



Voting System Requirements

WOTE '01

Tomales Bay, California, Aug 27-30, 2001.

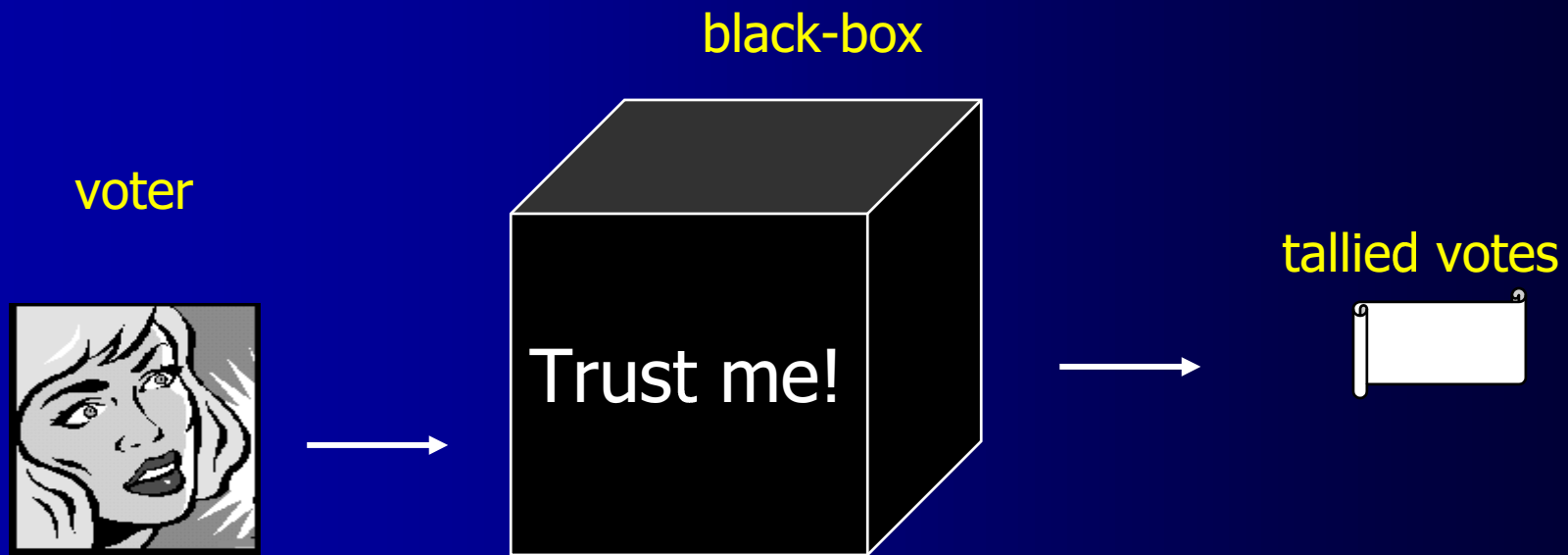
Presentation by:

Ed Gerck, Ph.D.

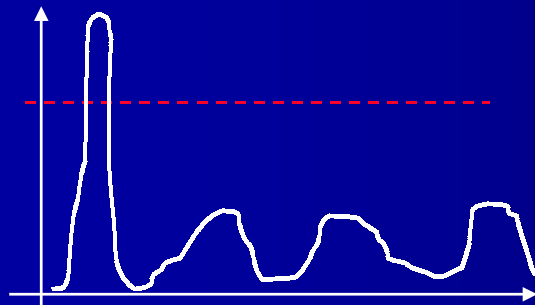
egerck@safevote.com

CEO & VP of Technology

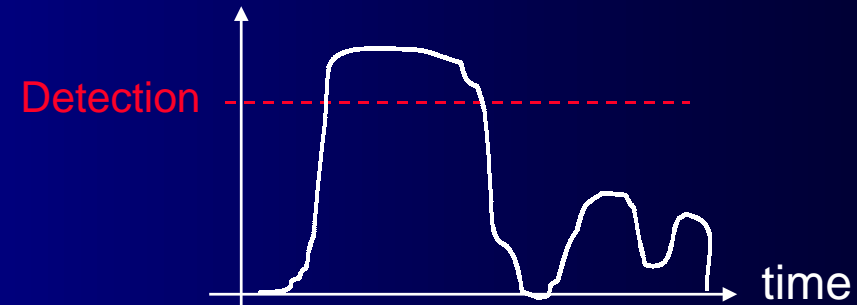
What We Don't Want in Voting Systems



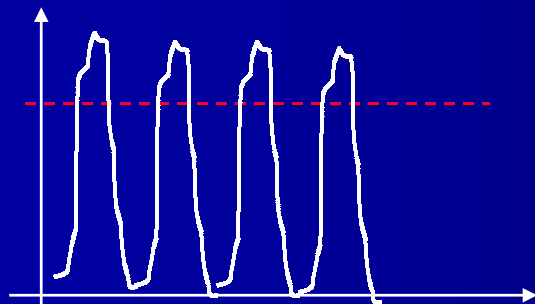
Accuracy vs Reliability



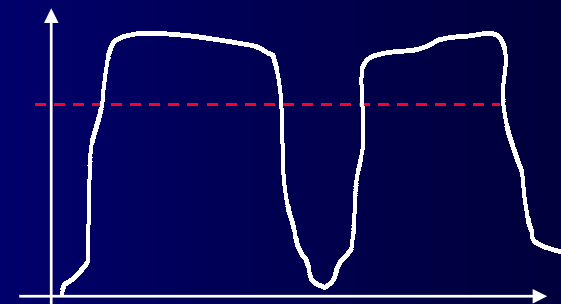
high accuracy, high reliability



low accuracy, high reliability



high accuracy, low reliability



low accuracy, low reliability

- Reliability may be close to 100%, but not equal to 100%.
- Accuracy can be 100% in digital systems.

Outcome Uncertainty

The outcome uncertainty of a voting system can be seen as accuracy and reliability problems in counting votes.

Lack of accuracy or reliability introduces two different types of errors:

- accuracy affects the spread of one event, for example whether a vote that was selected **to be** cast by a voter can be counted or not from a ballot;
- reliability affects a number of events in time and/or space, for example, count differences when repeatedly reading votes from the same stack of ballots.

Voting System Components

1. Voter Registration

Voter must be legally identified

2. Voter Authentication

Authenticate voter + ballot style + ballot rotation

3. Voting Station

Privacy + security

4. Ballot Box

Ballot integrity

5. Tallying and Auditing

Anonymity + Secrecy + Verification + Public proofs

Election Process Is A Web of Interactions



- Time synchronization: involves sequence and overlap
- Interdependencies: election phases are not independent
- Supervision: most tasks are not performed in isolation
- Cross-verification: naturally helps to stop errors & fraud
- Redundancy: naturally helps to provide fault-tolerance

HOWEVER: An election is an open-loop process!

An Election Is An Open-loop Process

- Open-loop
 - I know all voters and I know all votes
 - But ... if I see the vote, I must not see the voter
 - But ... if I see the voter, I must not see the vote

Not like accounting

Not like bank transactions

Not like e-commerce

HOW CAN INTEGRITY BE GUARANTEED?

Federal Election Commission (FEC) Voting System Standards

WHAT ARE THEY?

- Minimum Functional Requirements, and
- Performance Characteristics, and
- Documentation Requirements, and
- Test Evaluation Criteria

FEC

Voting System Standards

WHAT ARE THEY NOT?

- Not High-Level System Requirements
- Not Clear Definitions
- Not Technologically Neutral
- Not Consistent

THERE IS A NEED FOR A COMPLETE TECHNICAL VISION!

16 Strict Voting System Requirements

GOALS: Consistency, Clear Definitions, Technologically Neutral, Strict

1. *Fail-safe voter privacy*
2. *Collusion-free vote secrecy*
3. *Verifiable election integrity*
4. *Fail-safe privacy in verifiability*
5. *Physical recounting and auditing*
6. *100% accuracy*
7. *Represent blank votes*
8. *Prevent overvotes*
9. *Provide for null ballots*
10. *Allow undervotes*
11. *Authenticated ballot styles*
12. *Manifold of links* – avoid single points of failure even if improbable
13. *Off-line secure control structure*
14. *Technology independent*
15. *Authenticated user-defined presentation*
16. *Open review, open code*

16 Strict Voting System Requirements

WHAT ARE THEY NOT?

- Not The Only Answer
- Not A Solution
- Not Proprietary
- Not Closed
- Not Analytic
- Not dominated by today's limitations

1. *Fail-safe voter privacy*

- Voter privacy is the inability to link a voter to a vote.
 - Lack of voter privacy means: vote buying, voter coercion, and lack of election integrity!
 - Must NOT depend on policy or computation (crypto).
 - Must NOT depend on election officials.
 - Voter privacy is NOT anonymity.
 - US: Law is powerless to break voter privacy.
(However, in the UK legal procedures can break voter privacy)

2. Collusion-free vote secrecy

- Vote secrecy is the inability to know what the vote is.
 - Lack of vote secrecy means: vote buying, voter coercion, and lack of election integrity!
 - Must NOT depend on policy or computation (crypto).
 - Must NOT depend on any election official.
 - Must NOT depend on threshold of collusion (i.e., vote secrecy must not depend on a group of election officials not colluding, however large the group may be).

3. Verifiable Election Integrity

- Election integrity is the inability of any number of parties to influence the outcome except by properly voting.
 - Election integrity must be verifiable, not just trusted.
 - Must provide for election verifiability of all votes cast (open-loop problem)
 - Must provide verifiability of “one voter, one vote.”

4. Fail-safe Privacy in Verification

- If all ballots are verified, voter privacy is guaranteed.
 - Receipt-freeness applies to the entire system.
 - Voter privacy trumps verifiability, auditing.
 - Election privacy only exists for precincts.
 - Precincts may have from a few to ~600 voters.

5. Physical Recounting and Auditing

- Recounting and Auditing must not be like playing the same CD twice.
 - Must provide for reliability in auditing and vote recounting, with an error rate as low as desired or, less strictly, with an error rate comparable to or better than conventional voting systems.
 - The auditing and vote proofs must be capable of being physically stored, recalled and compared off-line and in real-time during the election, without compromising election integrity or voter privacy, and allowing effective human verification as defined by election rules.

6. 100% Accuracy

- Every vote or absence of vote (no vote) MUST be correctly counted, with zero error.
 - 100% accuracy is possible in digital systems with voter feedback.
 - Depends on voter. There is no way for usefully reading the “voter’s intent” except by that which is readable from the ballot.
 - 100% accuracy is not possible when digitization error is involved, such as in reading punch cards or optical scan ballots.

7. Represent Blank Votes

- A blank vote is a valid “no vote.”
 - A “no vote” is part of the “election language.”
 - A blank vote is NOT a residual vote, NOT a lost vote.
 - Voters could have a “none of the above” choice.
 - Must allow voters to change choices from ‘vote’ to ‘blank vote’ and vice-versa, at will, for any race and number of times, before casting the ballot.

8. Prevent Overvotes

- The system must be decidable.
 - As defined by election rules.
 - Must provide automatic “radio button” action for single-vote races.
 - If overvoting is detected in multiple-vote races, must warn the voter that a vote has to be cleared if changing choices is desired.
 - The warning must be made known only to the voter, without public disclosure.
 - Allowing overvoted races can be enable fraud by latter marking, which can disqualify an otherwise correctly voted race or ballot.

9. Provide for Null Ballots

- A “null ballot” is a valid voter choice.
 - A “null ballot” is part of the “election language.”
 - Lack of a “null ballot” option may lead to protest votes.
 - Voters could have “null race” and “null ballot” choices.
 - As defined by election rules, one may allow voters to null races or even the entire ballot as an option (e.g., to counter coercion; to protest against lack of voting options).
 - Overvoting, otherwise prevented by Requirement #8, may be used as a mechanism to provide for null ballots. However, this can enable fraud as noted.

10. Allow Undervotes

- An undervote is a valid “no vote” – but it may be a mistake, not an intent.
 - As defined by election rules, the voter may receive a warning of undervoting.
 - However, such a warning must not be public and must not prevent undervoting.
 - An undervote is NOT a lost vote, NOT a residual vote.

11. *Authenticated Ballot Styles*

- Ballot styles and ballot rotation need to be authenticated.
 - The ballot style (allowed races based on a voter's address) and ballot rotation (expected candidate shuffling in a race) to be used by each voter must be authenticated, otherwise the voter may be using a wrong ballot or seeing the candidates in a biased order.
 - Election integrity may be compromised if ballot styles and ballot rotation are incorrect, even if all other parts of the election system are not compromised.
 - Must be provided without any other control structure but that given by the voter authentication process itself, to avoid control splits that could be exploited at system interfaces.

12. *Manifold of Links*

- Avoid single points of failure.
 - Must use redundant links *and* keys to securely define, authenticate and control ballots.
 - Must avoid single points of failure – even if improbable.
 - A paper ballot is a single point of failure for that vote.
 - If networks are used, must forestall Denial-of-Service (DoS) and other attacks with an error rate comparable or better than conventional voting systems.

13. Off-line Secure Control Structure

- Ballots must have an off-line secure end-to-end control structure.
 - Voting systems must not be required to be always online in order to work or to be secure.
 - Voting systems may use digital certificates under a single authority.
 - Must avoid control splits that could be exploited at system interfaces.
 - Ballot control must control the least set of objects, to reduce complexity and thus improve fault- and attack-tolerance.
 - Ballot control must be data-independent, representation-independent and language-independent.

14. Technology Independent

- Technology may change, elections should not.
 - Voting system requirements should not define “how.”
 - Must allow ballots and their control to be used off-line and/or in dial-up and/or in networks such as the Internet, with standard PCs or hand-held devices used to implement their components in hardware or in software, alone or in combination for each part.

15. Authenticated User-defined Presentation

- Voters must be able to customize usability.
 - Usability must not introduce risks of compromise or induce changes to security-critical parts of the system.
 - Must enable the ballots to dynamically support multiple languages, font sizes and layouts.
 - Voters should be able to choose the language and display format that they are be most comfortable with when voting, as allowed by law.
 - As required by voters with disabilities.
 - To prevent design problems, voters must be presented with an authenticated list of choices defined by election rules.

16. Open Review, Open Code

- Allow all source code to be publicly known and verified.
 - The availability and security of the system must not rely on:
 - keeping its code or rules secret (which cannot be guaranteed), or
 - limiting access to only a few people (who may collude or commit a confidence breach voluntarily or involuntarily), or
 - preventing an attacker from observing any number of ballots and protocol messages (which cannot be guaranteed).
 - The system should have zero-knowledge properties (i.e., observation of system messages do not reveal any information about the system).
 - Object code must be verifiable against compiled source code.
 - Operating systems must be verifiable.
 - Only keys must be considered secret.

16 Strict Voting System Requirements

Since voting system requirements are a complex logical system, it is a mathematical fact that they cannot be both consistent and complete. The 16 Voting System requirements were chosen so that they are consistent.

1. *Fail-safe voter privacy*
2. *Collusion-free vote secrecy*
3. *Verifiable election integrity*
4. *Fail-safe privacy in verifiability*
5. *Physical recounting and auditing*
6. *100% accuracy*
7. *Represent blank votes*
8. *Prevent overvotes*
9. *Provide for null ballots*
10. *Allow undervotes*
11. *Authenticated ballot styles*
12. *Manifold of links – avoid single points of failure even if improbable*
13. *Off-line secure control structure*
14. *Technology independent*
15. *Authenticated user-defined presentation*
16. *Open review, open code*

Summary of References

Voting System Requirements:

<http://www.safevote.com/ifc01.pdf>

<http://www.thebell.net/papers/vote-req.pdf>

Specifications, demos, test results:

<http://www.safevote.com>

<http://www.MySafevote.com>



Voting System Requirements

WOTE '01

Tomales Bay, California, Aug 27-30, 2001.

Presentation by:

Ed Gerck, Ph.D.

egerck@safevote.com

CEO & VP of Technology