Technical Guidelines Development Committee
April 20, 2005 Plenary Meeting

Independent Dual Verification Voting Systems

Security Overview

John P. Wack

April 20, 2004

Overview

- Background - Jan ’05 resolutions
- Security Goals
- Overview of NIST’s Approach
- IDV System Definition
- Core Requirements for IDV systems
- IDV Voting System Approaches
- Discussion

Terminology

- **Direct Verification** – a verification using human senses, e.g., directly verifying a paper record via one’s eyesight
- **Indirect Verification** – a verification using an intermediary to perform the verification, e.g., verifying an electronic ballot image at the voting system
- **Ballot Audit** – a measure of whether a voting system has correctly recorded ballots as cast
- **Electronic Records** – ballot images in electronic form

Background

- TGDC Resolution #12-05, “Voter Verifiability I”
- TGDC Resolution #21-05, “Multiple Representations of Ballots”

What are our Goals?

Dick Tuck, upon losing an election said,
"THE PEOPLE HAVE SPOKEN, THE BASTARDS!"

- It is desirable that losers have confidence in the election results w/o recounts, lawsuits, etc.
- We must specify voting systems that inspire voter (and loser) confidence in election results
- We must specify voting systems that produce records such that election officials can readily perform ballot audits to high degrees of precision

Current Scenario

- Various types of electronic voting systems today make one record of ballot images, verified indirectly
- Despite many good security features, problem is that ballot audits, i.e., the **determination that ballots are recorded as cast, cannot be made independently of the voting system:**
  - Audits instead must rely on pre-election gauges of voter behavior
  - Audits instead must rely on post-election polls
  - Audits instead must rely on correctness of implementation and testing
- Ballot audits of this nature increasingly do not fare well in close elections when precise proof of result is demanded

Future Concerns

Information technology changes at rapid pace

Threats and attacks increasingly sophisticated

Voting systems and software potentially more difficult to assess and verify

Increasing likelihood for operational problems

Higher stakes in elections, higher risk of fraud

+ More demand for proof of results in close elections

= Voting systems must accommodate this future

Is VVPAT a good solution?

- One possible approach for ballot auditability
- But, solutions being developed w/o strict requirements firmly in place
- Paper records have inherent handling issues that require study, new concepts, new procedures
- Paper marginally suitable for efficient audits
- Usability and accessibility need study, new benchmarks
- **Near-term mandates for VVPAT do not necessarily permit time for best approaches to emerge**

NIST Analysis and Approach

- Voting systems must produce ballot records to withstand errors and fraud
- VVPAT not necessarily the best or only approach
- NIST is drawing a larger circle around a class of voting systems with potentially good ballot audit properties
- Vendors may wish to build to these requirements
- NIST will in the future recommend them as mandatory

Independent Dual Verification Systems (IDV)

- A general class of voting systems
  - Produces two distinct, independently verified records of ballot choices
  - Corresponding ballot records can be cross checked
  - Equality of content can be checked in determination that the ballot choices were recorded as cast

IDV Properties

- Simplicity of ballot audit procedures factored in record design
- Ballot records potentially have greater resistance to damage, accidents, fraud
- Voting systems potentially are more resistant to subversion
- Potential reductions in testing expense
- Ballot audits can result in greater levels of confidence that ballots are recorded as cast

IDV Record Production

1. Two records of voter's choices are produced; one on WO media (irreversible commitment to one record)

2. Voter verifies that both records are correct; verification processes are independent of each other

3. At least one record verified directly by the voter **OR** both records verified indirectly if on different systems

4. Content of the two records can be checked later for equality

Example IDV Approaches

- VVPAT
- Modified Op Scan
- End to End (Encrypted Ballot Systems)
- Witness (camera, screen shot)
- Split Process (“frog” protocol)

Core IDV Requirements

6.0.1.2.1.1 - The voter verifies the content of each record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

6.0.1.2.1.2 - The creation, storage, and handling of the records are sufficiently separate such that the failure or compromise of one record does not cause the failure or compromise of another…

6.0.1.2.1.3 - The processes of verification for the multiple records do not all depend for their integrity on the same device, software module, or system, and are sufficiently separate such that the records each provide evidence of the voter's choices independently of the other records.

Core IDV Requirements (cont)

6.0.1.2.1.4 - The records can be used in audits of one another, so that at least one set of records can be used in an efficient counting process, and another set of records can be used in an efficient process of verifying its substantial agreement with the first set of records. (both need to be cross checked against each other)

The records include a unique identifier for identifying each record uniquely in its set and for identifying each record's corresponding record in the second set.

6.0.1.2.1.5 - The records include an identification of the voting site/precinct.

6.0.1.2.1.6 - The records include information identifying whether the balloting is provisional, early, or on Election Day, and information that identifies the ballot style in use.

Core IDV Requirements (cont)

6.0.1.2.1.7 - The records include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

6.0.1.2.1.8 - The records include an identifier of the voting system that is unique to that style of voting systems (e.g., serial number)

6.0.1.2.1.9 - All cryptographic software in independent verification voting systems is in modules that have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable.

Ballot Audit Procedures

- New ballot audit procedures needed to make use of new capabilities, e.g.,
  - Targeted checks using correspondences of specific records
  - Cross-checks of record sets against each other
- NIST recognizes ballot audits must be uncomplicated, readily performed, fast
- Ease of ballot audit central to IDV record handling

VVPAT IDV Approach

- Voting system produces two records, commits to one record on paper
- Voter indirectly verifies electronic record, directly verifies paper record
- Structured properly, records can be cross checked and compared
- Requirements are covered in VVPAT presentation

Op Scan IDV Approach

- Voter creates paper ballot, directly verifies ballot choices
- Paper ballot is scanned; analog to digital process creates an electronic record
- 2nd indirect verification necessary to ensure correctness of scanning operation
- Similarities to Split Process approach …

End to End IDV Approach

- Encryption used as part of voting protocol
- Electronic record indirectly verified and encrypted
- Paper record receipt with cryptographic codes verified by voter; verification may be direct or indirect or other
- Some approaches permit voter to verify receipt against bulletin board system of counted, encrypted ballots
- Proof of correctness linked to mathematical proofs
- Many potential approaches

Witness IDV Approach

- Separate device that captures voter’s indirect verification of ballot at a voting station
- E.g., a camera or screen capture device
- Voter trusts witness device to be highly accurate and reliable and operational
- Strong requirements needed for testing
- Witness device capture operation requires 2nd indirect verification to be in IDV

Split Process IDV Approach

- Two stations, vote capture and vote verification
- Vote capture station used to record voter’s choices on a token object
- Voter takes token to vote verification station and…
- Voter verifies accuracy of token’s record, directly or indirectly depending on token media
- Copy of token’s record made, verified indirectly
- Potential reductions to s/w complexity
- Potential reductions to testing expense, time required

IDV Systems Discussion