Voting Advocates Roundtable Discussion

Thursday, April 24th, 2008
EAC Offices
1225 New York Ave, Suite 150
Washington, DC 20005

Discussion Questions

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. 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?
    b. How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks?
    c. How do you evaluate what is an allowable level of risk?

2. How can innovative systems be evaluated for purposes of certification?
    a. How can we create a certification process for innovative systems that isn't a backdoor around the standard certification process but at the same time isn't so cost prohibitive and restrictive that it presents a barrier and a disincentive to prospective inventors and manufacturers?
    b. Can a set of limited standards be created in order to make the path towards certification of innovative systems more clear? If so, how?

3. What is the value of the open-ended vulnerability testing (OEVT) model?
    a. Are there any risks associated with this kind of testing?

b. What are the best ways to limit the cost of this kind of open ended non-scripted testing so that it can be useable within the EAC's testing program?
c. If the EAC were to require OEVT how could it best be included into the EAC's Testing and Certification Program?

4. Do methodologies exist to test voting system software so it can be reliably demonstrated to operate correctly?
    a. If testing to a thorough set of standards is not enough to demonstrate the reliability of the system, what else can be done to improve confidence in electronic voting systems?

5. Throughout the creation of its draft VVSG, the EAC's Technical Guidelines Development Committee struggled to balance the need for useable and accessible systems with the desire to create the most secure system possible.
    a. How can the EAC best strike a balance between these sometimes competing needs?
    b. What level of usability or accessibility could be sacrificed in order to gain additional security or vice versa?

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?
    a. What needs to be added or removed from this document to strengthen it and the systems to be constructed to its specification?