Elections, Computer Security, and Electronic Voting

CS161 4/19/2010
David Wagner
For Delegate to Congress.
FRANCIS GEHON.
For Representatives.
John Forrest
A. S. Lothohl

For County Commissioners.
Abner Wolcott
John Morford

For Treasurer.
John Liguory

For Surveyor.
Cyrus Tender

For Assessor.
J. D. Mullahay

For Coroner.
John Howthers

For Constable.
John Royal
David Cooper
A. D. Hethen
REPUBLICAN TICKET.

For Mayor,
M. F. FAIRCHILD.

For City Solicitor,
J. P. DOLLIVER.

For City Assessor,
L. G. SPRING.

For City Treasurer,
BETH VINCENT.

For Councilman—4th Ward,
A. H. JOHNSON.

STATE TICKET.

For Governor,
WILLIAM LARABEE,
Of Payette County.

For Lieutenant Governor,
JOHN A. H. HULL,
Of Polk County.

For Judge of the Supreme Court
GIFFORD J. ROBBINS,
Of Baca County.

For Superintendent of Public Instruction,
HENRY SABIN,
Of Chaffee County.

COUNTY TICKET
For Senator Thirty-first District,
J. W. PATRICK.
For Representative Seventeenth District,
W. W. GOODWIN.
For Auditor
JULIUS H. BULMAN.
For Treasurer,

For Sheriff,
WILLIAM WILLMAN.
For County Superintendent,
WILLIAM D. WYATT.
For Sheriff,
PATRICK COSTIGAN.
For County Attorney
L. L. RENSHAW.
For Surveyor
SANFORD L. BARTLETT.

TOWNSHIP TICKET.
For Trustee
For Constable

For Road Supervisor District No. . . . . .
10th District.

ADMINISTRATION

UNION TICKET

For Mayor,
CALEB T. FAY
For County Judge,
THOS. W. FREELON
For District Attorney,
CHARLES H. PARCHER
For County Clerk,
JOHN A. MONROE
For Sheriff,
THOMAS J. POULETKER
For Recorder, to fill the vacancy for the unexpired term of G. W. HICKS, resigned.
GEORGE B. REEVE
For County Recorder,
GEORGE B. REEVE
For City and County Treasurer,
ASA T. LAWTON
For City and County Assessor,
THOS. D. MATHEWSON
For City and County Surveyor,
REED BIGLER
For Coroner,
DR. B. A. SHELTON
For Justice of the Peace,
CAPT. N. PROCTOR SMITH
For Superintendent of Common Schools,
JOHN H. BREWER
For Supervisor ...........STEPHEN C. STORY
For School Districts ...........J. M. HOLLING
Inspector of Elections ..........J. B. PHIPTA
Judge of Elections ..........J. M. KHANARY
Firm Treasurers
Justice of the Peace ..........LEO. T. BOLTON
Constables ..PHINEAS HOWARD, JR.

"Subsidies of three hundred thousand dollars to the San Francisco and San Jose Railroad Company!"

YES.

Tools—Brick Building westerly side of Third, between Oakland and Harrison streets.
Security Goals for an Election

• Integrity: No election fraud

• Transparency: Everyone – especially the loser – must be able to verify that the election was conducted appropriately

• Privacy: No one learns how the voter has voted

• Secret ballot: Voter cannot prove how she voted
Breakthrough! — the Australian secret ballot.

Ballot printed by govt. Ballot boxes monitored by observers. Ballots counted, by hand, in public. Competing interests keep each other honest.
**ABSENT VOTER BALLOT**
**STUB A No. 7720**

**PLACE HOLES OVER POSTS**

**INSERT CARD** **THIS SIDE UP**

**STUB B No. 7720**
**ABSENT VOTER BALLOT**

**IMPORTANT**
**DO NOT**
**DETACH STUB**

<table>
<thead>
<tr>
<th>1</th>
<th>20</th>
<th>59</th>
<th>77</th>
<th>146</th>
<th>173</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>21</td>
<td>41</td>
<td>60</td>
<td>78</td>
<td>147</td>
</tr>
<tr>
<td>3</td>
<td>32</td>
<td>42</td>
<td>61</td>
<td>76</td>
<td>167</td>
</tr>
<tr>
<td>4</td>
<td>43</td>
<td>43</td>
<td>62</td>
<td>74</td>
<td>154</td>
</tr>
<tr>
<td>5</td>
<td>54</td>
<td>44</td>
<td>63</td>
<td>72</td>
<td>151</td>
</tr>
<tr>
<td>6</td>
<td>65</td>
<td>45</td>
<td>64</td>
<td>70</td>
<td>148</td>
</tr>
<tr>
<td>7</td>
<td>76</td>
<td>46</td>
<td>65</td>
<td>68</td>
<td>146</td>
</tr>
<tr>
<td>8</td>
<td>87</td>
<td>47</td>
<td>66</td>
<td>66</td>
<td>143</td>
</tr>
<tr>
<td>9</td>
<td>98</td>
<td>48</td>
<td>67</td>
<td>64</td>
<td>140</td>
</tr>
<tr>
<td>10</td>
<td>109</td>
<td>49</td>
<td>68</td>
<td>62</td>
<td>137</td>
</tr>
<tr>
<td>11</td>
<td>110</td>
<td>50</td>
<td>69</td>
<td>60</td>
<td>134</td>
</tr>
<tr>
<td>12</td>
<td>121</td>
<td>51</td>
<td>70</td>
<td>58</td>
<td>131</td>
</tr>
<tr>
<td>13</td>
<td>132</td>
<td>52</td>
<td>71</td>
<td>56</td>
<td>128</td>
</tr>
<tr>
<td>14</td>
<td>143</td>
<td>53</td>
<td>72</td>
<td>54</td>
<td>125</td>
</tr>
<tr>
<td>15</td>
<td>154</td>
<td>54</td>
<td>73</td>
<td>52</td>
<td>122</td>
</tr>
<tr>
<td>16</td>
<td>165</td>
<td>55</td>
<td>74</td>
<td>50</td>
<td>119</td>
</tr>
<tr>
<td>17</td>
<td>176</td>
<td>56</td>
<td>75</td>
<td>48</td>
<td>116</td>
</tr>
<tr>
<td>18</td>
<td>187</td>
<td>57</td>
<td>76</td>
<td>46</td>
<td>113</td>
</tr>
<tr>
<td>19</td>
<td>198</td>
<td>58</td>
<td>77</td>
<td>44</td>
<td>110</td>
</tr>
<tr>
<td>20</td>
<td>209</td>
<td>59</td>
<td>78</td>
<td>42</td>
<td>107</td>
</tr>
<tr>
<td>21</td>
<td>2110</td>
<td>60</td>
<td>79</td>
<td>40</td>
<td>104</td>
</tr>
</tbody>
</table>
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.

---

(REPUBLICAN)

GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT

(DEMOCRATIC)

AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT

(LIBERTARIAN)

HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT

(GREEN)

RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT

(SOCIALIST WORKERS)

JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT

(NATURAL LAW)

JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT

(REFORM)

PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

(SOCIALIST)

DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

(CONSTITUTION)

HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

(WORKERS WORLD)

MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE

To vote for a write-in candidate, follow the directions on the long stub of your ballot card.
Another anomaly during the 2000 election

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".
Voting on an iVotronic is as easy as 1, 2, 3

1. Make your selections
   Touch the candidate on the screen to make your selection.
   Use the Next and Back buttons to view the ballot pages.

2. Review your selections
   Touch the contest or the candidate on screen to make changes.

3. Cast your ballot
   Press the Vote button at the top of the voting machine when it begins to flash OR press the "Cast your ballot now" when it appears on screen.

Best Automobile Manufacturer
Vote For ONE

- BMW
- MERCEDES
- GENERAL MOTORS
- HONDA
- FERRARI
- JAGUAR
- FORD
- VOLVO
- Write-In

Best Vocal Artist
Vote for Not More Than TWO

- FRANK SINATRA
- ELVIS
- PATSY CLINE
- JANIS JOPLIN
- BUDDY HOLLY
- BARRY WHITE
- BILLIE HOLIDAY
- STEVIE RAY VAUGHAN
- "MAMA" CASS ELLIOT
- FR
- Write-In
Summary Ballot Instructions

Press the candidate name or contest title to return to a contest.

Vote button will light up when you may cast your ballot.

Best Automobile Manufacturer
Vote For ONE

- FORD

Best Vocal Artist
(Vote for Not More Than TWO)

- (Blank)

No selection made.

Best Ice-Cream Flavor
Vote For ONE

No selection made.

Proposition 1
No selection made.

Proposition 2
No selection made.
Question: How do election security goals apply to touchscreen (DRE) electronic voting machines?

1. Machine must allow each authorized voter to vote exactly once; must prevent tampering with votes after they are cast.

2. Machine should be verifiably trustworthy.

3. Machine must randomize the order in which votes were cast.

4. Machine must not give voter a “receipt”.

Security Goals for an Election:
Integrity, Transparency, Privacy, Secret ballot
Nov 4, 2002:
State of Georgia votes on Diebold DREs.

March 18, 2003:
Diebold source code leaks.

July 23, 2003:
Tadayoshi Kohno, Adam Stubblefield, Avi Rubin, Dan Wallach, “Analysis of an Electronic Voting System”.
The voter authorization protocol

QueryStatus

ACTIVE (0x01)

(record vote)

SetStatus CANCELED (0x08)

Status = CANCELED

Succeeded

smartcard
The voter authorization protocol

QueryStatus [Are you a valid card?]

ACTIVE (0x01) [Yup.]

(record vote)

[Please cancel yourself.]

SetStatus CANCELED (0x08)

Status = CANCELED

Succeeded [Ok.]
Attack!

QueryStatus →
ACTIVE (0x01) ←

(record vote)

SetStatus CANCELED (0x08) →
Succeeded ←

QueryStatus →
ACTIVE (0x01) ←

(record another vote)

SetStatus CANCELED (0x08) →
Succeeded ←

malicious smartcard
Authenticating election officials

What kind of card are you?
An administrator card.

What’s the secret PIN?
2301

Ok, you have admin access.
Source code excerpts

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

DESCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize, DESKEY, NULL, DES_ENCRYPT);
Source code excerpts

// LCG - Linear Congruential Generator -
// used to generate ballot serial numbers
// A psuedo-random-sequence generator
// (per Applied Cryptography, Bruce Schneier)

int lcgGenerator(int lastSN) {
    return ((lastSN*1366) + 150889)%714025;
}

“Unfortunately, linear congruential generators cannot be used for cryptography.”
— Applied Cryptography, p.369
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 McCarthy, 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.
California Top-to-Bottom Review

In 2007, California Secretary of State Debra Bowen commissions a review of California’s voting systems.

43 experts (led by David Wagner & Matt Bishop) examine voting systems used nationally.
All voting systems examined have serious security problems:
• None followed sound engineering principles expected of security-critical systems.
• All were vulnerable to viral attacks: one outsider could subvert all voting machines countywide
Example flaw (Premier system)

Bug: The code that reads data off the memory card has buffer overrun vulnerabilities.

Attack:
1. Attacker writes malicious code onto 1 card
2. When central PC reads votes off card on election night, it gets infected
3. Infected PC writes malicious code onto all cards used in the next election, infecting entire county
Quotes from the reports

“We found pervasive security weaknesses throughout the Sequoia software. Virtually every important software security mechanism is vulnerable to circumvention.”

“Our study of the Diebold source code found that the system does not meet the requirements for a security-critical system. It is built upon an inherently fragile design and suffers from implementation flaws that can expose the entire voting system to attacks.”

“The Hart software and devices appear to be susceptible to a variety of attacks which would allow an attacker to gain control of some or all of the systems in a county. [...] Many of these attacks can be mounted in a manner that makes them extremely hard to detect and correct. We expect that many of them could be carried out in the field by a single individual, without extensive effort, and without long-term access to the equipment.”
Outcome of the CA TTBR

Bowen decertifies most DRE voting systems and imposes strict new procedural protections.

Result: Most Californians now vote on paper ballots.
Trojan Horses and the Insider Threat

Ronald Dale Harris

Employee, Gaming Control Board, 1983-1995

Arrested, Jan 15, 1995
Convicted, Sept 23, 1997, for rigging slot machines
... 
schedule();
goto repeat;
}
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
    retval = -EINVAL;
    retval = -ECHILD;
    end_wait4:
    current->state = TASK_RUNNING;
...
Trojan Horses and Voting Machines

Malicious logic hidden by an insider might, e.g., record votes incorrectly to favor one candidate. How would we defend a voting system against this kind of insider threat?

Potential solutions:
• Verify that the software is free of Trojans and will work correctly on all future elections. (beyond the state of the art)
• Assume sw might contain Trojans. Verify that sw worked correctly in this particular election. (voter-verified paper records + random audits)

Voting on Satan’s computer.
Touch the Print Next Page button to print and verify the next page.

OR

Touch the Reject Ballot button to go back and make changes.

NOTE: you may reject your printed ballot a maximum of two times, after which you will no longer be allowed to make changes and printing your ballot will cast your vote. Contact a pollworker if you are experiencing difficulty with this process.

PRESIDENT
(Vote for One)

ABRAHAM LINCOLN

POET LAUREATE
(Vote for One)

CARL SANDBURG

COMMISSIONERS
FOR NATIONAL PASTIMES
(Vote for Two)

No Vote Cast
No Vote Cast

COMMISSIONER OF
AMERICAN LITERATURE
(Vote for One)

No Vote Cast

MINISTER OF
TRANSPORTATION
(Vote for One)

CHUCK YEAGER

MINISTER OF
COMIC RELIEF
(Vote for One)

CAROL BURNETT

MINISTER OF ART
(Vote for One)

ALEXANDER CALDER

AMBASSADORS OF THE AMERICAN

Reject Ballot

Print Next Page
N.C. STATE SENATE
DISTRICT 25
You may vote for ONE
☐ WILLIAM R. (BILL) PURCELL DEM

N.C. STATE HOUSE
DISTRICT 69
You may vote for ONE
☐ FRITZ GIBSON DEM
☐ MELDA L. MORRISON REP

REGISTER OF DEEDS
You may vote for ONE
☐ JOANNE S. HUNTELY DEM

NON PARTISAN OFFICES
Non-partisan offices are not included in Straight Party voting and must be voted separately to be counted.

ASSOCIATE JUSTICE OF SUPREME COURT
You may vote for ONE
☐ SARAH PARKER
☐ JOHN M. TYSON

ASSOCIATE JUSTICE OF SUPREME COURT
You may vote for ONE
☐ POHIEANIMALY
☐ RACHEL LEA HUNTER
☐ HOWARD E. MANNING, JR.
☐ BETSY MCDONNELL
☐ FRED MATHIS, JR.
☐ PAUL MARTIN NEWBY
☐ MARVIN SCHILLER
☐ JAMES A. WYNNE, JR.

JUDGE, COURT OF APPEALS
You may vote for ONE
☐ LINDA McCARTY
☐ BILL PARKER

JUDGE, COURT OF APPEALS
You may vote for ONE
☐ WANDA G. BRADY
☐ ALICE C. STUBBS

JUDGE, COURT OF APPEALS
You may vote for ONE
☐ BARBARA JACKSON
☐ ALAN THORNBURG

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE
☐ HUNTER

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE
☐ LISA BLUE THACKER

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE
☐ TANYA WALLACE

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE
☐ W. DAVID McSHEEN
☐ JOSEPH J. WILLIAMS

NON PARTISAN OFFICES
Additional instructions to Voter
If you wish to write in a name for any of the following offices, write the name in the blank space provided and completely fill in the oval to the left of the name in order for your vote to count.

BROWN CREEK
SOIL AND WATER
CONSERVATION DISTRICT
SUPERVISOR
You may vote for ONE
☐ JOHN C. SPRINGER

STATE OF NORTH CAROLINA
CONSTITUTIONAL AMENDMENTS

AMENDMENT II
Constitutional amendment to provide that the General Assembly may enact the General Assembly to enact civil penalties, civil penalties, and civil penalties collected by a State agency in a State fund to be used exclusively for maintaining the public schools.

☐ FOR
☐ AGAINST

AMENDMENT III
Constitutional amendment to provide for the first term of office for magistrates of the General Court of Justice to be two years and for subsequent terms to be four years.

☐ FOR
☐ AGAINST

TURN OVER TO CONTINUE VOTING

BACK Card 3 SRQ 1
INSTRUCTIONS TO VOTERS

1. Insert ballot inside voting machine

2. Take ballot and secret ballot to Accu-Vote machine

3. Feed ballot straight into machine while holding onto the area below dotted line

When inserting ballot into Accu-Vote Machine,

GRIP BELOW DOTTED LINE
Statistical audit

- After election, randomly choose 1% of machines and manually recount the paper records on those machines. If paper count $\neq$ electronic count, there was fraud.

- If $\geq 100$ machines cheat, detection is likely. Consequently: If paper count = electronic count, then no more than $\sim 100$ machines cheated.

\[ \text{The tallies are } t_1, \ldots, t_n \]

\[ \text{Show me the paper for machine } i. \]

\[ \text{(voter-verif} \text{ied paper audit trail)} \]

Prover (Elec. Official) \hspace{1cm} \text{Verifier (skeptical voter)}
Trends in e-voting technology

Percent of Registered Voters

- Punchcard
- Datavote
- Lever
- Paper
- Optical
- Electronic
- Mixed

Adoption of paper records + random audits
Timeline

Florida

HAVA

Sarasota

TTBR
Conclusions

- E-voting security is hard, but...
- E-voting can be made secure and trustworthy, if it can be audited.

- Technical principles:
  - Two-person control, separation of duties
  - Statistical audit
  - Security against malicious insiders
Lessons

• Understand security requirements before you design & deploy an information system.
• Independent review is valuable.
• Sometimes technical threats can be handled through non-technical defenses.
• Seek independent, end-to-end checks that the system is working properly.
• Securing systems against malicious insiders is extremely challenging.
• Business structure determines the technology that is built & deployed. If buyers cannot measure how secure a product is, be prepared for market failures.
THE HAZARDS OF ONLINE VOTING...

President of the United States

George W. Bush R
John F. Kerry D
Ralph Nader I
Low-Cost Home Mortgage
Generic Viagra
Enlarge Your Thingy

Greetings! I am Ndugu Scamu, ex-Interior Minister of Nigeria, and I need your help to transfer $150,000,000 in funds to a bank.