Openness & Security

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

My Background

- Professor of Computer Science at Stanford University
- Founder of verifiedvoting.org
- Researcher in "formal verification" for 20 years.
- Voting
  - California Ad Hoc Task Force on Touch Screen Voting Feb - May 2003
  - Citizens DRE Oversight Board, Santa Clara County
  - IEEE P1583 Voting Standards Committee.

Outline

- **Principles**
- Trust and DREs
- Voter verifiable audit trail
- 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

Burden of Proof

We should be able to *prove* that elections are accurate.

- Procedures and equipment must be reliable and secure.
- Election results are routinely and *meaningfully* audited.

Audit: independently reconstruct election results from the original records.

With conventional paper-based systems, manual recounts.

Integrity With Paper Ballots

Integrity measures (with good procedures).

- 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 physical security of paper ballots.

Any new system should be at least this trustworthy.

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
- **DREs**
- Voter verifiable audit trail
- Conclusion

Clarification: DRE

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!

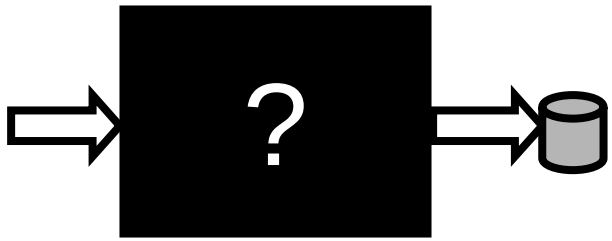
(analogy due to Dan Wallach and Drew Dean)

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.

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 desireable!

Technical Barriers

It is currently 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
- Trust and DREs
- **Voter verifiable audit trail**
- 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 (*unproven!*).
  - Other media than paper?
  - Cryptographic schemes?

For now, paper is the only option

Outline

- Principles
- Trust and DREs
- Voter verifiable audit trail
- **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.