DEFCON 25 Voting Machine Hacking Village

Report on Cyber Vulnerabilities in

U.S. Election Equipment, Databases, and Infrastructure

September 2017

Co-authored by:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago & Cambridge Global Advisors
Harri Hursti, Nordic Innovation Labs
Joseph Lorenzo Hall, Center for Democracy & Technology
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEFCON

Forward

I've spent my entire adult life in the national security arena: Europe during the Cold War, the Balkans in the 1990s, the Middle East since 9/11, in the Pentagon, the White House, and most recently at NATO headquarters in Brussels. I've studied national security at West Point and at Harvard. So, why am I now introducing a report on cyber hacking of our voting systems?

The answer is simple: last year's attack on America's voting process is as serious a threat to our democracy as any I have ever seen in the last 40+ years – potentially more serious than any physical attack on our Nation. Loss of life and damage to property are tragic, but we are resilient and can recover. Losing confidence in the security of our voting process – the fundamental link between the American people and our government – could be much more damaging. In short, this is a serious national security issue that strikes at the core of our democracy.

This report makes one key point: our voting systems are not secure. Why is this so serious? Why must we act now? Why is this a national security issue? First, Russia has demonstrated successfully that they can use cyber tools against the US election process. This is not an academic theory; it is not hypothetical; it is real. This is a proven, credible threat. Russia is not going away. They will learn lessons from 2016 and try again. Also, others are watching. If Russia can attack our election, so can others: Iran, North Korea, ISIS, or even criminal or extremist groups. Time is short: our 2018 and 2020 elections are just around the corner and they are lucrative targets for any cyber opponent. We need a sense of urgency now. Finally, this is a national security issue because other democracies – our key allies and partners – are also vulnerable.

Thousands of state and local election officials are responsible for administering elections but they are often overburdened and under-resourced. It is not their job alone to deal with this national security threat.

This important report highlights the problems that demand our attention and solutions. The "Voting Village" at DEFCON in July 2017 was not intended to be something to entertain hackers. It was intended to make clear how vulnerable we are. The report describes clearly why we must act with a sense of urgency to secure our voting systems.

For over 40 years I voted by mailing an absentee ballot from wherever I was stationed around the world. I assumed voting security was someone else's job; I didn't worry about it. After reading this report, I don't feel that way anymore. Now I am convinced that I must get involved. I hope you will read this report and come to the same conclusion.

Douglas E. Lute
Former U.S. Ambassador to NATO
Lieutenant General, U.S. Army, Retired

Contents

Introduction

Since its founding in 1993, DEFCON has become one of the world's largest, longest-running, and best-known hacker conferences. This year's DEFCON was held July 27-30, 2017 in Las Vegas and drew a record-breaking 25,000 participants. For the first time, DEFCON featured a Voting Machine Hacking Village ("Voting Village") to highlight cyber vulnerabilities in U.S. election infrastructure – including voting machines, voter registration databases, and election office networks. The voting machines available in the Voting Village were paperless electronic voting machines, and at a time when a number of U.S. voting jurisdictions are either committed to or considering purchasing newer equipment based on auditable paper records,[1] open examination of these types of systems could not be timelier. The event was organized by several cyber, voting equipment, and national security experts, along with DEFCON founder Jeff Moss.

The Voting Village acquired and made available to participants over 25 pieces of election equipment including voting machines and electronic poll books. Most models are still widely used in U.S. state and local elections today (with the exception of the AVS WinVote, described below). The Voting Village also featured a mock back-office training "range" to simulate databases and networks of real-world election administrators.

Hacking into voting machines is not new, but previously it was conducted in only in very limited academic or industrial settings under strict controls and publications restrictions. DEFCON's Voting Village represented the first occasion where mainstream hackers were granted unrestricted access to explore and share any discovered vulnerabilities. Legal restrictions including the 1998 Digital Millennium Copyright Act (DMCA)[2] and, to some extent, the Computer Fraud and Abuse Act, made such activities subject to criminal or civil liability.

A consequence of the limited access to voting machine hardware in the past, is that doubts have been frequently raised about if the various vulnerabilities identified in previous studies would be practical for technologists of ordinary skill to discover and exploit. At the DEFCON event, however, thousands of participants were invited to engage with and explore voting equipment and the network simulator in an environment free of restriction for the first time.

The results were sobering. **By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems**, including:

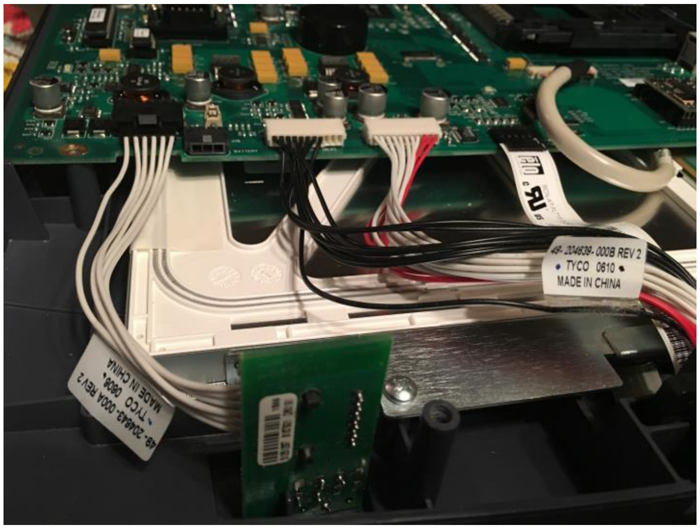
- The first voting machine to fall – an AVS WinVote model – was hacked and taken control of remotely in a matter of minutes, using a vulnerability from 2003, meaning that for the entire time this machine was used from 2003-2014 it could be completely controlled remotely, allowing changing votes, observing who voters voted for, and shutting down the system or otherwise incapacitating it.
- That same machine was found to have an unchangeable, universal default password – found with a simple Google search – of "admin" and "abcde."
- An "electronic poll book", the Diebold ExpressPoll 5000, used to check in voters at the polls, was found to have been improperly decommissioned with live voter file data still on the system; this data

[1] Jenni Bergal, "Russian Hacking Fuels Return to Paper Ballots", *Huffington Post Stateline*, (Oct. 3, 2017), http://www.huffingtonpost.com/entry/russian-hacking-fuels-return-to-paper-ballots_us_59d39962e4b092b22a8e398d

[2] U.S. Copyright Office Summary, The Digital Millennium Copyright Act of 1998, December 1998, https://www.copyright.gov/legislation/dmca.pdf

should have been securely removed from the device before reselling or recycling it.[3] The unencrypted file contained the personal information – including home residential addresses, which are very sensitive pieces of information for certain segments of society including judges, law enforcement officers, and domestic violence victims – for 654,517 voters from Shelby County, Tennessee, circa 2008.

Moreover, a closer physical examination of the machines found, as expected, multiple cases of foreign-manufactured internal parts (including hardware developed in China), highlighting the serious possibility of supply chain vulnerabilities. This discovery means that a hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line. With an ability to infiltrate voting infrastructure at any point in the supply chain process, then the ability to synchronize and inflict large-scale damage becomes a real possibility. Also, as expected, many of these systems had extensive use of binary software for subcomponents that could completely control the behavior of the system and information flow, highlighting the need for greater use of trusted computing elements to limit the effect of malicious software. In other words, a nation-state actor with resources, expertise and motive – like Russia – could exploit these supply chain security flaws to plant malware into the parts of every machine, and indeed could breach vast segments of U.S. election infrastructure remotely, all at once.



Given the federal government's recent designation[4] of election systems as critical infrastructure – and in light of what is known about the Russian attempts to infiltrate election networks in at least 21 states in the 2016[5] Presidential Election – it is overwhelmingly evident that election security is now an extension of *national security*. In addition to Russia, other state and private actors (including Iran, North Korea, organized crime, terrorist groups, and even lone-wolf hackers) also possess the technical capability to attack our voting systems or credibly sow distrust in election results. Organized crime is also a serious threat in the larger cybercrime ecosystem and they may also have motives to attack election systems or provide such services for hire, which we've seen in areas like botnets, ransomware, and malware distribution. **The bottom line is: No matter the level of nation-state hacking or interference in 2016, if our enemy's goal is to shake public confidence about the security of the vote, they may already be winning.** And with critical

[3] Michelle De Mooy, Joseph Jerome, and Vijay Kasschau, "The Legal, Policy, and Technical Landscape Around Data Deletion", *Center for Democracy & Technology*, (2017) https://cdt.org/files/2017/02/2017-02-23-Data-Deletion-FNL2.pdf

[4] See Presidential Policy Directive (PPD) 21: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[5] Congressional Testimony of Jeanette Manfra, then-Acting Deputy Under Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis, U.S. Department of Homeland Security, for a hearing entitled "Russian Interference in the 2016 U.S. Elections," before the Select Committee on Intelligence, United States Senate, on June 21, 2017. Link here: https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF

elections in 2018 and 2020, efforts to hack American democracy will only continue unless safeguards are put in place.

The encouraging news is that a growing, diverse group of stakeholders are embracing election security as national security. As evidenced by the robust, diverse turnout at the Voting Village, understanding cyber threats to our democracy is not just a "hacker thing." Bipartisan stakeholders from federal, state, and local government participated in the Voting Village. Advocacy groups, private sector businesses, think tanks, and national security, intelligence, and military leaders also contributed to the event. The level of interest and support from these groups and individuals parallels an outside movement that views election security as a national security imperative. Many are pressing for policy solutions and practical efforts that leverage best practices already embraced by the cybersecurity community, tailored to the unique nature of elections.[6]

On the Eve of DEFCON: The State of Our Election Security Landscape

For years, computer science and cybersecurity experts have been sounding the alarm on U.S. election infrastructure which can best described as a patchwork of aging, insecure voting systems that vary from state-to-state. As their research has shown, among the most vulnerable voting systems are Direct Recording Electronic (DRE) voting machines. These systems utilize digital touch-screen technology and record votes on the internal memory of the machine, with no paper backup. Cautions about DREs have prompted some changes and a few victories. For example, in 2015 just weeks before a primary election, the State of Virginia decommissioned use of the AVS WinVote (a DRE machine featured at the Voting Village) because of a litany of problems including its Windows operating system, unchangeable default password, the ability to hack the machine remotely, and the fact that its results were transmitted via wireless connections.

There is still more work to be done. Currently there are five states – Delaware, Georgia, Louisiana, New Jersey and South Carolina – that are still operating entirely on paperless systems. Another 9 are partially paperless, making a total of 14 states that are still operating in a highly vulnerable manner.[7] Yet even when leaders recognize change is needed, other competing policy priorities or lack of resources at the state and local level can impede action.

Election security threats grew even more urgent this past election cycle when Government officials confirmed that a foreign adversary, Russia, attempted to interfere in the 2016 United States Presidential Election via "a multi-faceted approach intended to undermine confidence in our democratic process." According to U.S. intelligence official reports, Russia targeted voter registration databases in at least 21 states and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.[8]

[6] Zetter, Kim. "Virginia Finally Drops America's 'Worst Machine'" *Wired*. August 17, 2015. Link: https://www.wired.com/2015/08/virginia-finally-drops-americas-worst-voting-machines/

[7] Verified Voting, "Voting Equipment in the United States" https://www.verifiedvoting.org/resources/voting-equipment/

[8] Congressional Testimony of Jeanette Manfra, National Protection and Programs Directorate, U.S. Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis, U.S. Department of Homeland Security, for a hearing entitled

Election administration has always been the constitutional responsibility of state and local jurisdictions. But when Russia – which has also been known to hack elections abroad[9] – decided to meddle in the 2016 U.S. election, it changed the game. The conversation has now been elevated to the level of military and homeland security experts who are increasingly getting involved to help dissect the motives, capabilities and implications of cyberattacks launched at the U.S. and our democracy, as well as assess what kinds of deterrents are available (beyond the scope of this report).

Voting Village Goals

It is through the lens of the complex election security landscape – and on the heels of the Russian 2016 attacks – that Voting Village organizers presented the idea for the village to DEFCON. Media coverage and Congressional testimony on the Russian hacks has helped to advance awareness regarding cyber threats to elections. Yet Voting Village organizers believed there was still much to unpack. Their belief was that the hacker community, if given unfettered access to voting machines and equipment, would be able to enrich the basis of knowledge. As the largest gathering of hackers in the world, DEFCON would also provide the ideal forum to shine the national spotlight on any findings.

To that end, the goals of the DEFCON Voting Village were to:

- Provide examples of working voting systems for security researchers to evaluate, attack, and otherwise study;
- Educate and raise public awareness about the machinery of U.S. democracy, from the machines to how election technology interacts with legal, market, and normative barriers in elections that do not exist in general purpose computing contexts;
- Stimulate a discussion and ideas regarding how security researchers and hackers can help to make our election infrastructure more safe and secure;
- Create a forum to engage with other non-hacker stakeholders, including federal, state, and local policymakers who will be essential to implementing changes and reforms;
- Provide a training opportunity for state and local elections IT staff to learn about their networks and machines in use in this jurisdiction. For many, the village represented the first opportunity for election officials to study and inspect the very machines they are using in their daily operations, yet have not been legally permitted to study previously.

Equipment

The Voting Village organizers procured a variety of voting equipment for examination. A recent DMCA waiver issued by the Library of Congress made it easier for the Voting Village to obtain the hardware for research purposes. Previous such an act was difficult, and in some cases illegal under the DMCA (of course, cyber criminals would not be so constrained by US law). Most of the equipment in the Village was purchased by DEFCON on secondary markets, such as eBay. The machines featured in the Village included:

- AVS WinVote DRE (software version 1.5.4 / hardware version N/A)
- Premier AccuVote TSx DRE (TS unit, model number AV-TSx, firmware 4.7.8)
- ES&S iVotronic DRE (ES&S Code IV 1.24.15.a, hardware revision 1.1)

"Russian Interference in the 2016 U.S. Elections," before the Select Committee on Intelligence, United States Senate, on June 21, 2017. Link: https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF

[9] Koval, Nikolay. "Revolution Hacking." *Cyber war in perspective: Russian aggression against Ukraine* (2015): 55-58. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Koval_06.pdf

- PEB version 1.7c-PEB-S
- Sequoia AVC Edge DRE (version 5.0.24)[10]
- Diebold Express Poll 5000 electronic pollbook (version 2.1.1)[11]

The Voting Village also featured a "cyber range" – a simulator that created a mock virtual "election official's office" and network, built with the guidance and assistance of a large U.S. election jurisdiction staff who ensured quality control and real-world likeness. This range provided a training opportunity for state and local leaders in attendance to better understand the threats to their specific systems and domains, as well as learned best practices to protect their information and networks. The range was operated by CyberBit – a Ft. Meade, Maryland-based cyber training facility that, beyond DEFCON, has provided multiple industry-tailored training services to government and private sector entities.

Limitations

There were significant limitations of the work at the Voting Village, including:

- Participants had no access to source code, operational data or other proprietary information that is not otherwise legally and publicly available. An actual nefarious actor might have little difficulty obtaining these materials.
- The Voting Village provided only a sample of voting technologies. Organizers obtained what they could get their hands on quickly, legally, and affordably. The most recently used system available was the AVS WinVote, which was decertified by the State of Virginia in 2014. A number of other systems, however, are still in use in U.S. elections including the AccuVote-TSx, Sequoia AVC Edge, and ES&S iVotronic.
- The Village had no access to optical scan or DRE systems with a Voter-Verified Paper Audit Trail (VVPAT). These systems, and those involving ballot marking devices, are the most software-independent and auditable systems, and are increasingly popular and heavily used.
- Finally, there was no access to any backend provisioning, counting, or voter registration systems. These kinds of systems are not generally available on the open market. This is especially significant as the evidence from the 2016 election seems to indicate strongly that these types of voting technologies – not voting machines themselves – were the primary target of Russian hacker attacks.

Technical Findings & "Accomplishments"

AVS WinVote

The Advanced Voting Solutions (AVS) WinVote is a DRE voting system that utilizes touch-screen technology to make a voting selection, and then transmits a voter's choice via a wireless local area network (LAN). The AVS WinVote system was the only system in the Village that had been earlier decertified (in Virginia). It was also the most easily compromised. In addition, physical access to the machine proved just as easy of a path to complete compromise.

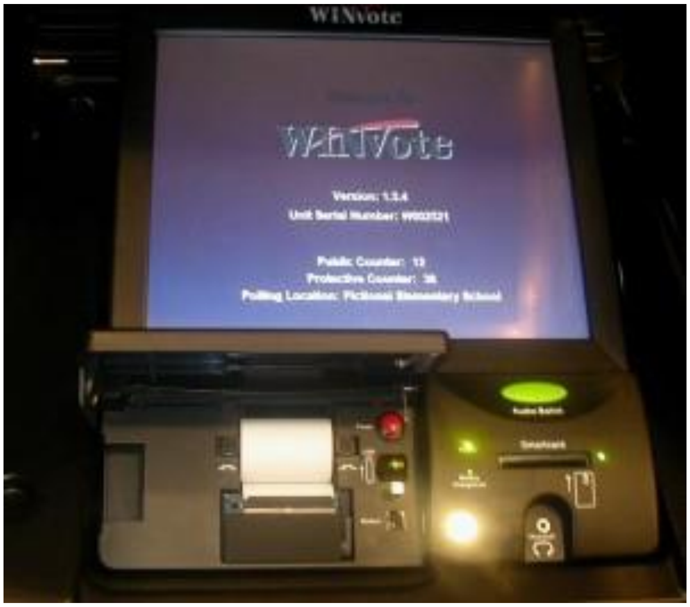
Carsten Schürmann, a democracy-tech researcher who hails from Denmark, was able to hack into the AVS WinVote within minutes remotely over Wi-Fi. The WinVote broadcasts its own Wi-Fi access point to which modern operating systems can easily connect. Using commonly available network tools (e.g., Wireshark)

[10] "PEB" stands for Personal Electronic Ballot, which functions similarly to a portable memory pack. It is used to authorize a new voting session by poll-workers and, when the polls close, poll workers move summary data from each machine onto the PEB. The PEBs are then transported to election headquarters or their contents transmitted via a computer network.

[11] An Electronic Pollbook is a system that essentially replaces the spiral-bound lists of registered voters in every polling place by putting that functionality into a laptop, tablet, or kiosk-like computing platform.

Schürmann determined immediately that the WinVote had a specific IP address and was able to use a vulnerability from 2003 (CVE-2003-0352[12]) and preinstalled attack payloads in Metasploit (a vulnerability analysis and penetration testing tool) to gain access to the filesystem and escalate privileges to an admin user – meaning he could make the machine think he was an administrator of the system, not simply a mere voter or poll-worker. Once he had this access, Schürmann was able to do anything on the system, from running code, to changing votes in the database, to turning the machine off remotely. This vulnerability had clearly been in the system since 2003, allowing anyone within 150-300 feet of a polling place complete control of any WinVote machine while it was being used. For $50, a hand-held high gain antenna could be purchased that would extend that range to over 1,000 feet and through walls.

Physical access to the machine afforded similar ease-of-access. The locked panel on the front of the device was easily picked or opened with readily available keys that could be purchased easily and cheaply online. The locked cover was easily bypassed without paying attention to the lock as well (by simply compromising the plastic hinge). The physical security protecting the USB port was ineffective and also irrelevant, due to the findings in the next paragraph.



While examining the case further, DEFCON hackers noticed that there were 2 unprotected, uncovered USB ports on the back of the machine. These were within easy reach of a voter, and unfortunately the privacy screen for the AVS WinVote is so private that it would be difficult to tell if someone was tampering with USB ports on the back of the machine while voting. There was no USB keyboard around in the Voting Village – a natural place to start with an unprotected USB port – but after an errand to a local electronics supply store to obtain one, all hackers had to do was to simply attach the keyboard, type "`ctrl-alt-del`" and the Windows task manager would pop up. At that point, they could type "`alt-f run`" and run any software they wanted to, including software on a USB stick that is inserted into the other USB slot on the back of the machine. As one hacker, Nick, remarked, "With physical access to back of the machine for 15 seconds, an attacker can do anything."

AccuVote-TSx

The AccuVote-TSx is touch screen DRE voting machine, manufactured by Premier/Diebold, that records votes on internal flash memory. In much the same way that an ATM works, voters insert a card into the machine and then pick their choice on a touchscreen. Votes are then recorded to internal electronic computer storage.[13]

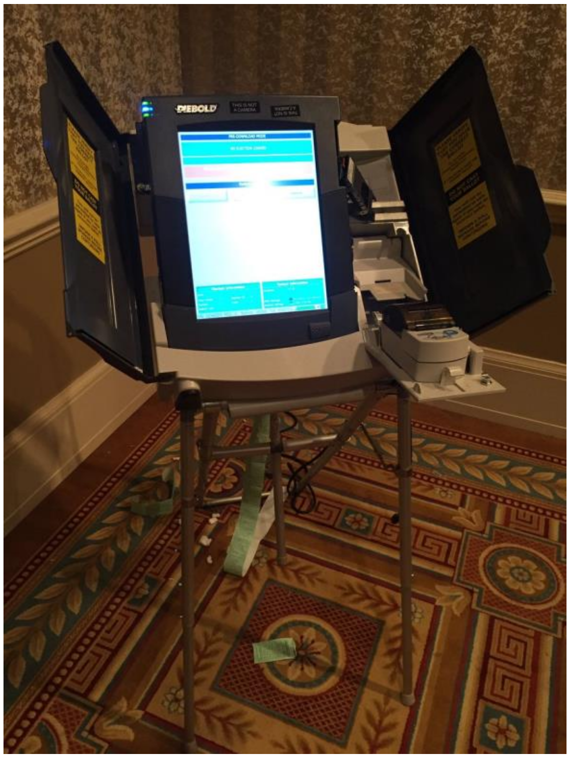
As is natural in any DEFCON Village structured around hardware artifacts, Voting Village hackers seemed to spend more time on platforms other than the AccuVote-TSx. Just as with the ES&S iVotronic below, much of

[12] See: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=can-2003-0352

[13] Verified Voting, "Premier/Diebold (Dominion) AccuVote TS & TSx" https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-tsx/

the work around this machine focused on examining the details of the internal hardware layout and examining the “firmware” – software that runs the low-level hardware functions and is not changed as often as the voting software itself.

Joe Fitzpatrick, Schuyler St. Leger, Ryan (@rqu45 on Twitter), Wasabi, and Ayushman were all involved in examining the innards of the TSx. First, Wasabi noticed that a particular chip (an EPROM chip) was wired to the machines battery controller, and removing this chip caused the machine to be completely inoperable. If not protected carefully, removing such chips from TSx machines could be used to selectively shut down voting in certain areas (assuming physical access and time necessary to open the case of the machine undetectably, remove the chip, and put the machine back together). This chip was socketed rather than soldered in place, making removal quite easy.



Wasabi also noticed that the `NK.bin` file (the main executable or “kernel” for the Windows CE operating system) had local networking and modem support, which would ideally be removed for software in jurisdictions that do not use those functions. Similarly, Ayushman noticed that there was a `.ini` configuration file that seemed to have passwords, users, and the modem configuration for the device, which he suspected could be changed (since there is little access control) with a serial (DB9) connection to the device. After the conference it was confirmed that connecting the debug jumped on the PCB would still activate the boot loader console on the DB9 VIBS.

Fitzpatrick, St. Leger, and Ryan focused on analyzing the firmware of the device and mapping the pins on the chips to functions useful for chip debugging tools. The TSx has what is called a JTAG interface which is a plug on the circuit board typically used during the manufacturing process to check correct functionality. However, after the unit is sold, the JTAG interface is still available and provides convenient access to the processor and the rest of the system. They noticed the TSx processor is an ARMv5 chip and common chip debuggers only go back as far as ARMv6. Therefore, they had to locate an older debugger in order to map the functionality of each pin and interact with the software. There are further details about this work available in the raw notes from the Voting Village on github.[14]

ES&S iVotronic

Like other DRE machines, the iVotronic, manufactured by ES&S, features a touch-screen interface and records votes in internal memory. A poll worker uses a device called a PEB (roughly the size of a deck of playing cards) to enable voting for each voter. PEBs are also used to store and aggregate the final vote tallies from all machines that are then physically transported to election headquarters. In some configurations, the PEB tally can be alternatively transmitted to headquarters over a computer network.[15]

[14] See: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md#premier-accuvote-tsx

[15] Verified Voting, “Election Systems and Software (ES&S) iVotronic” https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/

Similar to the AccuVote-TSx, many of the interesting findings about the iVotronic related to examining the internals of the various components. Hackers in the Village examined the PEB device, the PEB readers, and the iVotronic DRE machine.

A hacker named Scott Brion examined the PEB and PEB reader. He found the PEB contains an 8-bit processor, EPROM (non-volatile storage, not easy to update), flash memory (non-volatile storage, easy to update), an infrared communications port (IRdA), a magnet, serial pins and a battery. The PEB reader – a device that serves as an interface for reading PEBs one by one to transfer contents – contained similar elements, including an 8-bit processor, EPROM, USB port, serial pins, and an IRdA receiver port. Brion was able to establish communication to the firmware through the serial PINs, however nothing of value was obtained (in some cases "security fuses" may have been intentionally blown by the manufacturer to prevent analysis and readout of firmware). With a bit of research, it became clear that green PEBs were "supervisor" units used to start and end elections on a set of machines and the security fuses are blown on those, preventing analysis and extraction of firmware on those units. However, the red PEBs, used to accumulate election data and authorize each new voter to vote did not have their security fuses blown, so the firmware analysis proceeded on those units. This is likely an inferior security design as the red PEBs actually accumulate and transmit vote totals, which is exactly what an attacker seeking to change an election result would attack by changing the firmware in a PEB or swapping a PEB out with a clandestine attacker PEB.

Another Village participant, Kris Hardy, also focused on attacking the PEBs and PEB readers as possible ways to get into the iVotronic in a way that could be undetectable (and mimic the goals of a malicious election attacker). Hardy and his colleagues (who asked not to be identified) used a PICkit 3 chip debugger/programmer and were able to identify several PEB chips that were configured without their security fuses blown (meaning the chips could be easily analyzed and interacted with). They were able to extract firmware from one of the chips, which they were able to decompile (a process that turns binary computer code into source code that humans can read – the opposite of "compiling" source code software into a binary executable). The contents looked promising but they did not have time to fully examine the firmware before the Village had to close. They recorded the chip pin-outs (mapping the pins to functionality on a debugger/programmer) in an online github repository for future researchers.[16]

Sequoia AVC Edge

The Sequoia AVC Edge, a Dominion product, is another widely-used DRE machine where voters insert a "smart-card" into the machine (a credit card-sized card that authorizes a voter to vote), pick their voting choice on a touchscreen, and then the results are recorded on the machine's internal storage. When polls close, the votes for a particular machine are written to a "PCMCIA" flash memory card which is removed from the system and either physically transported to election headquarters or their contents transmitted via computer network.[17]

[16] See: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md#ess-ivotronic

[17] Verified Voting, "Sequoia (Dominion) AVC Edge" https://www.verifiedvoting.org/resources/voting-equipment/sequoia/avc-edge/

Note: As is the case with opportunistic hacking projects like the Voting Village, some equipment will receive more attention than others; in this case, the Sequoia AVC Edge did not attract as much attention as other systems. Below, we describe what are less findings and more features of what hackers found remarkable about this system.

Members of the University of Houston Cybersecurity Club – Tsukinaki and Joe (no last names given) – spent some time with the Sequoia AVC Edge. Through their investigation, it was determined that the AVC Edge has an internal CompactFlash (CF) card running on the pSOS operating system, a real-time operating system developed in 1989, before many of the Voting Village participants were born. This particular operating system has traditionally been used heavily in retail and kiosk equipment.

The Houston team also found that the Edge records data as a hex file; meaning it was difficult to figure out what the contents were without a bit more additional information or reverse-engineering of the file format (a labor-intensive activity not well-suited for the Village). Voting results were stored on the CF card, but then also sent to flash storage on a PCMCIA card in a slot in the back of the machine. It was obvious from the data that this particular AVC Edge was from the 24th precinct of Washington DC, which hackers got by just running the command strings on the data. In this process, one could definitely see the slate of candidates and such, though no voter identities or similar personal voter data was viable. (This was expected as no voter identity could make it from the pollbook process to the voting machine).

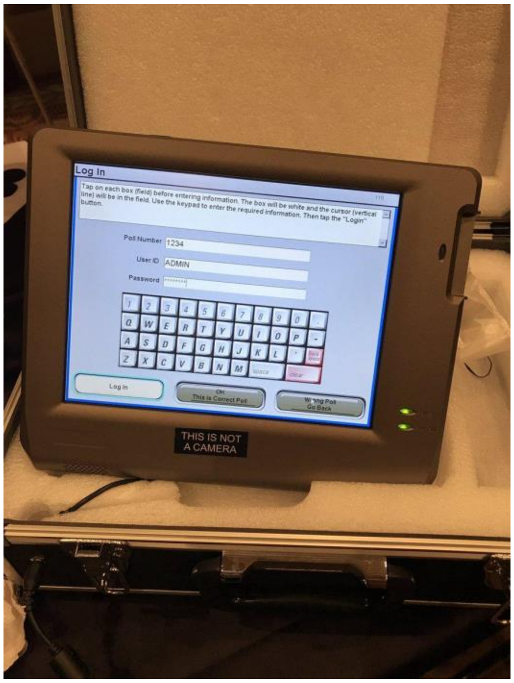
Hackers then tried to boot the operating system image in a virtual machine, but did not get too far; One could see a menu in the PSOS boot file – that is, could see the strings, but could not get it to boot. There was a RAM file that seemed to give them a "file not found" in the boot sequence. Nick used a utility called `binwalk` – a firmware reverse-engineering and analysis tool – to examine the firmware and it appeared that there may be use of an *8-bit cipher* (eight (8) bits is exceedingly insecure).

Diebold ExpressPoll 5000

While the devices detailed above are types of vote-recording and vote-casting equipment, the Village also had available an electronic pollbook (the ExpressPoll 5000), which is still currently used in states like Ohio to check in voters on Election Day. At the Voting Village, the pollbook was subject to a significant degree of scrutiny by participants, including:

Voter Data Leakage

On day 1 in the Voting Village, it was discovered that the ExpressPoll units obtained were not properly decommissioned and still contained voter records. Specifically, 650k voter records from Shelby County, Tennessee were still present on the pollbooks, containing names, addresses, dates of birth, driver's license numbers and a number of other potentially sensitive fields. Village organizers secured the data, removed it from the units available in the village, and one village organizer began a process of disclosure to Shelby County so that they could be aware of the issue.

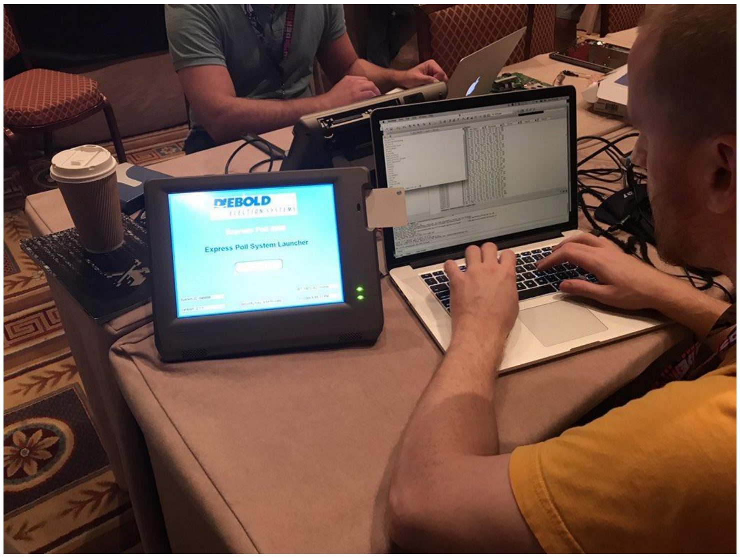


Technical Findings

The unit did not have much in the way of physical security protections, allowing someone with a screwdriver to remove and replace the election media, or simply remove it to accomplish a denial-of-service attack. The default username and password for this unit was available with a simple google search. There were also two USB ports that seemed unprotected.

The ExpressPoll runs on an obsolete embedded operating system, Windows CE 5, and validates no input or software updates (it would load without any prompting or checking both a new bootloader – commands that tell the system how to start up – and OS image – the operating system the device runs after start-up). This could allow attackers to inject a new bootloader (which appears to be proprietary) or Windows CE image without detection. Similarly, the unit reads a file "`ExPoll.resources`" that contains all the parameters for the election that could also be injected with parameters chosen by an attacker. When the pollbook software is launched, this file is loaded into memory and then saved to non-volatile storage for use in future elections. Village hackers were able to change the parameters in this file, get it to load and have their own parameters loaded (in this case they "bricked" – rendered inoperable – an ExpressPoll unit, but were confident that further testing would have resulted in successful modification of pollbook parameters).

Hackers attempted to crash the main application by loading large amounts of data into the database fields, but this only slowed the device, instead of crashing the main application and potentially allowing further access. The unit's networking seemed to be well-locked down with essentially only data being broadcast from the unit and hackers were unable to make a successful connection and inject data through the network interface.



There was some hope that changing the `Consolidation_ID` on a smartcard that the unit writes to in order to authorize a voter would have silently discarded that voter's vote, but that was not possible to test without a smart card reader/writer, which was unavailable.

The device keeps an event log with login, logout, power, load, and open events. However, this log would not be sufficient to prevent tampering; it is only written by the device and does not reflect any file changes that occur on the storage media (and, of course, is not integrity protected).

Impact & Lessons Learned

The technical findings of the Voting Village were not entirely new. As stated, hackers and researchers have breached these voting machines before under various circumstances. However, this experiment allowed mainstream hackers more time and access than ever before, generating several "real-world" lessons that policymakers should consider moving forward:

Lesson #1: Even with limited resources, time, and information, voting systems can be hacked.
The DEFCON Voting Village showed that technical minds with little or no previous knowledge about voting machines, without even being provided proper documentation or tools, can still learn how to hack the machines within tens of minutes or a few hours. Past official studies such as the California Top-To-Bottom Review[18] and the Ohio EVEREST Review,[19] conducted over ten years ago had significant restrictions on what participating researchers were allowed to try. Those studies were also done in a "white box" environment where researchers had access to source code, documentation, and equipment under strict non-disclosure agreement.

In the case of the DEFCON Voting Village, hackers had to create, copy, or cobble together their own tools though, in turn, they were given permission to fully experiment and take risks that may result in the machines being destroyed in the process.

The good news is, freedom to take such risks accelerates the process and can lead to completely new discoveries of new vulnerabilities. The bad news is, if relative rookies can penetrate a machine or system in a matter of hours, it becomes incredibly difficult to deny that a skilled, nefarious hacker – including sophisticated cyber criminals or nation-state attackers – with unlimited time and resources, could not do the same.

Lesson #2: Foreign-made parts introduce serious supply chain concerns.
"Phishing" scams via email are common, and for good reason: When successful, phishing can provide inside access to a machine, account, system or network without the hacker actually having physical access to the machine. Information can then be stolen or exploited in some fashion, without the victim ever knowing that entry has occurred. U.S. intelligence reports reveal that Russians were not only interested in hacking into voter databases but also into other aspects of the election, including the software supply chain. According to that report, Russian hackers affiliated with Russian military intelligence – the GRU – sent phishing emails to employees at a voting services company that provides state and local election offices with voter registration systems, comprising at least one account on that vendor's system that was then used to send spear-phishing emails to 120 local and state election officials.[20] Given the typical successes of a well-designed spear-phishing attack, we can be almost certain that one or more election officials fell victim to this attack, although we do not know what access and damage might have resulted (as this information is likely still classified).

Good cyber hygiene can help prevent some of these remote attacks. However, during the Voting Village, the extensive use of foreign-made computer parts – frankly, as expected given how many commercial computing devices are manufactured overseas – within the machines opened up a serious set of concerns that are very relevant in other areas of national security and critical infrastructure: the ability of malicious actors to hack our democracy remotely, and well before it could be detected. A frequent argument raised about the

[18] See: http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/

[19] See: https://www.eac.gov/assets/1/28/EVEREST.pdf

[20] National Security Agency, "Report on Russian Spear-Phishing" November 2016. Parts redacted. https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf

defensibility of election systems is that the diversified, decentralized nature of our election infrastructure provides at least some protection from wide-scale hacks. But via a supply chain originating overseas, voting equipment and software can be compromised at the earliest of stages in manufacturing process. For example, foreign actors could design or plant a virus in software, memory, or even a small microchip that could affect an entire make/model of voting machine, theoretically allowing them to be compromised in one coordinated attack. To be sure, while we've known for over a decade that some voting machines have hardware manufacturing and/or assembly in foreign countries, less is known about sourcing of software. We do know, for example, of one case when Election Systems & Software failed to disclose it was manufacturing products in a sweatshop in the Philippines in 2007.[21]

One additional implication of foreign parts includes inability to limit insider threats. Cyberattacks originating from inside an organization are a serious concern. Yet U.S. election officials, vendors, or those involved in the voting administration process can be vetted to some degree. This is not the case when the process involves foreign components and facilities, including complicated but common relationships such as subcontractors further subcontracting work out to other entities. To be sure, there are very few entities – the Department of Defense, the National Security Agency, and large tech companies such as Google and Facebook – that have the ability and resources to design, develop, and manufacture entire computer systems on their own; a controlled supply-chain is a first step towards reducing these kinds of threats, but it would be best if voting systems moved to more trusted system design.

Lesson #3: This was more than a "hacker" stunt and showed that a diverse community of stakeholders must be engaged.

Organizers did not maintain a precise count of how many entered the Voting Village but estimate that the number exceeded several thousand. In just three days, the Voting Village expanded the number of people who have now had first-hand experience and knowledge of these systems. By Sunday, the attendees who started hacking on Friday had become the experts and they were teaching and helping the new people who just started on Sunday. Exponentially expanding the knowledge base in this regard is sure to have great impact on the solutions and policy-making process. Remarkably, many of the hackers that stayed in the Voting Village for a considerable amount of time at DEFCON 25 were young, between the ages of 16-19, demonstrating to organizers that this kind of civic infrastructure hacking may be a promising way to reach out to younger elements of the information security community.

Additionally, given the wide scope of stakeholders involved in election security, Voting Village organizers believed it was essential the Village did not come to be seen only as a "hacker thing." Organizers reached out to and involved hundreds of other "non-hackers" in the event, ranging from senior leaders of NGOs, to cyber and voting experts, to elected officials to national security leaders. Staff from U.S. Senate Homeland Security & Governmental Affairs Committee and representatives from National Institute for Standards & Technology (NIST), the U.S. Department of Homeland Security (DHS) and the National Governors Association (NGA) attended.[22] Members of the U.S. Congressional Cyber Caucus including Representative Will Hurd (R-TX) and Representative Jim Langevin (D-CT) also visited the Voting Village.

The Voting Village also intentionally encouraged state and local election officials to attend. For many of them in attendance, the Village was their first opportunity to look themselves into the machines – machines they are required to use and manage, but have been prohibited to study in depth – and find answers to their own

[21] Kim Zetter, "ES&S Failed to Disclose Manila Manufacturer to Fed Agency," *WIRED News*, August 14, 2007. https://www.wired.com/2007/08/ess-failed-to-d/

[22] APPENDIX #1: Partial List of Attending Individuals & Organizations

questions and learn more about that equipment. Moving forward, it will be critical to incorporate all of these stakeholders into the security and solutions discussion.

Lesson #4: The Village challenged major criticisms – and reiterated the need for policy change. Finally, the Voting Village helped to dispel a few long-circulating criticisms – as well as helped to affirm what election security advocates have been arguing for years: There is urgent need for federal, state and local election officials to implement measures to secure U.S. election infrastructure.

First, though voting machine manufacturers have historically denied claims that their machines are insecure, some have suggested the Voting Village demonstration did not constitute a "true" test because it was not conducted in a real election setting. Yet, enemy hackers are certainly not operating in a "sanctioned" environment and if a voting machine can be hacked by a relative novice in a matter of minutes at DEFCON, imagine what a savvy and well-resourced adversary could do with months or years.

Second, there is a common misconception that the internet is required for voting machines to be hacked. Obviously, the WinVote hacked at DEFCON is particularly vulnerable because it creates a local network that is completely unprotected. But even for the machines in the Village (or real world) that do not, they are still not as distant from the internet as it may seem, and many contain software and hardware that can be used to connect them to the internet. Before each election, the ballots need to be created via a software application, which runs on a desktop computer or is web-based. From there, the formatted ballot is transferred and uploaded to voting machines through memory cards or USB sticks. And even well before election day – indeed before a voting machine is assembled, sold to a government, and brought online for an election – the foreign parts in the machines suggest multiple voting systems could be compromised by laying the seeds of future attacks in supply chain processes. This new revelation heightens concerns, and more must be done to protect our systems at every point in the process, including across the supply chain.

Finally, another common argument is that voting systems are insulated to a degree by the diversity and decentralized nature of our election infrastructure. It is true voting systems do vary greatly from state to state, making it difficult to penetrate multiple voting machines simultaneously. Yet, the confirmation of foreign-made parts and software raises the possibility that hackers could take remote control of at least an entire line of voting machines at a later point, with the right level of access in the supply chain. And as pointed out, machines also touch the internet and non-networked forms of data transmission (USB sticks, etc.) at various other points in the process, potentially weakening resilience if not done very carefully. Yet even if that did not happen, the Voting Village helped to show that simply manipulating a voter file (or in the Village's case, poll book data) could create enough problems or long lines to affect an election outcome.

Next Year's Voting Village: Moving Forward

The Voting Village will return to DEFCON in 2018. Organizers hope to expand the event next year to potentially cover a number of distinct areas in addition to hands-on hacking of voting equipment, including:

- **Closed-Loop System:** We would like to have a closed-loop system on which we can run an entire mock election using actual voting technologies. This would include voter registration, ballot generation, a mock polling place (with rules of engagement), and results reporting. This addition would allow us to go a step beyond just looking at the machinery of democracy on the technology level.

- **Election Tech Range:** Election officials and voting system manufacturers have some of their own security technologies, compositions, or solutions that they find work well in defending against certain threats. We would like to invite election officials and voting system vendors to come and get advice and even testing of their tech. A good example would be if an election official or manufacturer would like to get feedback on a particular security system or challenge security researchers to evaluate it and give feedback on how it could be improved.

- **Election Tech Challenges:** There are a number of activities in elections that are difficult to secure. Some small fraction of votes are cast by email, fax, and web and a larger fraction cast on paper through vote-by-mail. We would like to set up examples of these technologies and challenge Voting Village attendees to demonstrate what failures can happen and to what extent those can be avoided.

- **Election Technology Usable Security Evaluations**: A secure voting system can still be highly usable. We would like to invite usable security researchers to join the village to build up a resource of usability and needs assessment conclusions and profiles of past, existing, and future voting technologies.

- **Request for Donation of Machines, Software, Databases, etc.**: DEFCON has embraced the notion that the DEFCON hacker community's role in the election security debate is one of providing a public service. To that end, DEFCON is offering to test any clerk or secretary of state's election administration equipment and provide training for their IT staff at DEFCON 26. Our door is always open to those who want to make their voting process more secure.

Conclusion

DEFCON organizers believe the Voting Village was vital to growing the base of knowledge, expanding the circle of stakeholders beyond hackers, and shining a national spotlight on the serious cybersecurity weaknesses of U.S. election infrastructure.

The next step is to make clear that this is a conversation that cannot "stay in Vegas." It is imperative that leaders at the federal, state and local level come to understand this threat as a national security imperative and work together – leveraging the support of the national security and cybersecurity community – to better defend and protect the vote from cyberattacks in the upcoming elections in 2018 and 2020. Americans need the reassurance that their democracy is safe, starting at the ballot box.

Acknowledgements

A number of individuals and organizations contributed to the Voting Village and to this report. A special thanks to:

- Organizers, subject-matter-experts and other visionaries who turned the Voting Village concept into a reality and helped to author this report, including especially Sandy Clark.
- ISP/CyberBit and the Cook County, Illinois Clerk's Office for supporting the cyber back-office simulator at the Voting Village;
- Speakers who contributed to the Voting Village discussions including representatives from the Center for Democracy and Technology, Center for Election Integrity, the Center for Internet Security, the National Governors Association, the U.S. National Institute for Standards and Technology (NIST), and Verified Voting.

APPENDIX #1: Partial List of Attending Individuals & Organizations

Representatives attended the event from a variety of organizations including:

- Atlantic Council
- Aries Security
- Cisco
- Center for Internet Security
- Election Assistance Commission (EAC)
- IBM
- McAfee
- Microsoft
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- National Institute for Standards & Technology (NIST)
- National Governors Association (NGA)
- Nordic Innovation Labs
- Rochester Institute of Technology
- University of Buffalo
- University of Pennsylvania
- University of Texas San Antonio
- US-Computer Emergency Readiness Team (US-CERT)
- U.S. Department of Homeland Security (DHS)
- U.S. Senate Homeland Security & Governmental Affairs Committee
- U.S. Representative Will Hurd, Congressional Cyber Caucus (R-TX)
- U.S. Representative Jim Langevin, Congressional Cyber Caucus (D-CT)
- Verified Voting

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu