Ohio Election Voting Systems: The EVEREST Report

Prof. Patrick McDaniel
NSRC Industry Day
October 7, 2008
The hanging chad ...

*Thanks to Doug Jones for hanging chad pictures.
Concerns raised about electronic election systems

- Led to studies in California TTBR, Florida, and Connecticut
- Question: what is the impact in Ohio?

Goals

- Uncover software or security problems that affect the accuracy, integrity, auditability, or voter privacy of an election.
- Identify and confirm, to the degree possible, procedures that would mitigate or eliminate discovered problems.

Note: This talk focuses on the academic team report.
Mandate

• Academic researchers role/what is not our role?

"The art of war teaches us to rely not on the likelihood of the enemy's coming, but on our own readiness to receive him; not rely on the chance of his not coming, but rather on the fact that we have made our position unassailable."

-- Sun Tzu, The Art of War

• What is the project scope?

  ▸ Election Systems and Software (ES&S)
  ▸ Premier Election Solutions [previously Diebold], (Premier)
  ▸ Hart InterCivic (Hart)
Key Findings

• The team found, for *all studied systems*:

  1. Previously known or suspected security issues continue to exist in Ohio election systems

  2. Newly discovered exploitable hardware and software security failures exist, others suspected not known yet

  3. The increasing instability of Ohio voting systems is a cause of growing concern

*What remains*: how did we arrive at these conclusions?
Precinct Election Equip.

Management Station

Optical Scanner

DRE
County HQ Equip.

• Election management systems (EMS)*
  ‣ Create ballots
  ‣ Initialize vote counters
  ‣ Tally votes
  ‣ Produce reports
  ‣ Audit election activities

• High-speed optical scanners
  ‣ absentee votes, central counts

* Generally EMS systems are general purpose Windows systems.
How an election works

- **Election Official**
- **Printed VVPAT**
- **Results**

**Printed VVPAT**

**Results**

**County Election HQ**

**Polling Place**

**Election Official**

**Ballot Definition**

**Election Official**

**Precinct Mgmt. Station**

**Electronic Pollbook**

**Voter Authorization**

**Optical Scanner**

**Ballot**

**Voter**

**Token**

**Poll Worker**

**Token**

**VVPAT Printer**

**DRE**

**Token**

**Voter**

**Token**

**Results**
The Science of Security

• How do know when you find a problem?

• Vulnerability identification
  ‣ Establish the existence (causality)
  ‣ Demonstrate
  ‣ Document
  ‣ Independent confirmation

• Note: you are not supposed to believe us (or anybody else). Science is about the ability to independently confirm the hypothesis.
What are we looking for?

- Can the election be affected by attacker?
  1. Change election results
  2. Expose voter choices
  3. Prevent votes from being cast or counted
  4. Cast doubt on the electoral process or results

- Who should we consider as potential attackers?
  - Voters
  - Poll workers and other election officials
  - Vendors
  - Outsiders
  - (Basically everyone ...)

Systems and Internet Infrastructure Security Laboratory (SIIS)
Methodology

• Source-code/design analysis
  ‣ Read and manipulate the “instructions” to tease out their behavior to discover ways to manipulate the system
  ‣ Find poor quality designs, errors in coding, or hidden functionality (e.g., diagnostic modes)

• Red-teaming
  ‣ Misuse equipment, build attacker tools, penetrate
  ‣ Uncover poorly designed interfaces
  ‣ Abuse open functionality
  ‣ Force unanticipated error conditions, etc.
The study

• Starting point: assume nothing from prior studies
  ‣ But use them as guide to understanding

• PSU Team: Hart/Premier
  ‣ JHU/Florida/California studies
  ‣ reported vulnerabilities span a range of systems

• UPenn/WebWise Team: ES&S
  ‣ UPenn Source Code
  ‣ WebWise Red-teaming
Findings

"All of the studied systems possess critical security failures that render their technical controls insufficient to guarantee a trustworthy election."

-- pp. 3, EVEREST Academic Report

- Improper use or implementation of security technology
- Failure to provide for trustworthy auditing
- Insufficient security
"Our analysis suggests that the ES&S Unity EMS, iVotronic DRE and M100 optical scan systems lack the technical controls necessary to guarantee a trustworthy election under operational conditions."

-- pp. 29, EVEREST Academic Report

- Failure to protect election data, software, and hardware
- Failure to protect administrative interfaces
- Failure to use or implement security apparatus
Premier

"... [T]he Premier system lacks the technical protections necessary to guarantee a trustworthy election under operational conditions. Flaws in the system ... lead to a broad spectrum of issues that undermine the voting system’s security and reliability."

-- pp. 103, EVEREST Academic Report

- Failure to protect (data) integrity and privacy
- Failure to protect from malicious insiders
- Pervasive failure to follow security best practices
"... [the] Hart system lacks the technical protections necessary to guarantee a trustworthy election under operational conditions. The [system provides] numerous opportunities to manipulate election outcomes or cast doubt on legitimate election activities."

-- pp. 197, EVEREST Academic Report

- Failure to provide trustworthy auditing capability
- Failure to protect (data) integrity and privacy
- Failure to document and limit unsafe features
- Failure to protect from malicious insiders
Voting system stability

• Election systems are complex multi-faceted software systems that are continuously upgraded with features and bug fixes.

• An axiom of software engineering is that such system’s reliability declines over time, due to the general entropy created by many changes to the original designs, often from engineers not present or aware of the underlying design rational.
Summary

• Universal findings:
  ‣ Low quality designs
  ‣ Deeply flawed implementations
  ‣ Poor maintenance - fragile software
  ‣ Audit failures - if you have a problem, you will not know it

*Consequence*: exploitable systems
Where are we ...

• An information security perspective ...

• Attacks of opportunity: one must assume that the adversaries have as much or more access, have incredible expertise and are highly funded and motivated.
  ‣ Teams were able to penetrate these systems in days or weeks.

**Consequence**: how you form procedures is key
Thank you.

Patrick McDaniel (mcdaniel@cse.psu.edu)

http://www.sos.state.oh.us/sos/info/everest.aspx