Desirable Properties of Voting Systems

Svetlana Z. Lowry
National Institute of Standards and Technology
and
Poorvi L. Vora
The George Washington University
National Institute of Standards and Technology

Outline

- Propose Desirable Properties of Voting Systems
  - Security (auditability, ballot secrecy)
  - Usability and Accessibility

- E2E Voting Systems

- Comparisons among voting systems

- E2E Voting Systems: electronic vs. paper ballots
Outline

- Propose Desirable Properties of Voting Systems
  - Security (auditability, ballot secrecy)
  - Usability and Accessibility
- E2E Voting Systems
- Comparisons among voting systems
- E2E Voting Systems: electronic vs. paper ballots

Desirable Property I: Auditability

A voting system is **auditable** if it provides **evidence** – about an election, *to* voters and the general public – that can be used to determine the **correctness** of the *election outcome*.

Evidence provided to:

Voters: **Voter-auditable**
Public: **Publicly-auditable**

VVPAT records voter-auditable. Publicly-auditable if recounts are performed in public.

* First recommended to us by Stefan Popoveniuc
Other Desirable Properties

• Individual Votes Should Represent True Voter Intent

• Need:
  – **Desirable Property II – Ballot Secrecy**
    Voter does not fear someone will find out how he or she voted
  – **Desirable Property III – Usability**
    Voting technology and process do not thwart voter’s attempt to record intent

Desirable Property II: Ballot Secrecy

• Describe ballot secrecy from two points of view:
  – Evidence about ballot obtained from:
    • voting system
    • voting system + voter (incoercibility)
  – Provide a range of definitions: strict to lenient
  – Each definition re: ballot secrecy can be enhanced to one on incoercibility
Desirable Property II: Ballot Secrecy – Informational

A voting system is private if it (and the procedures/process for using it) does not make available additional information on an individual voter’s ballot choice(s).

- Knowing 1% votes accurately ≠ improving guess on all votes from 50% to 50.5%
- Unlike tally-accuracy, not possible to prove
- Can adversary can break crypto? (i.e. can encrypted votes be revealed?)

Desirable Property II: Ballot Secrecy – Deniability

A voting system is private if, given all the additional information provided by it (and the procedures/process for using it), there are at least two ballot choices (of reasonable probability) associated with each voter.

- Much more lenient
- Two ballot choices may represent the same views
- A best definition probably between these two
Desirable Property II
Ballot Secrecy – Incoercibility

A voting system is \textit{incoercible} if additional information provided by the voting system (and the procedures/process for using it), combined with any \textit{evidence provided by the voter}, does not improve an adversary's guess on how the voter voted.

- Ballot secrecy in spite of cooperation between adversary and voter
- Can modify most ballot secrecy definitions

Ballot Secrecy: Discussion

- Tension between auditability and secrecy
  - In attempting to provide verifiable information for audit, might leak information on votes

- Why ballot secrecy?
  - Policy, legal, civil rights motivations
    - Affect technical goals, research, etc.
  - And related: as a means of enabling the communication of true (impediment-free) voter intent
Ballot Secrecy: Discussion (contd.)

- How powerful is the ballot secrecy adversary?
  - Can break crypto?
  - Can communicate with voter during vote casting?
  - Has resources (humans, computers)?
  - Can change election outcome?
  - Inside (access to voting system data) or Outside?
  - Minimal: Doesn’t make special efforts?
  - Shares secret information (crypto key) with others?
  - What is a reasonable definition of the adversary vs. definitions in the crypto literature*

Outline

- Propose Desirable Properties of Voting Systems
  - Security (auditability, ballot secrecy)
  - Usability and Accessibility*

- E2E Voting Systems

- Comparisons among voting systems

- E2E Voting Systems: electronic vs. paper ballots

* Our thoughts greatly influenced by discussions with Sharon Laskowski
Desirable Property III: Usability – General

- Learnability
- Efficiency
- Memorability
- Errors
  - how many
  - how severe
  - how easy to recover
- Satisfaction

Desirable Property III: Usability, in TGDC-Recommended VVSG

TGDC-Recommended VVSG defines *usability* as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of *users* with a given *product* in the performance of *specified tasks*. 
Desirable Property III: Usability: Example Definition

A specific performance-based definition:

A voting system is **voter-usable** if its *total completion score* is at least 98%, its *perfect ballot index* at least 2.33, and its *voter inclusion index* at least 0.35 computed based on VPP (Voter Performance Protocol) data.

– Can debate the criteria and minimum acceptable scores

Usability: Discussion

- Auditability requirement introduces usability requirements
  - Three types of users:
    voters, poll workers, public (voters, observers, auditors)
  - “Product” includes auditability component

- Tension between usability and auditability
  - Perhaps voter needs to perform more tasks to enable auditability
Desirable Property: Accessibility
TGDC 2005

The accessibility of a voting device consists of the measurable characteristics that indicate the degree to which a system is available to, and usable by, individuals with disabilities. The most common disabilities include those associated with vision, hearing and mobility, as well as cognitive disabilities.

Desirable Property: Accessibility
HAVA 301(A) (3)(a)

An accessible voting system provides the same opportunity for access and participation (including privacy and independence) to voters with disabilities as to other voters.
Accessibility: Discussion

• Do users include poll workers and public?

• If voter uses specialized interface to vote, does he or she audit it or trust it?
  – Independent organization provides interface
  – Observational Testing: Interface also tested by voters without disabilities in a manner that the voting system cannot tell the difference
  – Voter brings own trusted device
    • Device should not see the vote

Outline

• Propose Desirable Properties of Voting Systems
  – Security (auditability, ballot secrecy)
  – Usability and Accessibility

• E2E Voting Systems

• Comparisons among voting systems

• E2E Voting Systems: electronic vs. paper ballots
Trust Model: Typical Assumptions

- Procedures are followed, count is correct
- Secure Chain-of-Custody
- Error-free Software
- Secure Hardware
- Secure Cryptographic Algorithms
- Trusted specialized user interfaces

Recall Software Independence*

A voting system is **software independent** if an (undetected) change or error in its software cannot cause an undetectable change or error in an *election outcome*.

≠ Don’t use software
  = Error-free software is not an assumption
    – Depends on the manner in which software is used to determine election outcome

* Our paper is modeled on the one on SI by Rivest and Wack
End to End Independently Verifiable

A voting system is end-to-end independently verifiable if an independent, honest observer can determine—with virtual certainty—whether a declared election outcome correctly represents the votes cast by voters.

To the extent that the observer is required to trust:

- entities, software or hardware, he or she should be able to choose said entities, software or hardware
- procedures*: these should be limited to those for vote casting, and be publicly observable

  (rationale: voter can complain if procedures not followed for her own vote)

Discussion

- Recall auditable system made evidence available to: voter (about her vote), public (about count)
- However, evidence of secure chain of custody* required to connect voter-auditability with public-auditability
  - Almost impossible with physical chain of custody
  - E2E systems use cryptographic techniques to provide evidence of chain of custody for digital information
    - Easier problem
    - Need to address ballot secrecy

* We first got this idea from Aleks Essex
Voter-Verifiable

A process is **voter-verifiable** if an honest voter can determine—with virtual certainty—whether the process was correctly carried out.

To the extent that the voter is required to trust:
- entities, software or hardware, he or she should be able to choose said entities, software or hardware
- procedures: these should be limited to those for vote casting, and be publicly observable

Universally-Verifiable

A process is **universally-verifiable** if an honest observer can determine—with virtual certainty—whether the process was correctly carried out.

To the extent that the observer is required to trust:
- entities, software or hardware, he or she should be able to choose said entities, software or hardware
- procedures: these should be limited to those for vote casting, and be publicly observable
Honest Observer’s Point of View

Independent honest observer notes that:

- **Ballot-casting is voter-verifiable**
  - Voters verify some information about votes that comes out of voting process
- **Tally-processing is universally-verifiable**
  - Voting system computes tally from this information in a universally-auditable manner
- Then is virtually convinced that the election outcome is correct

Usability and Accessibility of E2E Voting Systems

- How does one design user-friendly E2E systems?
- Do auditability and secrecy limit usability? Vice versa? Most usable E2E system?
- How do different demographic groups respond to the additional complexity of additional tasks?
- When does the complexity of casting a vote or auditing it defeat the purpose?
- How does the voter audit a specialized user-interface?
Outline

- **Propose** Desirable Properties of Voting Systems
  - Security (auditability, ballot secrecy)
  - Usability and Accessibility

- E2E Voting Systems

- Comparisons among voting systems

- E2E Voting Systems: electronic vs. paper ballots

---

An Election Model

- Election Set-Up
- Ballot Casting and Recording
  - Includes production of information for auditability
- Ballot Tallying
  - Includes production of information for auditability
- Election Audit(s)
Assumptions

- Secure Chain of Custody
  - Of ballots/equipment
- Procedures are Followed
  - Follow procedure, count/recount correctly
- Randomness*
  - Audits include element of randomness not predictable by voting system
- Usable/Human-Error-Resistant Auditability*
  - Auditability (e.g.: VVPATs) aspects easy to use

* Assumptions pointed out by John Kelsey

Comparison: Auditability

<table>
<thead>
<tr>
<th></th>
<th>Auditable</th>
<th>Voter Auditable</th>
<th>Publicly Auditable</th>
<th>Voter-Verifiable</th>
<th>Universally Verifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper + manual recount</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>DRE</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>DRE + VVPAT</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>E2E</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

10/19/2009 Desirable Properties of Voting Systems
Comparison: Auditability Assumptions

<table>
<thead>
<tr>
<th></th>
<th>Auditability Requires (Publicly Unobservable) Procedures Correctly Followed</th>
<th>Auditability Requires Secure Chain-of-Custody</th>
<th>Software Dependent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper + manual recount</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>DRE</td>
<td>Not Auditable</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>DRE + IVVR</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>E2E</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Outline

- **Propose** Desirable Properties of Voting Systems
  - Security (auditability, ballot secrecy)
  - Usability and Accessibility

- E2E Voting Systems

- Comparisons among voting systems

- E2E Voting Systems: electronic vs. paper ballots
Paper Ballots vs. Electronic Ballots

Electronic Ballots
- Can be made very accessible
- Elections easily administered and managed
- Security Issue: any electronic interface has deniability unless two-way communication is recorded

Paper Ballots
- Need trusted interface for accessibility
- Can prove that system did not do as voter communicated

Conclusions

- Discussion needed for desirable properties
- Research needed for:
  - secure electronic E2E systems
  - Interplay: usability, accessibility and auditability
Acknowledgements

• Significant Contributions From:
  – Sharon Laskowski, Andy Regenscheid, Nelson Hastings

• Discussions, readings, re-readings:
  – Barbara Guttman, Donna Dodson, John Kelsey, Rene Peralta, Stefan Popoveniuc

• Influences:
  – Benaloh, Chaum, Essex, Jones, Rivest, Wack