Making Every E-Vote Count

Friends of the Lehigh Libraries
October 2008

Daniel P. Lopresti
Department of Computer Science & Engineering
dal9@lehigh.edu
http://www.cse.lehigh.edu/~lopresti
E-voting in the news

Electronic Voting Systems: the Good, the Bad, and the Stupid

Pennsylvania voters: trust but verify
Poll finds most want ballot verification

Electronic Voting System Usability Issues

Hack-a-Vote: Security Issues with Electronic Voting Systems

Privacy Issues in an Electronic Voting Machine

SECURITY ALERT: May 11, 2006
Critical Security Issues with Diebold TSx

Trusted Agent Report
Diebold AccuVote-TS Voting System
Why are we interested?

Motivation:

• Fair and accurate elections are vital for a healthy democracy.
• Any voting system carries with it some risk. Past experience with paper ballots, lever machines, etc., has let us understand that risk.
• Electronic voting systems introduce whole new classes of risks.

Some questions we attempt to answer in our work:

• What are the risks associated with e-voting technologies?
• How can these risks best be mitigated?
• Can the current certification process identify bad e-voting systems?
• If not, what would be an effective certification procedure?
Main take-away points

- E-voting systems are nothing more than general-purpose computers running specialized voting software.
- Same concerns arise as in any complex software/hardware system.
- Current certification process provides little or no assurance: it is incapable of identifying many critical vulnerabilities.
- Other states have banned e-voting systems still in use in PA.
- We can – and should – do better.

Despite these concerns (or perhaps because of them) everyone should still actively participate in the democratic process. Vote!
How did we get here?

The infamous butterfly ballot from the 2000 Presidential election:

The Florida ballot is a classic example of bad user interface design. Computer software can suffer from such problems just as easily.

Votomatic technology used in Florida was prone to paper jams. This led to hanging and dimpled chads, making it hard to determine voter intent.

http://www.cs.uiowa.edu/~jones/cards/chad.html
http://www.pushback.com/justice/votefraud/DimpledChadPictures.html
The Help America Vote Act (HAVA) provides funds for states to replace punched card and lever voting systems. It does not mandate the use of direct recording electronic (DRE) systems.

Some general goals to keep in mind as we weigh alternatives:

• secure and transparent elections,
• accurate determination of voter intent,
• voter anonymity,
• accessibility for disabled voters and non-native English voters,
• if possible, prevent overvoting (invalidates voter's ballot),
• if possible, prevent unintentional undervoting (voter confusion?).

http://www.fec.gov/hava/law_ext.txt
E-voting Risks

While there are a number of DRE vendors, one truth holds: all computer hardware/software systems of this complexity have bugs.

Bugs can manifest themselves in different ways:

• cause system to be unreliable (crash, lose votes),
• create openings that allow an outsider to compromise election,
• create openings that allow an inside to compromise election.

Such attacks can be impossible to detect after-the-fact.
Diebold security

Diebold Election Systems provides secure, accurate and proven voting solutions to jurisdictions worldwide.

What we mostly worry about
May or may not be safe
What we mostly worry about

(But insider attacks can arise anywhere.)

Risk analysis of e-voting software

• Avi Rubin and colleagues at Johns Hopkins obtained copy of Diebold e-voting software which appeared on the Internet.*
• Studied it carefully – made results public in 2003.
• Findings include:
  • “... far below even the most minimal security standards ...”
  • “... unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, ...”
  • “... voters ... can cast unlimited votes without being detected ...”

* E-voting vendors often assert they must be allowed to keep their software secret to protect it. This proves the futility of that idea.

Risk analysis of e-voting software

Summary of potential vulnerabilities identified by Rubin, et al.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Voter (with forged smartcard)</th>
<th>Poll Worker (with access to storage media)</th>
<th>Poll Worker (with access to network traffic)</th>
<th>Internet Provider (with access to network traffic)</th>
<th>OS Developer</th>
<th>Voting Device Developer</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vote multiple times using forged smartcard</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td>3.2</td>
</tr>
<tr>
<td>Access administrative functions or close polling station</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td>3.3</td>
</tr>
<tr>
<td>Modify system configuration</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>4.1</td>
</tr>
<tr>
<td>Modify ballot definition (e.g., party affiliation)</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4.2</td>
</tr>
<tr>
<td>Cause votes to be miscounted by tampering with configuration</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4.2</td>
</tr>
<tr>
<td>Impersonate legitimate voting machine to tallying authority</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>4.3</td>
</tr>
<tr>
<td>Create, delete, and modify votes</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>4.3, 4.5</td>
</tr>
<tr>
<td>Link voters with their votes</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>4.5</td>
</tr>
<tr>
<td>Tamper with audit logs</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>4.6</td>
</tr>
<tr>
<td>Delay the start of an election</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>4.7</td>
</tr>
<tr>
<td>Insert backdoors into code</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>5.3</td>
</tr>
</tbody>
</table>

One potential exploit

Attempt is made to protect integrity of voting records by encrypting them before storage on PCMCIA memory card ...

... unfortunately, the key is hardwired in the code and now widely known across Internet (it's “F2654hD4”).

"There is a serious flaw in the key management of the crypto code that otherwise should protect the AV-TSx from memory card attacks. Unless election officials avail themselves of the option to create new cryptographic keys, the AV-TSx uses a default key. This key is hard coded into the source code for the AV-TSx, which is poor security practice because, among other things, it means the same key is used in every such machine in the U.S. Worse, the particular default key in question was openly published two and a half years ago in a famous research paper, and is now known by anyone who follows election security, and can be found through Google."

Later risk analyses

- In May 2006, Finnish security expert Harri Hursti exposed a serious flaw in the Diebold AccuVote TSx touchscreen system.
- This flaw allows the system to be permanently reprogrammed in a matter of a few minutes. No special hardware is required.
- Later, a team of Princeton researchers announced they had implemented Hursti's attack and proved that it works. They used an older Diebold system given by an anonymous donor.
- The Princeton team also implemented a virus form of the attack that spreads from one infected machine to others via memory card.
- Case opened using several methods, including picking the lock.

Our problems are far from over

New York Times, October 8, 2008

“Election officials, who will have plenty on their minds on Nov. 4, have one more thing to worry about: Diebold electronic voting machines that drop votes.

... In the case of Diebold, votes are being dropped when they are transferred from individual machines to the central server in a county’s election headquarters. When an election worker inserts the memory card from a machine into the server, a green arrow is supposed to light up after all of the votes have been uploaded and added to the county’s totals. In some cases, the green arrow is wrong, and none of the votes have been added.”
And a couple days ago ...

Wired Blog, October 20, 2008

“Voters using touch-screen voting machines for early voting in two West Virginia counties have complained that when they tried to vote for Democratic candidates, the machine registered their vote for other Republican candidates instead.

... Jackson County Clerk Jeff Waybright blamed voters for not touching the screen properly and said that 400 other voters had cast ballots on the machine with no problem. But he agreed to recalibrate the machine's screen after the Secretary of State's office contacted him.”
Misrepresentation #1

“E-voting machines are not computers.”
Diebold AccuVote System

Demo in Allentown:

Diebold AccuVote-TSx block diagram:

DRE systems are nothing more than specialized computers.

http://www.wfmz.com/cgi-bin/tt.cgi?action=viewstory&storyid=13711
http://www.bbvforums.org/forums/messages/1954/AccuVote-TSx_2_02_System_Overview-23267.pdf
More photos from Diebold demo

- PCMCIA slot
- PCMCIA card
- Built-in printer
- Paper tape (used for end-of-day tally)
E-voting Machines We Own

Danaher / Shouptronic 1242
(Bucks County)

Sequoia Advantage
(Northampton County)
E-voting Machines We Own

Circuit built by Lehigh undergrad to read EPROM (Danaher firmware)

Replacement EPROM cost is less than $3.00

EPROM programmer is $79.00
“E-voting machines have been tested by federal and state authorities, so they must be safe.”
CA and OH Toss Out DRE's

All of these machines were previously certified at the federal and state level. Some are still in use in PA counties.
“Computer security researchers are alarmists. They ignore the physical security designed to protect these systems.”
Physical security is questionable

Photos taken by Princeton Professor Ed Felten at four different polling places on the days preceding the June 3, 2008 presidential primary in NJ.

http://citp.princeton.edu/voting/advantage/
“E-voting machines have never malfunctioned or lost votes in a real election.”
Nearly 200 votes are lost through a combination of vendor and pollworker mistakes in May 2005 primary in Berks County.

Blame the pollworkers???
In reality, it was a combination of two errors: the main error was made by Danaher (the vendor). Pollworkers' mistake was secondary.

http://www.pollworker.us/articles%202005/kuznik_11-2-05_danaher.html
Case of the Sequoia Advantage

http://www.pollworker.us/articles%202005/kuznik_11-2-05_danaher.html

http://www.crn.com/government/206905445
Case of the Sequoia Advantage

Extensive analysis performed by team of researchers from Princeton.

“What Sequoia leaves out is that this programming error disenfranchised voters, by denying them the ability to vote in their own party’s primary.”

Gang Tan, a professor who recently joined our department, participated in the study last summer.

http://citp.princeton.edu/voting/advantage/
Who supports the use of DRE's?

Michael Shamos, Ph.D., J.D., is a Professor at Carnegie Mellon. He has extensive experience with electronic voting and is the primary independent expert responsible for certifying voting machines in Pennsylvania and other states.

In a 2007 article for the National Academy of Engineering, he writes:

“Voting machines are among the least reliable devices on this planet.”

Voting system use in the U.S.

E-Voting in Pennsylvania

AVS, once used in Northampton County, was decertified

ES&S iVotronic
ES&S Model 100/iVotronic
ES&S Model 100/AutoMark

Advanced WINvote
ES&S Model 650/AutoMark
Premier (Diebold) TSX

Danaher 1242
Sequoia Edge
Hart InterCivic eSlate2
Sequoia Advantage

Hart InterCivic eScan / Hart InterCivic eSlate

http://www.dos.state.pa.us/voting/cwp/view.asp?a=1218&Q=446365
A key recommendation from many security experts is the use of Voter-Verified Paper Records (VVPR).

As of today, this is only way to guarantee an independent recount.

Pennsylvania
Attempts to fix this in the courts


There are two points of contention in particular.

Pennsylvania Election Code, 25 P.S. § 3031 states:
“Electronic voting system” means a system in which one or more voting devices are used to permit the registering or recording of votes and in which such votes are computed and tabulated by automatic tabulating equipment. The system shall provide for a permanent physical record of each vote cast.”
What constitutes a “physical record”?  

As an expert witness in this case, I argue that:

“... none of the DREs certified in Pennsylvania is capable of retaining a “permanent physical record of each vote cast” as required by the Pennsylvania Election Code.  
... these systems maintain what is best described as an “electronic record” of the activity that occurs on the machine.  
The accuracy or permanence of data stored electronically cannot be guaranteed due to the inherent characteristics of electronic computer memory.”

Note: Michael Shamos is the lead technical expert for the state. Banfield v. Cortes is currently on hold in the PA Supreme Court.
25 P. S. § 3031.17. Statistical sample
The county board of elections, as part of the computation and canvass of returns, shall conduct a statistical recount of a random sample of ballots after each election using manual, mechanical or electronic devices of a type different than those used for the specific election. The sample shall include at least two (2) per centum of the votes cast or two thousand (2,000) votes whichever is the lesser.

Does simply printing out the contents of computer memory onto paper constitute a recount “of a type different” than the original tally produced by the same machine electronically?
PERFECT Project

NSF-funded research project centered here at Lehigh:

- Lehigh: Ziad Munson (Sociology) and Dan Lopresti (Computer Science & Engineering).
- Muhlenberg: Chris Borick (Political Science)
- RPI: George Nagy (Electrical, Computer & Systems Engineering)
- Boise State: Elisa Barney Smith (Electrical & Computer Engineering)

PERFECT stands for “Paper and Electronic Records for Elections: Cultivating Trust”
Research questions

Issues that arise from using paper ballots in elections:

- Accurate interpretation of marginal markings.
- Human cost, error rate, and bias in performing manual recounts.
- Failure modes in ballot imaging (e.g., paper jams).
- Systematic errors due to ballot layout (one candidate may be disadvantaged over another based on physical location on page).

Also keep in mind:

- U.S. Elections can be complex (10's to 100's of choices).
- Impact of “voter error” (e.g., improper markings, erasures).
- Potential for traditional ballot-box stuffing.
- Computer hackers attempting to manipulate the vote.
Counting votes is not so easy

Is this a legal vote?

- Courts would probably say so ...
- ... but op-scan readers might not count it.

Increasing demands that machine's interpretation match a human's.
Counting votes is not so easy

Real ballot from an election in CA:

One of these votes was counted correctly by the op-scan equipment, the other wasn't.

Note: this does not mean voting on paper ballots is bad, just (1) manual audits should be mandatory, and (2) more research is needed.

Another lawsuit filed just this week

Directive issued by the Secretary of State on September 3, 2008:

“... if all electronic voting machines in a precinct are inoperable, “paper ballots, either printed or written and of any suitable form,” for registering votes (described herein as “emergency back-up paper ballots”) shall be distributed immediately to eligible voters ...”

Emergency paper ballot measure

“... if all electronic voting machines in a precinct are inoperable ...”

What happens if all but one of the machines are inoperable?

Long lines, impatient (and angry) voters, some of whom can't afford to wait and thus are disenfranchised.

Emergency paper ballot measure

Our lawsuit seeks to lower Secretary of State's “100% rule” to a more reasonable failure rate before paper ballots are used, say 50%.

DRE failure rates of up to 20% have been observed. Our statistical analysis shows that this implies a precinct with 2 machines has a 32% chance of operating at 50% of capacity.

Interesting historical connection


Street was a member of the Lehigh Class of '06 (1906, that is).

Thanks to Ilhan Citak for finding and scanning this.
George L. Street Jr.'s 1906 thesis
Common retorts

- "These attack scenarios are unlikely."
- "Our e-voting systems are certified, so they must be safe."
- "Poll workers are trained to recognize potential problems."
- "Multiple copies of the data are stored in the system, so we're okay."
- "Re-printing the end-of-day tally is just as good as a recount."
- "There's no evidence of anyone having success in an attack like this."

My assessment:  ▶️ = optimistic  🟥 = wrong  🟠 = plain silly

There is no doubt we need good policies and procedures in addition to good, safe technology. (I believe almost everyone involved would like to do the right thing.)
My recommendations

For secure and transparent elections, we should insist on:

- Giving independent experts unfettered access to e-voting software and hardware for verification purposes.
- Use of Voter Verified Paper Records (VVPR).
- Mandatory audits (hand-count a random sampling of all ballots).

And tell our lawmakers to pass pending legislation:

- H.R. 550 (The Voter Confidence and Increased Accessibility Act).
- Pennsylvania H.B. 53.
(4.1) The voting system, pursuant to section 1122.1-A, shall produce or require the use of an individual voter-verified paper record of the voter's vote that shall be made available for inspection and verification.

(b) A voter-verified paper record may include any of the following:

1. A paper ballot prepared by the voter for the purpose of being read by an optical scanner.
2. A paper ballot prepared by the voter to be mailed to an election official, whether from a domestic or overseas location.
3. A paper ballot created through the use of a ballot marking device.
4. A paper printout of the voter's vote produced by a touch screen or other electronic voting machine if, in each case, the record permits the voter to verify the record in accordance with this section.
Last Word
Making Every E-Vote Count

Lopresti • October 2008 • Slide 51

http://perfect.cse.lehigh.edu/

Paper and Electronic Records for Elections: Cultivating Trust

Thank you!

This work was supported in part by the National Science Foundation under award numbers NSF-0716368, NSF-0716393, NSF-0716647, and NSF-0716543. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the National Science Foundation.