Analysis of an Electronic Voting System

Nikolaos Michalakakis

Confusion over Palm Beach County ballot

<table>
<thead>
<tr>
<th>Party</th>
<th>Candidate(s)</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Republican</td>
<td>George W. Bush, Dick Cheney</td>
<td>President</td>
</tr>
<tr>
<td>Democratic</td>
<td>Al Gore, Joe Lieberman</td>
<td>President</td>
</tr>
<tr>
<td>Libertarian</td>
<td>Harry Browne, Art Olivier</td>
<td>President</td>
</tr>
<tr>
<td>Green</td>
<td>Ralph Nader, Winona LaDupe</td>
<td>President</td>
</tr>
<tr>
<td>Socialist Workers</td>
<td>James Harris, Margaret Trowe</td>
<td>President</td>
</tr>
<tr>
<td>Natural Law</td>
<td>John Hagelin, Nat Goldhaber</td>
<td>President</td>
</tr>
<tr>
<td>Reform</td>
<td>Pat Buchanan, Ezola Foster</td>
<td>President</td>
</tr>
<tr>
<td>Socialist</td>
<td>David McReynolds, Mary Cal Hollis</td>
<td>President</td>
</tr>
<tr>
<td>Constitution</td>
<td>Howard Phillips, J. Curtis Frazier</td>
<td>President</td>
</tr>
<tr>
<td>Workers World</td>
<td>Monica Moorhead, Gloria Lu Riva</td>
<td>President</td>
</tr>
</tbody>
</table>

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform Party.
Introduction

- Electronic voting systems to replace traditional paper ballots
- DRE: Direct Recording Electronic Voting
- Certified DRE = Government approved
- Security through Obscurity
- Expect some serious security blunders
The analysis

- Main problem with DRE is security hinges on the terminal.
- Authors analyze a real system (Diebold’s AccuVote) using CVS source code.
- Diebold deployed in 37 states
- Discovered significant security vulnerabilities.
- Design: wrong use of crypto (or lack thereof)
- Code: bad quality
System Overview

- C++ on Windows!
- Setting up: load ballot definitions.
- Election: use voter smartcard to vote on the terminal
  - Election ends using ender or administrator card and pin
- Results: transferred from terminal to server by media or network
Smartcards

* Three kinds: voter, ender and administrator
* No cryptography code running
* Talk to the terminal in the clear
* Administrator cards also store a PIN
Creating homebrew smartcards

* No crypto -> no secure authentication to the terminal -> make your own card
* Terminal checks only your ElectionKey, Center and Version
* All are easily attainable
* Easy to reverse engineer the smartcard protocol
* Let’s see some attacks...
Casting multiple votes

* Once you vote your smartcard is cancelled.
* Cancellation is designed by flipping two bits in the card.
  * VOTER_CARD(0x01)
  * CANCELLED_CARD(0x08)
* If you don’t have enough homebrew cards...
* Program your card to not flip the bits.
Administrator privileges

- Administrator cards are “harder” to forge.
- Change card type from 0x01 to 0x04.
- Insert a random PIN and remember it.
- Or look at the message sent to the terminal. It’s cleartext.
- Using administrator privileges a voter can end the elections early.
Election configurations and data

* No integrity, no privacy of critical data
* Data stored in Windows directories in terminal and removable media
* Terminals are networked to receive configurations and report results
Tampering with configurations

- Data stored in the clear
- Configurations in Windows registry
  - modify registry to impersonate a different terminal
- FEC requires to keep a protective counter of total votes
- Counter stored in mutable file (how did that pass inspections??)
Tampering with ballot definitions

- Ballot definitions contain sensitive data for reporting results.
- Not encrypted or checksummed.
- Candidate names in ASCII.
- Can tamper while in terminal or in-transit
- A man-in-the-middle attack will work
Cryptography

* Votes and audit logs are encrypted and checksummed, but...

* Using DES with a hardcoded key!!

* the key is F2654HD4

* also DES keys can be easily recovered

* DES is used with CBC mode with 0 as initialization vector.

* Integrity Checksum stored in the clear
Election results

- Votes are encrypted in storage, not in the network.
- Man-in-the-middle can change votes when sent to a back-end authority
- SSL could help here
- Votes written sequentially \(\rightarrow\) link voters to votes
- Randomized during tabulation using non-secure PRNG.
Audit logs

* Logs are "encrypted".
* When logging occurs, log can be printed.
* If the printer fails, no record indicates failure.
* So printed logs are unreliable.
Attacking start of elections

* Ballot definitions must be installed before elections
* But might need to download them from the internet at the last moment...
* Serious DDoS attack that can delay elections
* Anyone can do it, even outside of the US.
* Using the internet is bad.
Software Engineering

- Sloppy coding style, bad documentation
- No software design documents.
- Relies on Windows CE and external audio library -> how can you trust them?
- Code review is nearly impossible
Code correctness

* or maybe we should say Code completeness?

* Some developer comments to illustrate...
* “This is a bit of a hack for now.”
* “need to work on exception caused by audio. I think they will currently result in double-fault”
* Crypto library added to code, but not used.
Conclusions & Questions

* Security design is broken. Cannot trust election results.

* Why is the system so bad?

* Bad programmers?

* Low standards?

* Is it not important enough?

* How is quality control performed?