Auditability Working Group

David Flater
National Institute of Standards and Technology
http://vote.nist.gov

Resolution from July

- The TGDC charges the Auditability Working Group with the responsibility of drafting a definition of auditability, and what characteristics an auditable system would possess. This definition, and these characteristics, should be developed independently of specific technology and even a consideration of whether or not the technology exists.
- The Auditability Working Group should also prepare a report that evaluates SI, and alternative technology, and their strengths and weaknesses for meeting the auditability objectives.

Charge from EAC

Alternatives to Software Independence (SI) – EAC directs the TGDC to develop draft requirements for audit methods to achieve the goal of Software Independence (SI). The goal is to develop requirements for the auditability of the election system without requiring a specific technology. The starting point for these requirements should be the work already completed by NIST on alternatives to SI.

Definition of Auditability

The transparency of a voting system with regards to the ability to verify that it has operated correctly in an election, and to identify the cause if it has not.

- Transparency means the existence and observability of evidence
- Error correction / recovery capability is important, but is not part of the definition

Characteristics—preface

- A voting system need not have all of these characteristics to be called auditable
- However, requirements for voting system auditability would directly or indirectly mandate some subset of these characteristics

Characteristics

- Enables detection of errors
  - Voter verification, independent records, integrity checks, event logging
- Enables diagnosis of faults
- Enables correction of errors
- Disambiguates voter intent
- Preserves records
- Supports sampling in post-election audits

Survey of architectures

- Voting system architectures × auditability characteristics (strengths and weaknesses)
- Additional discussion of VVPAT, EBM, and vote-by-phone
  - Unintended consequences
  - Accessibility *qua* serving the public
  - Accessibility *qua* legal/regulatory risk
- Non-architectures: parallel testing, software assurance, innovation class

Alternatives

- Mutually exclusive options for VVSG requirements
- Differentiated by consequences, not by goals
  - No one ever objected to the *intentions* of a requirement for SI
  - Requirements do not specify technologies, but specific technologies become uncertifiable as a consequence

Differentiating factors

- Auditability
- Transparency to voters/observers
- Expected outcome for accessibility
- Social and political consequences
- Future prospects for voting systems
- Complications for VVSG

Focus

- Dominant auditability characteristic is the potential for undetectable errors and the nature of that risk
  - Inherent risk: debatable
  - Control risk: do you believe our assurance case?
  - Detection risk: 100%
- Prevention without detection: a hard sell
  - A challenger may want evidence that the system as deployed operated correctly in a given election
  - "Trust" (the assurance case) vs. "verify" (audit)

Software Independence

- Robustly mitigates risk of undetectable error in recording of votes
- Expected outcome includes reinforcement of trend to deploy opscan with accessibility < DRE
  - Paper handling
  - Conversion of complete print content
- Accessible paper or paperless SI not precluded, in theory

Independent Verification

- Evidence may be software-dependent
- Risk of undetectable error resulting from common mode failures of "independent" devices
- Transparency < SI
  - Not responsive to distrust of "black boxes"
- Anticipate R&D, possible resurgence of electronic voting, better accessibility
- Independence hard to specify and test

Lossy SI

- Driven by Lossy VVPAT concept
- Evidence is retained for only a sample; risk of undetectable error for the others
- Advantages over SI
  - Save paper
  - *Maybe* manage a legal/regulatory risk (but not in a responsive way)
- Gives up error correction / recovery

VVSG 1.0

- Many jurisdictions already require a higher standard of auditability
- Relevance of VVSG may be harmed through inaction

Hybrid systems

- (SI-not-accessible) + (accessible-not-SI)
  - VVPAT or EBM hybrid would be SI
  - Must be DRE or vote-by-phone
- Auditability for some; risk of undetectable error for others
- Issues of equality
- Complicated to specify a double standard for vote-capture devices

Summary

- Software Independence—robustly mitigates the risk of undetectable error; effectively requires paper records
- Independent Verification—improves auditability without requiring paper; undetectable errors remain plausible
- Lossy SI—marginal value; undetectable errors remain plausible
- VVSG 1.0—no change; undetectable errors remain plausible
- Hybrid systems—explicitly requires a combination of different kinds of vote-capture devices, where some robustly mitigate the risk of undetectable error while others sacrifice this for accessibility

Conclusion

- "Paper or plastic" does not go away
  - Plausible, undetectable error means that the risk is not managed
  - Dual control is not entirely valid for complex software
- Once a choice among these alternatives has been made, a set of testable requirements can be derived

What now

- TGDC approve report or ask for rework
- Optional: TGDC resolution making recommendations to EAC
- EAC policy decision
- → Requirements development for VVSG 2.0