The Battle for Accountable Voting Systems

Prof. David L. Dill
Department of Computer Science
Stanford University
http://www.verifiedvoting.org

Outline

- **Principles & concepts**
- Trust and DREs
- Voter verifiable audit trail
- Future
- Conclusion

Role of Elections

Democracy depends on everyone, especially the losers, accepting the results of elections.

"The people have spoken . . . the bastards!"
- Dick Tuck concession speech

Transparency

It is not enough for elections to be accurate.
We have to *know* that they are accurate.

All critical aspects of the process must be
- publicly observable, or
- independently checkable

(Preferably both)

Transparency With Paper Ballots

Paper ballots are compatible with transparent processes.
- Voter makes a permanent record of vote.
- Locked ballot box is in public view.
- Transportation and counting of ballots are observed by political parties and election officials.

Everyone understands paper.

Any new system should be at least this trustworthy.

Levels of Accountability

We often have to trust people, but we rarely trust them without *accountability*.

Levels of accountability
- Can we detect error?
- Can we correct it?

Simple error detection is the most condition for trustworthiness.

Trust

"You have to trust somebody."

We only need to trust groups of people with diverse interests (e.g., observers from different political parties).

Outline

- Principles & concepts
- **Trust and DREs**
- Voter verifiable audit trail
- Future
- Conclusion

DRE Definition

DRE = "Direct Recording Electronic"

For this talk, "DRE" does **not** include machines with **voter verifiable paper records.**

The Man Behind the Curtain

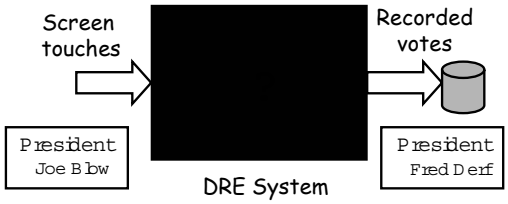
Suppose voting booth has a man behind a curtain

- Voter is anonymous
- Voter dictates votes to scribe.
- Voter never sees ballot.

There is no accountability in this system!

(analogy due to Dan Wallach and Drew Dean)

The DRE Auditing Gap



Any accidental or deliberate flaw in recording mechanism can compromise the election.
. . . **Undetectably!**

Integrity of DRE Implementations

Paperless electronic voting requires DRE software and hardware to be *perfect*.

It must never lose or change votes.

Current computer technology isn't up to the task.

Program bugs

We don't know how to eliminate program bugs.

- Inspection and testing catch the *easy* problems.
- Only the really nasty ones remain
  - obscure
  - happen unpredictably.

Security Risk

- What assets are being protected?
  - At the national level, trillions of dollars.
- Who are potential attackers?
  - Hackers, Candidates, Zealots,
  - Foreign governments, Criminal organizations

Attackers may be very sophisticated and/or well-financed.

A Generic Attack

- Programmer, system administrator, or janitor adds hidden vote-changing code.
- Code can be concealed from inspection in hundreds of ways.
- Code can be triggered only during real election
  - Using "cues" - date, voter behavior
  - Explicitly by voter, poll worker, or wireless network.
- Change small % of votes in plausible ways.

Generic attack

DREs are creating new kinds of risks.

Nationwide fraud becomes easier than local fraud.

Local election officials can't stop it!

Threats From Insiders

- FBI: "The disgruntled insider is a principal source of computer crimes."
  - The 1999 Computer Security Institute/FBI report notes that 55% of respondents reported malicious activity by insiders.
- Crimes are easier for insiders (e.g., embezzling).

Voting is Especially Hard

Unlike almost every other secure system, voting must *discard vital information:* the connection between the voter and the vote.

Comparison with banking

Electronic audit records have names of everyone involved in every transaction.

Banks usually have paper backup!

. . . And computer crime still occurs -- especially by insiders.

but

- Fraud can be quantified (we can tell when it happens).
- Customers are protected.

"We've never had a proven case of vote fraud on DREs"

- Votes have definitely been lost due to bugs (Wake County, NC, 2002).
- Fraud has never been investigated.
- Candidates don't bother asking for recounts
  They just get "reprints"
- Danger and motivation increases with number of DREs (twice as many votes this election than 2002).
- Applications with much more security and lower stakes have had sophisticated fraud (e.g., gambling).

What software are we running?

We cannot verify that desired software is running on a computer.

- Stringent software design/review (even formal verification) doesn't solve the problem.
- Open source does not solve the problem.
  - "Disclosed" source is, however, highly desirable!

Summary of Technical Barriers

It is currently (practically) impossible to create trustworthy DREs because:

- We cannot eliminate program bugs.
- We cannot guarantee program security.
- We cannot verify that the desired software is running on the computer.

Outline

- Principles & concepts
- Trust and DREs
- **Voter verifiable audit trail**
- Future
- Conclusion

The Man Behind the Curtain

Now, suppose the man who filled out the ballot

- Shows you the ballot so you can make sure it is correct.
- Lets you put it in the ballot box (or lets you watch him do it).

There is accountability

- You can make him redo the ballot if it's wrong.
- He can be fired or arrested if he does it wrong.

Voter Verifiable Audit Trail

- Voter must be able to verify the permanent record of his or her vote (i.e., ballot).
- Ballot is deposited in a secure ballot box.
  - Voter can't keep it because of possible vote selling.
- Voter verified records must be audited, and must take precedence over other counts.

This closes the auditing gap.

VVAT is not enough

Closing the audit gap is *necessary* but not *sufficient*.

Additional conditions:

- Physical security of ballots through final count must be maintained.
- Process must be transparent (observers with diverse interests must be permitted at all points).

There are many other requirements, e.g., accessibility.

Manual Recounts

Computer counts cannot be trusted.

Like other audits, *independent* recounts should be performed *at least*

- When there are doubts about the election
- When candidates challenge
- On a random basis

Computer-generated ballots can have additional security features.

- Digital signatures/time stamps
- Matching identifiers for reconciling with paper ballots.

Options for Voter Verifiable Audit Trails

- Manual ballots with manual counts.
- Optically scanned paper ballots.
  - *Precinct-based* optical scan ballots have low voter error rates.
- Touch screen machines with voter verifiable printers.
- Other possibilities
  - Other media than paper?
  - Cryptographic schemes?

For now, paper is the only option that is *available* and *well-understood*.

Outline

- Principles & concepts
- Trust and DREs
- Voter verifiable audit trail
- **Future**
- Conclusion

November, 2004

We've done what we can to get paper. In the short term, we're focusing on other initiatives.

- TechWatch
  - Computer-literate volunteers to observe election.
  - They will observe & document pre-election testing.
  - They will observe election (often as poll workers) & vote counting
- Election Scorecard
  - Questions about basic "best practices" related to election security
  - Working with Brennan Center, Leadership Conference on Civil Rights, Center for American Progres

Election Incident Reporting System

- Online capture of election incident reports.
- The Verified Voting Foundation is partnered with CPSR for SW development.
- Reports will be entered by Election Protection Coalition (60+ members)
- Hotline 1-866-OUR-VOTE
- Goals
  - Deal with incidents in real-time, when possible
  - Collect knowledge on how elections *really* work.

Medium-term

- Get a nationwide requirement for voter-verified paper ballots.
- Document existing practices based on Tech Watch results.
- Recommend best practices for election integrity.

Long Term

A continuing campaign for election transparency and trustworthiness

- Technology
- Procedures
- Election law
- Monitoring

Outline

- Principles & concepts
- Trust and DREs
- Voter verifiable audit trail
- Future
- **Conclusion**

Key points

- Election equipment should be proved reliable and secure before it is deployed.
- There is little evidence that DREs are safe, and a lot of evidence to the contrary.
- The problems cannot be fixed without a voter verifiable audit trail of some kind.
- With a voter verifiable audit trail and due attention to election practices, the problem can be solved.

The Big Risk

All elections conducted on DREs are open to question.

www.verifiedvoting.org

More information is available at our website.

Voting vs. Safety-Critical Systems

"If we can trust computers to fly airplanes, why can't we trust them to handle our votes?"

- Accountability: Failures in safety-critical systems are detectable
- Standards and practices of safety-critical software are not used in voting machine development.
  - "If we required that, we could only afford one voting machine for the state of Texas!"
- Safety-critical systems are not designed to be secure against attacks by insiders.