



Magical Seals, Secure Voting Machines, and Other Fantasies

Roger G. Johnston, Ph.D., CPP
Jon S. Warner, Ph.D.

Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
<http://www.ne.anl.gov/capabilities/vat>



Argonne National Laboratory

~\$738 million annual budget

1500 acres, 3400 employees, 4400 facility users, 1500 students
R&D and technical assistance for government & industry



Vulnerability Assessment Team (VAT)



A multi-disciplinary team of physicists, engineers, hackers, & social scientists.

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

The greatest of faults, I should say, is to be conscious of none.
-- Thomas Carlyle (1795-1881)

Sponsors

- DHS
- DoD
- DOS
- IAEA
- Euratom
- DOE/NNSA
- private companies
- intelligence agencies
- public interest organizations



Security Theater

1. Best way to spot it is with an effective thorough VA.

2. Next best is to look for the characteristic attributes:

- Sense of urgency
- A very difficult security problem
- Involves fad and/or pet technology
- Questions, concerns, & dissent are not welcome or tolerated
- The magic security device, measure, or program has lots of “feel good” aspects to it**
- Strong emotion, over confidence, arrogance, ego, and/or pride related to the security
- Conflicts of interest
- No well-defined adversary
- No well-defined use protocol
- No effective VAs; no devil’s advocate
- The technical people involved are mostly engineers
- Intense desire to “save the world” leads to wishful thinking
- People who know little about security or the technology are in charge



Video

(See <http://www.youtube.com/watch?v=frBBGJqkz9E>)



So Why So Much Bad Physical Security?

- Security Theater is easy, thinking and Real Security is hard
- Committees, bureaucrats, & knuckleheads are in charge
- People & organizations aren't used to thinking critically about it
- Physical Security as a "Taking Out the Garbage" slam dunk thing
- "If it's important, somebody must have thought it through" Myth
- Lots of hype, snake oil, & bad products
- Blind faith in precedence and "authorities"
- Physical security is not a well developed field



I watch a lot of game shows and I've come to realize that the people with the answers come and go, but the man who asks the questions has a permanent job.

-- Gracie Allen (1895? – 1964)



Physical Security: Scarcely a Field at All

- You can't (for the most part) get a degree in it from a major 4-year research university.
- Not widely attracting young people, the best & the brightest.
- Few peer-review, scholarly journals or R&D conferences.
- Lots of Snake Oil & Security Theater
- Shortage of models, fundamental principles, metrics, rigor, R&D, standards, guidelines, critical thinking, & creativity.
- Often dominated by bureaucrats, committees, groupthink, linear/concrete/wishful thinkers.



Harry Solomon: I didn't have enough experience to sell hot dogs, so they made me a security guard.
-- Third Rock from the Sun



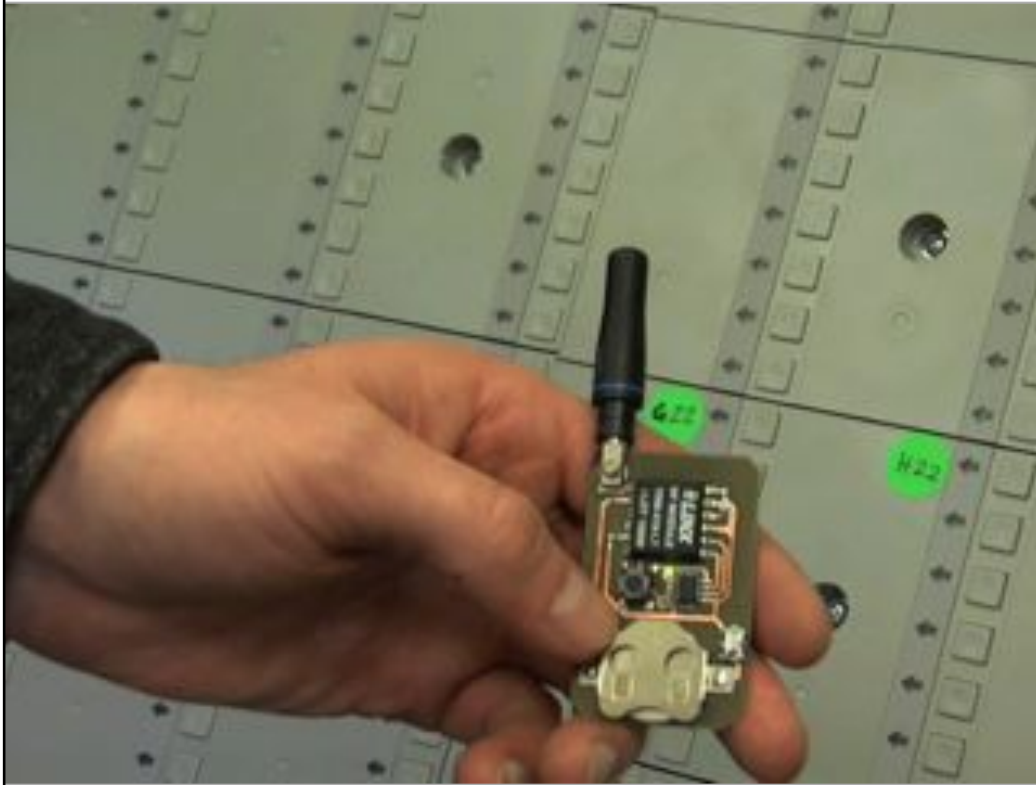
Hmm...

Usually we can defeat security devices (including high-tech ones) without attacking the computer/microprocessor, reverse engineering the software, or having an owner's manual!

Might this also be true for electronic voting machines?



Remote Toggling On/Off of Cheating



Ways to Disable Cheating

- Clock
- Magnet
- Accelerometer
- Remote Control (radio frequency)
- Voting That's Too Rapid



I hope you believe you understand what you think I said, but I'm not sure you realize that what you've heard is not what I meant.

-- Richard Nixon (1913-1994)

Probably Wrong Assumptions

1. Attacks on electronic voting machines must involve the microprocessor, software code, data storage, or communication channels.
2. The attackers must understand the software.
3. The attackers must tamper with hundreds or thousands of voting machines.
4. The attackers only motivation is to get their candidate elected.
5. The temptation to tamper and the ease of stealing an election are uncorrelated with how close or controversial an election is.



Probably Wrong Assumptions

6. Electronic voting machines have significant amounts of security built-in.
7. It's easy to tell if an electronic voting machine has been compromised.
8. "Certification" of (or standards for) a voting machine or a voting machine design means its security is good.
9. Tamper-indicating seals solve the tampering issue.
10. Adhesive label seals provide effective tamper detection, and they require little effort.
11. Attacks won't be surreptitious.



Probably Wrong Assumptions

12. A voter verified paper record (VVPR) eliminates the possibility of tampering.
13. Good security is mostly about technology and procedures.
14. A secure chain of custody involves lots of people putting their initials on seals, envelopes, boxes, and forms.
15. One size fits all. Security measures have to be identical at every precinct or polling place.
16. Existing election security measures are adequate.
17. Better security requires spending a lot more money.



Probably Wrong Assumptions

18. You can rely on vendors and manufacturers of security products for security advice.
19. Questions and concerns about election integrity constitute political attacks or insults to the efficacy and integrity of election officials.
20. Election security is thoroughly studied and well understood.
21. Election officials usually know what they are doing when it comes to election security.
22. Security by Obscurity. [Violates Shannon's (Kerkoffs) Maxim].
23. Election integrity is easy; vote tampering is unlikely.



Facts About Security Devices & Systems

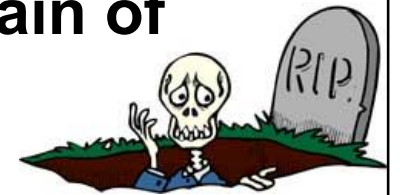
For most security devices (including biometrics and access control devices), it's easy to:

- clone the signature of an authorized person
- do a man-in-the-middle (MM) attack
- access the password or key
- copy or tamper with the database
- “counterfeit” the device
- install a backdoor
- replace the microprocessor
- tamper with the software



Backdoor, MM, or Counterfeit Attacks

The importance of a cradle-to-grave, secure chain of custody:



Most security devices can be compromised in 15 seconds (at the factory or vendor, on the loading dock, in transit, in the receiving department, in storage, or after being installed).

Most “security” devices have little built-in security or ability to detect intrusion/tampering.



The Air Force is pleased with the performance of the C-5A cargo plane, although having the wings fall off at eight thousand hours is a problem.

-- Major General Charles F. Kyunk, Jr.

Security of Security Products



Facts About Locks

- 1. Locks are meant to delay, complicate, and discourage unauthorized access.**
- 2. All locks can be defeated quickly, even by sufficiently motivated amateurs.**
- 3. Ways to defeat locks include picking, bumping, rifling, jigging a blank key, drilling out the lock, attacking the electronics, etc.**

-“Who are you and how did you get in here?”
-“I’m a locksmith. And, I’m a locksmith.”
-- Lieutenant Frank Drebin in *Police Squad*



Terminology

(tamper-indicating) seal: a device or material that leaves behind evidence of unauthorized entry.



I have been called dumb, crazy man, science abuser, Holocaust denier, villain of the month, hate-filled, warmonger, Neanderthal, Genghis Khan, and Attila the Hun. And I can just tell you that I wear some of those titles proudly.

-- Oklahoma Senator James Inhofe



Terminology (con' t)

defeating a seal: opening a seal, then resealing (using the original seal or a counterfeit) without being detected.



attacking a seal: undertaking a sequence of actions designed to defeat it.



I'd say, "It's a Buttmaster, Your Holiness."

-- Suzanne Somers on how she would respond if the Pope asked her the name of the exercise machine she promotes



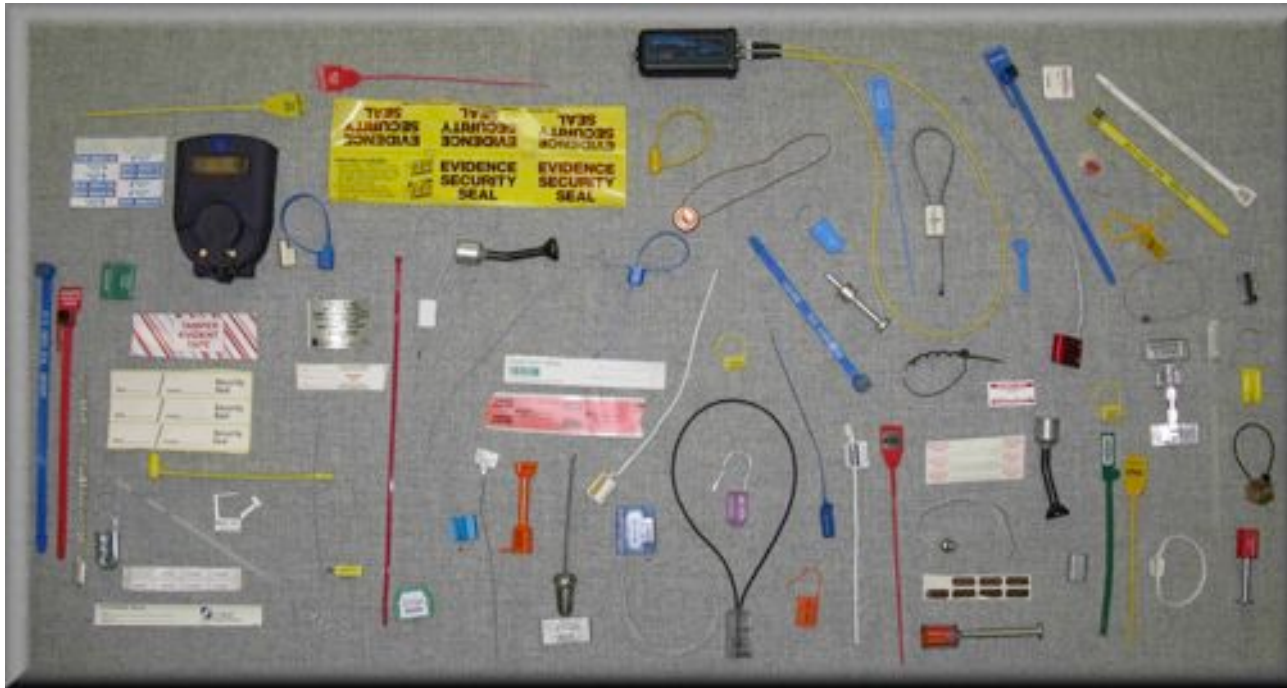
Seal Fact

A seal is not a lock.

Yanking a seal off a container is not defeating it!



Seals



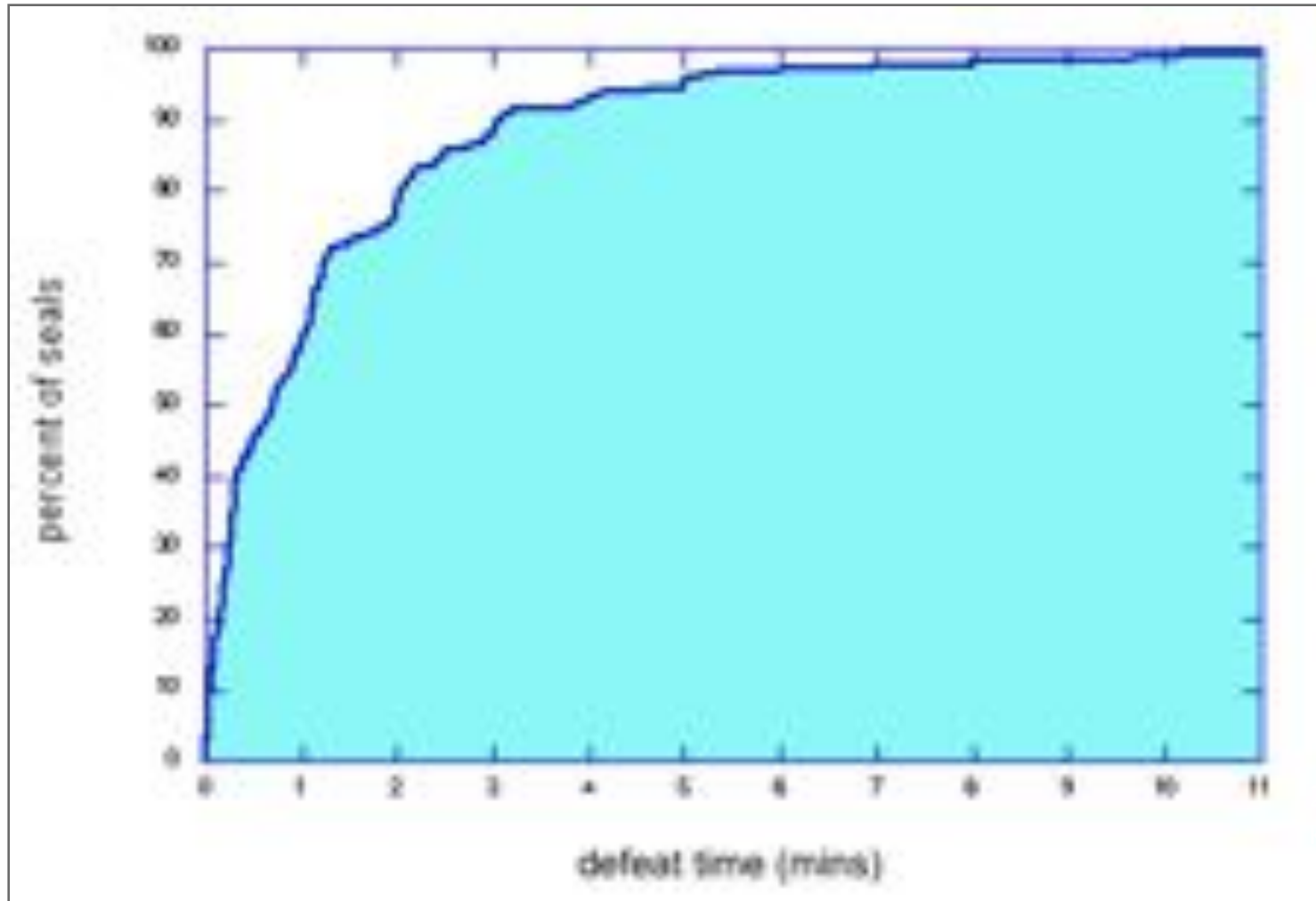
Some examples of the 5000+ commercial seals

Example Seal Applications:

- customs
- cargo security
- counter-terrorism
- nuclear safeguards
- counter-espionage
- banking & couriers
- drug accountability
- **records & ballot integrity**
- evidence chain of custody
- weapons & ammo security
- **IT security**
- medical sterilization
- instrument calibration
- tamper-evident packaging
- waste management & HAZMAT accountability



Seals are easy to defeat: Percent of seals that can be defeated in less than a given amount of time by 1 person using only low-tech methods



Summary of Seals Results

| parameter | mean | median |
|---|-----------------|----------------|
| attack time | 1.4 mins | 43 secs |
| cost of tools & supplies | \$78 | \$5 |
| marginal cost of attack | 62¢ | 9¢ |
| time to devise successful attack | 2.3 hrs | 12 mins |



Seal Facts

1. All seals need a unique identifier (like a serial number).
2. A seal must be inspected, either manually or with an automated reader, to learn anything about tampering or intrusion. The person doing this must know exactly what they are looking for.
3. Unlike locks & safes, defeating seals is more about fooling people & the inspection protocol than beating hardware.
4. Adhesive label seals do not provide effective tamper detection, even against amateurs.



It's better to be looked over than overlooked.
-- Mae West (1893-1980) in
Belle of the Nineties, 1934



Seal Use Protocol

A seal is no better than its formal and informal “use protocol” ...

...how the seal is:

- manufactured
- procured
- shipped
- stored
- checked out
- installed
- inspected
- removed
- destroyed after use



- And how the seal data and reader are stored & protected and
- How the seal installers/inspectors are trained.



Pressure Sensitive Adhesive Label Seals

- Lifting & Counterfeiting are easy.
- Lifting is usually the most likely attack.
- The difficulty of either attack is almost always greatly over-estimated by seal manufacturers, vendors, & users.
- If the recipient doesn't know what the seal and envelope (or container) is supposed to look like, you are wasting your time. [This information cannot accompany the seal.]



Nothing is like it seems, but
everything is exactly like it is.
-- Yogi Berra

Installation



- It is essential to feel the surface to check that the adversary hasn't pre-treated it to reduce adhesion.
- Full adhesion requires 48+ hours. A PSA seal is particularly easy to lift the first few minutes to hours. Heat can help.



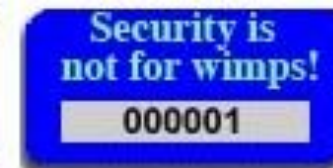
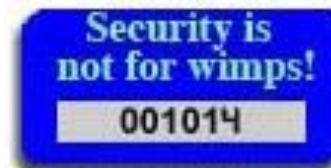
For the third goal, I blame the ball.
-- Saudi goalkeeper Mohammed Al-Deayea

Inspection

- Smell can be a powerful tool for detecting attacks. Or use a handheld chemical “sniffer” (\$150-\$9K).



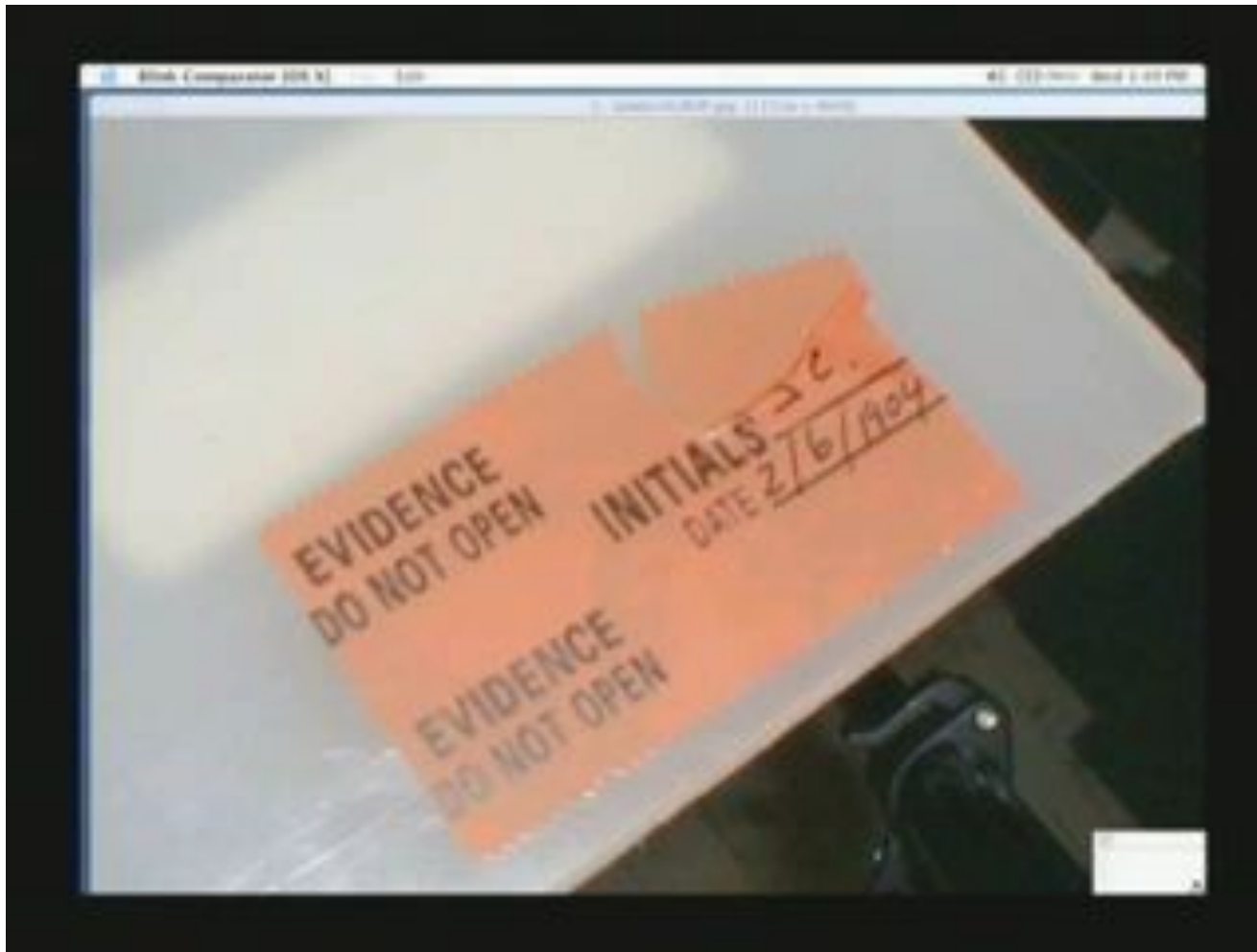
- (As with all seals) compare the seal side-by-side with an unused seal you have protected. Check size, color, gloss, font, & digit spacing/alignment.



- Carefully examine the surface area outside the perimeter of the label seal.
- **The best test for tampering is to closely observe how the label seal behaves when it is removed.**

Pressure Sensitive Adhesive Label Seals

A blink comparator is a very powerful tool for detecting tampering with PSA label seals.



The Good News: Countermeasures

- Most of the seal attacks have simple and inexpensive countermeasures, but the seal installers & inspectors must understand the seal vulnerabilities, look for likely attacks, & have extensive hands-on training.
- Also: better seals are possible!

The prophet who fails to present a bearable alternative and yet preaches doom is part of the trap he postulates.

-- Margaret Mead (1901-1978)



Tamper-Evident Packaging Test

7th Security Seals Symposium
Santa Barbara, CA
February 28 - March 2, 2006



- 71 tamper detection experts participated.
- Various consumer food & drug products were tampered with.
- A college student (Sonia Trujillo) did the tampering using only low-tech attacks.

Results: Statistically the same as guessing!

If tamper detection experts can't reliably detect product tampering, what chance does the average consumer have?

On a bag of Fritos: "You could be a winner!
No purchase necessary. Details inside."



Tampering with Urine Drug Tests

It's easy to tamper with urine test kits.

Most urine testing programs (government, companies, athletes) have very poor security protocols.

Emphasis has been on false negatives, but false positives are equally troubling.

Serious implications for safety, courts, public welfare, national security, fairness, careers, livelihood, reputations, sports.



Journal of Drug Issues **39**, 1015-1028 (2009)



Secure Chain of Custody

Not a piece of paper with scribbles in boxes!

| Name | Date | Initial |
|-------------|-------------|----------------|
| Moose | 4-1-2011 | Bm |
| Squirrel | 4-1-2011 | RJS |
| Mr. Magoo | 4-1-2011 | QM |
| Bad Guy | 4-1-2011 | BG |
| Yogi Bear | 4-2-2011 | YB |

It had only one fault. It was kind of lousy.
-- James Thurber (1894-1961)



Warning: Multiple Layers of Security ("Security in Depth")




- ❖ Increases cost & complexity
- ❖ Multiple layers of bad security do not equal good security.
- ❖ Often mindlessly applied: the layers are not automatically backups for each other, or may even interfere with each other
- ❖ Leads to complacency
- ❖ Tends to be a cop-out to avoid improving any 1 layer or thinking critically about security
- ❖ **How many sieves do you have to stack before the water won't leak through?**



Security is only as good as the weakest link. -- old adage

Suggestions for Better Election Security

1. If you're an election professional, avoid denial, cognitive dissonance, and knee-jerk rejection of any concerns or criticisms about election integrity. Mentally decouple security criticism from political criticism.
2. Seek advice and criticisms from everybody, including security experts (who maybe will consult pro bono as a public service or to get positive publicity).
3. Avoid binary thinking.
4. Think like the bad guy. How would you cheat?




I watch a lot of game shows and I've come to realize that the people with the answers come and go, but the man who asks the questions has a permanent job.

-- Gracie Allen (1895? – 1964)

Suggestions for Better Election Security

5. **Appreciate that security should be controversial.**
6. **Establish a healthy security culture & climate.**
7. **Exploit the existing adversarial nature of political parties among your poll workers to maintain an adversary-focused security culture.**
8. **Voting machine manufacturers and vendors/ manufacturers of security products cannot be your only major source of security information!**
9. **Security is hard work. If it sounds too easy or too good to be true, it is.**



You have to be careful if you don't know where you are going because you might not get there. -- Yogi Berra

Suggestions for Better Election Security

10. Arrange for background checks on the people who move and maintain the voting machines. Use bonded personnel if possible.
11. Escort the machines to and from the polling place if possible.
12. You must know for sure that there was no delay in delivery or return of the voting machines.
13. Make somebody accountable for receiving and at least semi-watching the voting machines at the polling place. Secure them!

Actual Courtroom Testimony:

Witness (a Physician): He was probably going to lose the leg, but at least maybe we could get lucky and save the toes.



Suggestions for Better Election Security

14. Watch out for swapping with “counterfeit” voting machines, and counterfeit used or unused ballots (including at the polls).
15. Don’t rely on initialed-only seals or seals lacking serial numbers. Check the serial numbers. Protect the database of serial numbers from tampering!
16. Minimize the number of seals!
17. Do serious seals training. Have good manuals, posters, & hands-on exercises.

“Product not actual size.”

-- Disclaimer on a TV ad for Burger King
that showed a giant Whopper crushing a car



Suggestions for Better Election Security

18. Have a unique secret password of the day for each polling station for officials. (Different each election.)
19. Enlist staff, custodians, admins, teachers, and students to watch the voting machines when the polling place is a school, church, etc. (A good civics learning experience!)
20. Recognize that a secure chain of custody is a **PROCESS**, not a piece of paper with initials or scribbled signatures (rarely if ever checked)!
21. Do not allow technicians to work on a specific voting machine in the warehouse without authorization and oversight.

Always strive to be the person your dog already thinks you are. -- Anonymous

Suggestions for Better Election Security

- 22. Arrange for periodic background checks for technicians who work on the voting machines.**
- 23. Deploy VVPR.**
- 24. Consider optical scan voting systems (But watch for them being rolled away & for loss of secrecy.)**
- 25. Try bribes (but wait 1 day).**
- 26. Security Management by walking around and talking to people.**



Shouldn't the Air and Space Museum be empty? -- Dennis Miller


Suggestions for Better Election Security

27. Reward & recognize good security practice & raising of concerns.
28. Pressure voting machine manufacturers for better cyber & physical security, and for better use protocols. Don't believe their snake oil.
29. Emphasize penalties for voting fraud to poll workers, but also give them upbeat encouragement about it being their patriotic duty to help prevent voting fraud.
30. Put up posters with eyes!



Suggestions for Better Election Security

- 31. Form a pro bono citizens advisory panel with security experts.**
- 32. Focus on where the risk is greatest and/or where your security is weakest.**
- 33. Test at least a random selection of voting machines before, after, & during the voting. Do effective tests: disassemble, inspect, and fully reverse engineering (don't just run them).**



If people don't want to come to the ballpark, how are you going to stop them? -- Yogi Berra

Suggestions for Better Election Security

34. Protect ballot secrecy by watching for improper voter use of cell phone cameras (especially for VVPR) and for planted mini wireless video cameras.



wireless, battery-powered, color video cameras, 100'-400' range; \$25-\$200



Actual overheard conversation between two teenage girls:
--So he's like, 'nuh uh,' and I'm like, 'uh huh,' and he's like, 'nuh uh,' and I'm like, 'um...uh huh,' and he's like, 'nuh uh.'
--No way!
--Way.



For More Information...

Related papers, reports, and presentations are available from rogerj@anl.gov
or
www.ne.anl.gov/capabilities/vat

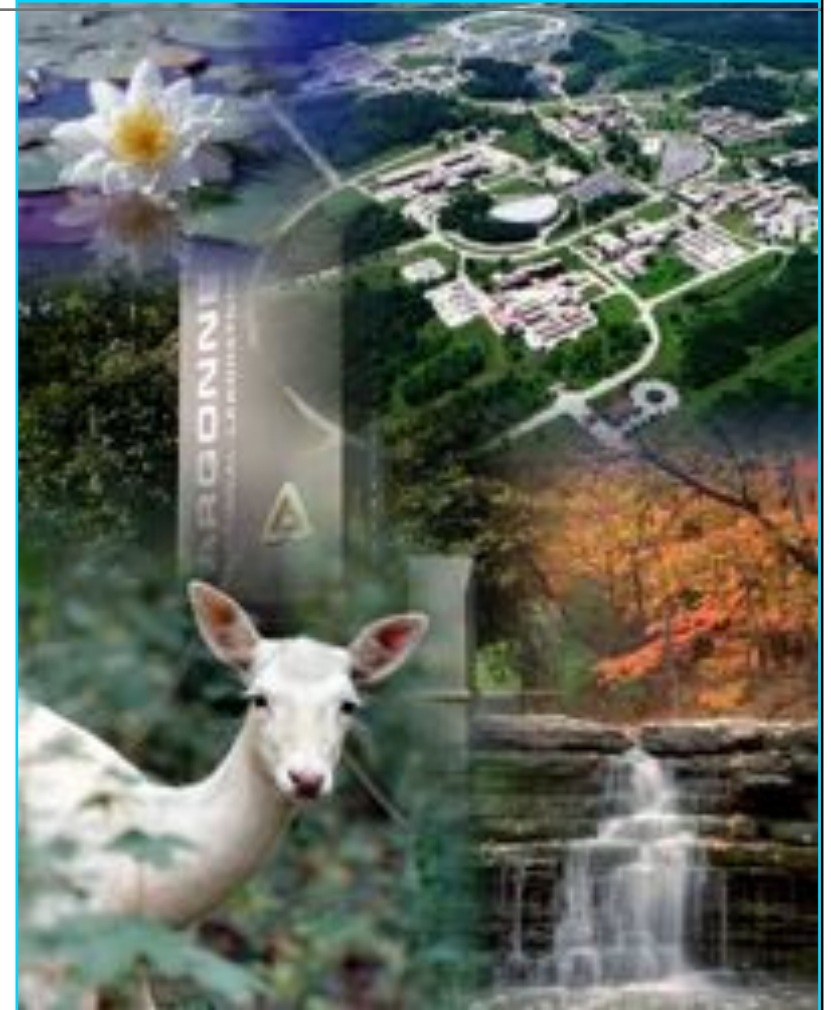
www.youtube.com/watch?v=frBBGJqkz9E

<http://blog.verifiedvoting.org/2010/10/15/1131>

M. Kassner, www.techrepublic.com, 2/14/2011

www.youtube.com/watch?v=51MxGK2q7Wo

www.grc.com/sn/sn-215.htm



If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort...only soft soap and wishful thinking to begin, and in the end, despair.

-- C.S. Lewis (1898-1963)



Blunder: Wrong Assumptions about Counterfeiting



- Usually much easier than developers, vendors, & manufacturers claim.
- Often overlooked: The bad guys usually only needed to mimic only the superficial appearance of the original and (maybe) some of the apparent performance of the product or the security device, not the thing itself, or its real performance.
- Rarely is full reverse engineering necessary.

Sincerity is everything. If you can fake that, you've got it made.

-- George Burns (1885-1996)



Why I Don't Want To Be An Election Official

- Election Security is a very, very tough problem.
- Even security professionals & manufacturers of security devices usually get it wrong, so why should we expect non-security experts to know how to have good security?
- Voting machine manufacturers are typically not very helpful or responsible when it comes to security.
- Voting is a complex process.



My definition of an expert in any field is a person who knows enough about what's really going on to be scared.
-- P.J. Plauger

Why I Don't Want To Be An Election Official

- Many thousands of people have access to the devices & user friendliness is essential (often not the case for other security applications).
- The public doesn't like security, but demands full election integrity.
- There are major time constraints.
- Budgets are brutally tight.
- You must often rely on amateur poll workers.



Radisson Welcomes
Emerging Infectious Diseases
-- Sign outside a Radisson Hotel



20+ New “Anti-Evidence” Seals

- better security
- no hasp required
- no tools to install or remove seal
- can go inside the container
- 100% reusable, even if mechanical
- can monitor volumes or areas, not just portals
- “anti-gundecking”—automatically verifying that the seal was inspected



Talking Cargo Seal



Tie Dye Seal



Chirping Tag/Seal



Time Trap

Security Culture & Climate

Effective Security Requires Effective Security Culture & Climate!

Security Culture: The official security policies, procedures, and practices.

Security Climate: The unofficial attitudes and mindsets about security.

If you think that technology can solve your security problems then (1) you don't understand your problems and (2) you don't understand the technology.

-- Bruce Schneier

