You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems

J. Alex Halderman
Princeton University

Eric Rescorla
RTFM, Inc.

Hovav Shacham
University of California, San Diego

David Wagner
University of California, Berkeley

Motivation

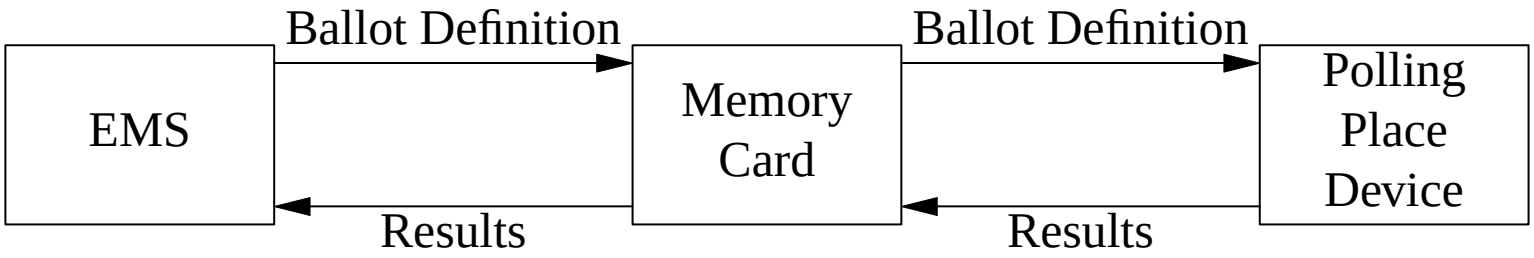
- All electronic voting systems studied have serious vulnerabilities
- Election officials have been deploying mitigations
  - Designed under tight time pressure
  - Limited input from security experts
  - Not clear how well these work
- Can we do better?

"With new but realistic procedures; with no changes to existing hardware; and with few and modest changes to existing software, how can we best secure elections?"

Basic Assumptions

- Threats
  - Software will remain vulnerable
  - Hardware will remain only modestly resistant to physical attack
  - Polling places have little physical security
  - Compromise is undetectable and irreversible
- Unfortunate limitations
  - County headquarters is kept physically secure

Main concern is viruses



- All studied systems can be subverted with minimal unsupervised access
- Polling place devices are poorly protected
  - Voters; poll workers; sleepovers
- Subverting a single machine isn't very useful
  - Too expensive to individually subvert every machine
- But viruses allow a single attacker to compromise the entire county

Managing Viral Spread

- We can't harden the polling place devices
  - Must assume that they will get infected
  - Objective is to prevent spread
- Vectors
  - EMS, Memory cards, Polling-place networks
- General principle: break dataflow cycles
  - All external machines assumed dirty
  - Avoid connecting dirty machines to clean machines
  - Once a machine is dirty, it's always dirty
  - Build safe(r) replacements for potential vectors
- Need to handle both in and out directions

Election Phases

- Device initialization
- Voting
- Early reporting
- Tabulation
- Auditing

Device Initialization

- Devices need to be programmed before each election
  - Load ballot definitions
  - Zero vote counters
- Generally done with a memory card
  - Program cards with EMS
  - Disseminate cards to field
- Cards get recycled through EMS
- This is an obvious infection vector

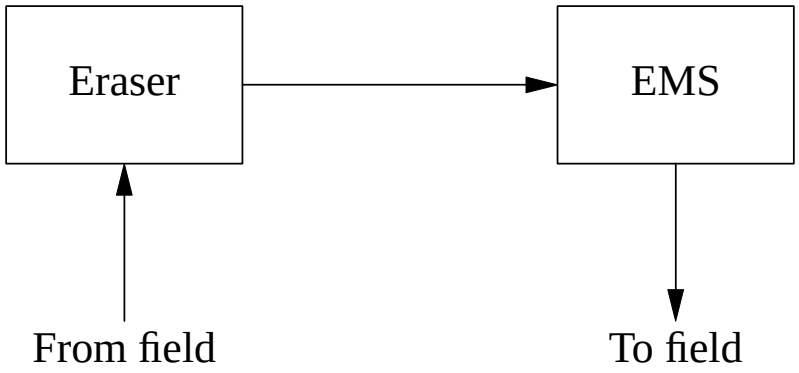
Initialization With Single-Use Memory Cards

- Use a new card for each election
  - Buy fresh cards
  - Initialize with trusted EMS
  - Deploy to field
  - When finished, discard or archive
- Logistical issues
  - Cost: \$20-\$100/card (~\$10 for CF + adaptor) = \$0.10/vote
  - Brittle if cards if are not handled carefully
  - Many systems use custom/legacy cards

Living With Reusable Cards: Initialization Gadgets

- Instead of an eraser, use a special purpose initialization gadget
  - EMS produces card images on CD
  - Initialization gadget copies CD to card
  - Gadget requires a hardware reset between cards
- Gadgets is not a vector for viral spread (unlike EMS)
  - Even if it has vulnerabilities, the reset clears infection
- No guarantee that malicious cards get cleared
  - Cards *must* be mated to their devices
  - ... otherwise we get increased infection each cycle
- This is logistically extremely tricky

Why not just erase the cards?



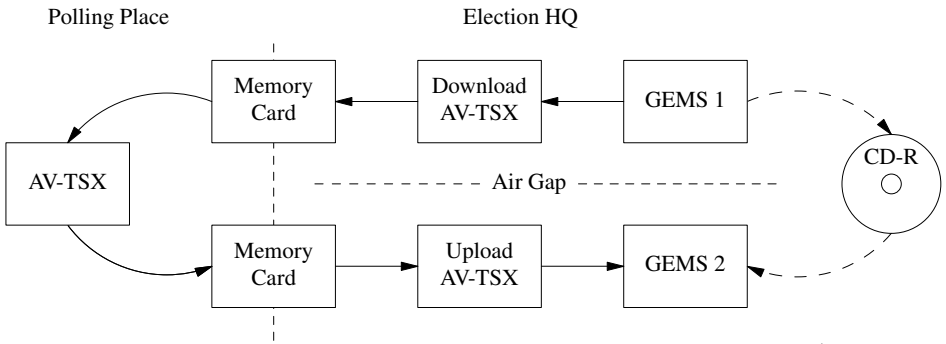
- Recommended by [Cal07a, Cal07b, CFH+07]
- Not possible to guarantee erasure
  - "Memory cards" are flash memory + a microcontroller
    - Some have replaceable firmware
    - Fake card?
  - What about bugs in the eraser?
- This does not guarantee safety of the EMS

How to build stateless gadgets

- Best case: new hardware
  - Firmware lives in ROM
  - Simple interface with hardware reset
- More likely: single-purpose computers
  - Boot from read-only media
  - We still have to worry about BIOS infection
  - Need to guarantee hard power switch
- What about VMs?
  - Now we're depending on security of the VM [VMw08]

Early Reporting

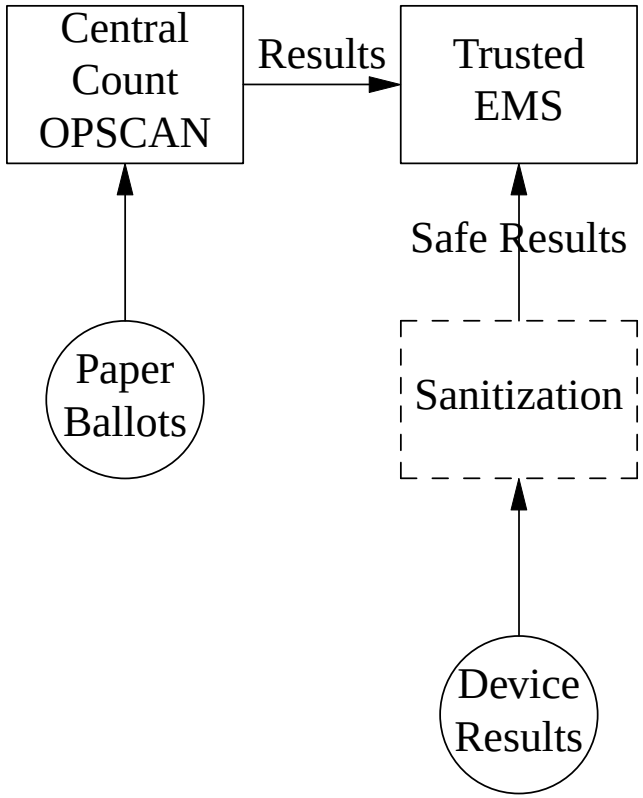
- Many jurisdictions want election-night results
  - One of the major value propositions of e-voting



From [CFH+07]

- Use a *sacrificial* EMS [CFH+07] and wipe after election
- No guarantee of correct results
  - A single infected card can compromise the EMS and all results
- Only safe with single-use cards
  - Requires extraordinarily careful procedures

Tabulation With Sanitization



- Sanitize the results prior to reading into EMS
  - Narrow input envelope
- Tabulate/aggregate the results as normal

Sanitization Options

- Transcribe results tapes
  - Estimated cost: \$1-\$10/tape $\rightarrow$ \$0.10/vote
  - What about latency?
    - Can this be contracted out?
  - Information density too low to carry shellcode
- OCR?
  - Current tapes cannot be reliably scanned [Fel08a]
  - Maybe add error correction/2-d bar code
- What about vulnerabilities in image processing/OCR code?

Auditing (1)

- Objectives
  - High confidence in accuracy
  - Transparency
  - Preserve vote privacy
- We don't have improvements here
  - Current precinct-based audits are less statistically powerful than we would like
    - e.g., A 500 precinct election requires 28% auditing to get a 99% confidence level with a 1% margin of victory
- Ballot-based auditing [CHF07] might help for opscan
  - But it's incompatible with current equipment
  - And there are privacy issues
- This is an open problem

Auditing (2)

- DRE with VVPAT
  - Auditing VVPATs is very inconvenient [GB07]
  - Lots of attacks even when a VVPAT is used [Eve07]
  - Some hope for spoiled ballot auditing
    - Not completely worked out yet
    - Also some attacks [Cra06]
- DRE without VVPAT
  - No practical audit mechanisms
  - Easy for attackers to harmonize electronic records
  - And not clear what to do when they don't match [Fel08b]

Deployment Scenarios (descending order of security)

- Opscan + Electronic ballot markers
  - Scan twice: precinct + central count with harmonization
  - Precinct count plus viral containment
  - Pure central count
- Opscan + DRE for accessibility
  - Do 100% manual recount of VVPAT (DRE as EBM)
- Pure DRE
  - 100% manual recount is impractical
  - Viral containment becomes imperative
  - If no VVPAT recovery seems unlikely

Summary

- Objective is to do the best we can with what we have
- So, how well did we do?
  - Containment of viral spread from polling place devices
    - But not the other way around!
  - Correct tabulation—even if some devices are compromised
  - Some detection of individual compromised devices
- Residual risks
  - Insider attack still possible
  - Limited ability to recover from DRE compromise
  - Auditing is still more expensive than we would like
- Still plenty more work to do

Questions?

References

[Cal07a] California Secretary of State. Withdrawal of Approval of Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & Optical Scan Voting System and Conditional Reapproval of Withdrawal of Approval of Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSX/AccuVote-OS DRE & Optical Scan Voting System. Part of [Cal07c], October 2007.

[Cal07b] California Secretary of State. Withdrawal of Approval of Sequoia Voting Systems, Inc., WinEDS v 3.1.012/AVC Edge/Indsight/OPTECH 400-C DRE & Optical Scan Voting System and Conditional Reapproval of Use of Sequoia Voting Systems, Inc., WinEDS v 3.1.012/AVC Edge/Indsight/OPTECH 400-C DRE & Optical Scan Voting System. Part of [Cal07c], October 2007.

[Cal07c] California Secretary of State D. Bowen. "Top-To-Bottom" Review of voting machines certified for use in California, 2007. Online: `http://sos.ca.gov/elections/elections_vsr.htm`.

[CFH+07] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller. Source code review of the Diebold voting system. Part of [Cal07c], August 2007.

[CHF07] Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Machine-assisted election auditing. In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 07)*, August 2007.

[Cra06] Ronald E. Crane. Paper Trail Manipulation III. NIST Workshop on Developing an Analysis of Threats to Voting Systems, November 2006. http://vote.nist.gov/threats/PaperTrailManipulationIII1.pdf.

[Eve07] Sarah Peterson Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. PhD thesis, Rice University, 2007.

[Fel08a] Ed Felten. Evidence of New Jersey Election Discrepancies. http://www.freedom-to-tinker.com/?p=1266, March 2008.

[Fel08b] Ed Felten. NJ Election Discrepancies Worse Than Previously Thought, Contradict Sequoia's Explanation. http://www.freedom-to-tinker.com/?p=1274, April 2008.

[GB07] Stephen N. Goggin and Michael D. Byrne. An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots. In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 07)*, August 2007.

[VMw08] VMware. VMware Security Advisory VMSA-2008-0005.1. http://www.vmware.com/security/advisories/VMSA-2008-0005.html, March 2008.

Bonus Slides

Example: Diebold Virus [CFH+07]

- Voter inserts infected memory card into AV-TSX
- AV-TSX automatically installs new software (Issue 5.2.1)
- Infected AV-TSX writes infected memory card for results
- Infected memory card placed in central office AV-TSX, infecting it
- Infected AV-TSX attacks attached GEMS (running Windows) via network
- Infected GEMS writes infected memory cards for next election
- Infected memory cards inserted into precinct AV-TSXs, infecting them

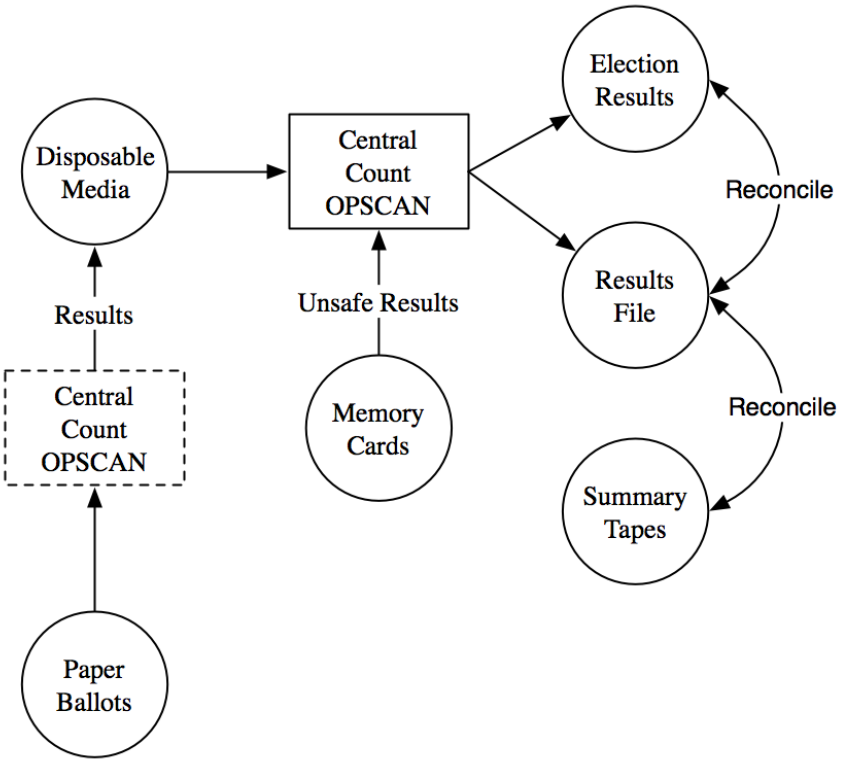
Network Initialization

- Hart's machines are also initialized via the network
  - Election definitions are on cards
  - Counter resets and cryptographic keys set via network
- Need a stateless network initialization gadget
- eSlate initialization is through the JBC
  - Need to marry eSlates and JBCs to prevent spread through this network

Firmware Updates

- We assume that election officials can verify correctness of firmware distribution
- Conventional procedure is to use a single memory card to update all devices
  - Can't guarantee card contents after first device processed
- Read only cards
  - Needs hardware enforcement
  - Can't trust card firmware
- Use same card management procedures as with initialization
  - Best to bring gadget to the machine
- No guarantees that this fixes compromised machines
  - They can refuse the update

Double-Checking Tabulation



- Tabulate on a sacrificial EMS
- Emit summary results in machine readable format
- Compare results tapes to summary entries
  - This can be done with random sampling