Electronic Voting: Problems & Solutions

Daniel P. Lopresti
http://www.cse.lehigh.edu/~lopresti

Department of Computer Science & Engineering
Lehigh University, Bethlehem, PA
E-Voting in the news

Security Analysis of the Diebold AccuVote-TS Voting Machine

SECURITY ALERT: July 4, 2005
Critical Security Issues with Diebold Optical Scan Design

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

THE MACHINERY OF DEMOCRACY:
PROTECTING ELECTIONS IN AN ELECTRONIC WORLD

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
Main take-away points

- E-voting systems are 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.
- Independent computer security experts left largely on the sidelines.
- Situation in Pennsylvania is troubling because we do not require Voter Verified Paper Records (VVPR), unlike many states.
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 my colleagues and I seek to answer:

- 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?
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.

Hanging chads & voter intent

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/DimplesChadPictures.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?).
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 risks

While there are several 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.)
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.

### 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”).

A more recent risk analysis

- Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAAB).
- Examined parts of both Diebold touchscreen system (AV-TX) and optical scan system (AV-OS) – published February 14, 2006.
- Findings include:
  - “Memory card attacks are a real threat ...”
  - “... anyone who has access to a memory card of the AV-OS ... and can have the modified card used ... can indeed modify the election results ...”
  - “The fact that the the [sic] results are incorrect cannot be detected except by a recount of the original paper ballots.”

“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.”

Even more recent risk analyses

- Last May, Finnish security expert Harri Hursti announced he found a serious flaw in the Diebold AccuVote TSx touchscreen system.
- This flaw allows system to be permanently reprogrammed in a matter of a few minutes. No special hardware is required.
- Last fall, 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.

Short video clip

From the official video record of the Pennsylvania certification examination for Diebold AccuVote and OptiScan systems conducted by the Office of the Secretary of the Commonwealth in Harrisburg on November 22, 2005.
Voter-Verified Paper Records

- A key recommendation from many security experts is the establishment of Voter-Verified Paper Records (VVPR).
- As of today, this is only way to guarantee an independent recount.
E-Voting in Pennsylvania

http://www.dos.state.pa.us/voting/cwp/view.asp?a=1218&Q=446365
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:  
- Green = optimistic
- Red = wrong
- Purple = 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.
Pennsylvania H.B. 53

6 (4.1) The voting system, pursuant to section 1112.1-A, shall
7 produce or require the use of an individual voter-verified paper
8 record of the voter's vote that shall be made available for
9 inspection and verification.

10 is cast.

17 (b) A voter-verified paper record may include any of the
18 following:
19 (1) A paper ballot prepared by the voter for the purpose of
20 being read by an optical scanner.
21 (2) A paper ballot prepared by the voter to be mailed to an
22 election official, whether from a domestic or overseas location.
23 (3) A paper ballot created through the use of a ballot
24 marking device.
25 (4) A paper printout of the voter's vote produced by a touch
26 screen or other electronic voting machine if, in each case, the
27 record permits the voter to verify the record in accordance with
28 this section.