Weakness in Depth: A Voting Machine's Demise

August 2015

Jeremy Epstein
Senior Computer Scientist
SRI International
Arlington VA

Disclaimer

- I am employed by SRI International
- I am on loan (IPA) to the National Science Foundation
- Nothing I am about to say represents the position of SRI, NSF, the US Government… and maybe not of the speaker

Outline

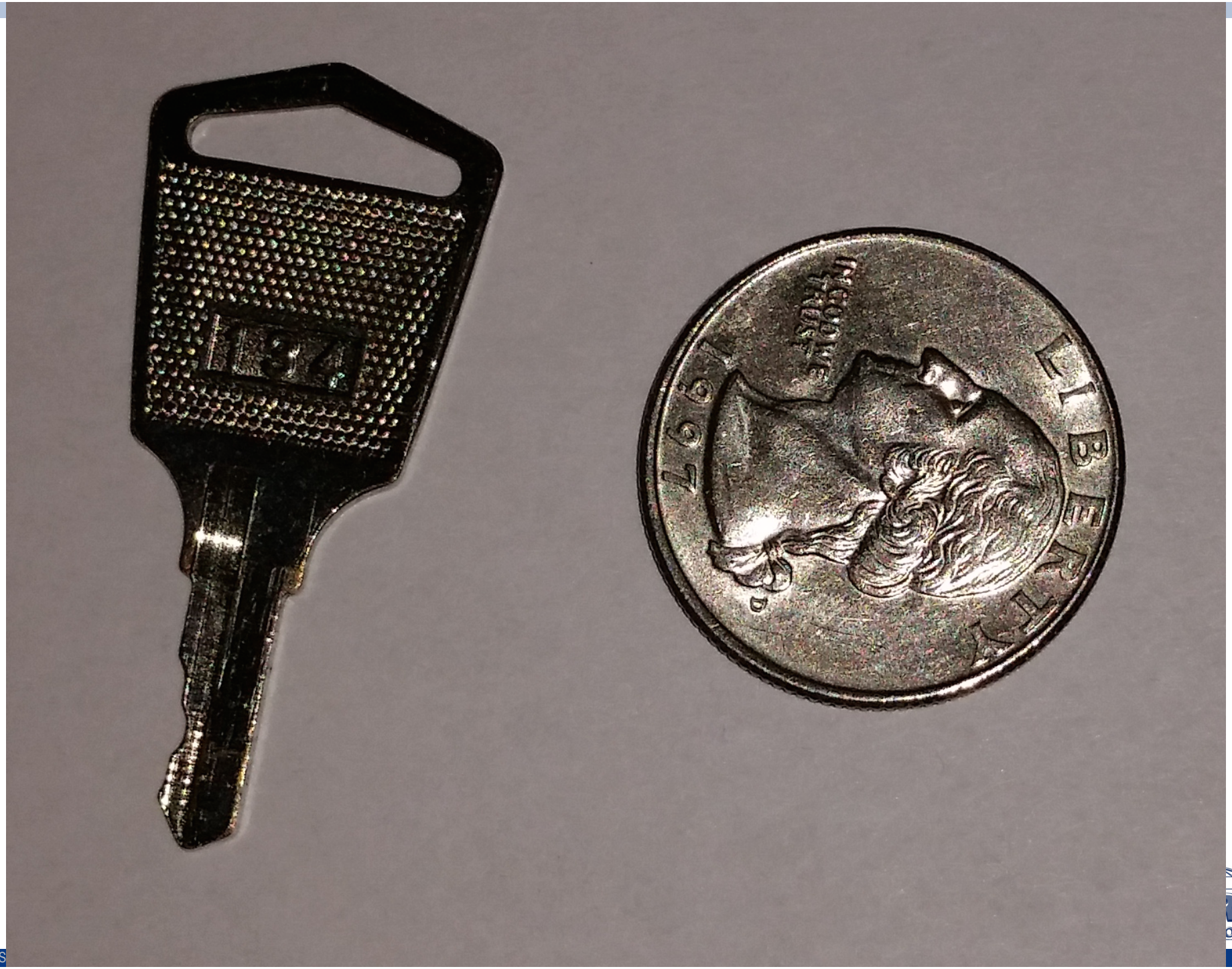
- WinVote system architecture
- The Virginia report
- Pennsylvania certification report
- What else we knew
- Lessons learned

Start with a quiz

Diebold Accuvote TSX

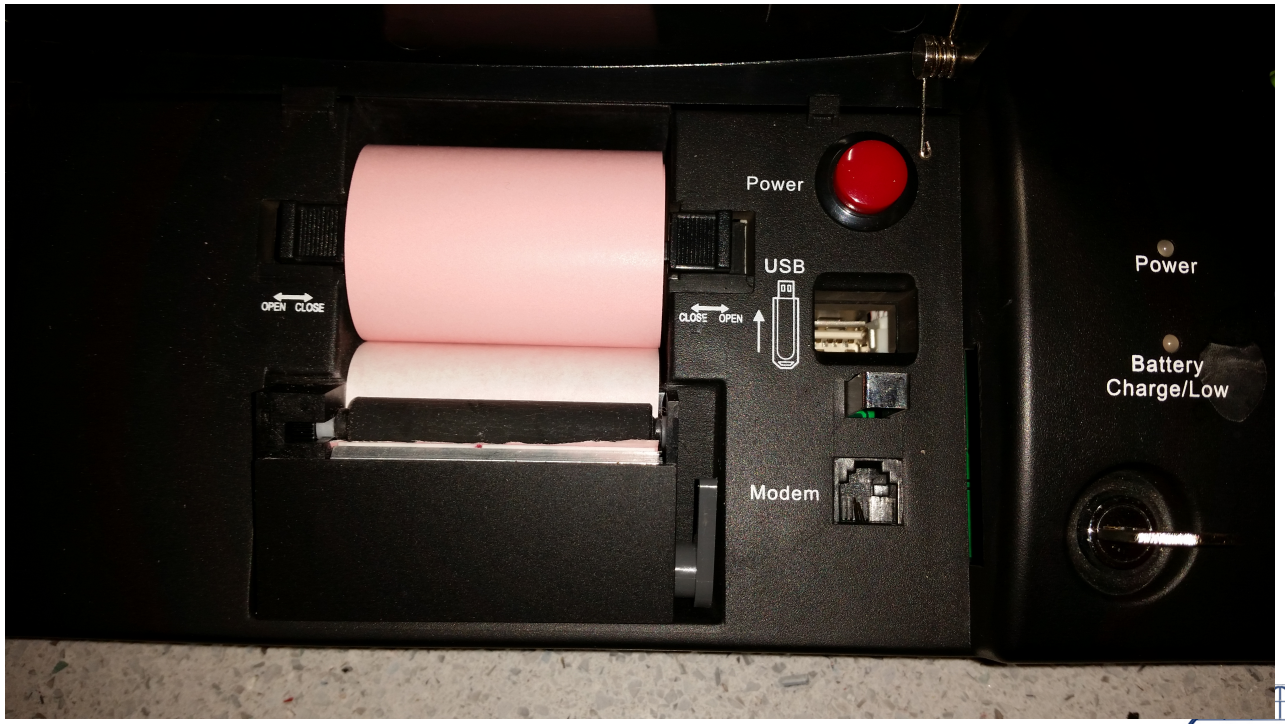
Hotel minibar

AVS WinVote


LIBERTY
1964
D

System Architecture

- Touchscreen running Windows XP
- Thermal paper printer and USB behind (trivially) locked door
- Printer used for zero tape and end of day totals
- Microsoft Jet / Access application



Weaknesses

- OS is Windows XP (Embedded?)
- No patches installed since 2004
- Wireless uses WEP with a hardwired key “abcde”
- Wireless can’t be turned off
- Admin password is “admin”
- File services are on, and can’t be turned off from admin interface
- Data stored in obsolete version of MS Access with hardwired key of “shoup”
- No logs to record changes

… plus physical security problems (minimally protected USB ports with autorun enabled)

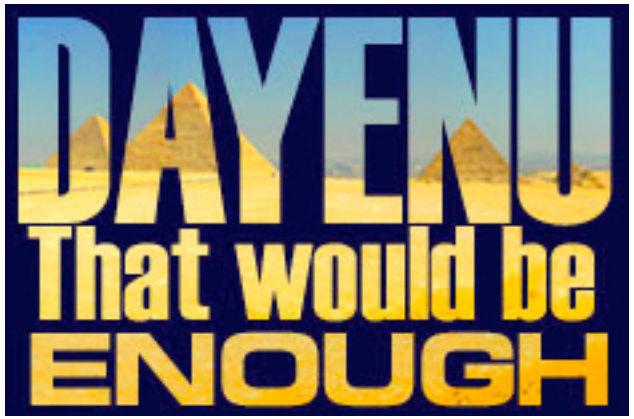
Steps to Modify an Election

1. Take your laptop to a polling place, and sit outside in the parking lot.
2. Use a free sniffer to capture the traffic, and use that to figure out the WEP password (which VITA did for us).
3. Connect to the voting machine over WiFi.
4. If asked for a password, the administrator password is “admin” (VITA provided that).
5. Download the Microsoft Access database using Windows Explorer.
6. Use a free tool to extract the hardwired key (“shoup”), which VITA also did for us.
7. Use Microsoft Access to add, delete, or change any of the votes in the database.
8. Upload the modified copy of the Microsoft Access database back to the voting machine.
9. Wait for the election results to be published.

All Before We Even Look at Voting Software…

- Even if the software written by the vendor is perfectly designed and implemented
- Even if every piece of hardware is stored completely securely
- Even if every piece of hardware is delivered completely securely
- Even if every election official is honest and avoids any mistakes
- Even if every pollworker is honest and avoids any mistakes

- … even then, the WinVote system is completely vulnerable!



How did we get here?

- Advanced Voting Solutions WinVote was first of a “new generation” of voting systems
  - Accepted and used in Virginia, Pennsylvania, Mississippi
  - Used in about 30 VA localities, some reliability problems
  - Subsequently decertified in PA because of security problems; in MS for reliability
- Certified in 2004 as meeting 2002 VSS
  - Security assessment was not part of the standard
  - Tried & failed to recertify against newer standards
  - Company went out of business in about 2008
- It’s a somewhat cut down version of Windows XP
  - Early version of the software was an unmodified installation (e.g., included Minesweeper, which worked quite well!)

Virginia Legislative Activity

- Hugo Commission ("Virginia Legislature Joint Subcommittee on Voting Equipment Certification Process"), 2005
  - Not specifically focused on AVS, but DREs in general
  - Brit Williams (examiner for Virginia) said he didn't know how to do a penetration test
  - Does it use WEP or WPA? AVS people didn't know
- Result was bill to prohibit purchase of more DREs, but no sunset on existing equipment
  - Goal of advocates was to force replacement as a result of machine failure and population growth

Trying to Reduce the WiFi Risk

- Virginia 2007 SB840: Prohibits use of WiFi in polling place
- Banning WiFi was unpopular with election officials because:
  - Increased time to prepare machines for an election
  - Increased end-of-day reconciliation and error rate
- Virginia 2008 SB52: Repeals ban after discovery that WinVote won't boot if WiFi disabled

- *The irony: Virginia has short ballots*
  - *2015: State Senate, State House, Board of Supervisors, School Board, Bonds*
  - *2016: President, Senate, House*
  - *2017: Governor, Lt Gov, Atty General, State House, Sherriff, School Bonds*

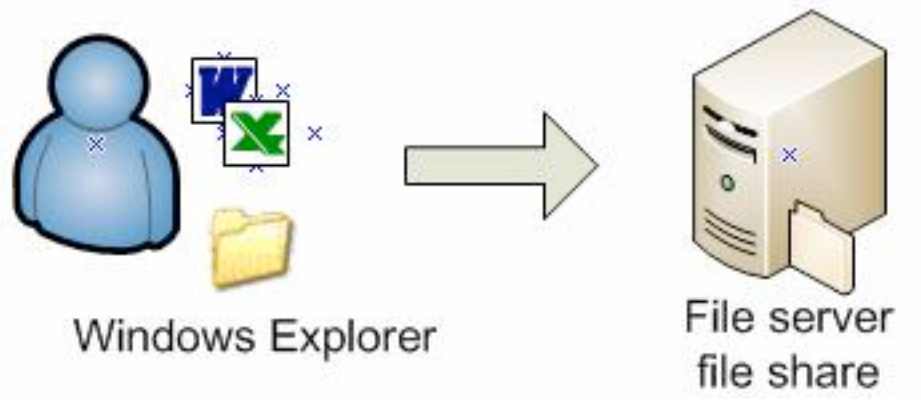
The Virginia Investigation

- Investigation started from problems with crashes in Nov 2014 election
  - Hypothesis was interference from an iPhone when downloading music
  - Never reproduced, but caused SBE to perform an examination
- Result: Virginia State Board of Elections decertified effective immediately (Apr 14 2015)
  - Localities must replace before June 2015 election
  - Some localities borrowed from neighboring jurisdictions for the June 2015 primary

Can The WiFi Be Disabled? (VITA 2015 report)

- *One additional important note is that while the WINVote application appears to have the ability to disable the wireless network from within the application, it does not disable the network interface on the device. When the wireless network is disabled using the WINVote interface, the application will no longer seek other devices on the network. Although the application will not find other systems, the device's network card remains online and will send and receive traffic even though the application indicates it is disabled. Based on VITA testing it is not possible to prevent network access by disabling the network using the WINVote application. To determine if wireless functionality could effectively be disabled by other means, VITA performed the following actions:*
  - *Physical removal of the wireless network adapter;*
  - *Disabling the wireless capability through the command line and network control panel;*
  - *Renaming the wireless zero configuration dynamic link library (dll).*
- *Both the physical removal of the wireless adapter and changes to the device software rendered the WINVote device unable to execute and administer an election.*

Or in simpler language



Disaster Missed by a Hair

Locality	Number of Precincts
Accomack	17
Appomattox	9
Arlington	
Botetourt	
Brunswick	
Buckingham	
Craig	
Dinwiddie	
Floyd	
Fluvanna	
Goochland	
Henrico	92
Henry	
Lynchburg City	18
Richmond City	65
Total Localities: 30	**568**

In 2014, Fairfax County replaced about 1200 WinVotes with DS200 scanners + ExpressVote BMDs

Pennsylvania Certification Reports

- Examination by Glenn Newkirk in 2005 of WInVote 2.0.2
  - NOTE: This is an improved version (2.0.2 vs. 1.5.4 in Virginia)
  - "The use of the wireless feature poses less a practical security issue based on interception, interference, or modification of critical data than it poses an operational issue based on creation of a situation in which poll workers become wireless LAN administrators."
  - Recommendation against use of Wireless LANs in polling places (but allowed in warehouses), but no discussion that wireless can't be turned off
  - "The Secretary recommends that Advanced [Voting Solutions] perform a periodic, independent third-party security risk and assessment review of the System's security."
  - Approved for use
- Reexamination by Glenn Newkirk in 2007 of WinVote 2.0.3
  - Unapproved hardware & software modifications
  - Reinforced that AVS needs to do what they were told previously
  - No mention of any third-party testing

Pennsylvania Decertification

- Decertification of all WinVotes in 2010
  - Have been unsuccessful in getting the report explaining why
- Was in use in three counties: Lackawanna, Northampton and Wayne
  - Northhampton County sold theirs to Kimberly Shoup-Yeahl, former president, Advanced Voting Solutions (June 2010)

What if There Were No WiFi?

- Probably comparable to other DREs
  - Vulnerable to similar types of insider threats
  - Vulnerable to unobserved voter threats (e.g., plug a keyboard in the back)
  - Will it boot from USB drive?
- Known architectural problems:
  - No logs of any sort, other than boot/shutdown
  - Effectively no encryption (as noted earlier)
  - Election master password is kept in the database (not hashed)
    - *The admin password – a six-digit random number – is embedded in the admin smartcard. The admin smartcard allowed us to access the admin functions in the WINvote, including loading a new election, resetting the election after L&A testing, running an automatic L&A, calibrating the screen, turning the wireless on/off, accessing/printing event logs, printing the ballot image.*
- Known failures:
  - 2009 local election, doubled results

What Can We Learn?

- Specifics
  - Hardwired values are dangerous (duh!)
- Threat environment changes
  - What was a risk in 2002 isn't the same as 2015
  - Computing is now everywhere; security/privacy risks are everywhere
- Reliance on closed-source isn't a solution
- How to provide updates for products that will be used for decades?
- Certification can't be once-and-you're-done
- *Need defense-in-depth, not weakness-in-depth*

Want One?

- No charge for machine
- Pay for your own shipping (about $55 within US)