I

Hacking The Machines

The Problem

A privatized electronic voting machine industry (corporations, some transnational) owns and therefore runs and controls our elections. Electronic voting machines can all be rigged: optical scan machines that use paper ballots that are then scanned electronically, and DRE's/touchscreen machines that don't use paper ballots. But take heed, anyone could hack these machines.

Some Noted Examples That Show Hacking Can Be Done To All Kinds Of Electronic Voting Machines

1. Research by Professor Edward W. Felten, Princeton University, showed that keys from hotel mini-bars, an office furniture store and those bought freely on the Internet, can open Diebold AccuVote-TS voting machines and leave no trace.[1]

2. The Vulnerability Assessment Team at the Argonne National Laboratory reported that an electronic voting machine model, Diebold AccuVote-TS, still expected to be used widely to count votes in the 2012 General Election, could be easily hacked—for about $10.50, by a student with an 8th grade science education using a remote control device. The Team states that voting results could be changed and no trace of the tampering[2] would be evident. VerifiedVoting.org has reported that over three million voters in Colorado, Indiana and Maryland will be using these machines.[3]

3. Alex Halderman (Univ of Michigan) and Ariel Feldman (Princeton), replaced the voting software of the Sequoia AVC Edge touch-screen DRE voting machine (used by almost 9 million voters in 2008) with Pac-Man.[4] They did this in three afternoons, without breaking any tamper-evident seals. "No word on plans to give Ms. Pac-Man suffrage."[5] says Kim Zetter of Wired.

4. The famous Hursti Hacks, by Finnish computer expert Harri Hursti—produced by Bev Harris and Black Box Voting—demonstrated (in multiple tests) that you can program a voting machine (Diebold Optical Scan) to do anything to votes, and with a little more work, you can make the fraud undetectable. Read the summary in the Wikipedia article[6] (has links to authoritative pages); then see "The Black Box Report," (July 4, 2005),[7] "Diebold TSx Evaluation," (May 11, 2006 and July 2, 2006),[8] and "Diebold TSx Evaluation Supplemental Report," (May 22, 2006 and July 2, 2006).[9]

5. "The federal agency responsible for inspecting voting equipment said Thursday [22 December, 2011] that a ballot scanner used in several key battleground states can freeze up without warning, fail to log errors and misread ballots." The Election Assistance Commission (EAC) [an independent agency of the US government, created by the Help America Vote Act—HAVA] put out a warning in December 2011 about ES&S DS200 IntElect optical scan electronic voting machines errors ***during voting*** [emphasis mine].[10] These machines were used in all or part of **Florida**, Illinois, Indiana, New York, **Ohio** and **Wisconsin** [emphasis mine]. Read more details on the "Politics Extra" blog at cincinnati.com[11] and on The Plain Dealer.[12] Shockingly, the machines will not be decertified. Said Brian Hancock of the EAC, "Our goal is not to decertify systems. We never want to be in a situation of putting counties in a position where they cannot run an election."

6. "Security experts have warned that electronic voting systems are decades away from being secure…,"and in a test of Washington DC's internet voting system for absentee ballots, Alex Halderman's team from the University of Michigan proved the insecurity of the system by hacking it to elect "drunken Futurama robot Bender" to be the head of the school board.[13]

7. At the RSA Conference 2012, David Jefferson, a computer scientist at Lawrence Livermore National Laboratories and chairperson of the election watchdog group Verified Voting, warned that "Internet voting systems are inherently insecure and should not be allowed in the upcoming general elections..."[14]

8. Clint Curtis, who used to be a Republican before this happened, was a computer programmer. He testified before Congress that Tom Feeney (Speaker of the House of Florida at the time) tried to pay him

to rig election vote counts by writing vote rigging software in South Florida.[15]

The Solution

Publicly observed, secure hand-counted paper ballots (HCPB) elections are the only way our votes must be counted. Votes must be hand-marked on paper ballots that are hand-counted twice at the polling place, right after the polls close, by opposing parties on the ballots, video taped and broadcast or streamed live over the internet, and results immediately posted in polling place windows for all to see. In "*Chapter XII: On-Site Observations of the Hand-Counting of Paper Ballots and Recommendations for the General Election Of 2008,"* Acton, ME could be and should be a model for the entire country (See p. 132).

This article originally appeared in Center for Hand-Counted Paper Ballots, 27 April, 2012 (http://www.handcountedpaperballots.org/documents/Hacking_the_Machines.html). Updated 13 July, 2012.

Endnotes

[1] Edward W. Felten, "Hotel Minibar Keys Open Diebold Voting Machines," Princeton University, 18 September, 2006 <https://freedom-to-tinker.com/blog/felten/hotel-minibar-keys-open-diebold-voting-machines/>.

[2] Brad Friedman, "Diebold voting machines can be hacked by remote control," 27 September, 2011 <http://www.salon.com/2011/09/27/votinghack>.

[3] VerifiedVoting.org has reported that over three million voters in Colorado, Indiana and Maryland will be using these machines. <http://www.verifiedvoting.org/verifier/searched.php?ec=allall&state=AS&equipment_type%5B%5D=All+Types&vendor%5B%5D=All+Vendors&model%5B%5D=AccuVote-TS&vvpat=all&submit=Search&rowspp=50&topicText=&stateText=>.

[4] J. Alex Halderman (University of Michigan) and Ariel J. Feldman (Princeton University), "PAC-MAN on the Sequoia AVC-Edge DRE voting machine," 09 August, 2010 <https://jhalderm.com/pacman/>.

[5] Kim Zetter, "Touchscreen E-Voting Machine Reprogrammed to Play Pac-Man," Wired, 24 August, 2010 <http://www.wired.com/threatlevel/2010/08/pac-man/>.

[6] Hursti Hack, Wikipedia, 18 May, 2012 <http://en.wikipedia.org/w/index.php?title=Hursti_Hack&oldid=493216669>.

[7] Harri Hursti, "The Black Box Report, SECURITY ALERT: 04 July, 2005; Critical Security Issues with Diebold Optical Scan System Design," Black Box Voting, July 4, 2005 <http://www.blackboxvoting.org/BBVreport.pdf>.

[8] Harri Hursti, "Diebold TSx Evaluation, SECURITY ALERT: 11 May, 2006; Critical Security Issues with Diebold TSx," Black Box Voting, Unredacted—Released 02 July, 2006, Black Box Voting <http://www.blackboxvoting.org/BBVreportIIunredacted.pdf>.

[9] Harri Hursti, "Diebold TSx Evaluation, SECURITY ALERT: 22 May, 2006; Supplemental report, additional observations," Black Box Voting, Unredacted on 02 July, 2006, Black Box Voting <http://www.blackboxvoting.org/BBVreportII-supplement-unredacted.pdf>.

[10] Gregory Korte, "Federal agency finds defects in ballot scanners," USA TODAY, 23 December, 2011 <http://www.usatoday.com/news/politics/story/2011-12-22/defective-voting-machines/52172034/1?mid=55>.

[11] "Cleveland voting machines miss votes, freeze up," Politics Extra blog (cincinnati.com) 23 December, 2011 <http://cincinnati.com/blogs/politics/2011/12/23/cleveland-voting-machines-miss-votes-freeze-up/>.

[12] Laura Johnston, "U.S. government investigation finds Cuyahoga County's election machines are flawed," The Plain Dealer, 23 December, 2011 <http://blog.cleveland.com/metro/2011/12/us_government_investigation_fi.html>.

[13] Iain Thomson, "Election hacked, drunken robot elected to school board," The Register, 01 March, 2012 <http://www.theregister.co.uk/2012/03/01/electronic_voting_hacked_bender/>.

[14] Jaikumar Vijayan, "Internet voting systems too insecure, researcher warns," Computerworld, 01 March, 2012 <http://www.computerworld.com/s/article/9224799/Internet_voting_systems_too_insecure_researcher_warns>.

[15] "Computer Programmer testifies that Tom Feeney (Speaker of the Houe of Florida at the time) tried to pay him to rig election vote counts." <http://www.youtube.com/watch?v=JEzY2tnwExs>.