



Department of Computer Science and Engineering
Building C
113 Research Drive, Bethlehem, PA 18015-4731
Office: (610) 758-3065
Web: www.cse.lehigh.edu

Senate State Government Committee
Public Hearing on Senate Bill 1249 and Voting Machine Demonstration
September 25, 2018
9:30 am 2 South Second Street Harrisburg, PA

Written Testimony of Daniel Lopresti, Ph.D.
Professor and Chair of Computer Science and Engineering, Lehigh University

September 20, 2018

Thank you Chairman Folmer, Minority Chair Williams, and members of the Committee for allowing me to submit written testimony about the subject of this hearing. The continued use of direct-recording electronic (DRE) electronic voting machines here in Pennsylvania concerns me, and I have spoken out numerous times in the past on this topic.

Since 2009, I have served as Professor and Chair of Computer Science and Engineering at Lehigh University in Bethlehem, PA. Prior to joining Lehigh in 2003, I spent 11 years in industrial research, including five years at Bell Labs. I started my career on the faculty at Brown University and received my Ph.D. in computer science from Princeton University in 1987. At a national level, I am a member of the Computing Research Association's Computing Community Consortium Council, where I co-chair the Intelligent Infrastructure Task Force and serve on the Cybersecurity and Cybercrime Task Force. I have authored over 150 papers in journals and conference proceedings, and hold 24 U.S. Patents. Over the years, my research has examined topics in computer security as well as voting systems.

Many states are now pushing for the use of voter-verified paper ballots, including here in Pennsylvania. I support this as a significant step forward toward more trustworthy elections. At the same time, I understand there is some opposition to making these changes, and that this opposition is supported by fundamental misunderstandings of the risks posed by DREs. My intention here is to correct those misunderstandings so that an accurate assessment of the risks can be made.

In early 2007, I obtained a Danaher 1242 full-face DRE electronic voting machine which was acquired from a government surplus sale in another state. So far as I am aware, this is the same Danaher DRE still in use today in several counties here in Pennsylvania. While I no longer have this machine, I spent time over a period of several years studying it with students at Lehigh to understand how the machine functions and to identify its vulnerabilities. We dismantled the machine, examined its construction and its internal computer circuit boards. We identified and extracted the ROM memory chip which stores the machine's firmware (i.e., built-in programming), which was easy to do because it was designed to be swappable with a new chip to update the firmware. For photographs of me with the machine in my lab, please see the webpage at <http://perfect.cse.lehigh.edu/Danaher.html>.

In addition to studying the machine itself, I reviewed a wide variety of documents relating to the Danaher 1242, including the manufacturer's manual entitled "Shouptronic 1242 Election System Information and Technical Specifications." (Shouptronic is now known as Danaher.) I also studied the certification reports and video recordings of the certification examinations conducted by consultants working for the Secretary of State.

From my experience examining the Danaher 1242, I know that it takes about 10-15 minutes and a regular screwdriver to remove the back of the machine. The ROM chip containing the firmware is socketed, as I have noted, which means it is easy to substitute a new one. Tamper-proof seals provide minimal or no protection against such manipulations.

The certification examinations I studied at the time involve testing with a relatively small number of votes in a predetermined pattern and can best be described as cursory for a machine as complex as a computer, and that is what this is.

Because DREs store a voter's selections in computer memory, there is no way for a voter to be certain that his/her intent is accurately recorded inside the machine's electronics because no other record of the voter's selections exists. Software or hardware bugs, or malicious intent, could alter the vote, and no one would know. Printing the contents of the computer's memory at the end of the day only provides a record of what is stored in the memory. It does not demonstrate that what is stored accurately reflects the voters' choices. A forensic examination after the fact might determine that something went wrong, but it would not necessarily permit recovery of the votes that were cast.

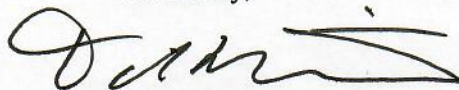
Since there may be some confusion regarding the security of the Danaher 1242 relative to other DREs, I wish to clarify several important points.

Some might suggest that because the Danaher 1242 does not run a common off-the-shelf (COTS) operating system like Microsoft Windows, it is therefore secure. While it is true this may provide immunity against some common attack vectors, it certainly does not guarantee that other similar attacks cannot be developed and aimed at the machine. All computers suffer from this issue; it is inherent in the components they use and the way they work.

Some may also suggest that because a machine does not contain networking hardware, and hence cannot be connected to the Internet, it is therefore secure. This is also incorrect. As I have already noted, the firmware chip in the Danaher 1242 can be swapped with a new one in a matter of minutes. But physical access to the DRE may not be necessary to compromise the voting system. The Danaher 1242 uses ballot definition files stored on memory cartridges that are programmed and inserted into the machine before each election. These memory cartridges are programmed using regular personal computers, running standard operating systems, and which may in fact be connected to the Internet or otherwise susceptible to computer viruses transmitted from the outside, e.g., via an infected USB memory stick inserted into the PC. One compromised PC could impact a large number of ballot memory cartridges without anyone realizing it. A single point of infection could in this way alter the results of an election.

For these reasons, I recommend making the move to voter-verified paper ballots across our entire state - we must not delay. Voter marked and verified paper ballots cannot be altered by software and provide a trustworthy record that can be used to confirm that voting systems have operated properly. As recent headlines have made clear, there are organized, determined, well-funded bad actors in the world who would undermine our trust in elections. We must not let them succeed.

Sincerely,

A handwritten signature in black ink, appearing to read 'Daniel Lopresti', written in a cursive style.

Daniel Lopresti
Professor and Chair