Testimony to Maryland Joint Committee: Election Cybersecurity

Micah Sherr, Ph.D.
Provost's Distinguished Associate Professor
Department of Computer Science
Georgetown University

September 6th, 2017

Chairperson Kaiser, Chairperson Conway, Members of the Joint Committee, thank you for the opportunity to appear today. As this Committee considers how Marylanders will register to vote, obtain and cast their ballots, and how election audits will be performed, it is my profound privilege to be here.

By way of background, I am an associate professor in the Department of Computer Science at Georgetown University, where I study the security of complex computer systems[1], including voting systems. While completing my doctoral studies at the University of Pennsylvania, I participated in two statewide studies of electronic voting systems, the first on behalf of the State of California[2] and the second on behalf of the State of Ohio[3,4]. Collectively, the studies examined voting systems from nearly all major voting machine vendors operating in the United States.

Our studies included voting systems manufactured by Election Systems & Software (ES&S)[5]; however, I would note that we did not evaluate the newer ES&S voting systems now used in Maryland.

---

[1] My curriculum vitae can be found at https://security.cs.georgetown.edu/~msherr/micahsherr-cv.pdf.
[2] Blaze et al., Source Code Review of the Sequoia Voting System, July 2007. Part of the California Secretary of State Top-to-Bottom Review of electronic voting machines.
[3] Aviv et al., Security Evaluation of the ES&S Voting Machines and Election Management System. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), August 2008.
[4] McDaniel et al., EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, December 2007.
[5] Ibid.

The studies themselves are notable in that they were the first in which computer security researchers had unfettered access to the voting systems' source code -- the computer codes that govern how these systems actually work.

The results of the California and Ohio studies demonstrated serious flaws in electronic voting machines. We found major, exploitable security vulnerabilities in every electronic voting system that we examined, including optical scanners. We discovered both fundamental design errors as well as programming mistakes that, for example, could allow a malicious voter to take full control of voting machines and install malicious software.[6] We demonstrated that backend election management software contained numerous programming mistakes that, if exploited, could lead to the reporting of falsified election results.[7] A hacked election management system could also provide falsified ballot images during an audit. And, we discovered vulnerabilities that could lead to the viral propagation of malware both between separate voting machines and between voting machines and the backend election management software, even when none of these systems are connected to the Internet or any other computer network.[8]

Given the existence of serious security vulnerabilities in voting systems, a primary recommendation of our studies was to mitigate these threats through the use of paper ballots -- ballots that can be tabulated by machine but could also be independently verified by humans. As a security researcher and as a Maryland voter, I am delighted that Maryland has mandated the use of paper ballots in its elections.

It is worth emphasizing that the security of paper ballots derives from their ability to be independently inspected and evaluated. Paper ballots allow separate, independent systems to form independent conclusions as to voter intent and to separately tally election results.

I applaud this Committee and the State Board of Elections in their efforts to carry out statewide election audits. Auditing is a critical component of secure elections, serving to increase the public's trust in the election process.

Importantly, however, audits that rely on scanned ballot images should not be considered reliable. The key problem is that any mistakes that the machines make in the original ballot scan will be duplicated in the audit. Such audits implicitly trust the behavior of the electronic voting machines, rather than allowing for human beings to double check that the ballots are being counted correctly. Put simply, audits based on digitized ballots assume that the images produced by the voting machines faithfully represent the ballots. Given our understanding of vulnerabilities in electronic voting machines, including optical scanners, such an assumption is unfortunately very dangerous.

---

[6] For example, see McDaniel, op. cit., pp. 75-78.
[7] Ibid., pp. 59-65.
[8] Aviv, op. cit.

"Hacking" a scanner has proven all too easy. In the Ohio study, we found numerous defects in both the software and the physical architecture in ES&S equipment, including the optical scanner that we evaluated. For example, we found that the scanner could be easily reprogrammed by inserting new media. This required picking a lock, which we could do easily, and removing and reapplying a security seal, which also can be done easily.[9] Or, as we have shown in the Ohio study, a scanner can be "infected" by some media (for example, a USB drive) that is prepared by an already-compromised election management system, bypassing the need to pick locks or undetectably break seals.[10] While to the best of my knowledge, the DS200 has not undergone as rigorous a security evaluation as was conducted in the California and Ohio studies, what we do know about the DS200 is troubling. In particular, its software is reportedly programmed in what is known as a memory-unsafe programming language[11], which allows for the same types of vulnerabilities that we discovered permeated the previous generation of ES&S voting equipment.

Crucially, since the current audit procedure has the ballot images extracted from the election management system, the images could be modified not just by corrupted voting machines, but also by corrupted backend election management software. In our evaluation of ES&S' Unity election management software, we discovered systemic vulnerabilities that could allow anyone with access to the machine to replace the software with a trojaned version that could surreptitiously change election results or alter election audit information.[12] This does not bode well for an audit that depends entirely on the correct operation of these backend election management systems.

An attacker intent on corrupting an election in Maryland would be foolish not to attempt to also corrupt the audit. Since both the election and the audit depend on the correct operation of the election equipment, the compromise of a voting machine or election management software can affect both election-day tallies as well as post-election audits.

An election audit should assume that the primary voting system might be corrupted. Otherwise, it is not independent and offers no meaningful guarantee of the integrity or accuracy of election results.

An *independent* audit assumes that the primary voting system is potentially vulnerable to attack. It logically follows that an independent audit cannot rely either on scanned images produced from the primary system's voting machines or images transferred via the primary system's election management software.

---

[9] Johnson, R. *Tamper-Indicating Seals*. American Scientist. Nov-Dec 2006.
[10] McDaniel, op. cit., pp. 75-76.
[11] VerifiedVoting.org, *Election Systems and Software (ES&S) DS200*. Available at https://www.verifiedvoting.org/resources/voting-equipment/ess/ds200/.
[12] McDaniel, op. cit., pp. 59-65.

So what does a secure election audit process look like? How might we design an audit in the face of potentially vulnerable software and hardware?

First, we must remove all reliance on the primary voting system. A straightforward method of performing an independent audit is to rescan the paper ballots using separate high-speed scanners that are not used in the primary system, and then re-tabulating the election results using these scanned ballots. The audit would essentially consist of repeating the election procedures, but with both independent software and independent scanners. Importantly, while this would "raise the bar" for an attack, still relying on digitized ballot images means that we are still trusting potentially vulnerable computer systems.

A more robust approach to election audits uses mathematically-sound sampling techniques to verify the integrity of election results. Simply put, rather than depend on potentially vulnerable software, it is always desirable to rely on approaches that can be proven accurate and correct.

In particular, so called "risk limiting audits" provide quantifiable assessments about the correctness of election results by manually verifying only a small subset of ballots.[13] There are several potential methods for risk-limiting audits that may be useful in Maryland. For example, if the audit targets a fixed threshold of risk (say a 0.5% probability that the primary election result is incorrect), then the audit procedures can inform auditors exactly how many paper ballots need to be manually examined. Or, if the resources available for conducting the audit are limited, then an audit could be conducted for a fixed amount of time, with the result being the established level of risk. For example, after six hours of inspecting randomly selected paper ballots, auditors could establish that the probability that the primary election result is incorrect is less than X%; additional hours of work could decrease that percentage further.

Although I cannot describe these techniques in the detail that they deserve given today's time constraints, it is important to note that these are simple techniques that do not require a mathematical or statistical background to carry out. Indeed, such methods have been used to carry out actual election audits in California[14] and other jurisdictions, and free software tools are available to help election workers perform an audit without having to understand its statistical underpinnings.[15]

[13] Lindeman and Stark, *A gentle introduction to risk-limiting audits*, IEEE Security & Privacy, vol 10(5), 2012.
[14] Ibid., pp. 5-6.
[15] Ibid., p. 1.

In conclusion, there is a voluminous amount of existing work that shows that voting machines are vulnerable to attack.[16] My own work has shown that voting machines and election management systems -- including systems manufactured by ES&S -- have systemic security flaws that allow an attacker to take total control over the machine and potentially cause the reporting of inaccurate election results.[17] Given the equipment that we have, our best defense is to perform independent audits of election results. *Independence* is a critical feature of a secure and meaningful audit, and an audit that relies on images provided by potentially faulty election equipment cannot be deemed independent. I urge the Committee to protect the integrity of Maryland elections and increase public confidence in the election process by performing truly independent audits.

I would like to thank the Committee again for the opportunity to speak here today. Securing and protecting the election process is an important and difficult responsibility, and one that is critical to our democracy. Thank you.

[16] Jones and Simons, *Broken Ballots: Will your Vote Count?*, Center for the Study of Language and Information, 2012.
[17] Aviv, op. cit.