ELECTRONIC VOTING RISKS & RESEARCH

DANIEL R. SANDLER
Department of Computer Science, Rice University
October 27, 2008 guest lecture for COMP301, “Identity Theft to the iPod”
ELECTRONIC VOTING
RISKS & RESEARCH

DANIEL R. SANDLER
DEPARTMENT OF COMPUTER SCIENCE, RICE UNIVERSITY

OCTOBER 27, 2008 GUEST LECTURE FOR COMP301, “IDENTITY THEFT TO THE iPOD”
electronic voting
risks & research

Daniel R. Sandler
Department of Computer Science, Rice University

October 27, 2008 guest lecture for COMP301, “Identity Theft to the iPod”
why vote?

(please see any number of excellent POLI courses)
why is public trust in elections important?
“It is enough that the people know there was an election. The people who cast the votes decide nothing. The people who count the votes decide everything.”

—Joe Stalin (?)
1. Convince the loser that he lost.
2. Convince the electorate.
1. Failures
2. Fraud
(equipment failure)
fraud, e.g.

Registration frauds
Repeat voting
Ballot box stuffing
Chain ballots
Voter assistance
Intimidation and Violence
Altering Ballots
Substitution of Ballots
False Count and False Returns
Altering Returns


it’s a lot easier if you can just get everyone together in one room
“this doesn’t scale”
technology
when did we start using machines to help us vote?
2008 e-voting
two flavors of electronic voting

optical scan (OS) (aka “mark sense”) marks made on paper scanned by a computer

direct recording electronic (DRE) input made on a mechanical or computer interface recorded directly to electronic/digital media

Source: http://www.cs.uiowa.edu/~jones/voting/optical/ (plus everything you might ever want to know about mark-sense)
benefits of DREs

human factors
feedback: prevent overvoting / point out undervoting
voter can review & correct mistakes
accessibility (e.g. vision impairment)
administrative: ease of running & canvassing elections
strong voter preference

technical
fast results
replace failure-prone mechanical systems
replace ambiguous analog systems
can support more sophisticated voting styles
hazards of DREs

human factors
voting user experience may be poor
more things for administrators to mess up, too
(modern) humans are pretty good with paper

technical
electromechanical failures
software bugs
software malice?

fraud: “retail” → “wholesale”
human factors issues

below: ballot screens from a DRE

pop quiz: how many races are shown?

PAGE 1

PAGE 2
The page contains various advertisements and news articles. Some headlines include:

- Lowest consumer confidence
- A condo so pricey it won’t be built
- Houston tower with limo service, maid suites and residences with 9 1/2 bathrooms: This replica is as close as you'll get. Here's why.
- Outside, inside: How it would've been if Houston need this anyway?
- Already built Houston condos for sale
- DJIA 8260.12 +84.35 | NASD 15126.65 +6.75 | OIL 63.53 +0.31

The page also includes sections for election 2008, Texans chat today, and latest reader photos. There are articles and updates on local news, real estate, and stock market information.
DEWEY DEFEATS TRUMAN

G. O. P. Sweep Indicated in State; Boyle Leads in City

REPUBLICAN TICKET AHEAD OF 1944 VOTE

Town Balloting Gives Trend

RECORD CITY VOTE SEEN IN LATE TALLIES

Suburban Ballot Near 375,000

BULLETINS ON ELECTIONS

Early Count Gives G. O. P. Senate Edge

PUTS G. O. P. BACK IN THE WHITE HOUSE

Sizable Electoral Margin Seen

REDACTED INFORMATION
you may have heard about this

2006 ballot in Sarasota County, Florida (FL CD 13)

massive undervote in the congressional race
massive = 18,000 votes (15%; typical is 1–4%)
margin of victory: 369 (after certified recount)

possible causes
“banner blindness”; touchscreen calibration issues; other undiscovered software problem?

an official explanation
voters skipped the race intentionally because of its negative tone
—Vern Buchanan (the winner)
technical failures
(faulty hardware & software)
why?
only 2 options:
incompetence
malice
malice
(no evidence as of yet)
incompetence
(evidence abounds!)
Diebold* AccuVote TS(x)
the most-studied voting machine
(until 2007’s source-code audits—TTBR (CA), EVEREST (OH))
thanks to source code leaked on the internet
findings by Kohno et al., 2004:
poor software engineering
incorrect cryptography & crypto protocols
possible for voters to cast multiple votes
vulnerable to malicious software upgrades

*now “Premier Election Systems”
e.g. encryption

```c
#define DESKEY ((des_key*)"F2654hD4")
```

one key for every voting machine, everywhere
originally discovered by Doug Jones, 1997
defense: “but the bad guys don’t know what it is”
analogy: anyone else own a Scion?

still the case as of 2007
although cipher is AES and key may be changed by officials

Source: CA TTBR
e.g. voter smartcards

Protocol:

I am an authentic voting machine and my password is... (8 bytes)

“Okay”

Are you valid?

“Yup”

Cancel yourself, please.

“Okay”
it gets worse

Feldman et al., 2006 (citp.princeton.edu/voting)
before the TTBR, so they had to reverse-engineer much of the then-current AccuVote TS findings

malicious (evil) software could steal/alter votes without detection; we have no way of knowing physical access (e.g. a voting session) is all that is needed to install malicious software

the software can be designed to:

1. spread to other voting machines
2. alter the tally
3. remove all traces

ZOMG VOTING MACHINE VIRUS!!1!!!one!
on the topic of viruses—

2007: Diebold/Premier machines used in OH found to have problems thanks to e-voting researchers’ “EVEREST study”
http://siis.cse.psu.edu/everest.html

hundreds of votes found to have been lost in 2004

Diebold’s original explanation:

**McAfee anti-virus software installed on the tabulation machines**

they are, after all, everyday Windows PCs

think about this for a second—how ridiculous is that?
Premier Election Solutions (formerly Diebold) has blamed Ohio voting machine errors on problems with the machines' McAfee antivirus software.


Why? Security is good, right? Of course. But, well-

Imagine you're at a parent-teacher conference, and the teacher reassures you that he always wears a condom while teaching.

Ah. Strictly speaking, it's better than the alternative—yet someone is clearly doing their job horribly wrong.

http://www.xkcd.com/463/
can’t we do this job horribly right?
NSF-funded multi-institution research center
Dan S. Wallach, Rice University, associate director

goals
technology research
policy research
education

explicit non-goal
build a voting machine

and yet…
VoteBox
a tamper-evident, verifiable voting system

DANIEL R. SANDLER, KYLE DERR, DAN S. WALLACH
RICE UNIVERSITY

EXCERTED FROM SLIDES DELIVERED AT
USENIX SECURITY ’08
AUGUST 1, 2008
why?

lots of research on individual pieces of the e-voting problem
VoteBox integrates these techniques in a single system trustworthy reliable tamper-evident verifiable
goals

minimized software stack
less code to audit → more practical software audits

resistance to failure & tampering
prevent or minimize data loss

tamper-evidence
if resistance is futile

verifiability

cast-as-intended; counted-as-cast
techniques
used in VoteBox

1. PRUI: pre-rendered user interfaces
   DRE user experience; minimized software stack

2. AUDITORIUM: network layer
   resistance to failure; tamper-evidence

3. immediate ballot challenge
   verifiability
very restricted graphics API

\[
\text{blit}(\text{bitmap}, x, y)
\]

\[
\text{next\_event()} \rightarrow \text{keyboard or (x, y) input}
\]

what’s not here?

windowing system; widgets; fonts & text rendering

inspiration: Pvote

pioneering work on PRUI in e-voting

(Yee, EVT ’06 & ’07)
To make your choice, click on the candidate's name or on the box next to his/her name. A green checkmark will appear next to your choice. If you want to change your choice, just click on a different candidate or box.

<table>
<thead>
<tr>
<th>President and Vice President of the United States (You may vote for one)</th>
</tr>
</thead>
</table>
| Gordon Bearce  
Nathan Maclean | REP |
| Vernon Stanley Albury  
Richard Rigby | DEM |
| Janette Froman  
Chris Aponte | LIB |
To make your choice, click on the candidate's name or on the box next to his/her name. A green checkmark will appear next to your choice. If you want to change your choice, click on a different candidate or box.

President and Vice President of the United States (You may vote for one)

- **Gordon Barse**
  - REP
- **Vernon Stanley Albury**
  - DEM
- **Janette Froman**
  - LIB
VoteBox ballot creator

...where the pre-rendering happens
even honest voting machines fail!

we can’t trust voting machines with critical election data

at least, not without redundancy
March 7, 2006:

Webb County, TX

2006 Democratic primary election

(County’s first use of DREs)
<table>
<thead>
<tr>
<th>Votronic</th>
<th>PEB#</th>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>5140052</td>
<td>161061</td>
<td>SUP</td>
<td>03/07/2006</td>
<td>15:29:03</td>
<td>01 Terminal clear and test</td>
</tr>
<tr>
<td>160980</td>
<td>SUP</td>
<td></td>
<td>03/07/2006</td>
<td>15:31:15</td>
<td>09 Terminal open</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>15:34:47</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>15:36:36</td>
</tr>
<tr>
<td>160999</td>
<td>SUP</td>
<td></td>
<td>03/07/2006</td>
<td>15:56:50</td>
<td>20 Normal ballot cast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>16:47:12</td>
<td>20 Normal ballot cast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>18:07:29</td>
<td>20 Normal ballot cast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>18:17:03</td>
<td>20 Normal ballot cast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>18:37:24</td>
<td>22 Super ballot cancel</td>
</tr>
<tr>
<td>160980</td>
<td>SUP</td>
<td></td>
<td>03/07/2006</td>
<td>19:07:14</td>
<td>10 Terminal close</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>18:41:18</td>
<td>20 Normal ballot cast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03/07/2006</td>
<td>18:46:23</td>
<td>20 Normal ballot cast</td>
</tr>
</tbody>
</table>
problem #1: logs starting mid-day

03/07/2006 15:29:03 Terminal clear and test
03/07/2006 15:31:15 Terminal open

Polls opened around 7 AM across Webb Co.

What happened to this machine between 7 and 3:30? Were votes cast and then lost?

(10 total machines)
problem #2
election events on wrong day

<table>
<thead>
<tr>
<th>Votronic</th>
<th>PEB#</th>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>5142523</td>
<td>161061</td>
<td>SUP</td>
<td>02/26/2006</td>
<td>19:07:05</td>
<td>01 Terminal clear and test</td>
</tr>
<tr>
<td></td>
<td>161115</td>
<td>SUP</td>
<td>03/06/2006</td>
<td>06:57:23</td>
<td>09 Terminal open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUP</td>
<td>03/06/2006</td>
<td>07:01:47</td>
<td>13 Print zero tape</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUP</td>
<td>03/06/2006</td>
<td>07:03:41</td>
<td>13 Print zero tape</td>
</tr>
<tr>
<td>161109</td>
<td>SUP</td>
<td></td>
<td>03/06/2006</td>
<td>10:08:26</td>
<td>20 Normal ballot cast</td>
</tr>
<tr>
<td>[... 9 more ballots cast ...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>161115</td>
<td>SUP</td>
<td></td>
<td>03/06/2006</td>
<td>19:29:00</td>
<td>27 Override</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUP</td>
<td>03/06/2006</td>
<td>19:29:00</td>
<td>10 Terminal close</td>
</tr>
</tbody>
</table>

The election was held on 03/07!
otherwise, a pretty normal voting pattern
(4 machines / 41 votes)
ABOUT HALF OF THE IMPOUNDED MACHINES
the AUDITORIUM polling place network joins all voting machines together
all election events are signed and broadcast
each broadcast is logged by every machine

hash chains

key ingredient in AUDITORIUM

every signed broadcast includes SHA(earlier events)

events “entangled” between machines

we can now reason about our audit logs

provable ordering & completeness of the record

…crucial in the voting context

query the log at runtime or offline

“cast as intended”

the biggest challenge for DREs

how can the voter be sure the computer:

- captured the voter’s choices faithfully,
- encrypted the ballot correctly,
- and broadcast it in the Auditorium?

unlike “counted as cast,” no amount of procedure or post facto auditing can correct this
ballot challenge

voter makes selections

voting machine commits publicly to voter’s choices

voter’s choice

challenge
• reveal commitment
• spoil ballot

cast the ballot
big finish
will next week's election be hacked?
will next week’s election results be trustworthy?
LIKE MY HALLOWEEN COSTUME?
WHAT IS IT?
I'M A TOUCH-SCREEN ELECTRONIC VOTING MACHINE.
COMPUTER EXPERTS HAVE BEEN WARNING FOR YEARS THAT THESE THINGS CAN BE EASILY HACKED, AND WITHOUT A PAPER TRAIL, THERE'S NO WAY TO VERIFY THE VOTE COUNTS WEREN'T TAMPERED WITH.
NOW, HERE WE ARE NINE DAYS BEFORE ELECTIONS, AND REPORTEDLY ONE-THIRD OF ALL JURISDICTIONS WILL USE THEM.
SERIOUSLY, CAN YOU THINK OF ANYTHING SCARIER?
JASON, MOST PEOPLE DON'T CARE ABOUT THIS STUFF.
HMM. THAT WAS A PRETTY GOOD ANSWER.
This Modern World,

October 28, 2003

How do you like my Halloween costume?

Sorry—what are you supposed to be, exactly?

Something truly terrifying. I’ll give you a hint—

I’m prone to technical glitches, I have huge security flaws and I leave absolutely no paper trail—

And the companies that make me are owned and operated by intensely partisan Republicans!

Give up? I’m certainly stumped!

I’m a touch screen voting machine! Bwah ha ha ha ha!

See, the point is, this is a really scary threat to democracy—

Yeah, yeah, I got that part.

I’m going to be a ghost!