Election Officials Roundtable

Friday, April 25th, 2008
EAC Offices
1225 New York Ave, Suite 150
Washington, DC 20005

Discussion Questions

(With Comments by George Gilbert in red.)

Voting systems manufacturers today must design their products to fulfill a broad and ever-expanding list of requirements to meet the needs of an increasingly diverse voting public, while at the same time attempting to provide an efficient and cost effective product for election officials. Election administrators place additional value on other attributes of a voting system including ease of system setup, operation, and maintenance; configuration simplicity; reliability of operation; processing accuracy; ability to audit entire process; and high polling place throughput. The demographic makeup of the voting public itself also influences voting system design to a great extent. These demographic factors include age, educational level, language proficiency, manual dexterity, physical mobility, sensory functioning, and commuting distance from polling place. Finally, and perhaps most importantly, voting system design must also mitigate a variety of potential threats to the voting process.

The voting system design process needs to take all these factors into consideration and strive to strike an optimum balance. This is a difficult task because many of these factors conflict with each other. As the scope of requirements increases, satisfactory solutions become harder to define. This is an environment where the design process must be open to innovative approaches and unbound by technological constraints so the very best solutions can be implemented in a timely manner.

The next iteration of the VVSG will dictate the direction of voting system design for the next generation of voting systems. The challenge for this next iteration of guidelines is how to properly balance the need for improved security, audit ability and accessibility while also creating guidelines that are not so prescriptive that they stand in the way of innovation. Technology in and of itself has a neutral value scale and can only be evaluated in the context of its application. A voting system is an information processing system. The historical trend in information systems technology has been to supply ever greater capabilities with simpler configurations at lower cost. Information processing has moved from paper and electro-mechanical devices to fully electronic processing and from a host of special purpose devices to general purpose devices.

As the issuer of these guidelines the EAC has a duty to examine these proposed guidelines and decide what the next generation of voting systems must be capable of. Two of the driving forces behind the suggested security requirements in the TGDC draft VVSG are concerns about the integrity and trustworthiness of electronic voting systems and the difficulty of verifying that software only does what it is intended to do and does not harbor malicious code.

The 2007 VVSG recommendations introduce a number of design requirements and validation concepts for the purpose of improving the security of voting systems. These recommendations constitute a radical change from previous voting system standards. These concepts include Software Independence (SI), Independent Voter-Verifiable Records (IVVR), Open Ended Vulnerability Testing (OEVT), and usability benchmarks. Each of these will introduce additional complexity to system design and development and therefore increase the cost and risk for vendors. And all except OEVT will impact voters through changes in the voting process itself. The concepts of Software Independence and IVVR offer additional security but also lead to concerns as to the accessibility and usability of the voting systems.

Before imposing these changes on the election community, it is the EAC's responsibility to determine the best means for providing a sufficient level of voting system security without requiring disproportionate tradeoffs against other highly desirable voting system features. To this end the EAC is convening roundtable discussions for the purpose of carefully considering the VVSG recommendations. This discussion will be conducted in six segments:

1. The VVSG has more than one audience, including vendors and VSTLs. Do you consider county and state election officials as one of the stakeholders in the VVSG and therefore one of the intended audiences?
   Are members of the armed forces stakeholders in the war in Iraq?

If county and state election officials are not among the VVSG stakeholders, then it has none. County election officials are the primary stakeholders in the VVSG. As voters, we have a common and equal interest with every other voter in the security and integrity of our voting systems. As the election administrators, our entire careers are at stake. Our ability to perform our jobs is at stake. Our personal reputations are at stake. The VVSG determines the options available to election administrators in carrying out their duties.

a. If yes, is the document intelligible to you?

Parts of it. It is, however, too expansive, far too detailed, for the vast majority of election officials, including me, to even read much less comprehend. I seem to recall that the cross referencing, at times, required multiple readings and, more than once, resulted in new interpretations of what was being stated.

Of the parts I have been able to read, most is "intelligible," and cause for great concern. One example is represented by Part 1, Chapter 7.5, "Casting." After reading:

> "The requirements in this section mandate that privacy of the ballot be protected throughout the entire process of credential issuance and ballot activation, and that **no information be maintained in reports or logs that could assist in identifying a voter's cast ballot (except for provisional voting on a DRE)**," (emphasis added)

the conflict this presented under North Carolina law made it difficult to assess the entire chapter. (NC law requires all "absentee" ballots to be identifiable and retrievable.)

(Further examples of these concerns I have addressed in my comments and will not repeat here. A copy is attached for those who are interested.)

b. If not, how could it be improved?

The "performance standards" assumed in the VVSG go well beyond those required to accomplish the objective, eg., as noted above, in specifying too far reaching a "privacy" standard. Further, they delve into specifying HOW these performance objective must be met.

Perhaps most troublesome is the apparent attempt to eliminate all possible technology based threats to the voting systems while ignoring the human threats, eg., the inevitable errors or mischief inherent in manual handling and tabulation of paper records.

A more effective approach, and far less expensive, would be to recognize that "voting systems" are not simply equipment. Voting systems are equipment and procedures associated with the deployment of that equipment. While this may place the technical folks in what they feel is an "ambiguous" position, the purpose of the VVSG's is not to enable the folks at NIST to sleep well at night. The purpose is to enhance the accuracy and security of elections. Technical standards, no matter how detailed and tightly specified, cannot close the human loophole in real world elections, threaten to stifle innovation and threaten to drive out of reach of many jurisdictions the cost associated with implementing the technology. I understand that NIST is technology oriented. The EAC, however, must take a more holistic view of "voting systems." Elections does not need a "fail safe" technology. It needs reliable equipment that can be efficiently employed through good management.

2. On October 7, 2005 the National Institute of Standards and Technology (NIST) held a "Risk Assessment Workshop" in order to evaluate threats to voting systems. The results of that workshop can be found at http://vote.nist.gov/threats/. In so doing NIST recognized the importance of evaluating threats when developing a secure voting system, but no formal risk assessment was developed. The EAC is now interested in learning how to best develop a risk assessment framework to provide context for evaluating the security implications of using various technologies in voting systems.
   a. What are the essential elements of a risk assessment?

Some thoughts:

All conceivable threats are possible (plus some that are not conceivable.) but few have a high risk

"Risk" includes the likelihood of a threat being realized.

"Risk assessment" should be accompanied by cost-benefit analysis.

Who has a vested interest in disrupting or redirecting the outcome of an election?

Who with a vested interest potentially has the means to carry out their disruption or redirection?
What are the costs (including the costs of being caught) of executing such a threat?
Are the benefits, to those attempting to disrupt or redirect the outcome of an election, greater than the potential costs?

Is the means available on a widespread or limited basis?
Is there a history of activity that indicates that an attempt will be made to carry out a potential threat?
What measures are in place to detect or deter such activity before its culmination?
What are the weak points in such existing measures?
Who has the means of exploiting those weak points?
What measures can be put in place to detect or deter exploitation of those weak points?
What are the costs (including management and functionality costs) of putting such measures in place.
What are the benefits of detecting or deterring such potential threats?
What is the likelihood that the results on an election would be changed as a result of successful execution of the threat?

b. How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks in an election environment?

It cannot.

However, as a starting point it can dispatch teams to participate, from the beginning, in local elections offices and take notes. Election officials, precinct officials and voters can create "threats" that no one could possible imagine or anticipate. Point out the threats you identify and then talk to us about how these threats can best be mitigated. Consider both changes in technology and management procedures.

The greatest threat to the integrity of elections in 2008 is the multiplicity of directives and devices for threat prevention with which election administrators are being enundated.

c. How do you evaluate what is an allowable level of risk?

Not allowable: Significant[1] undetectable error in vote recording
Not allowable: Significant undetectable error in vote tabulation
Not allowable: Unrecoverable loss of CVRs (cast vote records), including paper ballots

Allowable: Imperfect management that is not "significant"

[1] "Significant" is essentially defined by NC law as a large enough error to "materially affect" the outcome of an election with respect to a specific contested contest. Obviously this is potentially one vote, however, the likelihood of one vote being "significant" is very small.

Allowable: Voter error that is not “significantly” exacerbated by the voting system

Allowable: Irregularities that are not “significant”

3. Could you comment on the value of stability in the standard to your jurisdiction?
    a. Which is preferred, a standard with a short-shelf life that accommodates innovation and change or a stable standard that may discourage innovation, but creates longer certification lives of voting systems?

This depends on the quality of the certified voting system at any given point in time. If the cerfitied system is a good one, stability is certainly preferred. If it is not a good one, standards that facilitate change and innovation are preferred.

This leads me to the conclusion that the standards themselves should be structured to accommodate either situation. Systems working well should not be forced to change. For systems not working well, technically or in the judgement of the users, the standards should enable rapid and efficient modification. It should be as clear as possible that any set of standards establish a target for incremental change, not an absolute standard of accuracy and security.

4. What is the value of the open-ended vulnerability testing (OEVT) model?
    a. Would the current OEVT requirement in the standard reduce or decrease voter confidence in your system?

Would likely have no effect on voter confidence. Voter’s tend to trust or distrust people more than systems. If they are confident in their people and processes, they will likely be confident in their voting system. Further, they will neither know nor care to know what OEVT is. That doesn’t make OEVT a bad or useless idea, but it would not likely affect voter confidence.

    b. If the EAC were to require OEVT how could it best be included into the EAC’s Testing and Certification Program?

OEVT should not be included in the VVSG as a comprehensive “pass/fail” set of standards. There is a high likelihood that any “system” could “fail” the test criteria at some juncture but remain a viable voting system within the context of an acceptable risk assessment model. Further, management procedures can frequently be employed to mitigate technical vulnerabilities or weaknesses.

Having said this, I feel OEVT could serve a useful purpose if carried out in partnership with voting system vendors and election administrators with the objective of identifying potential vulnerabilities and threats and developing a set of alternative technical and/or management guidelines for addressing such vulnerabilities and threats.

An essential step, as noted above, would be for prospective OEVT teams to spend time engaged, with local election officials, in the actual preparation for and conduct of an election. There is no substitute for this experience. The subtleties of the numerous potential threats and vulnerabilities that emerge during the months of election preparation as well as on election day cannot be anticipated or communicated by any “expert”

The concept of OEVT appears to arise out of an expectation or desire that the VVSG must produce voting systems in which nothing can go wrong with a certified voting system. This is both counterproductive and an impossible standard to meet. The EAC will never be able to issue a voting system certification under this expectation…a situation on which we appear to be bordering at present.

5. Would component testing (the ability to test and certify components as they are modified or added to an existing system) be beneficial to your jurisdiction?

Comment [M1]: Good! This is an important question.

Yes. Anything that can reduce the cost and speed up the process of modifying/upgrading voting systems would be extremely important. I used to be able to have my vendors fix things that were wrong, inefficient or just stupid about my voting system. That is no longer possible.

There are numerous modifications of voting systems that likely have no functional relationship to most other features of the overall system. Likewise, superficial changes should be identifiable and subjected to a less rigorous standard (perhaps an equivalency statement only) for certification than functional changes.

6. Are there any changes to the VVSG, in either scope or depth, which would significantly reduce the cost (time and/or expense) of compliance without adversely affecting the integrity of the VVSG or the systems that are derived from its implementation?

Yes.

The VVSG should incorporate a section explaining what they mean and what they do **not** mean. What do the states need to understand about adoption or non-adoption of the VVSG and the implications for the their available voting systems. How can the states use the VVSG to avoid duplication of effort (ie., time and money).

Perhaps the VVSG should be limited to technical issues only involving system integrity and security. For instance, should the VVSG address the issue of voter privacy, which clearly involves matters outside the control of any set of hardware and software, or should it address only matters of data security within the system?

The only realistic purpose of the VVSG is to promote continual improvement in voting systems over the long run. Even aircraft safety standards are not expected to prevent all future plane crashes. Somehow the message has got to be understandably communicated to the users and evaluators of these voting systems….states, counties, voters, media….that the VVSG does not involve the pursuit of perfection ….only the pursuit of progress.

a. What needs to be added or removed from this document in order for it to meet what is needed from future voting systems?

As noted, few, if any local election officials have the time or expertise to read or understand the significance of the entire VVSG. I addressed specific issues in my comments and presume this is not a forum in which to to restate those in detail.

In general, standards need to be removed that are based on the assumption of uniform state procedure, eg., the "privacy" standards. Such standards, where state definitions and rules may exist, should be generalized to accommodate such state variations.

The VVSG's reliance on manual auditing of paper records (under the guise of "software independence") without any standards for judging the accuracy or security of such manual tabulation/auditing is contradictory to, and potentially undermines, the entire purpose of the VVSG.

Flexibility and a reduction in the cost of bringing new systems or features to market are essential if we are going to have "future voting systems" that are affordable by the majority of jurisdictions and that represent any significant improvement over what we have today.

b. How could the process of developing and vetting the VVSG be improved to ensure higher volume and higher quality input from election officials?

Start by having those writing the VVSG spend a 3-6 months working in local elections offices during the period leading up to and including a significant election.

Do not try to enlist major participation by election officials or vendors in new versions of the VVSG in presidential election years except on our turf.