U. S. ELECTION ASSISTANCE COMMISSION
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

EAC Academics Roundtable

Discussion Topics for the EAC's Academics Roundtable Discussion regarding the TGDC's Recommended Voluntary Voting System Guidelines

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 dictates 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 standards is how to properly balance the need for improved security, auditability and accessibility while also creating standards 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 standards the EAC has a duty to examine these proposed standards 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. It is difficult to have a meaningful discussion of these issues without a consensus on what constitutes an acceptable level of risk for such a fundamental process as voting. While steps have been taken to initiate this process, there has still not been any thorough risk assessment of the current generation of voting systems by the entities responsible for drafting the VVSG.

In spite of a risk assessment document and prioritization of acknowledged risks, 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 Paper Records (IVVR) and Open Ended Vulnerability Testing (OEVT). 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 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 EAC is convening a roundtable discussion for the purpose of carefully considering the VVSG recommendations. The discussion will be conducted in five segments:

1. How to develop a risk assessment framework to provide context for evaluating the security implications of using various technologies in voting systems?
    a. How do you evaluate what is an allowable level of risk?
    b. What are the essential elements of a risk assessment?
    c. How can the EAC best create a risk assessment that is more than just conjecture?

2. As stated in the 2005 VVSG, the goal for the next iteration of the VVSG is to create functional standards that promote innovation rather than design orientated standards that limit design choices. Do you think this document achieves that goal?
    a. Where does the document fall short of this goal?
    b. Do you view functional standards as testable standards?
    c. Is the definition of software independence as applied in the TGDC recommendations too technologically prescriptive? If so how would you change it to be more expansive?

3. Do methodologies exist to test voting system software so it can be reliably demonstrated to operate correctly?
    a. If yes, how do they compare with Software Independence in terms of effectiveness and impact on other factors such as accessibility and efficient election administration?
    b. What added security benefits are created by SI that are not met by the testing process?

4. What are the relative merits of the various types of Direct (by the voter) and Indirect (by automation) Independent Verification techniques?
    a. What are the merits of each type?
    b. What technologies have you worked with/seen that do not fit under the concept of Software Independence that you believe to be secure and accessible?
    c. What security is lost or gained by using Direct or Indirect verification?

5. How can innovative systems, for which there are no standards, be evaluated for purposes of certification?
    a. How do other industries deal with the testing and certification of innovative products?
    b. How do you 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 manufacturers?
    c. Can a set of limited standards be created in order to make the path towards certification of innovative systems more clear?

Participants List for Roundtable Discussion of TGDC/NIST Recommendations for VVSG

1. **Juan Gilbert, Ph.D**
   TSYS Distinguished Associate Professor
   Human Centered Computing Lab
   Department of Computer Science and Software Engineering
   Auburn University

2. **Michael I. Shamos, Ph.D., J.D.**
   Distinguished Career Professor, School of Computer Science
   Co-Director, Institute for eCommerce Director, Universal Library
   Carnegie Mellon University

3. **Ron Rivest, Ph.D**
   Professor,
   Department of Electrical Engineering and Computer Science
   Massachusetts Institute of Technology

4. **Eugene H. Spafford, Ph.D**
   Professor of Computer Science,
   Department of Computer Sciences
   Purdue University
   Founder, Executive Director,
   Purdue Center for Education and Research in Information Assurance and Security (CERIAS).

5. **Costis Toregas, Ph.D**
   President Ameritus
   Public Technology Inc.
   Lead Research Scientist
   George Washington University

6. **Peter Ryan, Ph.D.**
   International Association for Voting System Science
   School of Computing Science
   University of Newcastle, United Kingdom

7. **Daniel Castro**
   Senior Analyst
   The Information Technology and Innovation Foundation
   Pittsburgh, PA

8. **John Wack, Ph.D.**
   Computer Scientist

Software and Diagnostics and Conformance Testing Division
National Institute of Standards and Technology

9. **Alec Yasinsac, Ph.D.**
   Associate Professor of Computer Science
   Florida State University

10. **Merle King (Moderator)**
    Executive Director, Center for Election Systems
    Kennesaw State University