The State of Electronic Voting, 2008

David Wagner

UC Berkeley
An Abbreviated History of E-Voting
Confusion at Palm Beach County polls
Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot’s design.

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.
From: Lana Hires
Subject: 2000 November Election

I need some answers! Our department is being audited by the County.

I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded. Will someone please explain this so that I have the information to give the auditor instead of standing here "looking dumb".
Oct 2002: Congress passes Help America Vote Act (HAVA): states must upgrade voting systems by 2006; provides $3.6 billion in federal funding.

HAVA accelerates adoption of e-voting.
DREs used by 13% of voters in 2000 → 38% in 2006
Sequoia Voting Systems
Hart InterCivic
Premier (was: Diebold)
OFFICIAL GENERAL ELECTION BALLOT
SARASOTA COUNTY, FLORIDA
NOVEMBER 7, 2006

CONGRESSIONAL
UNIVERSAL STATES SENATOR
(Vote for One)

Katherine Harris  REP  
Bill Nelson  DEM  
Floyd Ray Frazier  NPA  
Belinda Noah  NPA  
Brian Moore  NPA  
Roy Tanner  NPA  
Write-In  

Page 1 of 21
Public Count: 0

Next Page
### U.S. Representative in Congress
13th Congressional District

(Vote for One)

<table>
<thead>
<tr>
<th>Name</th>
<th>Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vern Buchanan</td>
<td>REP</td>
</tr>
<tr>
<td>Christine Jennings</td>
<td>DEM</td>
</tr>
</tbody>
</table>

### State

Governor and Lieutenant Governor

(Vote for One)

<table>
<thead>
<tr>
<th>Name</th>
<th>Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charlie Crist</td>
<td>REP</td>
</tr>
<tr>
<td>Jeff Kottkamp</td>
<td></td>
</tr>
<tr>
<td>Jim Davis</td>
<td>DEM</td>
</tr>
<tr>
<td>Daryl L. Jones</td>
<td></td>
</tr>
<tr>
<td>Max Linn</td>
<td>REF</td>
</tr>
<tr>
<td>Tom Macklin</td>
<td></td>
</tr>
<tr>
<td>Richard Paul Dembinsky</td>
<td>NPA</td>
</tr>
<tr>
<td>Dr. Joe Smith</td>
<td></td>
</tr>
<tr>
<td>John Wayne Smith</td>
<td>NPA</td>
</tr>
<tr>
<td>James J. Kearney</td>
<td></td>
</tr>
<tr>
<td>Karl C.C. Behm</td>
<td>NPA</td>
</tr>
<tr>
<td>Carol Castagnero</td>
<td></td>
</tr>
<tr>
<td>Write-In</td>
<td></td>
</tr>
</tbody>
</table>
ATTORNEY GENERAL  
(Vote for One)  
Bill McCollum  
Walter "Skip" Campbell  

CHIEF FINANCIAL OFFICER  
(Vote for One)  
Tom Lee  
Alex Sink  

COMMISSIONER OF AGRICULTURE  
(Vote for One)  
Charles H. Bronson  
Eric Copeland
Poll: How many contests did you vote in?
Margin of victory: 369 votes (0.15% of voters)  
No vote recorded: 18,412 votes (14% of e-voters)
Margin of victory: 369 votes (0.15% of voters)
No vote recorded: 18,412 votes (14% of e-voters)
More than 4,500 North Carolina votes lost because of mistake in voting machine capacity

JACKSONVILLE, N.C. (AP) — More than 4,500 votes have been lost in one North Carolina county because officials believed a computer that stored ballots electronically could hold more data than it did. Scattered other problems may change results in races around the state.

Officials said UniLect Corp., the maker of the county’s electronic voting system, told them that each storage unit could handle 10,500 votes, but the limit was actually 3,005 votes.
Machine error gives Bush 3,893 extra votes in Ohio

By John McCarthey, Associated Press

COLUMBUS, Ohio — An error with an electronic voting system gave President Bush 3,893 extra votes in suburban Columbus, elections officials said.

Franklin County’s unofficial results had Bush receiving 4,258 votes to Democrat John Kerry’s 260 votes in a precinct in Gahanna. Records show only 638 voters cast ballots in that precinct. Bush’s total should have been recorded as 365.
Broward Vote-Counting Blunder Changes Amendment Result

POSTED: 1:34 pm EST November 4, 2004

BROWARD COUNTY, Fla. -- The Broward County Elections Department has egg on its face today after a computer glitch misreported a key amendment race, according to WPLG-TV in Miami.

Amendment 4, which would allow Miami-Dade and Broward counties to hold a future election to decide if slot machines should be allowed at racetracks, was thought to be tied. But now that a computer glitch for machines counting absentee ballots has been exposed, it turns out the amendment passed.

"The software is not geared to count more than 32,000 votes in a precinct. So what happens when it gets to 32,000 is the software starts counting backward," said Broward County Mayor Ilene Lieberman.

That means that Amendment 4 passed in Broward County by more than 240,000 votes rather than the 166,000-vote margin reported Wednesday night. That increase changes the overall statewide results in what had been a neck-and-neck race, one for which recounts had been going on today. But with news of Broward’s error, it’s clear amendment 4 passed.
We would like to explain in further technical detail what caused this issue, should you or others at the county have questions. The 32,767 capacity limitation at a single precinct level is a function of the design and definition of the results database used by ERM. The data storage element used to record votes at the precinct level is a two byte binary field. 32,767 is 2 to the 15th power, which is the maximum number held by a two byte word (16 bits) in memory, where the most significant bit is reserved as the sign bit (a plus or minus indicator). Additionally, ERM precinct count level data is stored in a binary computer format known as two’s complement. Data on ERM results reports are printed as the absolute value of the two’s complement of the associated data in the ERM database. This means that once the 32,767 limitation is reached, additional incremental tallies of vote results would not be printed correctly (32,768 through 65,536 would actually be represented as 65,536 to 32,768).
E-Voting Raises Security Concerns
KEYS TO THE KINGDOM
Photo taken from Diebold's online store. The keys that open every Diebold touch-screen voting machine. Working copies have been made from the photo.
Jun 2007: Secretary Bowen hires 43 experts to evaluate voting systems used in CA.
We found...
We found... significant security problems in all 3 systems.
Sequoia invented their own password encryption algorithm.
Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password “sekret” encrypts to “sekretXYZ”.*
Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password “sekret” encrypts to “sekretXYZ”.*

* Obfuscated for ’security’; “XYZ” are not the real letters.
“We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended.”

— Sequoia source team
One of Diebold’s passwords was
One of Diebold’s passwords was “diebold”.
In some places, Hart avoided trivially broken crypto by…
In some places, Hart avoided trivially broken crypto by… omitting it entirely.
In some places, Hart avoided trivially broken crypto by… omitting it entirely.

When you connect a polling-place machine to the county’s central PC, it trusts the PC implicitly. The county PC can instruct the machine to overwrite its software, and it will blindly comply. (No authentication!)
The code fails to follow sound engineering principles expected of security-critical systems.
void GlibPutPixel(UINT xx, UINT yy, Pixel_t Color) {
    // Check for library not initialized or (x,y) out of range
    if(FrameBuffer != FALSE || (xx < USER_X) || (yy < USER_Y)) {
        // Compute the frame buffer offset and write the pixel
        FrameBuffer[FB_OFFSET(xx,yy)] = Color;
    }
}
TCHAR name;
_stprintf(&name, _T("\\\Storage Card\\%s"), findData.cFileName);
Install(&name, hInstance);
All 3 systems allow malicious code to propagate virally.
The Diebold code that reads data off the memory card has buffer overruns and other vulnerabilities.
1. Attacker writes malicious data onto a memory card.
2. Uploading results at county HQ on election night infects county machines.
3. Infected county machines write malicious data and code onto memory cards that will infect all polling-place machines in the county in the next election.
After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.
After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

The voting machine can exploit buffer overruns in the code on the PC to take control of the PC.
1. Attacker installs malicious code onto a voting machine.
2. When connected to the county PC, it hacks the PC.
3. The county PC then installs malicious code onto every voting machine subsequently connected to it.
A single individual, with no special access, could introduce a virus onto a single voting machine,
A single individual, with no special access, could introduce a virus onto a single voting machine, and this virus could infect every machine in the county.
In August 2007, California Secretary of State Debra Bowen decertified these systems.

Consequence: In 2008 elections, most California voters voted on paper ballots.
So, How Did We Do In 2008?
We were fortunate; there seem to have been no major fiascos in the 2008 election.

Problem areas: equipment failures, long lines, registration matching issues.
Results tape from Bergen County, NJ, Feb. 2008

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Republican</td>
<td></td>
</tr>
<tr>
<td>US President C11</td>
<td>(1)</td>
</tr>
<tr>
<td>Rudw Giuliani</td>
<td>1</td>
</tr>
<tr>
<td>Ron Paul</td>
<td>1</td>
</tr>
<tr>
<td>Fred Thompson</td>
<td>0</td>
</tr>
<tr>
<td>Mitt Romney</td>
<td>6</td>
</tr>
<tr>
<td>Mike Huckabee</td>
<td>0</td>
</tr>
<tr>
<td>John McCain</td>
<td>14</td>
</tr>
<tr>
<td>Personal Choice</td>
<td>0</td>
</tr>
<tr>
<td>Democrat</td>
<td></td>
</tr>
<tr>
<td>US President- 19th Dist C18</td>
<td>(1)</td>
</tr>
<tr>
<td>Barack Obama</td>
<td>33</td>
</tr>
<tr>
<td>Joe Biden</td>
<td>0</td>
</tr>
<tr>
<td>John Edwards</td>
<td>2</td>
</tr>
<tr>
<td>Hillary Clinton</td>
<td>49</td>
</tr>
<tr>
<td>Dennis Kucinich</td>
<td>0</td>
</tr>
<tr>
<td>Bill Richardson</td>
<td>0</td>
</tr>
<tr>
<td>Uncommitted</td>
<td>0</td>
</tr>
<tr>
<td>Personal Choice</td>
<td>0</td>
</tr>
</tbody>
</table>

Write In Votes
No Write in Votes In Memory

Option Switch Totals

<table>
<thead>
<tr>
<th>Option</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unused</td>
</tr>
<tr>
<td>2</td>
<td>Unused</td>
</tr>
<tr>
<td>3</td>
<td>Unused</td>
</tr>
<tr>
<td>4</td>
<td>Unused</td>
</tr>
<tr>
<td>5</td>
<td>Unused</td>
</tr>
<tr>
<td>6</td>
<td>Republican</td>
</tr>
<tr>
<td>7</td>
<td>Unused</td>
</tr>
<tr>
<td>8</td>
<td>Unused</td>
</tr>
<tr>
<td>9</td>
<td>Unused</td>
</tr>
<tr>
<td>10</td>
<td>Unused</td>
</tr>
<tr>
<td>11</td>
<td>Unused</td>
</tr>
<tr>
<td>12</td>
<td>Democrat</td>
</tr>
</tbody>
</table>

Total

33 + 49 + 2 = 84 Democratic votes

83 Democratic voters
How Do Things Stand Going Forward?
Auditability and Recountability
Concluding thoughts

• Elections are a complex distributed system, with equipment operated and administered by volunteers.

• Despite its imperfections, electronic voting can be trusted if it can be audited.