2	in straight-party vote tabulation	due to use of incorrect rules for straight-party vote interpretation		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	unclear counting rules, misinterpret counting rules	logic and accuracy tests that include straight-party voting tests that test actual vs. expected counts	
T	3.6.3	due to improper tabulation technique	due to use of incorrect selection of tabulation algorithm (e.g., IRV variants)		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	improper tabulation technique	expert review of algorithm selection decision	
T	3.6.4	by omitting tallies from totals	due to human error in omitting some tallies from vote total		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fatigue, unclear counting rules, misinterpret counting rules	multi-person controls to verify correctness of human decisions	
T	3.6.5	by adding tallies multiple times	due to human error in including some tallies from vote total multiple times		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fatigue, unclear counting rules, misinterpret counting rules	multi-person controls to verify correctness of human decisions	
T	3.6.6	by losing a batch of ballots	by losing a batch of ballots		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fatigue, human error, lack of oversight	ballot accounting, chain of custody, personnel sanctions	
T	3.6.7	by mislabeling a batch of ballots	by mislabeling a batch of ballots		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fatigue, human error, lack of oversight	ballot accounting, chain of custody, personnel sanctions	
T	3.6.8	due to language differences	due to language differences		human-unintentional	voting, precinct closeout, canvass	poll worker	lack of multilingual skills among poll workers, unclear language requirements	clarify language requirements; employ poll workers with multilingual skills; use single multilingual rather than separate ballots	
O	3.7	make mistakes in ballot adjudication	make mistakes in ballot adjudication		human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	fallibility of human judgment; misinterpretation of rules; lack of oversight; human error; lack of voter being informed; inability of voter to protest	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	3.7.1	incorrectly accept provisional ballots	incorrectly accept provisional ballots enclosed in envelopes with disqualifying information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #5	human-unintentional	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	lack of oversight; human error; lack of voter being informed; inability of voter to protest	poll worker training, labeling provisional ballots or other distinguishing them from other ballots, audit provisional ballot data	In King County, Washington in 2005, it was alleged that election officials were counting provisional ballots in parallel with absentee ballots, which could have resulted in accepting provisional ballots for voters who had already voted absentee
T	3.7.2	incorrectly reject provisional ballots	incorrectly reject provisional ballots in envelopes with fully compliant information	Ervin (2005), Metropolitan King County Council (2005), Jones (2005a) #6	human-unintentional, operational	canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	fallibility of human judgment; misinterpretation of rules	training; auditing and logging	In a 2005 Washington governor's race, King County election officials admitted that 348 provisional ballots had been improperly counted before the voters' registration status could be determined.
T	3.7.3	disallow legitimate ballots	challenge the authenticity of legitimate ballots, including erroneous authenticity challenges, disqualifying marks, etc.	Jones (2005a) #23	human-unintentional, operational	canvass, state accumulation, post certification audit	validate total, recount	cannot bind a ballot to a voter	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	An elections official may apply non-existent or hyper-sensitive rules for accepting ballots during hand counting, hand recount, absentee ballot processing, etc.
T	3.7.4	incorrectly accept ballots	incorrectly accept ballots with non-legal marks		human-unintentional, operational	voting, precinct closeout, canvass	validate precinct results, resolve provisional ballots, reconcile voter feedback	fallibility of human judgment; misinterpretation of rules	poll worker training, clear rules for ballot adjudication, transparent processes, personnel sanctions	
T	3.7.5	by misapplying rules for determining voter intent	misapply the rules for interpreting the intent of the voter	Saltman (2006); Jones (2002)	human-unintentional	voting, precinct closeout, canvass	accumulation, retabulation, reconcile voter feedback	unclear rules of behavior or failure to follow rules, human error	clearly defined counting rules, poll worker training, multi-person integrity check	Without clearly defined counting rules, a team of hand counters interpret voter intent differently, when counting mark sense ballots by hand. Some counters count the prescribed marks, while others count acceptable marks (Jones 2002)
O	4	attack audit	render routine statistical audit ineffective	LTM-USA Delivery 01a	human-deliberate	voting system	election artifacts	no separation of duties; control by election officials over audit procedures, access to election artifacts	data protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication	An ElectionOfficial with the help of some auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited ElectionArtifacts. Then proceed to publish the election results.
O	4.1	attack election evidence	election evidence includes ElectionArtifacts, such as ballots, BallotPreparation data and artifacts, relevant PollBooks, PhysicalVoteRecords, PollWorker logs, voter feedback, etc.		human-deliberate	voting system	election artifacts	access to uncontrolled, accessible election artifacts	establish a chain of custody for all ElectionArtifacts used in audits; include separation of duties, access policies, audit logs, personnel policies, and media protections	
T	4.1.1	destroy ElectionArtifacts	physically destroy ElectionArtifacts, including ballot destruction	Jones(2005) #6, Norden(2006) #9	human-deliberate	voting system	deliver to jurisdiction	poor security during election artifacts delivery	Implement chain of custody and strong physical security during delivery	An ElectionOfficial destroys Paper Tape RemovableMedia during delivery of the ElectionArtifacts to the central location.
T	4.1.2	mishandle ElectionArtifacts	swap, replace, hide, mislay, or mislabel ElectionArtifacts containing election evidence		human-deliberate	voting system	election artifacts	access to election artifacts	implementation chain of custody on ElectionArtifacts including data protection policies	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.1.3	add new fraudulent evidence	replace real VotableBallots with VotableBallots designed to match the hand counted and audit in warehouse; results manipulation	Jones(2005) #421	human-deliberate	voting system	votable ballots	access to votable ballots	add more security features to the real VotableBallots to discourage attackers to duplicate VotableBallots, implement chain of custody and strong physical security	After the VotableBallots are printed, an insider who has access to the warehouse replaces the real VotableBallots with tampered VotableBallots.
T	4.1.4	modify ElectionArtifacts	modify poll books for audit; modify logbooks and log data used in audit		human-deliberate	voting, precinct closeout	check poll book for authenticate voter, poll worker logs for precinct closeout	lack of management oversight over poll worker, election-official, auditor	audit monitoring, analysis, and reporting	John, a corrupted poll worker, has access to the poll book and authority to authenticate a voter. John alters the poll books so the number of eligible voters matches the number of CommittedBallots which includes fraud ballots.
O	4.2	improperly select audit samples	use improper methods of selecting the scope of audit		human-deliberate	election audit	election audit	difficulty in discovery	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	
T	4.2.1	select audit units before election	audit manipulation - select audited items dishonestly	Jones(2005) #612	human-deliberate	results of the tabulation process	validate precinct results	lack of basic audit in effect	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	
T	4.2.2	select non-randomly	use non-random selection methods		human-deliberate	precinct close out	audit data	poor auditing practices or procedures; failure to follow procedures; lack of management oversight over auditing practices	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	break randomization pattern to leverage voting pattern of a precinct
T	4.2.3	use subverted selection method	use selection methods subject to outside influence		human-deliberate	election system, voting system	election artifacts	difficulty in detecting malware during computer use	access control, audit and accountability, identification and authentication, system and communications protection	
T	4.2.4	ignore proper selections	ignore randomly sampled audit units and audit something else		human-deliberate	election audit	validate precinct results	susceptibility of audit process to discretion of election officials	personnel security, audit and accountability	An auditor ignores properly (randomly or scientifically) selected audit units and instead audits other units
O	4.3	use poor audit process	use poor auditing processes and procedures		human-deliberate	election audit	election audit, validate precinct results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	Inside attacker, an ElectionOfficial, institutes poor auditing practices which are unlikely to detect the primary threat; Note: election Auditors may or may not be willing co-conspirators in these attacks
T	4.3.1	misguide auditors	give improper instructions to Auditors to render audit ineffective	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor policies allows election official to specify their own rules	revise policies to ensure that ElectionOfficial follows the guidelines for auditing process	
T	4.3.2	audit insufficient sample	audit manipulation - audit insufficient of sample to avoid tampered audit unit detected	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	An ElectionOfficial gives improper or unclear instructions to Auditors to audit insufficient data thus resulting in undetected tampered audit units.
T	4.3.3	exploit variation in batch sizes	audit manipulation - random sampling from large variation of audit unit size minimize the risk of detection	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor auditing practices or procedures	revise auditing practices or procedures to audit manipulation	An ElectionOfficial gives improper or unclear instructions to Auditors by creating a big variation in audit units size so that tampered audit units will not likely be selected during sampling.

node type	**outline number**	**threat action**	**description**	**reference**	**threat source category**	**scope of threat**	**vulnerable element**	**vulnerability**	**recommended controls**	**threat scenario**
T	4.3.4	establish single contest audit rule	election law manipulation - select a race randomly - assume audit untampered race only	Jones(2005) #612; LTM-Deliverable	human-deliberate	election audit	validate precinct results	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	Get a law or regulation in place that says that only one randomly selected race will be audited and assume your race will not be audited.
T	4.3.5	arrange contest audit	arrange selection of a non-subverted contest for audit	Jones(2005) #612	human-deliberate	election audit	validate precinct results	poor election laws / policies / guidelines	revise election law or regulation to audit more than one race	In a state that allows (but does not require) the auditing of only one randomly selected race, a dishonest election official could change procedures and institute an audit that is very unlikely to detect fraud.
T	4.3.6	select audited items before commit	tabulation manipulation - clean up data automatically based on poll worker	Jones(2005) #612	human-deliberate	election audit, accumulate totals	election artifacts	lack of tabulation server security	increase security features of tabulators	An ElectionOfficial with the help of some Auditors complete random selection first, then subvert the tabulation server so fraud is only committed against unaudited items. Then proceed to publish the election results.
T	4.3.7	tamper with audit totals	election results manipulation - precinct total do not add up to poll totals	Jones(2005) #612 Norden(2006) #3	human-deliberate	accumulate totals	precinct accumulation, precinct audit data	poor auditing practices or procedures	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	An ElectionOfficial releases precinct-level data that reflects the fraudulent results without tampering the Count. Thus, the precinct total does not tally with the actual total, which can be published in a way (across hundreds of pages of paper) that is difficult for anyone to count quickly
T	4.3.8	avoid correction	when audits reveal mismatches, avoid calling for a recount or other corrective measures by making excuses; election results manipulation - give reasons for mismatch - avoid recount, and fraud audit items detection	Jones(2005) #612	human-deliberate	accumulate totals	validate jurisdiction results	poor election laws / policies / guidelines	implement a policy that requires ElectionOfficial to give non-obscure reasons for result discrepancies and take corrective measures to avoid fraud	During the validation of the Jurisdiction results, a mismatch was found. The corrupted ElectionOfficial tries to offer obscure reasons to hide the actual attack.
T	4.3.9	overwhelm audit observers	overwhelm observers with too many auditors - auditor manipulation - incompetent Auditors ballot manipulation - dishonest audit	Jones(2005) #5,#6	human-deliberate	accumulate totals	validate precinct results	lack of management oversight over election officials and auditors	implement a policy that specifies only certain number of Auditors can be employed so that Observers can perform their duty efficiently	An ElectionOfficial hires as many incompetent or corrupt Auditors as possible knowing that an Observer can only monitor a limited number of Auditors at a time.
T	4.4	commit auditing error	human errors in following correct audit procedures, or overlooking errors		human-unintentional insider	election audit	ballot box accounting	election official has limited knowledge on discrepancies issues	personnel security, including personnel sanctions; awareness and training: auditor training	
T	4.5	compromise auditors	suborn (bribe, threaten) auditors to intentionally misreport or suppress discrepancies between election results and audit results		human-deliberate	election audit	auditors	willingness of auditors to be bribed or coerced	personnel security, including sanctions against violators	
O	4.6	attack audit results	attack audit-related process and data representing audit results		human-deliberate	election audit	election audit	lack of control over audit results	physical and environmental protection, media protection policy and procedures	
T	4.6.1	mishandle audit batch	swap, replace, hide, mislay, or mislabel batch of audit data; e.g. poll worker or election-official incorrectly labels batch of audit data		human-deliberate, human-unintentional	precinct closeout	precinct audit data	unintentional - vulnerability to human error due to carelessness; intentional - mislabel batch to cover fraud from being detected	audit monitoring, analysis, and reporting	John, a newly hired poll worker, is responsible for labeling batches of audit data. Unfortunately, he mislabeled one of the batches due to his inexperience.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	4.6.2	add fraudulent result data	inject fake votes to a back-end tabulating authority by impersonating a legitimate precinct	Kohno (2008)	human-deliberate	voting	marked ballots, especially prior to counting	poor physical security ballot boxes	increase physical security;	
O	4.6.3	attack audit data	poll worker changes audit data		human-deliberate	precinct closeout	precinct audit data	lack of management oversight over poll worker, election-official, auditor	audit monitoring, analysis, and reporting	Jane, a corrupted election-official, has access to audit data and modifies it during delivery to the jurisdiction.
T	4.6.3.1	modify deliberately	deliberately modify audit data		human-deliberate	precinct closeout	election artifacts	lack of management oversight over poll worker, election-official, auditor	establish a chain of custody on all ElectionArtifacts, including personnel security, physical and environmental protection, data protection policy and procedures	
T	4.6.3.2	modify unintentionally	modify audit data via poll worker error		human-unintentional	precinct closeout	election artifacts	lack of management oversight over poll worker, election-official, auditor	establish a chain of custody on all ElectionArtifacts, including personnel security, physical and environmental protection, data protection policy and procedures	
T	4.6.4	publish bogus audit results	penetrate jurisdiction web site and publish bogus audit results to hide attack	Jones(2005) #62	human-deliberate	results of the tabulation process	canvass, official report, report results	lack of publishing system security that leads to obscure results	increase security in both areas - tabulator and publication website	An outsider penetrates into the jurisdiction website and changes the audit results of the election.
O	5	disrupt operations	disrupt operations		human-deliberate, natural, environmental	election system, voting system	polling place, voting	exposure to natural or environmental events, fragility of ballots, susceptibility of voters to threats and intimidation	disaster planning, contingency planning, physical and environmental protection, incident response, and personnel security	
O	5.1	disruption from natural events	voting system failures attributable to natural events	Rackleff 2007	natural	election system, voting system	polling place, voting	exposure to natural events	disaster recovery planning; physical and environmental protection policies, incident response with coordination among government entities	
T	5.1.1	natural disaster	polling place hit by tornado, hurricane, tsunami, flood, earthquake, landslide, wildfire, lightening, strike, etc	Rackleff 2007	natural	voting system, election system	polling places, displaced voters	exposure to natural or accidental events	disaster recovery planning; hurricane and flood protection; contingency planning; incident response with coordination among government entities	Hurricane Katrina destroyed polling places, displaced voters, and caused elections to be postponed; many of the displaced voters were difficult to find even after basic utilities were restored
T	5.1.2	severe weather	polling place access impaired by severe weather conditions and side effects such as public transportation closure		natural	voting	polling place	exposure to severe weather events	contingency planning, such as use of alternate polling places or voting methods	a severe weather threat, including a tornado watch, was forecast for Super Tuesday in 2008; severe weather could have caused power outages or otherwise negatively impacted turnout in several states, including Alabama and Tennessee
O	5.2	disruption from environment events	disruption from environment events		environmental	voting	polling place	exposure to environment events	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
O	5.2.1	environmental failures	polling place facilities failures including power failure, electrical fire, kitchen fire, burst water pipes		environmental	election system	polling place	exposure to environment events	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
T	5.2.1.1	experience a fire	experience a fire that affects the availability of or effective operation of the polling place	Potts (2008)	environmental	voting	polling places	exposure to natural or accidental events	All electrical wiring and equipment should be thoroughly checked. Restrict smoking and presence of flammable materials in the polling place	An election eve fire adjacent to a small Pennsylvania town's only polling place caused a power outage and forced election officials to move the polling place in the middle of the night. Makeshift signs throughout town redirected voters to a new polling place for the November 4, 2008 election. The effect on voter turnout was unknown. (Potts, 2008)
T	5.2.1.2	experience power disruptions	experience unintended power disruptions		environmental	voting	rooms needing lighting	lack of control over utility providers	contingency planning, incident response	
T	5.2.1.3	experience effects of humidity	experience effects of humidity on ballots, including ink bleeding		environmental	voting system	votable ballots, marked ballots	exposure to humid environments	Marked ballots that have been stored in a high humidity (>90%) environment, and with ink that tends to bleed, are retrieved for recounting, and result in a different result because of bleeding being reinterpreted as stray marks	
T	5.2.2	hazardous accidents	polling place access impaired by nearby hazards including chemical spill, power wire fall, gas main explosion		environmental	election system	polling place, poll workers, voters	exposure to environment events; exposure to danger	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	
T	5.3	disruption from human-created events	disruption from human-created events		human-deliberate, human-unintentional	election system	polling place	fragility of ballots, mishandling	planning; physical and environmental protection, access control	
O	5.4	discourage voter participation	discourage voter participation		human-deliberate	election system, voting system	voter	susceptibility of voters to violence, intimidation, fear	awareness and training, planning, contingency planning, incident response, physical and environmental protection	
T	5.4.1	misinform voters	misinformation about polling places or transportation		human-deliberate	election system, voting system	voter	lack of voter awareness of false information	awareness and training: voter education, utilize new media to counteract misinformation campaign	
T	5.4.2	threaten personal violence	threaten personal violence, such as in blackmailing a voter to be a no-show or to vote for attacker's candidate; attacker focuses on a particular voter threatens him to vote against his will	Van Acker	human-deliberate	election system, voting system	eligible voter	susceptibility of voters to intimidation; lack of voter privacy	planning, strengthen laws against such crimes; physical and environmental security; voter privacy	a type of voter suppression that involves deliberate acts to cause fear in EligibleVoters, thus deterring them from coming out to vote.

node type	outline number	threat action	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
T	5.4.3	threaten mass violence	violence to prevent voting, (i.e., bomb scare, mail contamination scare (do not open mail), perhaps even targeting areas (by zip code)	Foxnews.com (2005)	human-deliberate	election system, voting system	voters	voters' fear for their safety	contingency planning contingency planning, incident response incident response, physical and environmental protection physical and environmental protection	In January, 2005, an Australian polling station for Iraqi exiles voting in their homeland's historic first post-Sadaam election was closed for an hour after a riot broke out and a suspicious bag prompted a bomb scare. The overall turnout was affected, it was thought. Many of Australia's estimated 80,000 Iraqis declined to register for the election, fearing their votes would make relatives in Iraq terrorist targets.
T	5.4.4	commit an act of terror	commit an act of terror		human-deliberate	election system, voting system	voters, election officials, voting equipment	exposure to terrorist acts of violence	physical and environmental protection: arms and ammunitions should not be allowed in the polling area. Unclaimed items should be continuously checked. Regular police patrolling required.	
T	5.4.5	intimidate to suppress turnout	coerce the voter to stay away from polls with threats and intimidation	Van Acker	human-deliberate	election system, voting system	eligible voter	susceptibility of voters to intimidation; lack of voter privacy	awareness and training, strengthen the election law against such crimes	'Republicans have at times been guilty of intimidation tactics designed to discourage voting. In the 1980s, the Republican National Committee hired off-duty policemen to monitor polling places in New Jersey and Louisiana in the neighborhoods of minority voters, until the outcry forced them to sign a consent decree forswearing all such 'ballot security' programs in the future.' (Fund 2004)

9 Voting System Risk Assessment Tools

The project team discovered four distinct voting system risk analysis approaches in the literature. Though none of these approaches was implemented as a mature voting system risk analysis tool, we nonetheless rigorously investigated each of them. We describe the four approaches in this section.

Threat Instance Risk Analyzer (TIRA)

In our proposal for this contract, the team offered to develop a perturbation analysis-based risk assessment tool. During this project, we implemented that tool as the Threat Instance Risk Analyzer (TIRA).

This approach allows the evaluator to quantify the stakeholder's intuition without having to construct sophisticated models that require estimates by stakeholder that are difficult if not impossible to attain.

TIRA solicits from stakeholders a "reasonable range of values" for each cost associated with overcoming a given defense (Jones 2005). Cost is broadly defined to include such factors as effort, difficulty, number of attackers, financial costs, specialized training or knowledge, and risk of detection. Monte Carlo simulation is used to randomly sample from distributions created from these reasonable ranges of values over many thousands of iterations. These iterations allow us to describe the risk of an attack over a wide range of values for costs and impact that incorporates the uncertainty and variance inherent in real human technical systems such as voting systems.

TIRA does not require stakeholders to provide precise estimates of cost factors and the construction of highly sophisticated models that potentially require "the assistance of specialized experts" (this is prohibited in the RFP). By asking stakeholders for a "best estimate" and a minimum and maximum value for a factor, we provide an effective vehicle for quantifying intuition while not asking for a level of precision that is difficult if not impossible to attain.

We decided to proceed with TIRA rather than incorporating one of the evaluated tools because of the project's unique requirements. Consider the following quote from the VSRA solicitation:

> "The second is documentation of the methodology and models developed so the EAC and other stakeholders can utilize these tools independently without the assistance of specialized experts. These products will assist the EAC and the election community in fostering a broadly-based consensus on a prudent and acceptable degree of risk for voting systems by evaluating trade-offs, running sensitivity analyses, and performing cost-benefit analyses of proposed voting system security requirements."

TIRA's methodology also avoids the complication of estimating cost and likelihood in multi-step, inter-dependent attacks. Rather than requiring stakeholders to provide conditional probabilities or cost estimates for each step in a multi-step attack, stakeholders provide a reasonable range of values for the entire sequence or collection of steps required for an attack.

TIRA quantifies the stakeholder's intuition without having to construct sophisticated models that require estimates by stakeholder that are difficult if not impossible to attain. Attack Dog, ASTRAL, and Little Jil each are excellent tools, but, based on our analysis of all four technologies, we are convinced that TIRA best meets the requirements of this project.

Review of Alternate Voting System Threat Analysis Tools

Before commitment to the development of TIRA, the team identified and analyzed three other tools presently being used for voting system risk analysis. These are described below.

Attack Dog

Attack Dog is an emerging voting system risk assessment tool that is the product of a combined effort primarily by Dr. David Dill of Stanford University, Dr. Doug Jones of the University of Iowa, and Eric Lazarus, who was the principle investigator on the 2006 Brennan Center study. The professors are long time voting system analysts and both are also principal investigators on National Science Foundation's ACCURATE voting system analysis project. Completion of some components of Attack Dog were resourced under the ACCURATE project.

Attack Dog is an integrated voting system risk assessment tool set that provides three primary functions:

- Threat tree context assisted editor
- Metric editor
- Attack generator

The user-friendly editor environment adopts common windows pull-downs for node and attribute creation. It presents hierarchy through indentation, effectively presenting several tree depth levels. The tool provides substantial icon-driven editing functions such as subordinate creation and attribute entry.

Attack Dog emphasizes the need to assess and analyze attack metrics. It integrates a sophisticated computational language, the R language , for expressing complex metrics at the node level, making Attack Dog a very powerful tool. It also adds to the system's complexity and need for special expertise in order to exercise the system.

The team conducted several individual and conference calls to discuss both the technical aspects of Attack Dog and the status of its development. These interactions with the Attack Dog developers were very helpful to the team and provided us the only formally documented threat tree (the PCOS threat tree) that we were able to acquire.

ASTRAL

ASTRAL is a specification language, that is, it is a software development language that is designed to create high level functional descriptions while supporting semantic representations that allow the developer to prove properties about implementations written in the language. Created in the Computer Security Lab of the University of California, Santa Barbara's Computer Science Department, it was initially intended for specifying real time applications with stringent security requirements.

ASTRAL is a mature tool/concept in the sense that it was developed over ten years ago. Its applicability to voting systems has reignited interest in the tool, so the system is again in development. Recently the research group, lead by distinguished formal methods expert, Professor Richard Kemmerer, applied the language's strengths to electronic voting systems.

As it was presented to the team, ASTRAL is a text-based specification language, though it is as powerful as many programming languages. One of its strengths is that it requires the analyst to capture the system requirements in great detail. ASTRAL is a complex system that allows computer experts to rigorously analyze complex voting system properties.

Little Jil

Like ASTRAL, LittleJil is a specification language that was intended to be used for a specific functional area (ASTRAL was intended for real time applications, while Little Jil targets programming autonomous agents.)

Unlike ASTRAL, Little Jil is graphics oriented, allowing the analyst to create graphical threat trees by popping in nodes from pull down boxes.

Little Jil is a powerful tool that integrates with the tool suite in the UMASS lab. These tools include a protocol property specification language, a consistency checker, and a property verifier. This integrated tool set allows an experienced analyst to capture important characteristics of the voting system processes and then to prove properties in the chosen model.

Our work with Little Jil began through a NIST-suggested series of discussions with Dr. Matt Bishop and his graduate student, Alicia Clay Jones, who was also a NIST employee. They were continuing the work of Borislava I. Simidchieva and other modelling work at the University of Massachusetts, Amherst.

We conducted several conference calls with Dr. Bishop and Ms. Jones and then calls with the research team at UMASS, Dr. Lee Osterweil and Dr. Lori Clarke. We culminated the collaboration with an on line Little Jil demonstration.

Summary of Voting System Risk Assessment Tools

The project team was encouraged to see ongoing research that is developing tools to assess voting system risks. We found ASTRAL, Little Jil, and Attack Dog to be powerful tools that each have different strengths and substantially advance the field of improving voting system accuracy and confidence. We applaud the work in these three projects.

The project team chose to implement TIRA based on perturbation analysis and Monte Carlo simulation because it best meets the requirements and constraints for this project. Our testing and reviews have shown that TIRA can be effectively used by EAC personnel without specialized expert assistance and we were able to meet all other constraints within the solicitation. Moreover, its consistency was confirmed though a series of sensitivity tests.

We are proud to present TIRA and trust that it meets the high standards demanded of this project.

10 Project Glossary

AbandonedBallot

A MarkedBallot that was not Committed by the Voter.

AbsenteeVoting

See RemoteVoting

AcceptedBallot

A CommittedBallot that:

- Is in the possession of ElectionsOfficials and
- Has successfully negotiated all filtering processes prior to Canvass and has retained its status as a legal ballot

AccidentalThreat

AccidentalThreats are those not intentionally posed by humans.

Accumulation

Collecting and synthesizing totals of AcceptedBallots. This distinguishes Accumulation where totals from several VotingMachines, precincts, etc. are combined, from a MachineCount or HandCount, where each ballot is analyzed and its contents are added to each candidate's ContestVoteTotal.

AccumulationError

Those Election errors that occur as totals are collected, synthesized, and reported.

Artifact

A physical or electronic item or record.

See also ContestArtifacts.

Attack

Attack is a deliberate malicious act carried out to effect the system.

AttackPatterns

AttackPattern is a generic representation of a deliberate, malicious Attack that commonly occurs in specific contexts.

AttackTree

AttackTree is a systematic method to characterize system security based on varying attacks.

Atomic

A basic element.

Audit

See: ElectionAudit or ContestAudit

Ballot

An official physical or electronic representation of all Contests in an Election. Ballots present Contests and capture Voter selections. Ideally, Ballots are designed to clearly delineate the available selections for each Contest and to accurately capture the Voter's intended selections.

In addition to the Contests, Ballots routinely contain BallotInstructions and other information as well as forms or structures intended to help Voters express their preferences.

BallotAccounting

Identifies the status of every Ballot created for the Election, usually by PollingPlace.

At the end of the VotingPeriod, the number of Ballots distributed to a PollingPlace should equal the sum of remaining VotableBallots, the AcceptedBallots, ProvisionalBallots and the SpoiledBallots.

BallotBox

An official container for holding AcceptedBallots.

BallotBoxStuffing

Adding Ballots to a physically committed BallotBox.

BallotConfiguration

A set of Contests in which Voters of a particular group (e.g., PoliticalParty and/or election district) are entitled to Vote.

BallotCreationMachine

A machine that produces physical or electronic ballots for an election.

BallotDelivery

Delivery of AcceptedBallots and to the Point Of Initial Accumulation (POIA), usually a county elections office. For PCOS PollingPlaces, the paper ballots themselves are delivered via courier, while preliminary results may be delivered soon after the polls close via telephone voice, computer transfer, or fax.

BallotFormat

Reflects presentation rules that are appropriate to the particular voting technology (physical, digital image, audio, etc.) such as background colors, headings, lines, instructions, text size, etc. on Ballots.

BallotImage

Electronic record of all Votes cast by a single Voter. The key connotation of this term is that it represents a marked, electronic ballot. BallotImages may be temporary or persistent. BallotMarkingDevices create temporary BallotImages in order to produce a physical Ballot for a Voter, while Direct Recording Electronic voting systems produce temporary BallotImages during VoterInteraction and then produce a persistent BallotImage for each CommittedBallot on the machine. BallotImage is the counterpart to PhysicalBallot.

BallotInstructions

Information provided to the Voter during the voting session that describes the procedure for executing a Ballot. Such material may (but need not) appear directly on the Ballot.

BallotMarkingDevice (BMD)

A voting machine that conducts VoterInteraction and generates a persistent physical MarkedBallot based on that interaction.

BallotPreparation

Creation of the VotableBallots to be used in an Election by selecting the specific Contests to be represented and applying the BallotFormat and related instructions for each distinct VotableBallot. BallotPreparation also includes preparing and testing election-specific software containing these selections.

BallotPresentation

Process of conveying the Ballot information (e.g., Contests and BallotInstructions) to the Voter. For paper ballots, the Voter must read the Ballot on a static page. On a Direct Recording Electronic, the Voter may change the presentation, e.g. by zooming or paging. Audio Ballots are presented through earphones.

BallotQuestion

An item on a VotableBallot that asks a question (e.g., Yes/No question).

BallotStyle

A conceptual representation of a VotableBallot. A concrete presentation of a particular BallotConfiguration. A given BallotConfiguration may be realized by multiple BallotStyles which may differ in the language used, the ordering of Contests and ContestChoices, etc.

BallotToken

A credential that binds a voter to a BallotStyle.

In many polling places during the VoterCheckIn process, voter authentication is managed separately from ballot management. In PollingPlaces that support more than one BallotStyle, once a voter is authenticated, they are sometimes given a credential that identifies their correct BallotStyle to PollWorkers that issue their VotableBallot.

BMD

See BallotMarkingDevice

Candidate

A person whose name appears as a Contest option on a Ballot in an Election.

Canvass

The compilation of election returns and validation of the outcome that forms the basis for political subdivisions to them to ReportResults. "Canvass" is routinely conducted at the local jurisdiction level.

CastBallot

The term "cast" has many connotations and has attained some legal distinctions that make its use ambiguous. Thus, we do not use this term in our models. *See also*: CommittedBallot and AcceptedBallot

CCOS

See CentralCountOpticalScan

CentralCountOpticalScan (CCOS)

A VotingSystem that employs marks sense technology to Scan and Count CommittedBallots recorded on PhysicalBallots at a central location. CommittedBallots are placed in a BallotBox at the PollingPlace and are transported or transmitted to the central location.

Certification

A CertifyingOfficial's act of designating (usually by signature) the final ContestVoteTotal for a jurisdiction or state.

CertifyingOfficial

The individual with legal authority to determine final ContestVoteTotals for that jurisdiction or state.

ClosedPrimary

PrimaryElection in which Voters receive a Ballot listing only those Candidates running for office in the PoliticalParty with which the Voter is affiliated. In some jurisdictions, NonpartisanContests and referendums, propositions, and/or questions may be included. In some cases, PoliticalParties may allow Unaffiliated Voters to Vote in their party's PrimaryElection.

Source: U.S. Election Assistance Commission’s Technical Guidelines Development Committee (TGDC) Recommended Guidelines

CommittedBallot

A physical or electronic MarkedBallot that contains the selections of a Voter in an Election, which are final and irreversible with respect to the Voter. A CommmittedBallot that is a BallotImage may contain only Votes, while a CommittedBallot that is a PhysicalBallot usually contains all Contests but reflects each Vote with a predefined LegalMark.

Complexity

Complexity is defined as the number of elements required for an Attack, the number of relationships among elements, and the degree of separation between cause and effect in time as associated with each element in the Attack.

ComplexityWeight

The relative importance of Threat Complexity in estimating a ThreatTree's probability.

ComponentFailure

ComponentFailure is an undesirable event that causes improper functioning of an element of a system.

Contest

Decision to be made within an Election, which may be a Contest for office or a referendum, proposition and/or question. A single Ballot may contain one or more Contests.

ContestArtifacts

ContestArtifacts represents all physical and electronic information captured for a specific contest in an election.

ContestArtifacts may include: ballots, BallotPreparation data and artifacts, relevant PollBooks, PhysicalVoteRecords, PollWorker logs, VotingMachine audit logs, voter feedback, VotingMachines themselves, etc.

Source: U.S. Election Assistance Commission’s Technical Guidelines Development Committee (TGDC) Recommended Guidelines

ContestAudit

ContestAudit conducts an ElectionAudit on a specific Contest. The ContestAudit may examine all or any ContestArtifacts.

ContestChoice

A value with which a vote in a given Contest is associated (e.g., a Candidate, the values Yes and No).

Source: U.S. Election Assistance Commission's Technical Guidelines Development Committee (TGDC) Recommended Guidelines

ContestDecision

Translates the ContestVoteTotals into the Voters' preference(s) in the Contest.

ContestError

In the macro, ContestError occurs when a ContestVoteTotal does not precisely reflect the IdealContestTotals.

ContestError in the micro (i.e., in terms of individual errors) is the accumulation of VoteErrors and AccumulationErrors relative to a given contest.

ContestFault

Occurs when uncorrectable ContestError impacts a ContestVoteTotal in a way that (1) the ContestDecision is different from the IdealDecision or (2) the ContestVoteTotal alone cannot determine if the ContestDecision is or is not equal to the IdealDecision.

ContestSuccess

Occurs when the ContestVoteTotal is sufficiently close to the IdealContestTotal that the ContestDecision is equal to the IdealDecision.

ContestVoteTotal

The ContestVoteTotal is the reported total of the number of voters that chose an option in a given contest.

Controls

Controls are non-functional processes that are put in place to ensure that functional processes operate correctly and that the fundamental system properties are preserved by the functional processes. For VotingSystems, controls include processes such as:

- Establishing chains of custody for election materials
- Conducting ElectionAudits
- BallotAccounting
- etc.

Judicial or elections official oversight for controls implementation may be legislatively mandated.

Count

There are many words used to describe the process of summing the votes for each candidate. We use the word "count" to reflect accessing each ballot to incorporate each vote into the appropriate ContestVoteTotal. This is distinguished from a machine count, where each ballot is analyzed and its contents are added to candidate totals. It is also distingished from accumulation or aggregation, where totals from several sources are combined, for example where MachineCounts are accumulated at a PollingPlace.

CountAuditMismatch

A CountAuditMismatch occurs if either the original count or the Audit data is maliciously modified to cause a detectable mismatch.

CountyAccumulation

The Accumulation of Votes for all Contests for a County.

CountedBallot

A CommittedBallot that has at least one contest whose vote is included in the ContestVoteTotal.

CreateElectronicBallotStyle

Designing every BallotStyle electronically based on the applicable Contests and policies on Rotation as well as BallotInstructions and other formatting issues. The resulting electronic BallotStyles are used on electronic VotingMachines.

CrypticKnock

A CrypticKnock is an action taken by a user of the machine that will trigger (or silence) the Attack behavior. The cryptic knock could come in many forms, depending upon the Attack program: voting for a write-in candidate, tapping a specific spot on the machine's screen, a communication via wireless network, etc.

Decompose

To separate a threat into its components.

DeliberateAttack

DeliberateAttack is a malicious attempt to gain unauthorized access to system in order to compromise system and data integrity, availability, or confidentiality.

DeliberateThreat

DeliberateThreats are those caused by people who interact with the system and are intentionally posed.

DirectRecordingElectronic (DRE)

A VotingMachine that conducts VoterInteraction, VoteCommitment, and VoteCapture; Counts each Vote; and generates a persistent BallotImage based on VoterInteraction.

District

See VotingDistrict

DRE

See DirectRecordingElectronic

DuplicatedBallot

An instance of an AcceptedBallot that is created by elections officials to facilitate further processing, e.g. to create a mark-sense ballot from an AcceptedBallot that was damaged or otherwise cannot be read by an optical scanner. DuplicateBallots require exceptional handling procedures to ensure that:

1. Each DuplicateBallot is included in the official count and
2. The DuplicatedBallot, of which any DuplicateBallot is a duplicate, is NOT included in the official count and
3. Ballot counts are carefully recorded to ensure that accurate numbers are available for any subsequent ElectionAudit.

Election

A series of processes that present options to voters, capture their selections, and accumulate those selections. The accumulations are used to decide voter-preferred options in contests.

ElectionArtifact

See ContestArtifacts

ElectionAudit

A process or set of processes that analyze data and processes in an election to identify ContestErrors or to validate ContestVoteTotals.

ElectionDefinition

Definition of the Contests that will appear on the Ballot for a specific Election.

ElectionDatabase

Data file or set of files that contain geographic information about political subdivisions and boundaries , all Contests to be included in an Election, and the allowed selections for each Contest.

ElectionError

In the macro, an ElectionError occurs when a ContestVoteTotal does not precisely reflect the IdealContestTotal.

ElectionError in the micro (i.e., in terms of individual errors) is the accumulation of VoteErrors and AggregationErrors.

ElectionsOfficial

A person associated with administering and conducting Elections, including permanent government personnel and temporary PollWorkers.

ElectionSpecificProgramming(ESP)

The data (and sometimes code, too) that is inserted into the device to provide information about how to represent a DirectRecordingElectronic or BallotMarkingDevice VotableBallot or parse a PrecinctCountOpticalScan or CentralCountOpticalScan CommittedBallot.

EligibleVoter

An LegalVoter who has registered to vote meeting all federal and state requirements and can therefore receive a VotableBallot. It is possible for an individual to be qualified to vote but not be an EligibleVoter. This can occur if the individual registers to vote after the deadline for a specific election. In this case, the person will be a QualifiedVoter but not an EligibleVoter for that election.

A QualifiedVoter and an EligibleVoter can both return to LegalVoter status if the voter moves and is no longer registered to vote in their new location.

ESP

See ElectionSpecificProgramming

FacilitatedRiskAnalysisProcess

FRAP is a formal methodology developed through understanding the previously developed qualitative RiskAssessment processes and modifying them to be faster and simpler to conduct.

FederalElection

An election that will decide at least one contest for a federal office.

FaultTree

FaultTree is a tree whose leaves represent ComponentFailures and whose interior nodes are LogicGates such as and's and or's and whose root represents SystemFailure.

GeneralElection

A regularly scheduled Election in which Voters, regardless of PoliticalParty affiliation, are permitted to Vote in Contests.

HandCount

The final Vote Count for each Contest for a given subdivision (e.g., Precinct) where a machine is not used to Count the Votes. The counterpart to HandCount is MachineCount.

HandCountedPaperBallots (HCPB)

A VotingSystem where PhysicalBallots are used for VotableBallots and machines are not used to Accumulate ContestVoteTotals.

HandRecount

Hands-on, human assessment of each ballot to retabulate the ContestVoteTotal.

An important distinction of HandRecounts is that stray and other non-LegalMarks on the HandRecounted ballots may be identified and acted upon during the HandRecount process.

HCPB

See HandCountedPaperBallots

IdealContestTotal

The ideal, or perfect, ContestVoteTotal. That is, the IdealContestTotal in a Contest is the accurate Count or Accumulation of each Voter's selection in that Contest. This is distinguished from the ContestVoteTotal in that the ContestVoteTotal may include ContestErrors, while the IdealContestTotal are perfect or ideal, without error.

It is important to note that the while accomplishing the ideal IdealContestTotal is the goal of every Election, the ideal is rarely (if ever) accomplished in practice and is impossible to identify in non-trivial cases.

IdealDecision

The IdealDecision in a contest translates the IdealContestTotal for a Contest into the Voter's preference(s) in the Contest.

Impact

The adverse consequences resulting from a successful Threat exercise of a Vulnerability.

InherentRisk

InherentRisk is the Risk related to the nature of the activities.

InternetVoting

A VotingSystem that utilizes the Internet to deliver a VotableBallot to a RemoteVoter who completes the VoteCapture process and Commits their Votes by returning the CommittedBallot via the Internet.

Jurisdiction

The lowest level organization that has statutorial, electoral responsibilities as a jurisdiction. A jurisdiction also usually is the lowest government level that employs full time ElectionsOfficials.

LegalMark

The defined sign for Voters to place on physical Ballots to indicate their selection for each Contest or for a BallotMarkingDevice to generate based on its interaction with the Voter.

LegalVoter

An individual who meets the federal age and citizenship requirements and any additional requirements define by their state of residence and who is not disqualified by any other criteria (e.g., felon).

LikelihoodAdjustmentFactor

It indicates the probability that a potential Vulnerability may be exercised within the construct of the associated Threat environment.

LogicAndAccuracyTesting

Election testing that:

1. Verifies that all voting devices are properly prepared for an election and collect data that verify equipment readiness;
2. Verifies the correct installation and interface of all system equipment;
3. Verifies that hardware and software function correctly; and
4. Segregates test data from actual voting data, either procedurally or by hardware/software features.

LogicGate

A LogicGate performs a logical operation on one or more logic inputs and produces a single logic output.

MachineCount

The final Vote Count for each Contest on a given Accumulating VotingMachine. The counterpart to MachineCount is HandCount.

MachineRecount

Utilizing the mechanical or electronic counting method to retabulate the ContestVoteTotal.

MarkedBallot

A VotableBallot, physical or electronic, that has been presented to a voter during VoterInteraction; that is, a VotableBallot becomes a MarkedBallot when it is presented to the voter before it is actually marked.

MockElections

One way to analyze VotingMachine behavior is to exercise them under circumstances that simulate the relevant election. These simulations are sometimes called MockElections. MockElections may be scripted events that compare the scripted outcome against those reported by the machines during the MockElection. MockElections may use machines that were used in the relevant election or machines that were prepared but not used.

See also: ParallelTest

MonteCarloSimulation

MonteCarloSimulation is a widely used computational method for generating probability distributions of variables that depend on other variables or parameters represented as probability distributions.

MotivationFactors

Factors that influence willingness of attackers to carry out Threat.

MotivationWeight

MotivationWeight is the relative importance of ThreatSource motivation in estimating a ThreatTree's probability.

Node Type

Addresses whether a threat, as a node in its primary threat tree, can be decomposed into a series of independent (OR) or dependent (AND) sub-threats, or else should be defined as an atomic leaf (TERMINAL); values are A - AND,O - OR, and T - TERMINAL.

Non-functional processes

Non-functional processes are processes that are not part of the core purpose of a system. Consider, for example a Chain of Custody (CoC) process. CoC is not a fundamental election process; rather, its purpose is to ensure that fundamental election processes (gathering and counting votes) operate properly and are not corrupted.

NonpartisanOffice

Elected office for which Candidates run without PoliticalParty affiliation.

NotSignedInVoter

An EligibleVoter who has not signed in at the PollingPlace for the current Election. The counterpart to NotSignedInVoter is SignedInVoter.

A NotSignedInVoter, once they have signed in for the current election at the polling place, becomes a SignedInVoter

OfficialResult

The OfficialResult is the final ContestVoteTotal for a Contest in an Election. It is determined by the CertifiedResult that is signed by the senior ElectionsOfficial of the Jurisdiction or state, usually several days after election day.

See also: UnofficialResult

OpenPrimary

PrimaryElection in which all Voters can participate, regardless of their PoliticalParty affiliation. Some states require Voters to publicly declare their choice of PoliticalParty Ballot at the PollingPlace, after which the PollWorker provides or activates the appropriate VotableBallot. Other states allow Voters to select their PoliticalParty Ballot within the privacy of the voting booth.

Source: U.S. Election Assistance Commission’s Technical Guidelines Development Committee (TGDC) Recommended Guidelines

OpticalScanner

A device that utilizes light reflection technology to interpret and Count Votes made by LegalMarks on physical, usually paper, VotableBallots. The devices produce an electronic MachineCount and may produce a paper Count and/or persistent BallotImages for each Ballot. Ballots interpreted by OpticalScanners are routinely called Mark Sense Ballots.

Outline Number

Denotes the position of the threat in a threat tree e.g., 1.1.3

OverVote

A condition that occurs when a Voter selects more than the maximum allowable selections in any Contest on a CommittedBallot.

ParallelTest

Tests that randomly select some VotingMachines from a jurisdiction and conduct a MockElection on ElectionDay. The purpose of ParallelTests is to determine if any of the jursdiction's VotingMachines have been infected with malicious software.

PartisanOffice

An elected office for which Candidates run as representatives of a PoliticalParty.

PCOS

See PrecinctCountOpticalScan

Person

The superclass of Voters, LegalVoters, EligibleVoters, QualifiedVoters, ElectionsOfficials, Candidates, and all other people that may be involved in elections.

PerturbationAnalysis

PerturbationAnalysis is a method that provides performance sensitivities by analyzing a single sample path of a stochastic discrete system.

PhysicalBallot

Physical record of all Votes cast by a single Voter. The key connotation of this term is that it represents a marked Ballot. BallotMarkingDevices create temporary BallotImages in order to produce a PhysicalBallot for a Voter. PhysicalBallot is the counterpart to BallotImage.

PhysicalVoteRecord

A non-electronic rendering of all selections made by a voter in an election.

POIA

See PointOfInitialAccumulation

PointOfInitialAccumulation(POIA)

The physical location where ballot counts are accumulated. In most cases, this will be the county elections office, but may also be a regional accumulation site.

PoliticalParty

An organization that nominates or selects a candidate for election to office whose name appears on the VotableBallot as the candidate of the organization.

Adapted from the Election Code of Federal Regulations

PollBook

VoterList containing only information relative to a specific Precinct or PollingPlace.

PollBookGeneration

A process definition for the generation of a VoterList containing only information relative to a specific Precinct or PollingPlace.

PollingPlace

Facility to which Voters are assigned to receive a VotableBallot, conduct their VoterInteraction. and make their VoteCommitment. There are several types of polling places utilized in elections, including:

- Election Day Precinct-Specific Polling Place – Each voting precinct is assigned to a unique polling place.
- Election Day Consolidated Precinct Polling Place – Two or more voting precincts are assigned to a unique polling place. This is often based on several factors, including the number of voters in each precinct, size/location of the polling place facilities and the expected voter turnout for each polling place.
- Election Day Vote Center (jurisdiction-wide) – Several polling place/vote centers strategically located throughout the jurisdiction where any voter in the entire jurisdiction can vote on Election Day.
- Election Day Vote Center (regional) – Several polling place/vote centers strategically located by region where any voter within a specific region can vote on Election Day.
- Early Voting Vote Center (jurisdiction-wide) – Several early voting vote centers strategically located throughout the jurisdiction where any voter in the entire jurisdiction can vote during the designated early voting time period.
- Early Voting Vote Center (regional) – Various early voting vote centers strategically located by region where any voter within a specific region can vote during the designated early voting time period.

PollWorker

Person who prepares the Precinct by setting up voting equipment, greets Voters, verifies registrations and provides Voters with appropriate Ballots. At the end of the day, PollWorkers close the Precinct and prepare election materials for delivery or actually deliver the material to the Elections office.

Possibility

Condition of whether or not a Threat is realistically capable of being exercised.

Precinct

Administrative, electoral geographic division in which Voters cast Ballots at the same PollingPlace. A Precinct may contain more than one VotingDistrict and thus a PollingPlace that is assigned to a single Precinct may manage a separate BallotStyle for each VotingDistrict contained therein.

PrecinctAccumulation

Accumulation of all MachineCounts and HandCounts from a given Precinct.

PrecinctCountOpticalScan (PCOS)

A VotingSystem that employs marks sense technology to Scan and Count CommittedBallots recorded on PhysicalBallots at a Precinct-based PollingPlace. A distinctive feature of a PrecinctCountOpticalScan (PCOS) device is that it can be programmed to identify and reject UnderVotes and Overvotes on ballots that it scans.

PrecinctDefinition

Election administration division corresponding to a continuous geographic area that forms basis for determining Voter eligibility relative to a given Contests.

PrimaryElection

An Election held to determine which Candidate will represent a PoliticalParty for a given office in the GeneralElection.

Source: U.S. Election Assistance Commission’s Technical Guidelines Development Committee (TGDC) Recommended Guidelines

ProvisionalBallot

A CommittedBallot that was committed by a Voter whose Eligibility is disputed by an ElectionsOfficial or another person who is qualified to dispute a Voter’s Eligibility.

PublicAnomaly

A PublicAnomaly is any public event that may suggest that the voting system is corrupted, e.g. if an attacker is able to display a custom pop-up on the voting screen via corrupt software.

QualifiedVoter

QualifiedVoter is a type of LegalVoter who has registered to vote but did not register in time to be an EligibleVoter for a specific election. A QualifiedVoter and an EligibleVoter can both return to LegalVoter status if the voter moves and is no longer registered to vote in their new location.

Receipt

A record of a transaction that binds the details of the transaction to the entity that holds the receipt.

Recommended Controls

Steps to minimize or eliminate the likelihood (or probability) a vulnerability exercised or to reduce the impact of the threat. Similar to countermeasure or mitigation.

Recount

In its pure form, a Recount is a retabulation of (original) Votes on AcceptedBallots in a particular Contest to confirm, or correct, the OfficialResult of the Canvass. The requirement to conduct a recount is determined by each state, with most states requiring a recount of Contests based on a difference threshold.

RegistrationDatabase

Collection of all registered Voter’s data that is used to create PollBooks.

Registration

See VoterRegistration

RejectedBallot

A RejectedBallot is a MarkedBallot whose votes are not included in the ContestVoteTotals, without replacement to the voter.

RemoteBallot

Ballot that is used for RemoteVoting.

RemoteVoter

A voter that receives, marks, in most cases commits their ballot at other than their designated PollingPlace.

RemoteVoting

Voting that occurs at a location other than an official PollingPlace.

RemovableMedia

A form of computer memory that may be removed from one computer or VotingMachine and subsequently inserted and read into another computer or VotingMachine.

ResidualRisk

ResidualRisk is the that portion of Risk left after security measures have been implemented.

RetailAttack

A RetailAttack is an attack that has a low cost or high probability of success, but low impact that is algorithmically characterized as being linear on the number of votes impacted against the cost or the number of participants required to carry out the attack.

Risk

Risk is the net negative Impact of the exercise of a Vulnerability, considering both the probability and the Impact of occurrence.

RiskAssessment

RiskAssessment is a process which includes identification and evaluation of Risks and Risk Impacts, and recommendation of risk-reducing measures.

RiskManagement

RiskManagement is the process of identifying Risk, assessing Risk,and taking steps to reduce Risk to an acceptable level.

RiskMitigation

RiskMitigation is a process that involves prioritizing, evaluating, and implementing the appropriate Risk-reducing controls recommended from the RiskAssessment process.

Rotation

Generally, Ballots are represented as lists, with lists of Candidates or questions contained within lists of Contests. Some studies show that list representations can inject bias, by favoring the first Candidate in a list, or by emphasizing the first Contest over subsequent Contests. To avoid this potential bias, some states/jurisdictions require that Candidate order be rotated, creating many versions of each BallotStyle. There are many algorithms for accomplishing Candidate rotation, but their goal is to mitigate list order bias. Contest rotation is usually dictated by law, usually involving precedence based on federal, state, and local policies.

RunoffElection

SpecialElection whose purpose is to select a winner following a PrimaryElection or a GeneralElection, in which no Candidate in a Contest received the required minimum percentage of the ContestVoteTotal necessary to determine the ContestDecision.

Scope of Threat

The boundary around which the exploited vulnerabilities reside. Values are ElectionSystem, VotingSystem (or a specific activity within the VotingSystem such as BallotDefinition), Voting, Canvass, PrecinctCloseout, StateAccumulation, or PostCertificationAudit, or any of their sub-activities

SeniorPW

The PollWorker in a PollingPlace who is generally responsible for:

- Managing and overseeing PollingPlace operation
- Providing advanced technical guidance to other PollWorkers
- Resolving voter conflicts
- Spoiling and reissuing ballots
- Etc.

The SeniorPW is referred to by various names throughout the country, including Precinct: Judge, Clerk, Chair, Coordinator, etc.

SignedInVoter

An EligibleVoter who has signed in at the PollingPlace for the current Election. The counterpart to SignedInVoter is NotSignedInVoter.

SpecialElection

An election that is held outside the normal election scheduling process, e.g. to fill an office that has become vacant between regularly scheduled elections.

SpinButton

The SpinButton is a Widget that allows the user to select a value from a range of numeric values.

SpoiledBallot

A MarkedBallot that whose votes will not be included in the ContestVoteTotalss, but for which a replacement VotableBallot is provided to the voter that spoiled the ballot.

State

Each State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

Source: Federal Code of Elections

Steganographic

The branch of cryptography where messages are hidden inside other messages.

SystemFailure

SystemFailure is an undesirable system event that causes improper functioning of a system.

Tabulation

See Accumulation

Threat

The potential for a particular ThreatSource to successfully exercise a particular Vulnerability.

Threat Action

A short name for a threat (short enough to fit on the shapes in the tree diagrams), usually a short form of a threat action, in which a longer form is provided in description

ThreatCatalog

ThreatCatalog is a numbered list of the Threats to the voting system, with clear documentation of each Threat.

Threat Description

A longer description of a threat action, which is a realization of a threat, i.e., an occurrence in which system security is assaulted as the result of either an accidental event or an intentional act.

Threat Id

A unique identifier for a given threat integer; a primary key, unique within a single voting technology.

ThreatMatrix

ThreatMatrix is a practical framework that can be used to anticipate potentially detrimental events that might effect the system.

ThreatProbability

The likelihood that a potential Vulnerability may be exercised within the construct of the associated Threat environment.

Threat Reference

Source of identified threat.

Threat Scenario

A brief narrative serving as a specific illustration of a threat being carried out.

ThreatSource

A ThreatSource is defined as 1. either (a) intent and method targeted at the intentional exploitation of a Vulnerability, or (b) a situation and method that may accidentally trigger a Vulnerability. 2. any circumstance or event with the potential to cause harm to the system.

Threat Source Category

A category of common threat sources. Values are: human-deliberate, human-unintentional, environmental, technical, and natural (see NIST 800-30, sec 3.2.1). Insider or outsider may be appended to the two human categories to denote whether or not insider access is required.

ThreatTaxonomy

ThreatTaxonomy is the classification of Threats into groups based on the similarities between them or origin.

ThreatTree

ThreatTree is a hierarchy of Threats or vulnerabilities with the goal of the attack on the top and each subordinate level showing the steps required to carry out an Attack.

Tree

A tree is a connected set of linked nodes and it is acyclic.

Token

Physical device or digital representation given to an EligibleVoter to aid in authentication and provide access to the VotingSystem or their appropriate VotableBallot. A Token can be used to activate an electronic Ballot and may contain the information needed to determine the correct BallotStyle. Tokens are very commonly used when the PollWorker at the PollBook does not hand out VotableBallots.

Source: U.S. Election Assistance Commission's Technical Guidelines Development Committee (TGDC) Recommended Guidelines

UnderVote

A condition that occurs when a voter marks less than the maximum allowable selections on any contest on a CommittedBallot.

UnofficialResults

Results other than OfficialResults. While UnofficialResults may be released by competent authority, they are unofficial in the sense that they are preliminary and are generally expected to change. Often, they do not include all ballots that are known to be counted, e.g. absentee ballots are sometimes added after UnofficialResults are released.

VBM

See VoteByMail

VBP

See VoteByPhone

VotableBallot

An instance of a BallotStyle that incorporates rotation rules and BallotFormat to form a physical, electronic, audio, etc. ballot that a voter can mark or otherwise use to indicate their selections. Every distinct, legitimate ballot used in an election is termed a VotableBallot.

Since VotableBallots become MarkedBallots when they are issued to a voter, VotableBallots remaining at the end of the VotingPeriod are UnusedBallots.

Vote

A selected candidate or issue in a contest on a ballot. Indication by a Voter of support for a particular Contest choice on a VotableBallot.

VoteByMail (VBM)

A VotingSystem that utilizes the postal service to deliver a Physical VotableBallot a remote Voter who completes the VoteCapture process and Commits their Votes by returning the MarkedBallot.

VoteByPhone (VBP)

A VotingSystem that utilizes a telephone system to deliver a VotableBallot to the Voter and to capture voter selections. While VoteByPhone may be used for remote voting, its primary deployment today is as a polling place system to support disabled voter access.

VoteCapture

The process of transitioning a VotableBallot from a "pre-vote" or "vote in process" to CommittedBallot. VoteCapture is the voting system action that is triggered by a Voter's VoteCommitment act. For a PhysicalBallot, VoteCapture may entail the MarkedBallot falling into a BallotBox or being fed into an OpticalScanner. For Direct Recording Electronic, it reflects transfer frsom temporary storage to a final, persistent storage format.

VoteCoercion

VoteCoercion occurs when the vote is not free, i.e. when the voter is forced or bought into voting for an option which he would not have chosen had he not been under pressure or if he had not been offered a bribe.

VoteCommitment

A Voter commits their selections by taking a clearly identifiable action that finalizes their Votes. For PhysicalBallots, the Voter may insert their MarkedBallot in an OpticalScanner or BallotBox. For a Direct Recording Electronic, the Voter may touch or press a "vote" button that transfers their selections from temporary storage to a final, persistent storage format and ends the voting session. A VoteByMail Voter inserts their Ballot into the mail system to commit their Votes.

VoteFlipping

Vote Flipping describes a wide variety of attacks that are related by their result, which is that a vote intended for one candidate is redirected and tallied for the wrong candidate.

VoteFlipping

Vote Flipping describes a wide variety of attacks that are related by their result, which is that a vote intended for one candidate is redirected and tallied for the wrong candidate.

VoterCaging

Voter caging is a practice of sending mass direct mailings to registered voters by non-forward able mail, then compiling lists of voters, called “caging lists,” from the returned mail in order to formally challenge their right to vote on that basis alone.

VoterConfidence

Effective democratic government demands that citizens can have deserved trust that their Elections are conducted according to law, that their Votes count, that all citizens have reasonable opportunity to vote free of coercion, and that no one can vote more than once. The term VoterConfidence is used to capture this notion of trust in the electoral process. There are no perfect Elections and every ElectionError or mishap offers an opportunity to negatively impact VoterConfidence.

VoterImpersonation

VoterImpersonation is a type of VoteFraud in which a person claims to be someone else when casting a vote.

VoterIntimidation

Voter intimidation involves putting undue pressure on a voter or group of voters so that they will vote a particular way, or not at all.

VoterPurging

Voter purging is a type of voter suppression where the name of the citizens is purged from the voter roll.

VoterSuppression

Voter suppression is a form of electoral fraud and refers to the use of governmental power, political campaign strategy, and private resources aimed at suppressing (i.e. reducing) the total vote of opposition candidacies instead of attempting to change likely voting behavior by changing the opinions of potential voters

VoteTabulatingMachine

A device that Counts Votes.

Voter

A person that votes in an election. Only EligibleVoters can vote in any election. A voter is an individual who has been issued a VotableBallot.

VoterConfidence

Effective democratic government demands that citizens can have deserved trust that their Elections are conducted according to law, that their Votes count, that all citizens have reasonable opportunity to vote free of coercion, and that no one can vote more than once. The term VoterConfidence is used to capture this notion of trust in the electoral process. There are no perfect Elections and every ElectionError or mishap offers an opportunity to negatively impact VoterConfidence.

VoterInteraction

This is the phase of the voting process where the Voter interprets a VotableBallot, reasons about their Contest choices, and takes action to reflect their selections. For PhysicalBallots, the interaction may be reading, marking, and reviewing the VotableBallot.

VoterList

This self-descriptive term contains all necessary information on prospective voters needed to properly issue (or to refuse to issue) their correct VotableBallot).

VoterRegistration

The process of creating VoterLists. This involves requiring voters to provide information before the election that can be used to: (a) Determine their eligibility to vote (b) Authenticate them at the polling place and (c) Identify their voting district or otherwise select their proper VotableBallot.

VoterVerifiedPaperAuditTrail (VVPAT)

A VotingSystem that supports voter-verification through voter-verifiable paper records (VVPR).

Source: U.S. Election Assistance Commission’s Technical Guidelines Development Committee (TGDC) Recommended Guidelines

VoteError

All errors that affect one Vote in one Contest are VoteErrors.

VotingDistrict

The smallest administrative, electoral geographic division and is the basis for determining which contests the LegalVoters residing in that VotingDistrict are eligible to vote. The smallest geographic area where all resident voters receive the same VotableBallot.

There may be more than one VotingDistrict in a precinct.

VotingMachine

An electronic or mechanical device that creates or processes VotableBallots during the voting process.

VotingSystem

Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and BallotStyles, configure voting equipment, identify and validate voting equipment configurations, perform logic and accuracy tests, activate ballots, capture votes, count votes, reconcile ballots needing special treatment, generate reports, transmit election data, archive election data, and audit elections.

Note: Much of this definition is taken from Source the U.S. Election Assistance Commission’s Technical Guidelines Development Committee (TGDC) Recommended Guidelines. This definition closely maps to HAVA's definition. In some cases the team felt the need to extend the HAVA definition to more closely map to voting systems today.

Vulnerability

A flaw or weakness in system security procedures, design, implementation, or internal controls, that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerable Element

One or more people, process, technology, or data elements that are source of vulnerability for the given threat

VVPAT

See Voter VerifiedPaperAuditTrail

WholesaleAttack

A WholesaleAttack is a high cost or low probability of success, but high impact attack that is algorithmically characterized as being exponential on the number of votes impacted against the cost or number of participants required to carry out the attack.

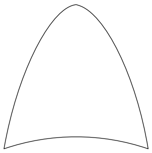
Widget

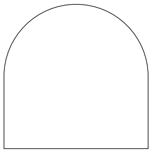
Widget is an element of a graphical user interface such as a button or scroll bar.

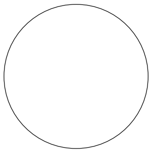
WriteInBallot

An instance of a MarkedBallot that includes at least one contest in which the voter made a write-in selection. Write-in selections generally cannot be interpreted by an optical scanner.

11 Key to Graphical Threat Tree Symbols

 An “or” node – it can be decomposed to a group of independent sub-threats. Only one of the sub-threats immediately below it must be true for this threat to be true.

 An “and” node – it can be decomposed into a group of dependent sub-threats. All of the sub-threats immediately below it must be true for this threat to be true.

 A terminal node – it is not decomposed any further. An atomic leaf.

12 Bibliography

Advancement Project (2008) Provisional Voting: Fail-Safe Voting or Trap-Door to Disenfranchisement, Sept 2008, http://www.advancementproject.org/pdfs/Provisional-Ballot-Report-Final-9-16-08.pdf.

Ballotpedia (2008) Illegal third-party registration conduct, Retrieved from http://ballotpedia.org/wiki/index.php/Illegal_third-party_registration_conduct.

Blaze, Matt (2007) "Source Code Review of the Sequoia Voting System" http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf

Brief History of Problems with Diebold Optical Scan System Used In Vermont (1998) (11/1998 Pima County, Arizona), Retrieved from http://vtvoters.org/docs/diebold-history-problems.pdf.

Butler,Kevin (2007) Everest: Evaluation and Validation of Election-Related Equipment , Standards and Testing http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf Campbell, Tracy (2006) Deliver the Vote: A History of Election Fraud, An American Political Tradition-1742-2004. New York: Perseus Books Group: Palgrave Macmillan.

Commissioner of Elections (2008) Provisional Voting, State of Delaware, Retrieved Apr 5, 2007, http://hava.delaware.gov/provisional.shtml.

Dekel, Eddie, Matthew O. Jackson, Asher Wolinsky (2004) Vote Buying, Revision: October 19, 2004, Retrieved from http://else.econ.ucl.ac.uk/newweb/esrc_seminars/nov2004/dekel.pdf.

Diebold in the News — A Partial List of Documented Failures, http://www.votersunite.org/info/Dieboldinthenews.pdf.

Dill, David L., Rebecca Mercuri, Peter G. Neumann, and Dan S. Wallach (2008) Frequently asked questions about DRE Voting System http://www.verifiedvoting.org/article.php?id=5018

Direct Recording Equipment : http://www.eac.gov/election/practices/bpea/dre

Electronic Voting Machine Information Sheet : http://www.verifiedvoting.org/downloads/2008SequoiaAVCEdgeInfoSheet-full.pdf

Epstein, Jeremy(2007) "Electronic Voting" Aug 2007 http://www2.computer.org/portal/web/csdl/doi/10.1109/MC.2007.271

Epstein, Jeremy (2009) "ABQORDIA-THOUGHTS ON SECURITY AND SOCIETY" http://abqordia.blogspot.com/2009_06_01_archive.html

Ervin, Keith, "GOP says hundreds of ballots suspect," Seattle Times, January 6, 2005, Retrieved from http://seattletimes.nwsource.com/html/localnews/2002142483_recount06m.html on July 13, 2009.

Estep, Bill (2008) "Former Clay official to change plea in vote-buying case," Lexington Herald-Leader, May 29, 2009, Retrieved from on July 28, 2009.

Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten (2006) “Security Analysis of the Diebold AccuVote-TS Voting Machine”, Center for Information Technology Policy and Dept. of Computer Science, Princeton University, September 13, 2006, Retrieved from http://itpolicy.princeton.edu/voting/ts-paper.pdf on July 15, 2009.

Fienberg, Howard (2000) "Internet Voting: E-Foolishness", Retrieved from http://www.hfienberg.com/clips/evote.htm.

Fishcher, Eric A. (2003),Election Reform and Electronic Voting Systems (DREs) :Analysis of Security Issues http://people.csail.mit.edu/rivest/voting/reports/Fischer-ElectionReformAndElectronicVotingSystemsDREs.pdf

Florida League of Conservation Voters Education Fund (FLCVEF) (1994) http://www.flcv.com/fraudpat.html.

Foxnews.com (2005), "Riot, bomb scare at Australian polls," Associated Press, Fox News Network LLC, January 29, 2005, Retrieved from http://www.foxnews.com/story/0,2933,145763,00.html on July 13, 2009.

Frisina, Laurin, Herron, Michael C., Honaker, James, Lewis, Jeffrey B. (2008) "Ballots Formats, Touchscreens, and Undervotes: A Study of the 2006 Midterm Elections in Florida", Election Law Journal: Rules, Politics, and Policy. March 2008, 7(1): 25-47. DOI: 10.1089/elj.2008.7103

Fund, John (2004) "Democracy Imperiled: America's election problems," National Review Online, September 13, 2004, Retrieved from http://www.nationalreview.com/comment/fund200409130633.asp on July 21, 2009.

Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007

Greenemeier,Larry (2008) "Citizens for ELECTION INTEGRITY|MN" http://www.ceimn.org/news/planning_evote_read_first

Hackett, Alexandra, "Clearwater post office loses 1100 absentee ballots", 10Connects.com, 3/15/2008 10:56:26 PM, http://www.tampabays10.com/includes/tools/print.aspx?storyid=76237

Hasen, Richard L., "Vote Buying" California Law Review, Vol. 88, p. 1323, October 2000; Loyola-LA Legal Studies http://ssrn.com/abstract=257564

Hester, Tom Sr, "Roselle council president charged with illegally filling out absentee ballots", NewJerseyNewsRoom.com, August 27, 2009

Hommel, Theresa (2004) "How to Hand Count Votes Marked on Paper Ballots", http://www.wheresthepaper.org/CountPaperBallots.htm

Independent Political Report (2008), "Update from Black Box Voting: Trouble with straight party voting and how you can help on Election Day," Retrieved July 10, 2009, http://www.independentpoliticalreport.com.

Jefferson, David, "The Inherent Security Vulneribilities with Internet Voting", Retrieved from http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b4.

Johnson, Kirk (2009) "Rise in Voting by Mail Transforms Race in Colorado", http://www.nytimes.com/2008/10/17/us/politics/17colorado.html, August 27, 2009

Jones, Doug W. (2005a) University of Iowa, Threats to Voting Systems, NIST workshop on Threats to Voting Systems, 7 October 2005, Gaithersburg, MD.

Jones, Doug W. (2005b) Chain Voting, aug 26, 2005, http://vote.nist.gov/threats/papers/ChainVoting.pdf.

Jones, Doug W. (2002) "Counting Mark-Sense Ballots: Relating Technology, the Law and common Sense," The Voting and Elections web pages, University of Iowa, 2002, http://www.cs.uiowa.edu/~jones/voting/optical/.

King, Merle, Requirements for a Voting System, www.vote.nist.gov/PublicHearings/9-21-04%20Panel%201%20%20KING.doc

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. "Analysis of an Electronic Voting System," 27 Feb. 2004. IEEE Computer Society Press. 20 Sept. 2008 <http://avirubin.com/vote.pdf>.

Konopasek, Scott O. (2004) Audit Trail or “New-fangled” Chad? The Phenomenon of Unintended Consequences, http://www.forefrontelections.com/Reference%20Library/Audit%20Trail%204-26-04.pdf

Levitt, Justin and Allison, Andrew (2007) A Guide to Voter Caging, Brennan Center For Justice, Jun 29, 2007, http://www.brennancenter.org/content/resource/a_guide_to_voter_caging/

LTM-USA Delivery-01 (2009) LTM Election Threat Models, Lazarus Technology Mentoring, Inc.

Metropolitan King County Council (2005), "King County Election Reform Initiative," King Country, January 31, 2005, Retrieved from http://www.metrokc.gov/MKCC/News/2005/0105/KC_Elect_Reform_Init.htm on July 13, 2009

Mote, C. D. Jr. (2002). Report of the national workshop on internet voting: issues and research agenda. ACM International Conference Proceeding Series, 129, 1-59.

NIST (2005) Developing an analysis of threats to voting systems: Preliminary workshop summary,7 October 2005, Gaithersburg, MD

NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008; Available at http://vote.nist.gov/uocava-threatanalysis-final.pdf.

Norden, Lawrence D.(Chair) (2006) "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, Voting Rights & Election Series, 2006, Brennan Center for Justice at NYU School of Law, Website: www.brennancenter.org

Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) “Better Ballots.” July 20 2008. Brennan Center for Justice. http://www.brennancenter.org/content/resource/better_ballots

Pew: No Time to Vote, Challenges Facing Americas Overseas and Military Voters, January 2009, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf

Potts, Ted (2008) "Fire Guts Patton Store, Forces Change of Polls," The Tribune Democrat, November 5, 2008, Retrieved from http://www.tribune-democrat.com/local/local_story_310012455.html on July 21, 2009.

Poulsen, Kevin (2009). "Arizona's Internet Voting System." Splice Today, 5 June 2009. http://www.splicetoday.com/politics-and-media/arizona-s-internet-voting-system

Rackleff, Robert (2007) "Voters of Hurricane Katrina," Carnegie Reporter, Vol. 4 No. 2, Spring 2007, Carnegie Corporation of New York.

Regenschied, Andrew, and Nelson Hastings (2008) "A Threat Analysis on UOCAVA Voting Systems", NISTIR 7551, U.S. Department of Commerce, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf on July 15, 2009.

Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html on July 15, 2009.

Saltman, R. G. (2006). The history and politics of voting technology: In quest of integrity and public confidence. New York: Palgrave Macmillan.

Schryen, Guido (2004) "How Security Problems Can Compromise Remote Internet Voting Systems", Lecture Notes in Informatics, Electronic voting in Europe - technology, law, politics and society, July 2004, Retrieved from http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-13.pdf.

Sheridan, Peter, Dorothy A. Harbeck, and Christopher J. Keale (2002) "Neither Snow nor Rain, but Maybe Anthrax: Bioterrorism and Absentee Ballots in New Jersey", Election Law Journal: Rules, Politics, and Policy, September 2002, Vol. 1: 3, pp. 415-420. doi:10.1089/153312902760137640.

Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, Tuesday August 18, 2009, 6:31 PM http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html

Stoneburner, Gary, Goguen, Alice, Feringa, Alexis (2002) "Risk Management Guide for Information Technology Systems", Recommendations of the National Institute of Standards and Technology, Special Publication 800-30, July 2002.

Van Acker, Bernard, Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions, http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-6.pdf.

VNOTA (2009) Vote for None of the Above, Retrieved July 10, 2009, http://nota.org.

Wikipedia (2009) Optical scan voting system, Wikipedia: The Free Encyclopedia, Retrieved Mar 25, 2009, http://en.wikipedia.org/wiki/Optical_scan_voting_system.

WV Votes.com (2008) 2008 Automark Poll Worker Manual, WV Votes.com, Retrieved Sep 30, 2008, http://www.wvvotes.com/poll-workers/documents/OPT-SCAN-BLUE-Lewis.pdf.

Yasinsac, A., D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, “Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, Final Report”, Security and Assurance in Information Technology (SAIT) Laboratory, Florida State University, February 23, 2007,

Yasinsac, A & Yap, P.F. & Colvin, C., "Issues with Vote By Mail Ballots", Unpublished letter, February 16, 2009.

Zetter, Kim (2008) "Serious Error in Diebold Voting Software Caused Lost Ballots in California County-Update" http://www.wired.com/threatlevel/2008/12/unique-election/.