Project Everest

Ohio Secretary of State Commissions an E-Voting Security Review

http://electiondefensealliance.org/project_everest_security_review_ohio_e_voting_systems

In 2007, Ohio Secretary of State Jennifer Brunner ordered **Project Everest**, a security analysis of the electronic voting systems (both touch screen and optical scanners) used in Ohio, based on an earlier study commissioned by California Secretary of State Debra Bowen. Three different academic teams were hired, one for each of the e-voting system manufacturers of machines used in the state. **In the end, the recommendation was to discontinue all of them.**

The University of Pennsylvania team handled the Election Systems & Software (ES&S) systems. In the aftermath, a video was made of them describing their experience and what they found. The entertaining video, called Hacking Democracy (a nod to the HBO-produced move of the same name), is available on YouTube at

https://www.youtube.com/watch?v=YR83iD01YvM

They analyzed ES&S's iVotronic touch screen, its local and large-batch optical scanners (M100 & M650), and its "Unity" EMS (election management software). The video is an occasionally jaw-dropping sequence of revelations of Swiss cheese security. This page is a brief summary of only the optical scanners, since Maine uses ES&S optical scanners.

> **IMPORTANT:** Although the M100 and M650 were the previous generation of ES&S systems, and thus their relevance to today's DS200 and DS850 systems might seem limited, it should be noted that they passed federal and initial state certification before the massive number of security holes were revealed. **So there is no guarantee that the current systems are immune from such problems.**

Some of the general problems they found with all systems:

- Locks: these were simple wafer locks, pickable with a paper clip
- Keys: there were 2 keys, which were easy to make, and they were the same for every machine!
- Seals over sockets for removable media: tampering with these was supposed to leave evidence, but they could be removed with steam or WD40, andcould be bought from the manufacturer listed on the seals.
- Ports: there were many open ports, including ethernet or modem ports
- Printer port:
  - Access to the port allowed printing of whatever you'd want on the audit trail.
  - The connecting plug was easy to pull out (voters did it),
  - Pulling the plug disabled the audit trail, making tampering invisible

Some of the problems they found with the Optical Scanners:

- Both local and batch scanners: No password required for removable media, insert and uploads firmware auto
- No encryption on results on removable media, can alter with no trace
- Useless locks allow access to glass, put post-it note to block undesireds
- forge-able paper ballots -- non-read ink security, if sees anything where this is used (e.g., photocopy, which makes readable marks), notes possible counterfeit, but if you make a copy and then white out those sections, no problem. Might be noticeable, so best to replace security, but can't buy black, so make it by mixing colors of ink-jet cartridge.
- Can put malicious code on removable media, which goes to central tabulator and uploads and runs.

The Presentation Slides

Below are the optical-scanner-related slides they used in their presentation, with an approximate time stamp as to where they occur in the video (Note: EMS = election management system, PEB = personal electronic ballot). Note in particular the "Quick Summary" slide in the "Analysis" section on the next page.

Optical Scanner Overview

https://www.youtube.com/watch?v=lE5REYsnsXE&t=1746

e-voting, in practice (25:57)
- County election management software
  - ballot definition & printing
  - voting machine configuration / provisioning
  - election day operations
  - tallying and auditing
- Voting machine firmware
  - DRE and optical scan
- Communications (machines <-> backend)
  - typically via removable media
- Procedures, physical security, people
  - huge temporary workforce

Some attacks against e-voting (26:13)
- Denial of service
- Alteration of precinct counts
- Forgery of precinct counts
- Compromise of official tally
- Compromise of machine firmware
- Compromise of ballot display
- Compromise of audit/recount data
- Compromise of ballot secrecy
- Viral propagation

ES&S Precinct Optical Scan: M100 (29:06)
- Portable optical scan ballot reader
- Attaches to ballot box
- Accepts or rejects ballots
  - maintains tallies for accepted ballots
- Internal memory card holds ballot definition and tallies
  - returned to county at end of day

M100 Software (30:11)
- Intel x86 processor
- About 30,000 lines of code
  - C, assembler, scripts
- Plus code in backend system for provisioning and tallying
  - stay tuned

ES&S Central Count: M650 (30:20)
- High speed batch ballot counter
- Big, heavy, expensive
  - typically one per county
- Used for counting absentee ballots at county and for recounts
- Communicates with backend via Zip drives
  - ballot definition and tally

M650 software (31:12)
- Intel x686 processor
- About 22,000 lines of code
  - C, C++, scripts
- Plus code in backend system

ES&S Backend EMS: "Unity" (31:13)
- Comprehensive election management software suite
  - ballot definition
  - provisioning of iVotronic, M100, M650
  - tallying and results reporting
  - audit and recount
- Runs on Windows PC in county office
  - Can be networked via Windows file sharing
  - Hardware for reading PEBs, memory cards, etc.

Unity Software (32:19)
- Standard Windows platform
- About 400,000 lines of code
  - C, C++, SQL, Visual Basic, COBOL
    - yes, COBOL
- Includes modules to provision and tally for iVotronic, M100, M650

Optical Scanner Analysis Slides

https://www.youtube.com/watch?v=lE5REYsnsXE&t=2501

Quick Summary (34:26)

- **We could compromise virtually every component of the ES&S system (OPScan and touch screen)**
  - alter/forge precinct results
  - alter firmware in precinct equipment
  - erase / tamper with audit records
  - use altered precinct data to attack central EMS
  - viral propagation across elections
- **Serious, practical, undetectable attacks can be carried out by individual voters and pollworkers**
- **Not easily mitigated by improved procedures**

OK, what about the optical scan system? (41:49)

- Precinct results easily tampered with
  - no cryptographic protection on MCMCIA results media
- Precinct scanner firmware easily tampered with
  - firmware loaded through PCMCIA card
  - viral propagation to/from backend
- Central scanner firmware easily tampered with
- Every lock and seal easily defeated

Consequences (46:27)

- With project EVEREST, we learned that every current e-voting system has serious exploitable vulnerabilities
  - ES&S, Hart, Premier, Sequoia have now all comprehensive independent review
- The certification and testing process seems to be a failure
- All of the systems are far below the standard normally associated with high assurance systems.