Climbing Everest

EVEREST:
Evaluation and Validation of Election-Related Equipment, Standards and Testing.

12/07/2007
OHIO

Penn State University
University of Pennsylvania
WebWise Security, Inc.
MOUSE
FOR
OVERLORD
Voting 101
Voting in the US

• Highly decentralized:
  – *Federal* government sets broad standards
  – Each *state* has own laws, rules, requirements
  – Elections run by *counties* (>3000 in US)
  – Voting takes place in neighborhood *precincts*
    • tens, hundreds or thousands per county

• Complex:
  – Typical election has many races
  – Precinct may have several different ballots
Feds vs. States
HAVA

Pregnant

Dimpled

Hanging

CHADS
• Favorite HAVA quote:

“For States that do not use electronic equipment to assist voters with ‘detecting errors’, they must:

   Establish a voter education program
   Provide voter with instructions*

*emphasis added
Who are we?

Project Personnel

Pennsylvania State University Team
Patrick McDaniel, Principal Investigator & Team Lead

Kevin Butler
Pennsylvania State University

William Enck
Pennsylvania State University

Harri Hursti
Independent Contractor

Steve McLaughlin
Pennsylvania State University

Patrick Traynor
Pennsylvania State University

University of Pennsylvania Team
Matt Blaze, Team Lead

Adam Aviv
University of Pennsylvania

Pavol Černý
University of Pennsylvania

Sandy Clark
University of Pennsylvania

Eric Cronin
University of Pennsylvania

Gaurav Shah
University of Pennsylvania

Micah Sherr
University of Pennsylvania

WebWise Security, Inc.
Giovanni Vigna, Team Lead

Richard Kemmerer
WebWise Security, Inc.

Davide Balzarotti
WebWise Security, Inc.

Greg Banks
WebWise Security, Inc.

Marco Cova
WebWise Security, Inc.

Viktoria Felmetsger
WebWise Security, Inc.

William Robertson
WebWise Security, Inc.

Fredrik Valeur
WebWise Security, Inc.

Policy and Document Consultants

Joseph Lorenzo Hall
University of California, Berkeley

Laura Quilter
University of California, Berkeley
ES&S Structure

- County, Election, and Candidate Data
  - Election Data Manager

- Ballot Design, Layout, and Audio
  - ES&S/iVotronic Image Manager
  - Hardware Programming Manager

- Removable Media
  - M100/M650/iVot Voting and Tabulation

- Election Results
  - Election Reporting Manager
Computerized Voting

• Direct Recording Electronic (DRE)
  – specialized voting computer, typically with touch-screen interface
  – records voter selections internally

• Precinct Counted Optical Scan
  – voter fills out a paper ballot (fill in circles)
    • ballot marking devices can assist disabled
  – voter inserts ballot into precinct ballot reader, which either accepts ballot and records vote or rejects and returns ballot to voter

• Centrally (County) Counted Optical Scan
  – absentee ballots
The Horror, the Horror
27.8 Hart VBO Vulnerabilities
   27.8.1 The VBO record is easily manipulable by an eSlate program
   27.8.2 VBO printer allows the paper to be rewound
   27.8.3 VBO ballots are printed sequentially
27.9 Hart Tally Vulnerabilities
   27.9.1 The Tally interface allows a Tally administrator to “adjust vote totals”
   27.9.2 Precinct IDs are improperly handled by the system
   27.9.3 Users can tally unclosed or corrupted MBBs
   27.9.4 MBBs are only processed if the Tally database allows it
   27.9.5 Rally and Tally allow a user to accept previously unrecognized certificates
27.10 Hart Ballot Now Vulnerabilities
   27.10.1 Ballot Now ballot counters are stored in a database

28 Hart Private Report - New Issues
28.1 Hart General Vulnerabilities
   28.1.1 An MBB image can be copied and restored without any credentials.
   28.1.2 EMS systems make improper use of the Windows registry
   28.1.3 Hart EMS passwords can be bypassed
   28.1.4 Hart EMS audit logs can be modified or erased
28.2 Hart eCM Vulnerabilities
   28.2.1 eCM keys may be quietly recorded to a debug file
28.3 Hart eScan Vulnerabilities
   28.3.1 The flash memory containing the eScan executable and file system can be replaced
   28.3.2 The eScan runs a telnet server
   28.3.3 The eScan scanner surface can be occluded to affect ballot processing
   28.3.4 The eScan ballot box collecting votes allows vote order to be reconstructed
   28.3.5 The eScan ballot box is vulnerable to attacks that may destroy ballots
   28.3.6 The eScan may be modified to allow casting of duplicate ballots
   28.3.7 The eScan has an open interface allowing erasure of vote and audit log records
   28.3.8 The Premier ballot box key works in the Hart ballot box
   28.3.9 New Vulnerability 09
28.4 Hart JBC Vulnerabilities
   28.4.1 The JBC can rapidly create an unlimited number of access codes on election day
   28.4.2 The JBC has an open interface allowing erasure of vote and audit log records
   28.4.3 JBC/eSlate voting can be completely automated
28.5 Hart VBO Vulnerabilities
   28.5.1 The VBO Printer is controlled via an accessible 1/8” port
   28.5.2 The serial number of the VBO can be modified
   28.5.3 The VVPAT paper record may be forged
28.6 Hart Tally Vulnerabilities
   28.6.1 Tally is susceptible to eavesdropping
   28.6.2 Tally is susceptible to replay attacks
   28.6.3 Tally is susceptible to man-in-the-middle attacks
Sorry there are so few, we were limited on time.
Lines of Code vs. % of Market Share*

ES&S - 670000+ - > 40% market share
Premier- 334000+ - > 40% market share

Other > 20%:
Hart - 300000+
Sequoia - 800000+

*sorry, there’s no correlation
My Buffer Overfloweth
If it’s good enough for a minibar...
Any Port in a Storm
“With a little token...”
“Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin”
-- John Von Neumann, 1951

“Random numbers should not be generated with a method chosen at random”
-- Donald Knuth, The Art of Computer Programming Vol 2

“The best defense against logic is ignorance”
-- anon

Well… it has passwords and encryption.
It’s not a backdoor, it’s a feature
i’m in ur DRE, changin’ ur votes
Micah's hands
EVEREST software installed :)

**REPORTS**
- FORMAT
- GRAND TOTALS
- PREC. PROCESSED
- TOTALS BY PRECINCT
- LAST PRECINCT

**MODE**
- ABSENTEE

**Buttons**
- STOP
- START
- LAMP TEST
PennState alternative voting-OS Linux
PennState alternative voting-OS Linux Red Team

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands before booting, or 'c' for a command-line.
<table>
<thead>
<tr>
<th>Favorite Ohio President</th>
<th>Minister of Art</th>
<th>Commissioner for The Nat Pastime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Vote for ONE</td>
<td>Vote for ONE</td>
</tr>
<tr>
<td>James A. Garfield</td>
<td>George Bellows</td>
<td>Kenisaw M. Landis</td>
</tr>
<tr>
<td>Ulysses S. Grant</td>
<td>Robert Henri</td>
<td>Jack Niclaus</td>
</tr>
<tr>
<td>Benjamin Harrison</td>
<td>Maya Lin</td>
<td>Annie Oakley</td>
</tr>
<tr>
<td>Rutherford B. Hayes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>William McKinley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>William H. Taft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Favorite Ohio President</td>
<td>Minister of Art</td>
<td>Minister of Space Travel</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Ulysses S. Grant</td>
<td>Robert Henri</td>
<td>Nancy Currie</td>
</tr>
<tr>
<td>Benjamin Harrison</td>
<td>Maya Lin</td>
<td>John Glenn</td>
</tr>
<tr>
<td>Rutherford B. Hayes</td>
<td></td>
<td>William McKinley</td>
</tr>
<tr>
<td>William H. Taft</td>
<td></td>
<td>Write-in</td>
</tr>
<tr>
<td>James A. Garfield</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Favorite Ohio President</td>
<td>Minister of A</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>Vote for ONE</td>
<td>Vote for ONE</td>
<td></td>
</tr>
<tr>
<td>Ulysses S. Grant</td>
<td>Robert Henri</td>
<td></td>
</tr>
<tr>
<td>Benjamin Harrison</td>
<td>Maya Lin</td>
<td></td>
</tr>
<tr>
<td>Rutherford B. Hayes</td>
<td>George Bello</td>
<td></td>
</tr>
<tr>
<td>William McKinley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>William H. Taft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>James A. Garfield</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Give me an R
Give me a U

Unlimited Votes
• Give me a C -
  Cast multiple votes,
  Erase audit logs
  Disable VVPAT
  Zero Totals
  IOW, *Anything*
What’s that Spell?

PRUC!

of course it may spell PRUC, but it means...
VIRAL PROPAGATION
Conclusions

• All academic, right?
Conclusions

• All academic, right?
• Unsafe at any speed.
Conclusions

- All academic, right?
- Unsafe at any speed
- What can you do?
Conclusions

• All academic, right?
• Unsafe at any speed
• What can you do?
  – VOTE!
Conclusions

• All academic, right?
• Unsafe at any speed
• What can you do?
  – VOTE!
  – Become a Poll Worker
Conclusions

• All academic, right?
• Unsafe at any speed
• What can you do?
  – VOTE!
  – Become a Poll Worker
  – Build a better system
WE ARE GOING TO WIN ANYWAY.

CATS: ALL YOUR VOTE ARE BELONG TO US.