DEF CON 26
Voting Village

Report on Cyber Vulnerabilities in

U.S. Election Equipment, Databases, and Infrastructure

September 2018

Co-authored by:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago
Harri Hursti, Nordic Innovation Labs
David Jefferson, Verified Voting
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEF CON

Contents

Introduction - "Election officials have plenty to learn from hackers"

By: Alex Padilla, Secretary of State, California
Originally published: *The Hill,* August 19, 2018[1]
(reproduced with permission of the author)

Every year, DEFCON convenes thousands of hackers who attempt to breach the security of important technologies in an effort to expose vulnerabilities. For the past two years, this has included voting machines in a room dubbed the "Voting Village."

Rather than watch from the sidelines, or read about the findings in the news, I wanted to see for myself. So, I went to DEFCON. I listened, I observed and I had the opportunity to address attendees.

While it's important to constantly search for and understand the vulnerabilities of any voting system, a unifying message at the conference — from hackers to elections officials alike — is that we must be on alert and Congress must invest more to better secure our elections.

Threats to the integrity of our elections are constantly evolving. Not too long ago, a primary focus for election officials was securing voting machines. Today, cyber attack vectors have expanded — and so must our defenses.

This includes protecting our state voter registration databases, county election management systems, election night reporting websites, state and local government social media accounts and ensuring the information voters consume is accurate.

Intelligence officials tell us that the "warning lights are blinking red" — and our adversaries are getting more sophisticated. It's clear to me, as California's chief elections official, that we cannot become complacent.

That's why attending DEFCON was important. Though, as my secretary of State colleagues are right to point out, the environment under which voting machines were "hacked" at DEFCON do not precisely reflect real-world conditions.

On Election Day, voting machines aren't left on tables to be opened or exposed for hours on end, and there isn't unlimited public access to equipment at polling places or county offices.

Still, we could learn a lot from friendly hackers. Their insight can help us stay one step ahead of those who seek to undermine our democracy. It forces us to take second, third and fourth looks at systems. Elections officials must constantly scrutinize, test, adapt and upgrade security measures.

But no matter how much we learn or how much we innovate, we cannot succeed without adequate resources. Election administrations in America has been historically underfunded and understaffed. The burden of funding for election administration typically falls on the limited budgets of local governments.

[1] Padilla, Alex. "Election Officials Have Plenty to Learn from Hackers." The Hill. August 21, 2018. Accessed September 25, 2018. https://thehill.com/opinion/cybersecurity/402458-election-officials-have-plenty-to-learn-from-hackers.

States have a responsibility when it comes to properly funding election administration, including security. I'm proud that in California we secured $134 million in this year's budget to upgrade or replace voting systems plus additional funding for the creation of the offices of Election Cybersecurity and Enterprise Risk Management.

We're also updating hardware and software, monitoring our networks around the clock, and we've strengthened communications and information-sharing channels with federal authorities.

Still, we can and must do better.

You may have heard that Congress recently appropriated $380 million for election security nationwide. Not quite. Remember butterfly ballots and hanging chads? The recent federal appropriation was simply the final disbursement of money originally approved in 2003 to address the debacle of the 2000 presidential election in Florida.

There has been no new additional funding authorized to address our modern security challenges. To make matters worse, this month, the Republican majorities in both the House and the Senate defeated measures that would have appropriated $250 million for election security grants to states.

Meanwhile, they approved a $700-plus billion national defense appropriation — with not one cent for shoring up our nation's election systems.

Protecting our elections from foreign interference is a matter of national security. That's why our election infrastructure has been designated as critical infrastructure by the Department of Homeland Security.

For elections officials to implement needed election security measures, state and local governments need ongoing funding from federal and state budgets. We can't let up, and we can't rely on dated equipment. The stakes for our democracy are too high.

Until Congress takes our requests seriously and makes the necessary investments to further fortify our voting equipment and systems, election officials must think and act outside the box.

While I'm told I was the first secretary of state to attend DEFCON, I'm confident I won't be the last. We have a responsibility to learn from hackers, particularly those wanting to help. We owe it to the nation to do all we can to protect our elections.

Nothing short of our democracy is at stake.

New Findings on the Eve of the 2018 Midterm Elections

Back for its second year at DEF CON, the world's largest and best-known hacker conference, the Voting Machine Hacking Village (Voting Village) dramatically expanded its hands-on activities and audience in advance of the 2018 midterm elections. When the Voting Village first launched in 2017 - and was attended by thousands of white hat hackers, government leaders, and media - it aimed to identify vulnerabilities within the U.S. election infrastructure. In 2017, intelligence about Russian adversaries hacking the 2016 presidential election was increasing but the severity of the threat to U.S. election infrastructure was dying down. This year, DEF CON dramatically expanded its inquiries to include more of the election environment, from voter registration records to election night reporting and many more of the humans and machines in the middle. DEF CON had a greater variety of voting machines, election officials, equipment, election system processes, and election night reporting. Voting Village participants consisted of hackers, IT and security professionals, journalists, lawyers, academics, and local, state and federal government leaders.

This year, the Voting Village made more than 30 pieces of voting machines and other equipment available to its participants. All of the equipment (with the exception of the AVS WINVote, described below) is still used throughout the United States today. The Voting Village is the only public forum in United States at which hackers have nearly unrestricted access to discover vulnerabilities in the equipment. In addition, this year the Voting Village conducted unprecedented outreach to state and local election officials, inviting them to participate in the Village's activities and receive free training from cybersecurity experts.

As was the case last year, the number and severity of vulnerabilities discovered on voting equipment still used throughout the United States today was staggering. Among the dozens of vulnerabilities found in the voting equipment tested at DEF CON, all of which (aside from the WINVote) are used in the United States today, the Voting Village found:

- A voting tabulator that is currently used in 23 states is vulnerable to be remotely hacked via a network attack. Because the device in question is a high-speed unit designed to process a high volume of ballots for an entire county, **hacking just one of these machines could enable an attacker to flip the Electoral College and determine the outcome of a presidential election**.

- A second critical **vulnerability in the same machine was disclosed to the vendor a decade ago**, yet that machine, which was used into 2016, still contains the flaw.

- Another machine used in 18 states was able to be hacked in only two minutes, while it takes the average voter six minutes to vote. **This indicates one could realistically hack a voting machine in the polling place on Election Day within the time it takes to vote.**

- Hackers had the ability to **wirelessly reprogram, via mobile phone, a type of electronic card used by millions of Americans to activate the voting terminal to cast their ballots**. This vulnerability could be exploited to take over the voting machine on which they vote and cast as many votes as the voter wanted.

Further, in partnership with two other DEF CON villages, including r00tz Asylum, which allows children (accompanied by an adult) to learn and test white hat techniques, and Capture the Packet (CTP), the most popular competition at DEF CON, young DEF CON attendees were given the opportunity to hack mock ups of secretary of state election results websites for the thirteen Presidential Battleground States. In less than

10 minutes, an 11-year old in the competition hacked into a mock up of Florida's election results website, changing its reported vote totals. The attack the children were trained to use on the sites (SQL injection) is the same attack the Senate Intelligence Committee warned was used in a majority of Russian cyber attacks on election websites in 2016.[2] Further, the Open Web Application Security Project (OWASP), one of the leading organizations on website security globally, has cited this type of attack as the top web application security risk for organizations around the world.[3] While children in the r00tz Asylum village used this vulnerability for a variation of 'de-facing,' which is generally considered to be an easily found, "show-off" attack, in the hands of more skilled and malicious adversaries the underlying vulnerability can be used to initiate much more serious types of attacks.

Aside from introducing the youngest members of the DEF CON community to issues related to civics, media, and cybersecurity, the r00tz Asylum exercise was ***the first time the voting public was made aware of how fragile our election night reporting systems are to the ultimate fake news: hacked election results***. No organization can protect a website from a determined nation-state, as was evidenced by the Iranian attacks on nearly dozens of financial institution websites from 2011 to 2013. The financial industry spends billions on cybersecurity and hires some of the best cyber defenders on the planet to protect their systems. Yet even with all their resources, they could not stop a determined nation state from hacking their websites despite two years of trying. Even more disconcerting, Russia has already executed an attack on election reporting websites in Ukraine, changing results and announcing the prefered Russian candidate won when in fact he had not. Thus democracies around the world need to prepare for this threat. DEF CON is stepping up as the first organization to publicly release Election Day crisis communication protocols (below) for election jurisdictions across the globe to train in advance of Election Day.

Over 100 election officials passed through the Voting Village over the course of three days, with many training on the KIG CyberRange generously donated to the Voting Village by Cyberbit. The CyberRange is a virtualized environment allowing election officials to be trained in defending a voter registration database and simulated state-of-the-art attacks. This year the defenses of the virtual election office were beefed up by an order of magnitude from the last year's exercise. Further, to our knowledge, this is the only capture-the-flag style training available for election officials to learn how they can protect a voter registration database from attackers already in their network.

High-profile experts lined the speaking track at the Voting Village. Speakers included leaders from the Department of Homeland Security; state and local election officials, including Alex Padilla, Secretary of State of California; Noah Praetz, Director of Elections for Cook County, Illinois; Neal Kelley, Chief of Elections and Registrar of Voters for Orange County, California; Amber McReynolds, former Director of Elections for City and County of Denver, Colorado; and the senior *New York Times* correspondent and best-selling author, David Sanger. Biographical information can be found more in detail in Appendix #2.

The unprecedented attendance of election officials at DEF CON did not happen by accident. The Voting Village sent thousands of invitations via mail and email, and even made 2,500 live phone calls to election officials across the country.

---

[2] US Senate Intelligence Committee, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInst lmt1-%20ElecSec%20Findings,Recs2.pdf.

[3] "OWASP Top 10 Application Security Risks - 2017, " *Open Web Application Security Project,* Accessed September 21, 2018, https://www.owasp.org/index.php/Top_10-2017_Top_10.

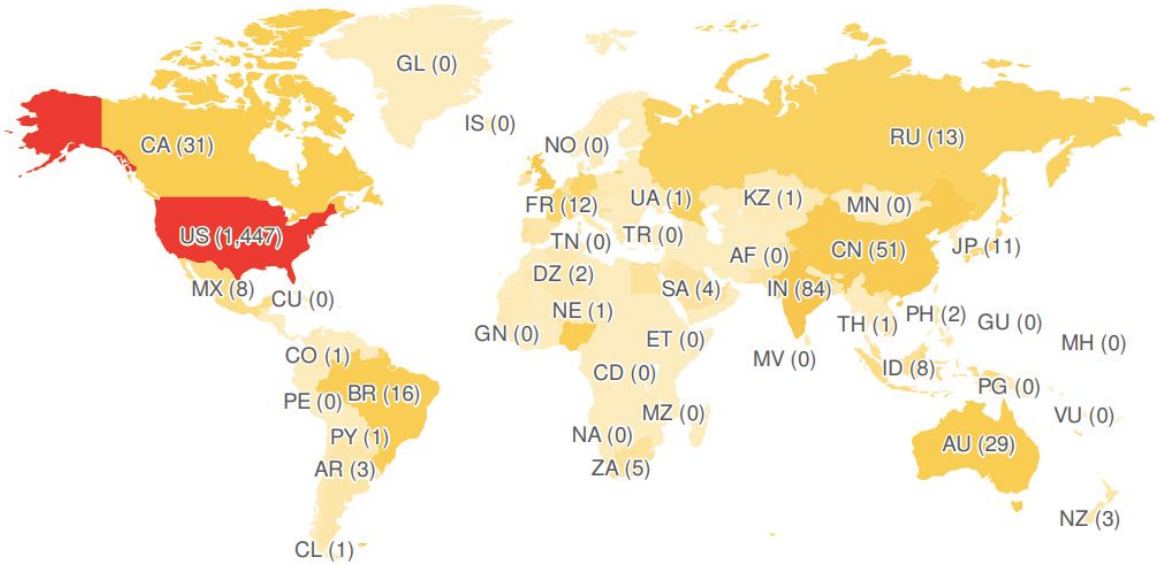
Matt Blaze, co-founder of the Voting Village, said, “It’s been incredible, the response we’ve received. We’ve had over 100 election officials come through here and they expressed over and over again how much they have appreciated learning from this opportunity.”

He went on, “Before the first DEF CON Voting Village in 2017, there were only a handful of experts on voting infrastructure cybersecurity in the United States, as well as an unknown number in Russia. Now, thanks to the efforts of the Voting Village, there are thousands of experts. Now is the time to leverage that expertise to improve election security across the United States.”

Harri Hursti, another co-founder of the Voting Village, added: “It would be extremely expensive for professionals and trained experts to match the diversity of ideas, approaches, speed, and overall creativity generated by this unorganized, large group of highly skilled people working on a common objective. The reason why many industries and government agencies have implemented bug bounty programs and other ways of crowdsourcing security work is because they are incredibly effective tools to capture this energy and innovation to help to improve their own security. For the U.S. election system, the challenges at hand are much larger than just software bugs: there are fundamental design issues to sort out and fix. The innovation inherent in this kind of exercise can be of immeasurable impact.”

Media Overview

The public and media response to the second year of the DEF CON Voting Village has been truly staggering, both in terms of its reach and in terms of the conversations it has sparked about election security. In total, the media coverage following the annual DEF CON Voting Village reached more than 2.8 BILLION people. As reflected in the Heat Map below, almost 2,000 media stories were published world wide, covering every major continent except Antarctica.



Not only did prominent publications such as *The Washington Post,* CNN, *The Wall Street Journal*, *The New Yorker*, and BBC cover the event, the Voting Village also engaged with an active audience via social media, which touched more than 146 million people. Twitter alone garnered 33,400 engagements from just one tweet on the opening day of the DEF CON Voting Village. Since July 24, 2018 and covering the dates of DEF CON, Voting Village tweets earned 1.4 million impressions, with high activity during the event itself. With a successful and active media outreach, social media accounts continued to generate interest throughout the event. With thousands of followers, the Twitter handle for the Voting Village (@VotingVillageDC) provided continual updates on what was occurring at DEF CON, engaging followers and interested parties inside and outside the event.

Other top publications that covered the event included *TIME*, *USA Today*, CNBC, *Reuters*, NBC News, *The Los Angeles Times*, ABC News, and *Politico*. Articles covered the vulnerabilities of election infrastructure and the variety of machines investigated at the event. Some news sources developed the conversation further, covering not only the threats posed to traditional election infrastructure but the rising threat of disinformation. CNN, for example, after highlighting the importance of the work being done at DEF CON, used the hacker conference as a discussion platform to voice its fear of a future influence by coordinated information warfare campaigns. Additionally, top officials from DOD, NSA, DHS and the U.S. Congress attended the Voting Village.

Equipment

The Voting Village organizers procured a variety of voting equipment for examination. The 2015 Digital Millennium Copyright Act exemption issued by the Library of Congress for good faith security research allowed Voting Village participants to find vulnerabilities without worrying about anti-circumvention liability. Prior to 2015, hackers might have faced significant liability for some of the research described in this report. Most of the equipment in the Village was purchased by DEF CON on secondary markets, such as eBay and government surplus auctions. The machines and equipment featured in the Village included:

- Dominion: Premier/Diebold AccuVote TSx
- Dominion: Diebold AccuVote OS
  This machine was lent to the Voting Village by an election official for display purposes only. Because it was needed for use in the midterm elections in November 2018, it was not used for any research or analysis by Voting Village participants.
- Dominion: AVC Edge
- ES&S: ExpressPoll Tablet Electronic Pollbook
- ES&S: M650
- AVS: WINVote
- AVC Edge activation device
- ACOSJ dual interface Java card

In addition, the Voting Village also featured the KIG CyberRange powered by Cyberbit, which provided a virtual exercise that was designed to mirror an Elections Voting Office. In a safe, virtual, and isolated network, hackers were asked to use common tools to penetrate a web application behind firewalls and manipulate records. The CyberRange exercise leveraged Kali Linux, which is a common Linux distribution including a wide range of free hacking tools and used by hackers, security professionals, and researchers today. Using the Kali Linux toolset, the hackers attempted to perform attacks like SQL Injections as a means to compromise the simulated elections office and exfiltrate the data designated as the target. However, it is noteworthy that Kali Linux offers only a small subset of the tools real cyber criminals have at their disposal. Offering Kali Linux was to facilitate participation without requiring hackers to bring their own computers and tools. However, it was also a disadvantage for the attackers as they were limited to certain tools and an environment which they may not have used otherwise.

The KIG CyberRange depends upon Cyberbit simulation technology. The Range is deployed as an isolated virtual environment, giving KIG the ability to customize network configurations to mirror real-world environments and develop unique attack scenarios.

As in the real world, the virtual exercise was not timed, and hackers were encouraged to continue trying to hack the system as long as they desired. Several made it past the web application, but none were able to penetrate the last firewall to retrieve voter records. Had hackers been successful, it is possible they could have potentially altered voter polling data – changing polling data or adding/deleting records. However, no hackers were successful in getting to the data in the simulated virtual attack exercise. It is noteworthy that this year the defenses of the virtual election office were fortified using Israeli military defense software, while attack tools were limited to what is available with Kali Linux.

The Voting Village does not manufacture opportunities for hackers to easily exploit the elections system. It is a forum for experimentation to improve the security of the U.S. elections infrastructure. The fact that no

one was able to fully penetrate the last firewall in the exercise provides useful information on a way to better protect voter data. If any state or local election official would like to better understand how the CyberRange works, please reach out to votingmachinevillage@gmail.com for more information.

Limitations

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

- Participants only had access to publicly available information and the contents of the machines. In contrast, nefarious actors would not be so constrained, and could attempt to gain access to proprietary information.

- The Voting Village provided a sample of voting technologies. Organizers obtained what they could get their hands on quickly, legally, and affordably.

- The Voting Village did not provide any Election Management Systems to attendees. In a real election environment, this system is a key element as originator and aggregator of election data, and in formal studies it has been found to be the most vulnerable element, particularly in its capacity to radiate additional attack surfaces and vectors across the elections system as a whole.

- Finally, there was no access to any backend provisioning or voter registration systems. These kinds of systems are not generally available on the open market.

"Election Security is National Security"

By: Rob Joyce, Senior Advisor for Cybersecurity Strategy, National Security Agency
Originally published: *The Cipher Brief*, September 27, 2018[4]

Opinion - Many different organizations and individuals need to pull together to ensure we have secure and trustworthy elections. The distributed nature of our elections throughout the state and local governments means there are widely varying levels of expertise and resources available, even when state and local officials leverage the federal government for support. This election infrastructure can be expansive, and includes the voting machines themselves, the tabulation processes, the voter registration databases and the associated networks. Each of these requires a detailed focus from many entities to protect against adversaries seeking access to data for influence operations, threatening the availability of the services, or posing threats to the integrity of the information.

I recently caught a glimpse of the kind of offensive focus I'm talking about at the Voting Village at DEF CON 26. I witnessed private individuals donating their time to improve the security of our election processes. They've made incredible contributions, and are offering advancements for federal, state, and local election programs, as well as insights for the manufacturers of voting technology. Strongly connecting all the contributors to our election process needs to be a goal for improving election security. These connections are vitally important to ensure everyone is aware of the threats, best practices and needed improvements.

Amazing talent and expertise gathers at DEF CON with an enthusiasm to make things better. The combination of skilled cybersecurity experts in partnership with industry and the ultimate end users of the technology – state and local election officials – is a powerful alliance. . . . Steering the voting village to similar collaborative relationships will take us to the next level and address the constant erosion of trust, which only helps further the objectives of our adversaries.

Ignorance of insecurity does not bring you security. As time passes, the security of any device begins to erode. New exploitation techniques are developed. New investigative tools are created. Zero days are discovered in operating systems. The capabilities and repertoire of the exploiters grows. Developers of the security models for a device can never predict every creative idea that will be tried during exploitation. For these reasons, we need to continuously red team our devices and processes. This independent testing provides great benefit by straining assumptions and uncovering hidden flaws.

Another key aspect of securing our election processes is simply focusing on the fundamentals. As we embrace electronic technology, the basic security practices of updating and patching are critical. Having strong adherence to recommended security design practices is vital. Often, paying attention to detail in the things that we already know how to do, removes significant risk.

While DEF CON continues to foster a venue to investigate election infrastructure in the Voting Village, the focus cannot simply be about calling out the state of security in our current technology. Rather the result needs to be developing tangible actions that lead to collaborations that will make us more secure.

[4] Joyce, Rob. "Election Security is National Security." The Cipher Brief. September 27, 2018. Accessed September 27, 2018. https://www.thecipherbrief.com/column_article/election-security-is-national-security.

Election security is a matter of national security, and there's no question that progress has been made since 2016 – government-industry partnerships exist today that simply did not exist even a year ago. These security-focused engagements between election officials, the federal government, and vendors will undoubtedly contribute to making the 2018 mid-terms the most secure elections in recent memory. But there's more to be done, and securing our elections is like a race without a finish line. Together as a community – hackers, government and industry – can bring powerful assurances to a foundational component of our freedom: fair and trustworthy elections.

Technical Findings

Diebold ExpressPoll-5000
The Diebold ExpressPoll-5000 is an electronic pollbook, designed for use by individual pollworkers. It is used in precincts to check voters in before they are permitted to vote. The product line currently belongs to ES&S, but the ones used at DEF CON were models running Diebold-branded software, which is also still in use in several places in the U.S. Its operating system is a version of Windows CE, a system built by Microsoft for embedded applications. The pollbook application software was version 2.0.27. The data in an ExpressPoll-5000 is stored on a removable Compact Flash card with additional ability to utilize PCIMCI cards.

The principal investigators of the ExpressPoll-5000 machines at DEF CON were Miguel S., a software engineer, and Akin O, a Nigerian application software security engineer. These investigators were able to access the file system and read and write the voter databases using SQL Lite, a free database program widely available. The investigators found entries in the database where the passwords to the ExpressPoll-5000 were stored in cleartext.

The root password for the machine was “password”.

The admin password was “pasta”.

There are several security mistakes here if a jurisdiction is serious about security. First, the root password is apparently unchanged from the operating system default. When setting up a new machine the first thing one should always do is assign a new root password. It also is extremely bad practice to store passwords *in the clear* (i.e. unencrypted) and in a place that will ever fall into someone else’s hands (as this ExpressPoll-5000 did). Presumably any poll worker in the jurisdiction from which this machine came can use the passwords to gain control of the machine and make arbitrary changes to it.

The admin password, “pasta”, is probably not the default password, i.e. it probably was changed to that when the machine was configured. But it is a poor choice because it is short, all lower-case, and contains no digits or special characters. More significantly, it does not matter what the admin password is if the root password is the default value, since the root user has more privileges than the admin user. Additionally, it demonstrates that Federal Information Processing Standard rules, as defined by the National Institute of Standards and Technology (NIST), are not enforced by the software.

Dominion AVC Edge
The AVC Edge is an electronic voting machine manufactured by Sequoia Voting Systems, later acquired by Dominion Voting Systems. It is a touch-screen machine with direct-recording electronic capabilities. It is activated by a smart card, and records votes on internal flash memory. Each unit contains a slot for a vote activation card. After the voter’s ballot is cast, the smart card is deactivated to prevent multiple votes from being cast. Votes are subsequently documented. When polls close, the votes recorded in each machine are either physically or electronically relayed to election headquarters. It is currently in use in Arizona, California, Florida, Illinois, Louisiana, Missouri, New Jersey, Pennsylvania, Washington, and Wisconsin.

As the whole execution environment is stored on the removable storage device with no permanent physical security protections in the form of locks or even tamper-evident seals, researchers were able to simply open the machine’s outer casing with common screwdrivers, gain access to the storage device slot, and

swap the device with a new device with a different operating system installation and application. Tamper-proof seals specific to a particular election would not protect against this, as an attacker would only need to swap out the removable media once during the lifetime of the device.

In the Voting Village the removable media were replaced with new media with completely different programming to verify that there were no security measures, such as secure boot or cryptographic signatures, preventing the device from accepting arbitrary new programming. Though old, the AVC Edge hardware is common; therefore there are no obstacles to creating rogue software deployments for the device.

Dominion Premier/Diebold AccuVote TSx

The AccuVote TSx is an electronic voting machine manufactured by Premier Voting Solutions, later acquired by Dominion Voting Systems. The product line currently belongs to ES&S, but it is unclear if the machines used at DEF CON are Dominion or ES&S products. The AccuVote TSx is currently in Alaska, Arizona, California, Colorado, Florida, Georgia, Illinois, Indiana, Kansas, Missouri, Mississippi, Ohio, Pennsylvania, Tennessee, Texas, Utah, Wisconsin, and Wyoming.

During DEF CON, the Voting Village organized a mock election to demonstrate vulnerabilities in the AccuVote TSx. The software used in the demonstration was unmodified from the software that is still used widely. Additionally, there are older, potentially more vulnerable versions of the software still in use.

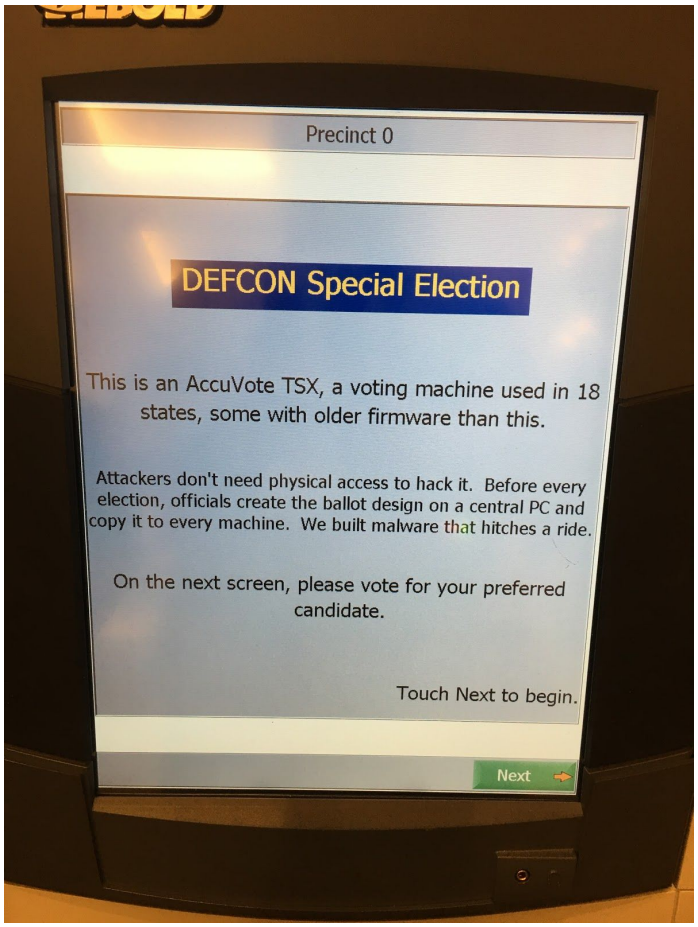
The mock election demonstration consisted of multiple elements:

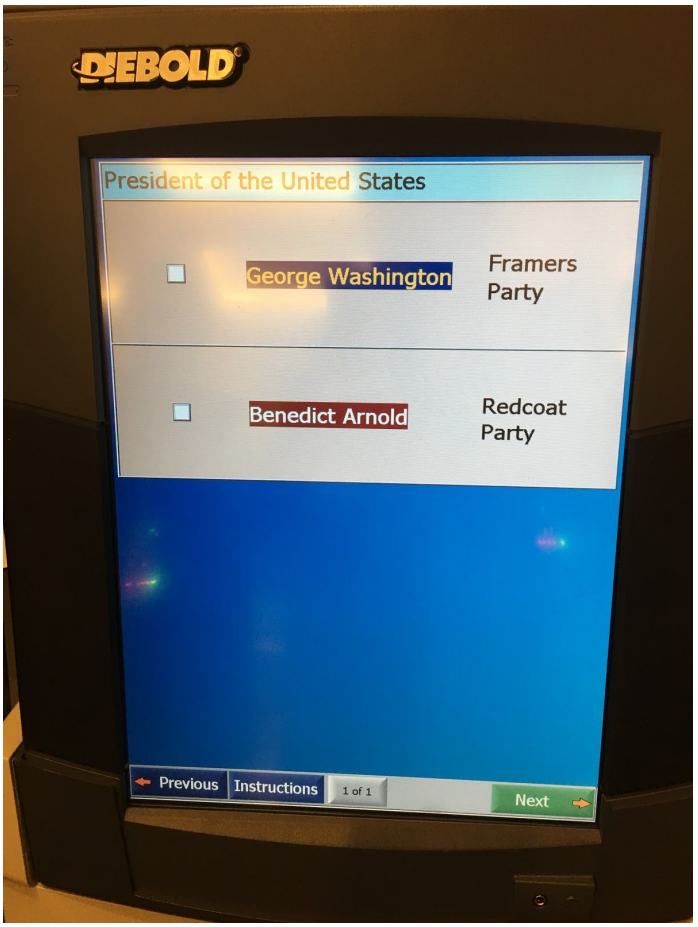
- All voters used the same voter activation smart card without the card being reactivated with a device of any kind to allow the next voter to cast their ballot. This is because the voter activation card was programmed to automatically reset itself after activating the device, therefore allowing it to be used to cast unlimited number of ballots.

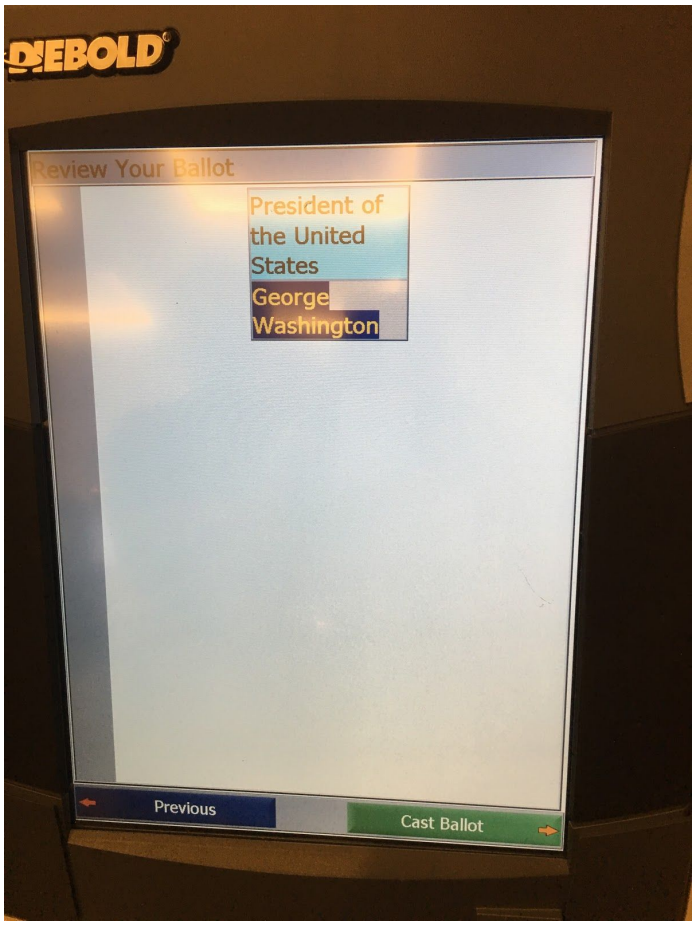
- The election was programmed without using software provided by the vendor, therefore proving that a chain of custody of the election management software does not prevent new elections from being programmed. This also indicates that third parties with no access to the election management system can create rogue election definitions which are indistinguishable from real elections.

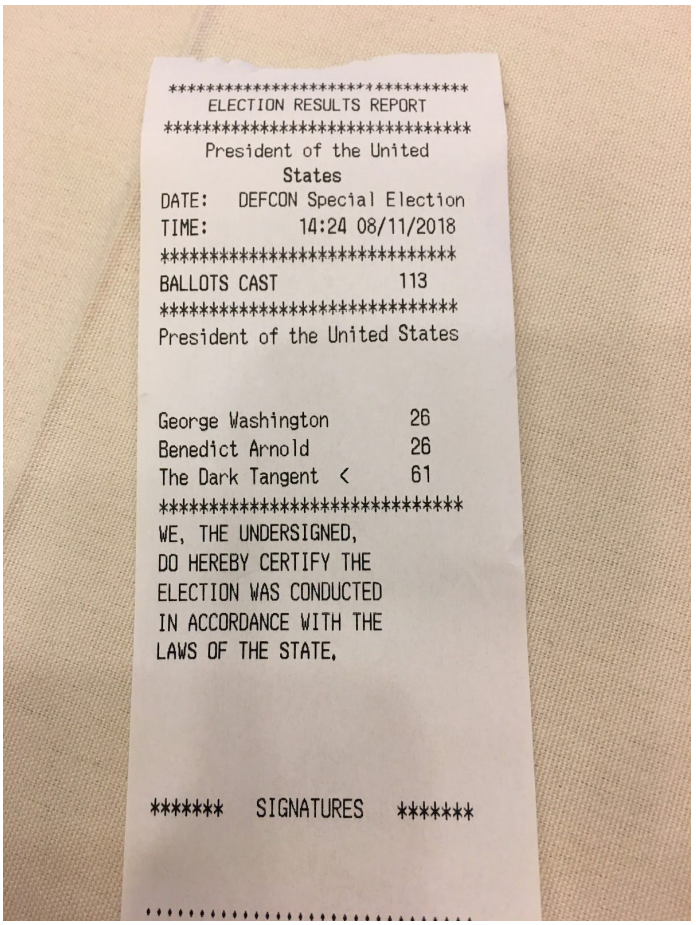
- An attack can be distributed remotely with no physical access to the voting machine. Malware needed in this demonstration can be distributed with the ballot/election definition. This also demonstrates the mechanism enabling a wholesale attack. Depending on how a particular county's system is set up, there may be multiple centralized systems in the chain of the information flow to the voting machines, and compromising any of the links in the chain enables a wholesale attack.

- Paperless, unauditable systems are extremely vulnerable to this kind of attack, as the only record of a voter's intent is in digital form.


Precinct 0
DEFCON Special Election
This is an AccuVote TSX, a voting machine used in 18 states, some with older firmware than this.
Attackers don't need physical access to hack it. Before every election, officials create the ballot design on a central PC and copy it to every machine. We built malware that hitches a ride.
On the next screen, please vote for your preferred candidate.
Touch Next to begin.
Next


DIEBOLD
President of the United States
George Washington
Framers Party
Benedict Arnold
Redcoat Party
Previous
Instructions
1 of 1
Next


DIEBOLD
Review Your Ballot
President of the United States
George Washington
Previous
Cast Ballot


ELECTION RESULTS REPORT
President of the United States
DATE: DEFCON Special Election
TIME: 14:24 08/11/2018
BALLOTS CAST 113
President of the United States
George Washington 26
Benedict Arnold 26
The Dark Tangent < 61
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE,
****** SIGNATURES ******

As a surprise, the largest social media visibility from the village was for viral video posted by social engineer Rachel Tobac. At the time of writing, the video (https://twitter.com/racheltobac/status/1028437783050776576?lang=en) has been viewed over 2 million times. While this hack that Tobac demonstrated was known before DEF CON, we revisit it here in light of the renewed public attention. The AccuVote TSx voter activation smart card reader unit is held in the place by a flimsy piece of plastic which can be easily pulled from the main casing and re-installed. The process requires no tools, very little physical force, and can be done in a matter of seconds within the privacy shield of the voting machine. By separating the piece, an attacker gets access to the connector cable of the reader unit. If an attacker disconnects the cable, during the next start-up the voting terminal will allow the attacker to enter the system settings dialog without any authorization checks. This vulnerability allows an attacker to potentially disrupt the election process, but based on the current understanding will not affect the integrity of the votes.

ES&S M650

The M650 is an electronic ballot scanner and tabulator manufactured by ES&S. The ES&S M650 is used for counting both regular and absentee ballots. It launches ballots through an optical scanner to tally them, and keeps count on an internal 128 MB SanDisk Flash Storage card (pictured below). Election staff are responsible for configuring the M650 for each election. It is currently in use in Arkansas, California, Florida, Idaho, Illinois, Indiana, Kansas, Minnesota, Missouri, Montana, North Carolina, Nebraska, New Jersey, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Washington, West Virginia, and Wyoming.

The M650 runs QNX 4.2* on an Octagon 5066 Board with an AMD Am5x86 processor at 133MHz. QNX is a Real Time Operating System (RTOS) that has some loose parallels to modern-day Linux and Unix operating Systems. The version of QNX running on the M650's at DEFCON was last updated in 2008, and QNX 4.2 was released in 1996.

Physical Security

There is a common misconception that physical security precautions (tamper-evident seals, locks, etc.) keep voting machines safe from malicious attacks. While all equipment was shipped to us with keys, the researchers wanted proof that the locks in the machine did not inhibit access. In under a minute, a Voting Village researcher picked the lock on the back of the M650 (pictured at left) and unlocked its case, gaining full access to the computer systems and electronics via a serial connection to the main board. Features of note include two OKI Microline 9-pin dot matrix printers connected to two exposed parallel ports, an exposed ethernet jack, and a ZIP disk reader/writer. There was no other type of tamper-evident security on the machine. Physical security such as this lock, even in a small county office, is not sufficient to protect voting systems.

Serial Terminal

With a $10 adapter (VTC-9F to DB-9 adapter cable, item 1041), a serial connection can be established to the M650 by connecting to the main 5066 CPU board. The connection is extremely simple to establish, as it uses the default serial parameters for popular, free programs like Putty and TeraTerm (Windows), as well

as Linux commands like `screen` (where the only requirement to successfully opening a serial console is specifying a baud rate of 9600). Connecting a laptop allows root access to a serial terminal session with username 'root' and no password. There is not even minimal account security.

From this connection, an attacker can tamper with election data. All these data are stored in `/flshdr/elecdata`, the mount point for the 128MB SanDisk Flash Storage device that is on a standalone board inside the M650 computer board cage. An attacker could also conduct a denial of service (DoS) attack against the system, or display any message to the screen or printers connected to the computer.

Furthermore, there exist commercially available tools which can be used to automate an attack of this nature, as well as small, commercially available devices which can be installed into this interface to enable remote and wireless access to this port. Because the serial is not used during normal operations, adding such a device without detection is possible. Researchers estimated that it would take one to two minutes to pick the lock, carry out the installation of the attack and relock the device.

Ethernet Port Vulnerability

The ES&S M650 voting machine has two communication media options - Ethernet connection or Zip drive. On the side of the M650 is an RJ45 jack. This connection allows the M650 to send data over a network to a system running ES&S Unity, the election management system software.

During bootup the M650 makes a DHCP request to obtain an IP address using the DHCP client provided in the QNX TCP/IP module, dhcp.client. This DHCP client shares a substantial amount of DHCP protocol handling code with the ISC DHCP server version 1.0.0, although the client-specific portions seem to be closed source. Version 1.0.0 of the ISC DHCP server has several known buffer overflows. However, we were not able to trigger these overflows with server-provided data in this client implementation.

After obtaining an IP, the M650 sends a packet on port 6500 to the Unity server expected at a fixed IP address. This initial packet carries the following hexadecimal payload: `01 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00`. The significance of this message (which is part of one of the TCP packets) is currently unknown.

Zip Disk Vulnerabilities

A second investigation of the M650's vulnerabilities revolved around the Zip drives and Zip disks used on the machine. The Iomega products that are used by the M650 are an old and obsolete removable disk technology. Zip disks were intended to be treated as if they were a "fat" floppy disks, but with a much larger capacity (100 MB or 250 MB compared to the 1.44 MB capacity of a common 3.5 inch "high-density" floppy).

There are eight different types of Zip drive devices, and each is different in terms of electronics, storage capacity and other aspects. As an added layer of complexity, the description of a 'super floppy' is an operating system-specific description, referring to Windows. Other operating systems commonly see the drive as more like a removable hard drive. In the M650 operating environment "Unity," the election management system uses a Windows Operating System while M650 itself uses QNX as its operating system. (Voting Village participants did not have access to Unity software.) Therefore they see and operate with the

drive and the file system(s) on it in an inconsistent way. The main difference is that a super floppy is a single file system, while the disk is not subdivided into separate sections, called partitions, which can not see each other - the hard drive type of media includes a partition table, which means that the disk can have multiple separate file systems. If the machine mounts one of the partitions assuming it is the whole disk, the computer will not be aware of the other file systems or the files stored on them.

As stated previously, the Zip drive's primary purpose is to store and transfer the election specific definitions and, ultimately, the results. However, the Zip drive also has the ability to alter or replace any and all of the programming stored on the internal storage devices. This kind of attack is called an advanced persistent threat (APT). APTs are a family of stealthy and continuous computer hack processes designed to be hard to detect, hard to clean, and potentially virally propagating.

On bootup, the M650 executes a startup script called "`sysinit`" (stored on the flash storage device, under `/flshdr/sysinit`). The `sysinit` script is run on every boot-up of the M650. It is responsible for starting drivers, mounting storage locations, and initiating an update. To decide if an update will be run, the machine runs this line:

```
if [ -f /dos/a/<redacted_1> -a -f /dos/a/<redacted_2>.etp -a -f
/dos/a/<redacted_3> ] ;
```

Although we have redacted the file names, they are all single, commonly used English words that can be easily guessed from the context.

In this line—one of the two checks required to perform an update—the machine runs a file presence check (`-f <file>`) on three files (`<redacted_1>`,`<redacted_2>.etp`, `<redacted_3>`) that should be on the zip disk (mounted as `/dos/a/`) to move on to the next step of running an update. This next step is even more trivial: a version check. The `sysinit` script, provided that it finds the three files listed above, runs this line to "check" version numbers:

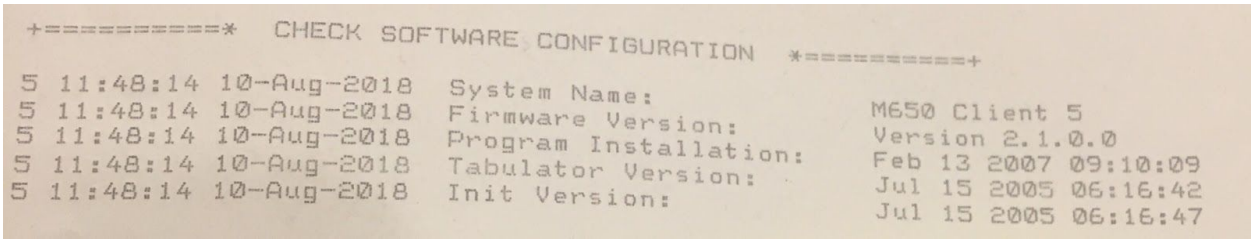
```
if [ "$new_vers" != "$curr_vers" ] ; then
```

This line simply ensures that the new version of software (read from `/dos/a/<redacted_2>.etp` on the zip disk) is *not the same as the existing version* (thus the use of the `!=` operator). The existing version is stored in (`/flshdr/<redacted_2>.etp`). By using the "`!=`" operator, the software could theoretically be downgraded as well as upgraded: a lower software version on the Zip disk would still make that "`if`" statement true. Following these two trivial and insecure checks, the machine continues to copy the update script to the root directory (`/`) and then runs:

```
display "Updating firmware to $new_vers."
/<redacted_1> &
```

Through this function, the machine checks for the presence of "`<redacted_1>`" (any script), "`<redacted_2>.etp`" and "`<redacted_3>`" on the Zip disk (mounted as `/dos/a/`) and, provided that the versions are dissimilar, runs the update script without checking any further. The lack of checks here would allow a knowledgeable attacker to run an arbitrary script on the machine - no integrity checks, passwords, or signatures are performed on any file from the Zip Disk (including the `<redacted_2>` script itself). The system also lacks any kind of potentially security-enhancing subsystems like sandboxing. If the

M650s are networked at the clerk's office, this vulnerability would allow a malicious actor to spread malware across the network, possibly infecting other machines.



Zip drives and Zip disks are discontinued end-of-life products, but the M650 depends upon this technology for loading and updating its software and firmware. This causes a number of serious security vulnerabilities. If a Zip drive in an M650 fails, it is difficult to replace. However, the Zip disks are even more problematic. Often jurisdictions have to buy them used, which means that they have already been formatted, probably on a Windows machine, and they may have files already recorded on them. Even if bought from Amazon, they in turn may have been purchased from random eBay sellers.

A Windows-formatted disk can be read by a machine running QNX. Thus, a used Windows-formatted Zip disk with files recorded on it will appear to work normally when inserted into an M650. But this necessary and useful capability opens the door to a serious security vulnerability.

The two operating systems, Windows and QNX, use different device drivers, volume drivers, and file system implementations. In fact, the QNX operating system is not on the list of officially supported operating systems for Zip disks, so presumably someone originally ported the Zip software from yet another platform, possibly Linux, with an unknown level of testing and skill. This leads to the possibility of differences in the two operating systems' use of Zip disks, and we know such differences exist at least in their handling of partition tables on Zip disks. Generally, with independent implementations on different platforms of the "same" software one always expects different behaviors in corner cases, different bugs, and different error behavior, leading to security vulnerabilities when the implementations attempt to interoperate.

One major potential security vulnerability arises from the possibility that used disks originally written on a Windows or Mac machine might be procured and used on the M650 without being reformatted. In that case the differences in operating systems provides a potential vector for attack. As described elsewhere in this report, a Zip disk is used to update the software of the M650. If there is an executable file named "update" on the disk at the time the M650 is booted (and a couple of other simple conditions are met) then the M650 will immediately run the update program. Normally the update program would install a new version of the code running on the M650, but it could do literally anything else, including inject malware to miscount votes or inject a virus that could spread among all the M650s in a jurisdiction through the exchange of Zip disks.

A clever attack on an election would start by the attacker writing a malicious QNX executable file named "update" on a bunch of Zip disks and giving those files the Windows attributes `hidden` and `system`. Then the attacker could find a way to offer those malicious disks for sale to a jurisdiction that needs more Zip disks and is having trouble buying brand new ones.

If an IT person inserts one of the malicious disks into an M650 without reformatting it first, the update file

will immediately and silently install the malicious software into the M650, thereby undermining the integrity of the election. If the IT person took the precaution of examining the contents of the Zip disk first, he or she would see nothing because the files have the `hidden` attribute. If he took the further precaution of issuing a command to delete all files from the Zip disk, the malicious files would not in fact be deleted because they are marked with the `system` attribute. Only if the disk is reformatted on a known clean machine before being inserted for the first time into an M650 would the malicious update file be destroyed.

It is very doubtful that the operators of M650s all over the U.S. are aware of the necessity of this precaution of reformatting every Zip disk before using it in the M650. As the M650s get older and Zip disks become scarcer, this vulnerability grows in importance.

This is an example of a broad class of vulnerabilities that are well-known in the computer security world — `autoplay` or `autoexecute` features in removable storage media alongside with Master Boot Record and other types of lower level attacks. We have seen attacks like it before with the auto-update feature in Diebold voting machines through their memory cards, and similar capabilities in other vendors' voting machines. We have also seen it historically with autoexecute features in CD drivers, in email clients, and in thumb drives (the latter believed to be one of the ways Stuxnet was introduced into the Natanz uranium enrichment facility in Iran). But the new feature here is that the scarcity of obsolete Zip disks will drive M650 jurisdictions to buy them from second-hand sources. Such disks must be treated as contaminated, even if they appear clean.

In other words, the M650 is simply looking for a file with a certain file name and is trusting it and executing it with the maximum level of privileges, which has never been an acceptable practice from a security point of view. This practice is made more dangerous because the different operating systems involved in making data hygienics difficult and making it possible to hide critical files, and even complete file systems, and making those potentially able to survive many commonly utilized methods of erasing content.

If the machines are disconnected from a network the attacker could initiate the printout of a false report from the report printer or Zip disk - the means used to record the totals. Of course, the attacker can also, through this vulnerability, change election data stored on the machine and create matching false digital records to be reported to the central tabulator.

Any of these vulnerabilities seriously compromises the integrity of an election. They require no passwords and necessitate only basic knowledge to successfully complete. **The dangerous update procedure was documented but file names were redacted in the 2007 EVEREST report because of the grave security risk.**[5]

Mitigation against this combination of factors would require additional measures for the secure cleaning of all residual data from the drive on the lowest level possible - not only when the drive is put into use, but also between every instance it is used in order to prevent a viral attack to utilize the drive as a distribution media in and of itself. All storage devices or removable media should be formatted before first use in any machine that is part of, or networked with, any voting system. This has to be a routine precaution faithfully practiced. Injection of malicious software through unclean media is one of the ways that it is possible to hack voting systems that are not connected to the Internet. Isolating a voting system from the Internet is

[5] Pennsylvania State University, the University of Pennsylvania, and WebWise Security Inc, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Compiled by Patrick McDaniel. By Matt Blaze and Giovanni Vigna. December 7, 2007. Accessed September 25, 2018. https://www.eac.gov/assets/1/28/EVEREST.pdf.

necessary to protect it, but it is not sufficient. Malicious logic can enter by other means, and only careful diligence (or luck) can prevent it.

Cross-Device Vulnerabilities: Smart Cards

Several types of voting machines, including the Dominion Premier/Diebold AccuVote TSx and the Dominion AVC Edge, use smart cards to enable voters to vote on Election Day. Smart cards are commonly also referred as Java-cards, as the chip on the card is a low-powered computer which runs programs written in Java, a common programming language. When the card is plugged in, it gets its power from the connection to boot up. Once up and running, the card starts to communicate with the host computer. In the election environment, the smart card is set up for the voter to cast their ballot either by an ePollbook, such as the ExpressPoll 5000 (discussed above), or by a specialized programming device called Voter Card Encoder (VCE). It can also be used to select the voter's ballot.

Researchers in the village were able to set the VCE device to a mode accepting a new program image to be flashed in, completely replacing the old programming. However, the researchers ran out of time to create malicious demonstration image for the device. Installing new software on a VCE does not require any authentication or check mechanisms. Simply by pressing the "Off" button, the device will query if the user wants to upload a new software image.

Advances in electronics have enabled the power consumption of the chip to be reduced greatly enabling the chip to be powered wirelessly over Near-field Communication (NFC) without a physical connection. These cards are called dual-interface cards and have both a physical chip interface and a wireless NFC interface. These cards are readily available for purchase and retail for about $20. Modern mobile phones have NFC capability built-in, meaning that dual-interface cards are field-programmable by simply using a mobile phone as the programming device over wireless. The same programming is also able to communicate over the physical chip connection.

Due to a lack of security mechanisms in the smart card implementation, researchers in the Voting Village demonstrated that it is possible to create a voter activation card, which after activating the election machine to cast a ballot can automatically reset itself and allow a malicious voter to cast a second (or more) unauthorized ballots. Alternatively, an attacker can use his or her mobile phone to reprogram the smart card wirelessly. All elements of the system seem to accept smart cards with the hardcoded default password (0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08). Among other factors, the obviousness of the password makes forging smart cards easy. This password has been previously published as part of the EVEREST report in December 2007.[6]

In addition to allowing a malicious actor to vote more than once in jurisdictions where the voting terminals have more than one ballot style available, the modification of the voter activation card could also enable the malicious actor to cast multiple ballots, including for races for which the attacker is not eligible to vote at all.

In-flight Email Ballot Modification

Over thirty states allow at least some voters (usually overseas and military voters) to cast ballots as

[6] Pennsylvania State University, the University of Pennsylvania, and WebWise Security Inc, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Compiled by Patrick McDaniel. By Matt Blaze and Giovanni Vigna. December 7, 2007. Accessed September 25, 2018. https://www.eac.gov/assets/1/28/EVEREST.pdf. Page 145.

attachments to an email message. This is an extraordinarily dangerous practice because email is not end-to-end encrypted, not authenticated, its headers (including the "From:" and "Date:" lines) are forgeable, and offers only "best effort" delivery, i.e no strong guarantees. Email is not remotely a secure transmission medium. Anyone who controls an email forwarding agent or email server is in a position to modify, copy, re-route, or discard any ballots he does not like. And since the ballots must be accompanied by the name of the voter, the secrecy of a ballot transmitted by email is totally compromised. Two DEF CON investigators helped demonstrate one of the innumerable kinds of potential attacks on email ballots.

The two principal investigators of email ballot modification at DEF CON were both researchers at Free & Fair, a company that provides open source elections services and systems: Dan Zimmerman, Principled Computer Scientist, and Lyell Read. Their investigation was not of any particular machines, but of general vulnerabilities inherent in email voting. In the past, Dan Zimmerman has demonstrated how a home router could be hacked to intercept an emailed ballot before it even leaves the voter's home. The malicious code in the router could modify votes arbitrarily, with neither the voter nor the election official running the server having any way to detect the problem.

In this case, the investigators demonstrated a similar hack, but instead of attacking the sending side of the communication, they attacked the *receiving* side, inside the email server such as a jurisdiction's election agency might run. They assumed that an emailed ballot consisted of three JPEG images attached to an email message, presumably to contain voter ID and authentication information, a signed oath or affirmation, and the voted ballot itself.

A modern email server has hooks to allow linking with "filter modules." The purpose of filter modules is to allow preprocessing of an email before it is delivered to the final recipients. Such modules are commonly used for spam filtering and other purposes, such as disabling URLs embedded in the email, stripping executable attachments, auto replying with a vacation message, blocking certain senders, apply classification rules, etc. An email filter can be written to do literally anything with an incoming message before it is delivered to the addressee.

The investigators wrote an email filter that modified the JPEG attachment that contained the incoming ballot. Technically the filter was a BASH script that ran the ballot through ImageMagick (an open source Linux utility for editing images) and used its `Convert` command to swap two known ovals on the ballot, before replacing it as a message attachment and delivering the email to the recipient's Inbox. The swapping of the two ovals, which represents moving a vote from one candidate to another, is just an example of the kind of arbitrary vote manipulation that could be done in an email filter. The malicious processing of the ballot would probably delay its delivery by a few milliseconds — essentially unnoticeable.

The programming of the demonstration was completed in approximately two hours, start to finish.

This hack illustrates how vulnerable email voting is to undetectable manipulation while in transit. A rogue individual (and it can easily be a single person) who maintains the email server can write and install such a filter module and later remove it after the election. It would be difficult to detect that the email ballots were manipulated to reflect the programmer's vote choices because neither voters nor election officials will see anything suspicious.

Alternatively, the email server might be remotely hacked by anyone on the Internet — criminals, domestic partisans, or foreign intelligence agencies. The hackers might install such a filter (and later remove it) and thus control the outcome of the election.

Forensic Studies - AVS WINVote

The AVS WINVote machine is an electronic voting machine manufactured by Advanced Voting Solutions (AVS). It possesses a touch-screen voting terminal, a full color screen, as well as zoom capabilities. It is equipped with a wireless local area network and battery backup power, a printer, and modem. The AVS WINVote stands supported in a voting booth and was designed to function as a stand-alone system and it can be used as both a precinct voting device and as a non-geographic station. WINWare is the software used for election management in the WINVote system. As of the 2016 elections, the AVS WINVote is no longer in use.[7] Its reputation as "America's worst voting machine" is well-documented[8] and well-deserved.[9] Given the surfeit of information available about the WINVote's many vulnerabilities, this report will focus on new discoveries as reported at BlackHat 2018 by Carsten Schurmann, Associate Professor at the IT University of Copenhagen, and as uncovered at the DEF CON Voting Village.

The AVS WINVote machines used at the DEF CON Voting Village originally came from Virginia. The principal investigators at the Voting Village were Carsten Schurmann and Will Baggett, a computer forensic examiner. They were assisted by Minoo Hamilton, a security engineer.

The WINVote machine runs an early version of Windows XP from 2002. It thus has none of the updates (Service Packs 1, 2, and 3), bug fixes, or security patches that were offered by Microsoft in the seven subsequent years that the operating system was supported. Application of updates would require recertification of the whole system (according to Virginia law and practice).

In addition to one physical machine, the investigators had access to a total of 16 NTFS file system images from a total of eight WINVote machines, all from machines that had been used in Virginia for years, so they were able to do some comparative studies. At the end of DEF CON the investigators were still studying the WINVote system and the file system images, so this report is only inclusive of what they had discovered as of the end of the conference.

The investigators used the free forensics tool Autopsy to examine the file system images to look for anomalies. They also used various Windows utilities and a forensic undelete utility that could recover files that had been deleted but not overwritten.

Music software and music file

The first discovery that Schurmann made was that four of the eight machines investigated showed evidence of being used for ripping and playing music. The machines contained a copy of coolplayer.exe, an MP3 player program. One possible legitimate use of this program would be to play audio for blind voters, though there is no indication that this is the reason the program was added. However, the machines also had a copy of the "No1" CD-ripping program, a program used to copy music from an audio CD and store it as MP3 files. The WINVote does not have a CD drive, so one would have to plug a CD drive into the USB port on the

[7] Jeremy Epstein, "Decertifying the worst voting machine in the US," *Freedom to Tinker*, April 15, 2015, https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/.

[8] Virginia Information Technologies Agency, "Security Assessment of Winvote Voting Equipment for Department of Elections," *Wired*, April 14, 2015, https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf.

[9] Shaun Nichols, "Default Admin Password, Weak Wi-Fi, Open USB ports ... No Wonder These Electronic Voting Boxes are Now BANNED," *The Register,* April 17, 2015, https://www.theregister.co.uk/2015/04/17/virginia_nixes_highly_pwnable_voting_boxes/.

machine to use this program. There is evidence that this is exactly what happened at some point, because on the same four machines the investigators found copies of a Chinese-language pop song, the same one on each machine.

Since the same Chinese-language song was found on four different machines, this indicates that the song was copied onto the machines at the time the master software distribution for the WINVote was being built, i.e. from before the machines were delivered to Virginia. Most likely an engineer (presumably someone from China, or at least someone interested in Chinese music) was configuring the master software for the WINVote and also ripping CDs and listening to music while doing so. When the engineer committed the final software configuration he failed to erase the music, the MP3-player, and the CD ripper, and they were distributed along with the rest of the voting machine software to at least one jurisdiction in Virginia.

The Virginia jurisdictions that received the machines with the music and CD ripper probably never examined the application software that was installed on the machine. They apparently just accepted the system as delivered and used it for several years. There is no telling what other software, possibly malicious software, may have been installed on the WINVote machines that Virginia officials never noticed in the approximately ten years they were in use. Needless to say, the presence of such rogue files within the software image can only happen with extremely careless and unprofessional development practices and with complete negligence or disregard of any known best practices and quality controls.

Records of past elections
Aside from the musical discovery, the investigators found records from numerous past elections stored in a Microsoft Access Database (.mdb) file in the file system images. There were lists of candidates, voted ballot images, and vote totals. There is nothing inherently wrong with retaining data from past elections in a voting machine, since the data is not confidential, but it is a very poor management practice. First, Microsoft Access has notoriously weak security, which would not be an important point if the machines were forever isolated. However, these machines have WiFi connectivity, and as we describe below, there was clearly no prohibition on connecting the machines to the Internet.

Second, it shows that for many years the file systems of the machines were not re-initialized. The best practice would be to reinitialize the software at least once for each general election, if not for every election. That way errors in the file system do not accumulate, and any bad registry entries, bad data files (caused by I/O errors or power outages), or any software, especially any malicious software, that may have been installed since the last use would be wiped clean for the next election.

Finally, the fact that this data from past elections was still present on the voting machines as acquired by the investigators indicates that the machines were not wiped before they were disposed of by the Virginia jurisdictions that used them. It is always good practice to wipe a file system before disposing of a machine.

Log files show election data had been transmitted over the Internet to a third party
On at least one of the machines there are log files showing that the entire database of an election was transmitted to a third party company. It was transmitted via FTP, unencrypted and unauthenticated, to the IP address 184.69.193.146 which belonged to a server named ftp.enfocom.com. That server is still online. Today the Enfocom International Corporation is a technology company located in Calgary, Alberta, Canada, and its mission is “To be the leader in providing technology solutions in secure network services and secure software products.”

Since the data in the WINVote database is not confidential, the transmission to Enfocom does not

necessarily represent any kind of privacy breach regarding the data itself. The investigators just do not know why voting data would ever be transmitted to any third party, or why they were transmitted to Enfocom in particular. The investigators also do not know whether the IP address they used was located outside the U.S. at the time of the transmission. They did determine that apparently that particular IP address is no longer associated with Enfocom, though that is not necessarily significant.

However, the log clearly shows that there was a direct FTP connection from a voting machine to a distant server over the Internet. This is a potentially disastrous security blunder because it could enable external attackers to penetrate and control the voting machines. Established best practices are that voting machines should *never* be connected to the Internet, even briefly. This is especially true of systems running old, unpatched Windows XP, which are often penetrated and infected with malware within a few minutes of their first connection to the Internet. Furthermore, from a basic operational security point of view, discontinuing the use and blocking of unsafe protocols like FTP has been recommended for years prior to the log entries found, further demonstrating that the baseline external security measures have not been in place at all, or were deeply flawed. These log entries cast doubt upon the claim that election environments are shielded from hostile environments with external security mechanisms.

Deleted files
The investigators ran a forensic "undelete" utility on one of the WINVote images and were able to recover 1764 deleted files, i.e. files which were put in the Windows Recycle Bin, and the Recycle Bin emptied, but the files were never overwritten. When examined, the files appeared to be routine information, including:

- change logs for years of changes
- photos of components
- a ringtone (modem noises)
- a deleted copy of the Windows registry
- .zip file of cast vote records
- an external drive insertion log
- a directory named "crypto"

The investigators did not have time to examine these files any further, but nothing appeared suspicious. The existence of these deleted files is, however, further evidence that the file system had never been re-initialized in the many years the WINVote machine was in use.

Physical vulnerabilities
A fourth major vulnerability was discovered by Mixael (pseudonym), a mathematician who was also working on the WINVote machines. In this case, the investigator noticed a simple keylock on the front panel (faceplate) of the WINVote. He applied the simplest lock picking tool there is, a "jiggler key." A jiggler key is a simple metal key cut from a totally flat blank with one or more generic bumps along one or both edges. It is not specific to any particular lock — it is intended just to move the mechanical components of the cylinder in a more or less random way until the lock spontaneously opens. This only works on the simplest, cheapest locks. A pack of 10 jiggler keys is available for less than $4 on Amazon.

The investigator was able to open the lock in just about five seconds using what was in fact the simplest of his jiggler keys. He was then able to open the panel, which exposed:

- The power switch
- The USB port

- The modem port
- The printing mechanism

The investigator also noticed that there was no sensor to indicate when the faceplate was opened or closed, so even when the machine is powered on and running there was no possibility of logging the occasions when it was opened or closed.

Anyone who has a few seconds access to the WINVote machine can open the front panel. This obviously includes election officials, warehouse workers, and poll workers. And, if a voter hides the front of the machine with her body as she jimmies the lock, she may be able to open the panel without detection.

Once the panel is open, anyone with sufficient time and preparation could:

- Power the machine on or off. Powering off at the wrong moment may result in a corrupted file system or database;
- Install malicious software through the USB port. This includes malicious software which could modify vote counts arbitrarily with no logging or forensic evidence that it happened;
- Connect the machine to the Internet through the modem port. Connecting a voting machine to the Internet opens it to a host of threats, including remote login and the installation of malicious software, particularly because the WINVote runs a very early and extremely vulnerable version of Window XP; or
- Disable the print mechanism.

Recommendation:
Make A Crisis Communications Plan Before Your Website is Hacked

Given the scope of vulnerabilities inherent in the U.S. election system, it is vital that state and local election officials not only seek to prevent cyber attacks on their systems, but also plan how best to recover from an attack. One of the primary challenges in this new era of foreign propaganda is disseminating accurate information to constituents in a reliable manner. The following is a list of recommendations to prepare for an attack against an election results reporting website on Election Day. These recommendations are intended to ensure results are communicated in a way that engenders trust in the election results from voters. This list is tailored to specifically address a cyber attack on an election website but was largely sourced from the Local Government Association of England and Wales[10] who created these recommendations for any government crisis communications plan in response to a cyber attack. We would like to thank the Local Government Association of England and Wales for their thoughtful work on this important topic.

1. **Anticipate crisis conditions and create a crisis communications plan**
   Organizational leaders should anticipate what conditions might be created by a cyber attack on their systems, such as the publication of false election results on official websites, as happened in Ukraine,[11] or a Distributed Denial of Service (DDoS) attack that could shut down the site altogether, as happened to many U.S. banks in the Iranian attack[12] and create a plan for how to communicate with the public and other stakeholders under such conditions. This plan should be part of a local or state government's overall emergency planning. Effective crisis communications plans should include:

   - Who will be part of the crisis communications team
   - Timeline of when the crisis communications team should meet during the first hours, days, and weeks following a crisis
   - Who has ultimate authority for signing off on key messages
   - List of audiences who need to be reached during a crisis, including contact details
   - List of stakeholders to reach out to or work with during a crisis, including contact details
   - List of channels to be used to communicate messages, including multiple backup options
   - Copies of passwords needed to access official communication channels

   Needless to say, this crisis communications plan should be kept in hard copy in case of compromised systems.

2. **Prepare and practice**
   Designated crisis communications teams should practice their response processes to ensure the plan works smoothly and each team member knows his or her role during an emergency. In case of

[10] "Crisis Communications - Cyber Attack," Local Government Association, https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/cyber-attack-crisis.
[11] Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar, June 20, 2017, https://www.wired.com/st ory/russian-hackers-attack-ukraine/.
[12] Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

a cyber attack, team members should be aware of what dangers they can expect and how to report concerns about suspicious activity.

3. **Establish facts, communicate early and regularly**
   During a crisis situation, the crisis communications team should proactively communicate known facts as early as possible, rather than reacting to rumor and speculation. The team should also continually update the public and other stakeholders at regular intervals to remain in control of the messaging.

4. **Identify a spokesperson**
   Before a crisis event, organizational leaders should designate a senior member of the organization to act as spokesperson for the team in case of a crisis. This should be a designated team member who is not directly involved in solving the crisis, which would distract them from focusing on key messages and relaying information in a timely manner.

5. **Avoid email and website updates**
   If an organization is the target of a suspected or confirmed cyber attack, team members should stop using email and website messaging immediately.

6. **Embrace traditional channels**
   When digital communications platforms are compromised by a suspected or confirmed cyber attack, the designated spokesperson should utilize other communications channels to relay key messages, including holding telephone calls with local media, staging in-person press briefings, or utilizing telephone trees to share updates with staff members.

7. **Brief media outlets and elected officials**
   If a cyber attack takes place, the crisis communications team alert news media and elected officials that they may experience a surge in calls from the public. These stakeholders should also receive timely updates on the crisis so they can keep members of the public who contact them informed of the situation.

8. **Use personal devices if possible**
   If an organization's IT systems are compromised, employees may still have access to the organization's digital communications platforms, such as social media accounts, via their personal devices. The crisis communications team should keep hard copies of social media passwords available for this situation.

9. **Use partner and community networks**
   If an organization is targeted by a cyber attack, the crisis communications team should reach out to established partner organizations for help disseminating accurate, up-to-date information on their respective digital platforms. The crisis communications team should establish these relationships before a crisis occurs.

10. **Engage with IT and legal colleagues**
    Members of the crisis communications team should work closely with the organization's IT and legal team when preparing to brief the public on updates throughout the crisis. Particularly in the case of a cyber attack, technical details may be difficult to communicate clearly and understand in the appropriate technical and legal contexts.

11. Communicate with employees

In the midst of a crisis, an organization's leaders should share updates with staff members before communicating with the broader public. If staff members hear updates via social media or other channels before hearing it from their leadership team, it can damage trust within an organization and undermine efforts to control and mitigate the effects of the crisis.

12. Respond to the new normal

Following a crisis like a cyber attack, an organization's leaders should craft messages for stakeholders and the broader public that communicate the lessons learned from the crisis and how the organization is evolving to safeguard against such attacks in the future. Such messaging can repair trust in the organization and help other organizations protect themselves against future crises.

Conclusion

Over the last 26 years, DEF CON, and for the last two years, the Voting Village, have operated under two core principles:

1. **It is important to derive facts through reason and inquiry rather than blind faith.**

2. **When we discover new facts, it's important we share this information with the general public so individuals can decide how best to use the information.**

We did not make these principles up ourselves. Rather, these principles are the foundation of the Enlightenment, which has guided modern science to achieve the medical, engineering, and IT advances, among others, that underpin the modern world. Since these principles have largely guided the human race toward progress for the last 500 years, we plan to continue to follow them.

These principles matter most when we put them into practice. Therefore, it is relevant to ask what new facts all the poking and inquiring into our voting systems has identified since the Voting VIllage was established.

Among the dozens of vulnerabilities identified in the last two years, four key DEF CON Voting Village findings are grave and undeniable:

1. **Supply Chain Insecurity:** The voting machine parts supply chain is global and has essentially no security procedures to determine whether the machine parts are trustworthy or pre-hacked before the machine is assembled. Thus if an adversary compromised chips through the supply chain, they could hack whole classes of machines across the U.S., remotely, all at once.

2. **Remote Attacks Proven:** Despite insistence the fact that machines are "air gapped" from the Internet protects against all remote attacks, both DEF CON 25 and 26 found exploits to hack machines remotely, requiring physical access to the machine.

3. **Hacking Faster Than Voting:** This year DEF CON also demonstrated that while, on average, it takes about six minutes to vote, machines in at least 15 states can be hacked with a pen in two minutes. It is thus possible for someone to hack a machine while voting in a polling place on Election Day.

4. **Hacks Don't Get Fixed:** Finally, we discovered that even when vendors are told about serious flaws in machines by their customers, those flaws go unfixed.

These flaws are relevant and disturbing under the best circumstances. However, the fourth flaw suggests another reason for alarm - disclosing vulnerabilities does not seem to be enough to get them fixed, even years later. For example, the M650's lack of update authentication was noted in the 2007 EVEREST report, initiated by the Secretary of State of Ohio and reported to Election Systems & Software at the same time.[13]

[13] Pennsylvania State University, the University of Pennsylvania, and WebWise Security Inc, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Compiled by Patrick McDaniel. By Matt Blaze and Giovanni Vigna. December 7, 2007. Accessed September 25, 2018. https://www.eac.gov/assets/1/28/EVEREST.pdf.

Hackers found the same design flaw in a current M650, eleven years later. As of 2018, the M650 was used in elections in 23 states.

The failure to fix existing, reported vulnerabilities and the disconnect between the reports of election security experts and the reactions of some election equipment vendors speaks directly to the reason Voting Village was created. The Voting Village aims to increase access to election security knowledge in order to better protect American democracy and the electoral system. We believe that knowing the risks involved in how America votes is always better than sticking our heads in the sand. Although we have redacted some information from this report, it is a realistic, if pessimistic, view of how easy it is for individuals to exploit bad design and sidestep election protections. We hope that it will move the United States towards action.

Next Steps:

1. **Congress Must Act:** The problems outlined in this report are not simply election administration flaws that need to be fixed for efficiency's sake, but rather serious risks to our critical infrastructure and thus national security. As our nation's security is the responsibility of the federal government, Congress needs to codify basic security standards like those developed by local election officials.

2. **Congress Must Fund Election Security:** National defense is not the role of state and local government. Further, no state or local government will ever be able to raise enough capital to defend itself from a determined nation state. Thus, having codified the basic security standards developed by local election officials above, Congress must finance the implementation of these security standards.

3. **Create a Crisis Communications Plan Now:** State and local government election results web pages are, by their very nature, the most insecure component of our election infrastructure. Using the crisis communications plan listed in this document, election administration teams can plan for this attack in advance so they are not scrambling for solutions if an attack happens on Election Night.

4. **National Security Leaders Must Act:** While many local election officials have worked tirelessly to advocate for Congress to act and fund robust security practices, it's not enough. National security leaders must also remind Congress daily of the gravity of this threat and national security implications. It is the responsibility of both current and former national security leaders to ensure Congress does not myopically view these issues as election administration issues but rather the critical national security issues they are.

End Notes

By: Noah Praetz, Director of Elections, Cook County, Illinois

There is nothing more important to election officials than security. Period. Security yields trust and participation. We have been securing votes and voter records for a long time. The threat environment has changed dramatically, we accept the admonitions of our intelligence community, and we understand the significantly increased likelihood of a successful cyber-attack on the election infrastructure. The Secretaries of State, State Election Directors, and local election officials are committed to ensuring that the election results we release are trusted and true.

In this new environment, and in light of existential threats to American faith in democracy, election officials will marshal all available resources, and work with all possible partners, in defense of elections. Those of us who manage elections, and our vendor community, have long-standing partnerships with private security researchers. However, those partnerships are no longer enough; we are building new partnerships with a broader security research community. Building these new partnerships, with organizations like DEF CON, has proven challenging for some in our community over the past two years. Maturing this partnership will require mutual trust and appreciation of each other's roles, responsibilities, and motives. Ultimately, a successful relationship will be forged, out of necessity.

Election officials recognize that today's cyber threat environment necessitates access to the highest levels of security expertise. This talent is expensive. Therefore, we must accept that our new partners are indispensable but bring stylistic and cultural differences that we'll need to learn to manage and accept. Our new partners must accept that the security and resiliency of the election infrastructure and process demands a unique level of sensitivity and care. When other industries are alerted to issues, there are patches at hand or in a pipeline. Frequently, election technology is frozen in time by federal and state certifications that make immediate fixes impossible.

This change in attitude and posture, from election officials and security researchers alike, is a dramatic one. This cultural difference is most pronounced when the public messaging over the same information sets about election security are diametrically opposed. In the security community, exploitable vulnerabilities are a binary fact that should be publicly disclosed and remediated with updated technology as soon as possible. The election official community sees the same vulnerabilities and recognize them as something to be mitigated with physical controls and managed with audits immediately and then remediated as soon as the technology and funding is available.

Despite the differences, the goals are the same for election officials and security researchers. It's the requirement to operate elections in the time between vulnerability disclosure and vulnerability fix, and to provide trust in the process simultaneously, that causes consternation and tension.

Given the capability and intent of American adversaries, whether nation states, groups, or individuals, election officials' failure to capitalize on the expertise of the broader security research community is no longer acceptable. Likewise, given the dire need for the expertise of the security community, failure of that community to appreciate and respond to sensitivities about the sanctity and security of American elections is also no longer acceptable. We must make this relationship work.

Our elected Clerk in Cook County, Illinois, David Orr, understood this two years ago and decided to seek

help where available, to interface with experts where possible, and to be available to well-meaning Americans focused on election security.

One of our first avenues of engagement was with the organizers of the Voting Village at DEF CON in the spring of 2017. We offered consulting services on what an election office backend network might reasonably look like to ensure that the conclusions reached by the security researchers, and by extension the lessons learned by election administrators, were grounded in reality. It does little good for the community of researchers or election officials if the conclusions drawn in the reports can be readily dispelled, either in fact or in art.

After DEF CON released its report in 2017 we drafted a white paper that laid out priorities for funders like federal, state and local governments, and for election officials. It was built around an election security framework, Defend, Detect, Recover. Do everything possible to defend the myriad digital systems relied upon to run modern elections. Recognize perfect defense may not be possible all the time. Ensure that defensive shortfalls can be detected. And that business continuity, or recovery, can be established such that our elections can be run even in the event of successful cyber-attacks.

Between 2017 and 2018 the Voting Village dramatically increased their focus and shifted their research and training to more vulnerable areas that are more likely to be attacked, like emailed ballots, voter registration databases, election officials' computer networks, and informational or election night results webpages. Some election officials consulted with the organizers in some of these areas. Where there was consultation, like on the computer network and voter registration databases, the resulting research and training is more valuable. Where there was less election official participation, like on the webpages, the research was less valuable. And while the headlines about 11-year-olds hacking website were overstated, and frustrating given the websites were not actual replicas, the DEF CON Voting Village has done as much to raise awareness about our needs for resources as we have been able to do for ourselves. For that we owe some acknowledgement and credit, even as some of us have been forced to reassure our voters that not everything they have read about applies. I believe that the leaders and participants in the Voting Village and of the DEF CON project broadly, are talented committed Americans dedicated to ensuring that election officials know what they are dealing with from a product standpoint, and that we are supported in our efforts to raise the funds necessary to ensure the highest possible state of readiness.

Simultaneous to the activities of the security research community, the U.S. Department of Homeland Security created a set of councils to help drive their investments in election security. They rely on election officials at all levels and on the vendor community. I co-chair the Government Coordinating Council. In that role I have sought to bring visibility to that fact that nearly the entire profile of election security is borne by the 8,800 local election officials in this country; and though we locals find overheated rhetoric about election security difficult and angering, our real and present needs to access security expertise supersedes those frustrations.

In closing, I'll repeat, there is nothing more important to election officials than security. The security researcher community, like those who managed and attended the Voting Village at DEF CON, also care greatly about election security. We need these security researchers on our team; and we also need them to be as careful and responsible with their disclosures and language as possible. We won't always agree and there will be very uncomfortable times. But I see a strong partnership moving forward as both communities learn to work together and appreciate each other's needs and perspectives.

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;
- KIG and CyberBit, for providing use of the KIG CyberRange;
- Speakers who contributed to the Voting Village discussions, including representatives from the U.S. Department of Homeland Security, Free & Fair, Verified Voting, and the University of Chicago Harris Cyber Policy Initiative; and
- The Michael and Paula Rantz Foundation, for their generous support of this work.

APPENDIX #1: Partial List of Attending Individuals & Organizations

Representatives attended the event from a variety of organizations including:

Voting Village Speakers

- **Diego Aranha**, Assistant Professor - Department of Engineering, Aarhus University
- **Matthew Bernhard,** PhD Candidate - Computer Science, University of Michigan; Data Science Consultant, Verified Voting Foundation
- **Matt Blaze**, Cryptographer & Associate Professor of Computer & Information Science, University of Pennsylvania
- **Jake Braun**, Executive Director, University of Chicago Harris Cyber Policy Initiative; CEO, Cambridge Global Advisors
- **Alex Halderman**, Professor of Computer Science & Engineering, University of Michigan; Verified Voting Technology Fellow
- **Jason Hill,** Director, Red Team Lead, Department of Homeland Security
- **Harri Hursti,** Co-Founder, Nordic Innovation Labs
- **Rob Karas**, Director, National Cybersecurity Assessments and Technical Services (NCATS), Department of Homeland Security
- **Neal Kelley**, Chief of Elections, Registrar of Voters, Orange County, California
- **Joe Kiniry,** Principal Scientist, Galois; Principled CEO and Chief Scientist, Free & Fair
- **Margaret MacAlpine**, Founding Partner, Nordic Innovation Labs
- **Jeanette Manfra**, National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), DHS
- **Alejandro Mayorkas,** Partner, WilmerHale; former Deputy Secretary, U.S. Department of Homeland Security
- **Amber McReynolds**, Executive Director, National Vote at Home Coalition; former Director of Elections, City and County of Denver, Colorado
- **Alex Padilla**, Secretary of State, California
- **Noah Praetz**, Director of Elections, Cook County, Illinois
- **David Sanger**, National Security Correspondent and Senior Writer, *The New York Times*; Author, *The Perfect Weapon*

Other Key Stakeholders in Attendance

- **Barb Byrum**, County Clerk, Ingham County, Michigan
- **Rob Joyce**, Senior Advisor for Cyber Security Strategy to the Director of the National Security Agency (NSA)
- **Brian Markus**, Co-Founder and CEO, Aries Security
- **John Odum**, City Clerk, Montpelier, Vermont
- **Nico Sell**, CEO, Wickr; Founder, r00tz Asylum

APPENDIX #2: Biographical Information: Voting Village Speakers

Diego Aranha, Assistant Professor - Department of Engineering, Aarhus University
Diego F. Aranha is an Assistant Professor in the Department of Engineering at Aarhus University. He was previously an Assistant Professor at the University of Brasília and the University of Campinas. His professional experience is in Applied Cryptography and Computer Security, with a special interest in the efficient implementation of cryptographic algorithms and security analysis of real-world systems, and includes coordinating two teams of independent researchers capable of detecting and exploring vulnerabilities in the software of the Brazilian voting machine during controlled tests organized by the national electoral authority. He received the Google Latin America Research Award twice for research on privacy, and the MIT TechReview's Innovators Under 35 Brazil Award for his work in electronic voting.

Matthew Bernhard, PhD Candidate - Computer Science, University of Michigan; Data Science Consultant, Verified Voting Foundation
Matt Bernhard is a third year computer science Ph.D. candidate at the University of Michigan with Professor Alex Halderman. He graduated with a B.A. in Computer Science from Rice University in 2015, where he worked with Professor Dan Wallach on STAR-Vote. He has also spent time at Microsoft Research working on remote attestation and security protocols involving secure kiosks with Josh Benaloh, and at Cloudflare working on certificate transparency and SSL/TLS features. His research interests focus on the broad social implications of technology and privacy, delving into computer security, cryptography, networks, usability, censorship, systems, and voting technology.

Matt Blaze, Cryptographer & Associate Professor of Computer & Information Science, University of Pennsylvania
Matt Blaze is a professor at the University of Pennsylvania, where he directs the Distributed Systems Lab and conducts research in security, privacy, surveillance, cryptography, scale, and the relationship between technology and public policy. His work has included the discovery of fundamental flaws in the Clipper chip and other surveillance systems, foundational work in network security, file encryption, trust management and two way radio security, and security evaluations of major electronic voting systems used in the US.

Jake Braun, Executive Director, University of Chicago Harris Cyber Policy Initiative
Jake Braun is Executive Director of the University of Chicago Harris Cyber Policy Initiative (CPI), CEO of Cambridge Global Advisors (CGA), and Co-Founder of the DEF CON Voting Village. Previously, he was the White House Liaison to the Department of Homeland Security (DHS). He has twenty years experience in national security and strategic communications initiatives.

Alex Halderman, Professor of Computer Science & Engineering, University of Michigan; Verified Voting Technology Fellow
J. Alex Halderman is Professor of Computer Science & Engineering at the University of Michigan and a Verified Voting Technology Fellow. His research spans computer and network security, applied cryptography, security measurement, censorship resistance, and electronic voting, as well as the interaction of technology with politics and international affairs. Halderman helped discover the cold boot attack and the TLS Logjam and DROWN vulnerabilities, and he co-founded the ZMap Project, Censys.io, and Let's Encrypt. A noted expert in election cybersecurity, he has performed numerous evaluations of real-world voting systems, both in the U.S. and around the world. After the 2016 U.S. presidential election, he advised recount initiatives in Michigan, Wisconsin, and Pennsylvania in an effort to help detect and deter

cyber attacks, and in 2017 he testified to the U.S. Senate intelligence committee about cybersecurity threats to election infrastructure. He has been named by Popular Science as one of the "brightest young minds reshaping science, engineering, and the world."

Jason Hill, Director, Red Team Lead, Department of Homeland Security
Jason Hill came to the Department of Homeland Security (DHS) in 2013 to help create the Nation's Red Team. Hill has over 24 years in the Information Security field and over 22 years in the Army National Guard within the cyber security domain. Hill serves as the Deputy Chief of the National Cybersecurity Assessments and Technical Services (NCATS) Risk Evaluation team and as the Chief of the Red Team conducting Red Team Assessments for Federal Government customers. Prior to DHS, Hill served as a Red Team instructor to military and Federal Government employees. He holds a B.S. in Computer Information Systems and several industry certificates.

Harri Hursti, Co-Founder, Nordic Innovation Labs
Harri Hursti is among the world's leading authority in data and election voting security, critical infrastructure, and network security systems. Beginning his career as one of the minds behind the first commercial, public email and online forum system in Scandinavia, he went on to cofound EUnet-Finland. Hursti has authored many studies on election security and vulnerability in both academic and corporate publications. He worked for Black Box Voting where he performed voting machine hacking tests, which became known as the Hursti Hacks. These tests were filmed and later turned into the acclaimed HBO documentary *Hacking Democracy.*

Rob Karas, Director, National Cybersecurity Assessments and Technical Services (NCATS), Department of Homeland Security
A certified information systems security professional with over 17 years of experience in information security in the commercial and federal sectors, Karas has extensive experience conducting risk and security assessments and managing information security programs. In his current role as Director, Karas manages the NCATS team at DHS and provides cybersecurity services to Federal Agencies, State, Local, Tribal, and Territorial governments. He is responsible for creating and identifying new services and developing the NCATS program into the civilian governments leading security services provider. Prior to joining DHS, Karas worked in the private sector for 12 years developing security operations. He holds a Bachelor of Science in Information Management from James Mason University.

Neal Kelley, Chief of Elections, Registrar of Voters, Orange County, California
Neal Kelley is Registrar of Voters for Orange County, California, the fifth largest voting jurisdiction in the United States. As the Chief Election Official, Kelley has led the Registrar of Voters' office through the largest cycle of elections in the County's 129-year history. He has been the recipient of numerous state and national awards for election administration and was recently awarded the "Public Official of the Year" award by the National Association of County Recorders, Election Officials and Clerks.

Kelley is an appointee of the U.S. Department of Homeland Security, Government Coordinating Council (GCC), which helps to oversee the protection of the nation's election infrastructure, Kelley holds an M.B.A. from the University of Southern California and a Bachelor of Science from the University of Redlands.

Joe Kiniry, Principal Scientist, Galois; Principled CEO and Chief Scientist, Free & Fair
Dr. Joseph Kiniry is a Principal Scientist at Galois and the Principled CEO and Chief Scientist of Free & Fair. Previously, he was a Full Professor at the Technical University of Denmark where he was the Head of the Software Engineering section. Since the early 2000s he has held permanent positions at four universities in

Denmark, Ireland, and The Netherlands. Dr. Kiniry has extensive experience in formal methods, high-assurance software and hardware engineering, foundations of computer science and mathematics, and information security.

Margaret MacAlpine, Founding Partner, Nordic Innovation Labs
Margaret MacAlpine is a system testing technologist and election auditing specialist. Her work includes projects with electronic testing of voting registration systems, election security, and election fraud. MacAlpine is a specialized technologist in testing and performing risk limiting and transitive audits on election results. Before joining Nordic Innovation Labs, MacAlpine served as an advisor for the office of the Secretary of State of California, specifically with the Risk Limiting Audit Pilot Program where she developed her expertise on the use of high-speed scanners for conducting post-election audits. In partnership with the University of Michigan, MacAlpine contributed to the research of security analysis and the Estonian internet voting system. MacAlpine earned her Bachelor of Arts from Trinity College in Hartford, Connecticut.

Jeanette Manfra, National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), DHS
Ms. Manfra leads the Department of Homeland Security (DHS) mission of strengthening the security and resilience of the nation's critical infrastructure. Prior to this position, Ms. Manfra served as Acting Deputy Under Secretary for Cybersecurity and Director for Strategy, Policy, and Plans for the NPPD.

Previously, Ms. Manfra served as Senior Counselor for Cybersecurity to the Secretary of Homeland Security and Director for Critical Infrastructure Cybersecurity on the National Security Council staff at the White House. At DHS, she held multiple positions in the Office of Cybersecurity and Communications, including advisor for the Assistant Secretary for Cybersecurity and Communications and Deputy Director, Office of Emergency Communications, during which time she led the Department’s efforts in establishing the Nationwide Public Safety Broadband Network.

Before joining DHS, Jeanette served in the U.S. Army as a communications specialist and a Military Intelligence Officer.

Alejandro Mayorkas, Partner, WilmerHale; former Deputy Secretary, U.S. Department of Homeland Security
Alejandro Mayorkas represents clients in civil litigation and internal investigations, and augments the firm's formidable strengths in strategic counseling, crisis management and national security, with a particular focus on cybersecurity.

Before joining WilmerHale, Mayorkas served as Deputy Secretary of Homeland Security, where he managed some of the most complex and critical responsibilities of government, including preventing and responding to terrorist attacks on US soil, enhancing both the government's and the private sector's cybersecurity, enforcing the nation's immigration laws, facilitating lawful trade and travel, and helping stricken communities recover from disasters. For his service as Deputy Secretary of Homeland Security, Mayorkas received the Department's Distinguished Service Award, its highest civilian honor; the US Coast Guard's Distinguished Service Award; a special commendation from the National Security Agency for his achievements in national security and, specifically, cybersecurity; and numerous additional awards and commendations.

As Deputy Secretary, Mayorkas was the Obama Administration's highest ranking Cuban American and was named to Latino Leaders' list of the nation's most influential Latinos. In 2008, The National Law Journal recognized him as one of the "50 Most Influential Minority Lawyers in America."

Prior to becoming Deputy Secretary, Mayorkas served as Director of US Citizenship and Immigration Services, the federal agency that administers the largest legal immigration system in the world.

From 1998 to 2001, Mayorkas served as the US Attorney for the Central District of California, where he oversaw prosecutions of national significance, including the investigation and prosecution of financial fraud, violations of the Foreign Corrupt Practices Act (FCPA), public corruption, cybercrime, international money laundering, and immigration fraud. He was promoted to the Senate-confirmed position of US Attorney after having served for nearly nine years as an Assistant US Attorney specializing in the prosecution of financial fraud.

After leaving the US Attorney's Office, Mayorkas developed a civil litigation and internal investigations practice representing a wide range of corporate clients across the country.

Mayorkas serves as Chairman of the US Chamber of Commerce's Cyber Leadership Council. The Cyber Leadership Council serves as a forum for businesses to openly discuss cybersecurity policy and practices, direct Chamber advocacy and education efforts, and serve as a key voice of industry for dialogue with policymakers.

Amber McReynolds, Director of Elections, City and County of Denver, Colorado
A subject matter expert on elections, Amber McReynolds has been involved in the election's office thirteen years and has been focused on improving the election experience for the people of Denver. McReynolds has played a critical role in modernizing the election model in Colorado and has taken steps to promote innovation and election efficiency in Denver. McReynolds is currently preparing to step into the executive director role of a voter-based nonprofit, National Vote at Home Institute and Coalition. McReynolds holds a Master of Science in Comparative Politics from the London School of Economics and a Bachelor of Science from the University of Illinois.

Alex Padilla, Secretary of State, California
Alex Padilla was sworn in as California Secretary of State on January 5, 2015. He is committed to modernizing the office, increasing voter registration and participation, and strengthening voting rights.

Padilla previously served in the California State Senate (2006-2014) where he chaired the Committee on Energy, Utilities, and Communications. As chair, he shepherded legislation to combat climate change and create a greener and more sustainable economy. He pursued an ambitious agenda in the areas of renewable energy, energy efficiency, smart grid, and broadband deployment. In 1999, at the age of 26, Padilla was elected to the Los Angeles City Council to represent the same east San Fernando Valley community where he grew up. In 2001, his colleagues elected him to the first of three terms as Council President, becoming the youngest member and the first Latino to serve in this capacity.

Noah Praetz, Director of Elections, Cook County, Illinois
Responsible for all matters of election administration in one of the largest jurisdictions in the country, Praetz has extensive experience in election day management, election security, and voter registration modernization. Praetz also serves on the executive committee of the Government Coordinating Council

where he represents local election officials. Additionally, he serves as co-chair of the Election Center Cyber Security Committee and is a member of the International Association of Government Officials and the Illinois Association of County Clerks and Recorders. Praetz publishes articles on cybersecurity, Election Day administration and referred law in Illinois.

Praetz began his career doing data entry prior to the 2000 presidential elections. He worked his way through the ranks in the elections department before taking the position of Deputy Director and then advancing to his current position as Director. Praetz holds a Juris Doctor from DePaul University College of Law.

David Sanger, National Security Correspondent and Senior Writer, *The New York Times*; Author, *The Perfect Weapon*

David E. Sanger is a national security correspondent and a *Times* senior writer. In a 36-year reporting career for *The New York Times,* he has been on three teams that have won Pulitzer Prizes, most recently in 2017 for international reporting. His newest book, "The Perfect Weapon: War, Sabotage and Fear in the Cyber Age,'' examines the emergence of cyberconflict as the primary way large and small states are competing and undercutting each other, changing the nature of global power.

He is also the author of two Times best sellers on foreign policy and national security: "The Inheritance: The World Obama Confronts and the Challenges to American Power," published in 2009, and "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," published in 2012. For The Times, Sanger has served as Tokyo bureau chief, Washington economic correspondent, White House correspondent during the Clinton and Bush administrations, and chief Washington correspondent.

Sanger spent six years in Tokyo, writing about the emergence of Japan as a major American competitor, and then the country's humbling recession. He wrote many of the first articles about North Korea's emerging nuclear weapons program.

Returning to Washington, Sanger turned to a wide range of diplomatic and national security issues, especially issues of nuclear proliferation and the rise of cyberconflict among nations. In reporting for The Times and "Confront and Conceal," he revealed the story of Olympic Games, the codename for the most sophisticated cyber attack in history, the American-Israeli effort to sabotage Iran's nuclear program with the Stuxnet worm. His journalistic pursuit of the origins of Stuxnet became the subject of the documentary "Zero Days," which made the short list of Academy Award documentaries in 2016. With his Times colleague Bill Broad, he also described, in early 2017, a parallel cyber effort against North Korea.

Sanger was a leading member of the team that investigated the causes of the Challenger disaster in 1986, which was awarded a Pulitzer in national reporting the following year. A second Pulitzer, in 1999, was awarded to a team that investigated the struggles within the Clinton administration over controlling technology exports to China. He has also won the Weintal Prize for diplomatic reporting for his coverage of the Iraq and Korea crises, the Aldo Beckman prize for coverage of the presidency, and, in two separate years, the Merriman Smith Memorial Award, for coverage of national security issues. "Nuclear Jihad," the documentary that Sanger reported for Discovery/Times Television, won the duPont-Columbia Award for its explanation of the workings of the A. Q. Khan nuclear proliferation network. That coverage was also a finalist for a Pulitzer.

A 1982 graduate of Harvard College, Sanger was the first senior fellow in The Press and National Security at the Belfer Center for Science and International Affairs at Harvard. With Graham T. Allison Jr., he co-teaches

Central Challenges in American National Security, Strategy and the Press at the Kennedy School of Government.

Carsten Schurmann, Professor of Computer Science at IT University of Copenhagen
With 10 years of experience conducting research in elections, Carsten Schuermann is an expert in election security. Schuermann has written over academic 60 papers, contributed to books, and hacked at DEF CON 2017 the WinVote voting machine shortly after the Voting Machine Voting village opened. Schuermann is a member of the computer science faculty at IT University of Copenhagen and leads the Center for Information Security Research. He has worked with the Carter Center, USA, Council of Europe, Venice Commission, and International IDEA (Sweden).

Before, joining the University of Copenhagen, Schuermann was a member of the Computer Science Department at Yale University. Schuermann holds a Ph.D. degree in Computer Science from Carnegie Mellon University, and a German Master in Computer Science from University of Karlsruhe.

APPENDIX #3: Don't Take Our Word For It

The DEF CON Voting Village provides vital information about vulnerabilities in the U.S. election system to state and local election officials in order to better safeguard the foundations of our democracy. Cross-sector collaboration is critical in overcoming the challenges posed by cybersecurity threats. But you don't have to take our word for it.

Senator James Lankford, Oklahoma
December 21, 2017
Press Release[14]

> "Safe and free elections run by individual states are at the core of our national identity…. During the 2016 elections, Russia tried to interfere in our elections. Although they didn't change actual votes or alter the outcome, their efforts were an attack on our democracy. It is imperative that we strengthen our election systems and give the states the tools they need to protect themselves and the integrity of voters against the possibility of foreign interference. In this new digital age, we should ensure the states have the resources they need to protect our election infrastructure."

Senator Amy Klobuchar, Minnesota
December 19, 2017
Letter to Department of Homeland Security Secretary Kirstjen Nielsen[15]

> "We must … provide states with resources, best practices and manpower to help combat attacks and update voting technology. State and local officials are on the front lines of our democratic process. It is wrong to leave them defenseless against sophisticated cyber hackers backed by the Kremlin and other adversaries."

Senator Bernie Sanders, Vermont
August 13, 2018
Facebook

> "This November may be the most important election of our lifetimes, and we must do everything in our power to protect our democratic processes. Congress must move aggressively to protect our election systems from interference by Russia or any foreign power, and work closely with our democratic partners around the world to do the same."

Senator Kamala Harris, California
Senator Mark Warner, Virginia
Senator James Lankford, Oklahoma
Senator Susan Collins, Maine
August 22, 2018

---

[14] James Lankford, United States Senator for Oklahoma. "Senators Lankford, Klobuchar, Harris, Collins, Heinrich and Graham Introduce Election Security Bill." News release, December 21, 2017. Accessed September 26, 2018. https://www.lankford.senate.gov/news/press-releases/senators-lankford-klobuchar-harris-collins-heinrich-and-graham-introduce-election-security-bill.

[15] Amy Klobuchar, United States Senator for Minnesota. "Department of Homeland Security Secretary Nielsen Begins Tenure, Klobuchar, Lankford Urge Making Election Cybersecurity a Top Priority." News release, December 19, 2017. Accessed September 26, 2018. https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=B3961145-FBA8-4B71-BA36-0EB4FAB29C0E.

Letter to Tom Burt, President, Election Systems & Software (ES&S)[16]

> "The reality of these unprecedented security risks was on full display at the DEF CON cybersecurity conference, where researchers at the "Voting Village" successfully probed a variety of electronic equipment used to administer elections. We are disheartened that ES&S chose to dismiss these demonstrations as unrealistic and that your company is not supportive of independent testing. We believe that independent testing is one of the most effective ways to understand and address potential cybersecurity risks."

Congresswoman Jackie Speier, 14th District, California

August 13, 2018

Twitter[17]

> "If an 11 yr old can change votes on a FL election system, what can a nefarious, trained Russian spy do? There are only 7 companies making election machines that contract with our states and counties, and these companies refuse to let anyone test their software! @VotingVillageDC"

Congresswoman Tulsi Gabbard, 2nd District, Hawaii

August 14, 2018

Press Release[18]

> "Kids being able to hack into our election infrastructure in mere minutes highlights the severe vulnerabilities in our election infrastructure that threaten our American democracy. These vulnerabilities erode voter confidence and expose our election outcomes to manipulation. With the 2018 general election quickly approaching, Congress must act now to pass my Securing America's Elections Act, and work with the states to safeguard our electoral infrastructure, ensuring that each and every American vote is counted faithfully and accurately."

Jeanette Manfra, National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), Department of Homeland Security

August 10, 2018

Panel at DEF CON Voting Village[19]

> "We'd love it if you [DEF CON attendees] worked for us. We'd love it if you worked with us."

Secretary of State Alex Padilla, California

August 10, 2018

Panel at DEF CON Voting Village[20]

> "While I thank the United States Congress for appropriating $340 million last month, let me be abundantly clear, we need more resources. All the things that we know we have to do, all the things

---

[16]Kamala D. Harris, Mark R. Warner, Susan M. Collins, and James Lankford to Tom Burt, President & Chief Executive Officer, Election Systems & Software, LLC. August 22, 2018. In Kamala Harris, U.S. Senator for California. August 22, 2018. Accessed September 26, 2018. https://www.harris.senate.gov/imo/media/doc/August 22 2018 - Letter to ESS.pdf.

[17] Speier, Jackie. Twitter Post. August 13, 2018, 2:49 PM. https://twitter.com/RepSpeier/status/1029122674801500160.

[18] Congresswoman Tulsi Gabbard, Hawaii's 2nd District. "Rep. Tulsi Gabbard on Vulnerability of US Election Systems Exposed at DEFCON." News release, August 14, 2018. Accessed September 26, 2018. https://gabbard.house.gov/news/press-releases/rep-tulsi-gabbard-vulnerability-us-election-systems-exposed-defcon

[19] Ng, Alfred. "US Officials Hope Hackers at Defcon Find More Voting Machine Problems." CNET. August 10, 2018. Accessed September 27, 2018. https://www.cnet.com/news/us-officials-hope-hackers-at-defcon-find-more-voting-machine-problems/.

[20] Hay Newman, Lily. "At DEFCON, the Biggest Election Threat Is Lack of Funding." WIRED. August 10, 2018. Accessed September 27, 2018. https://www.wired.com/story/defcon-election-threat-funding/.

that I'm going to learn and observe when I go down to the Village after this panel, to implement and act on all of these findings, recommendations, and discoveries we need official resources."

Secretary of State Jay Ashcroft, Missouri
August 14, 2018
KRCG[21]

> "I want to work with them [DEF CON Voting Village] to make examples that are real world, that actually reflect what's actually happening in the states…. All those different points of views and ways of life and background, they help different individuals to see things that other people might miss."

Joel Miller, Linn County Auditor and Commissioner of Elections, Iowa
August 13, 2018
Blog post[22]

> "At a recent Iowa State Association of County Auditors (ISACA) meeting in Iowa City, I heard officials from the Iowa Secretary of State's Office (SoS) discounting the value of any news or reports coming out of the Voting Machine Hacking Village at DEF CON® 26. Contrary to what the SoS said, I found the opposite. Every person I met seemed interested in elections, interested in the equipment we use, and interested in showing us the vulnerabilities of the equipment we use with an unexpected twist. That twist: What can I do to help election officials fix the problems?"

John Odum, Montpelier City Clerk, Vermont
July 19, 2018
GOVERNING[23]

> "Too many election administrators are putting their faith in cybersecurity tools that by themselves don't provide nearly the level of security they need."

Joseph Holland, Santa Barbara County Registrar of Voters, California
County of Santa Barbara website[24]

> "Attended DefCon 2017 (annual hacking conference) to observe their first ever Voting Systems Hacking Village. This was quite informative as it led to many ideas about how an election could be disrupted, including various social engineering attacks. This has led to internal discussions on how to mitigate these disruptions."

Amber McReynolds, Executive Director, National Vote at Home Institute and Coalition
August 14, 2018
Twitter[25]

---

[21] Lee, Kyreon. "Secretary of State Ashcroft Working toward Maintaining a Secure Election System." KRCG. August 14, 2018. Accessed September 27, 2018.
https://krcgtv.com/news/local/secretary-of-state-ashcroft-working-toward-maintaining-a-secure-election-system.
[22] Miller, Joel. "DEF CON: A Confirmation about the State of Elections in Iowa." JoelMiller.us (blog), August 14, 2018. Accessed September 26, 2018.
https://lcauditor.wordpress.com/2018/08/13/def-con-a-confirmation-about-the-state-of-elections-in-iowa/.
[23] http://www.governing.com/gov-institute/voices/col-election-security-use-training-tools-penetration-testing.html
[24] "Cyber Security - Frequently Asked Questions." County of Santa Barbara. Accessed September 27, 2018.
https://countyofsb.org/care/elections/about/cyber-security.sbc.
[25] McReynolds, Amber. Twitter Post. August 14, 2018, 12:59 PM.
https://twitter.com/AmberMcReynolds/status/1029457487051649024.

"Thanks @D_Hawk & @washingtonpost for covering #Defcon2018 ~ Improving the security of our #election systems requires commitment, collaboration, coordination, and communication. Continuous improvement is paramount! #DenverVotes"

Ashley Dittus, Democratic Commissioner, Ulster County Board of Elections, New York
August 24, 2018
Email to DEF CON Voting Village

"Thank you for the work you are doing to highlight this issue."

Cassandra Suettinger, Village Clerk/Treasurer, Village of McFarland, Wisconsin
August 27, 2018
Email to DEF CON Voting Village

"We are willing to take all the help we can get in securing our elections. While the hackers at DEF CON may not have all the answers, we are eager to learn about any vulnerabilities or security flaws that we can address and mitigate."

APPENDIX #4: Firewall Democracy: Best Practices for Securing America's Vulnerable Voting Infrastructure

FEBRUARY 2018

Firewall Democracy: Best Practices for Securing America's Vulnerable Voting Infrastructure

A secure vote forms the bedrock of our American democracy. Yet the lessons of 2016 made clear that nefarious actors possess the cyber capabilities to meddle in elections and undermine voters' faith.

Defending democracy is not a responsibility limited to any political party. This is an American challenge requiring a united effort to prepare for the 2018 elections and beyond.

Influenced by a host of cyber, national security, and election experts, this compilation offers 12 of the most widely-embraced best practices for securing U.S. election infrastructure.

PRODUCED IN PARTNERSHIP WITH

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

DEFCON

Overview:
Cyber Threats & Challenges To Our Democracy

In 2016, Russia – a foreign adversary – led a campaign to infiltrate voter databases in at least in 21 U.S. states, possibly more. As that intelligence comes to light, it reiterates decades of expert warnings that, beyond Russia, many hostile actors have the cyber capability to tamper with our election infrastructure, perhaps best defined as a "patchwork" of outdated, aging voting equipment, registration databases, and networks that vary by state.

The ability to address the vulnerabilities in our elections is further complicated by the multiplicity of stakeholders charged with their protection. Voting systems are under the constitutional and administrative control of 50 states and thousands of local voting jurisdictions, many of which are under-resourced when it comes to cybersecurity. Yet election security is now firmly a national security matter, necessitating an evolving role for the federal government, particularly agencies like the U.S. Department of Homeland Security (DHS).

In short, firewalling democracy for 2018 and beyond will require significant coordination and funding at all levels – local, state, and federal – and action must come urgently.

> "Russia perceives its past efforts as successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations."
> *-Dan Coats,*
> *Director of National Intelligence*

> "Russia's activities in the 2016 election constituted the high-water mark of their long running efforts to disrupt and influence our elections. They must be congratulating themselves for having exceeded their wildest expectations with a minimal expenditure of resource. And I believe they are now emboldened to continue such activities in the future…"
> *-James Clapper,*
> *Former Director of National Intelligence*

Best Practices:
12 Action Items For Election Security

As the 2018 elections approach, this list of widely-accepted best practices from a variety of sources outlines **12 action items** to secure our elections.

Safeguard Voting Equipment

- Implement **universal use of paper ballots**, marked by hand and read by optical scanner, ensuring a voter-verified paper audit trail (VVPAT).
- **Phase out touch-screen voting machines** – especially the most vulnerable direct-recording electronic (DRE) devices
- **Update pollbooks** used to check-in voters.
- Verify voting results by requiring election officials to conduct **"Risk-Limiting Audits" (RLAs)**, a statistical post-election audit before certification of final results.

Protect Voting Networks & Databases

- **Secure voting infrastructure, especially voter registration databases**, using time-tested cyber hygiene tools such as the CIS "20 Critical Security Controls" or NIST's Cybersecurity Framework.
- **Call upon outside experts** to conduct cyber assessments – DHS, white-hat hackers, cybersecurity vendors and security researchers – where needed.
- **Provide resources and training** to state and local election leaders for cyber maintenance and on-going monitoring.
- **Promote information-sharing** on cyber threats and incidents in and across the entire voting industry.

Coordinate with Stakeholders

- **Appropriate federal funding** to states to implement infrastructure upgrades, audits, and cyber hygiene measures.
- **Establish clear channels for coordination** between local, state, and federal agencies, including real-time sharing of threat and intelligence information.
- Maintain DHS's **designation of elections as a Critical Infrastructure Subsector.**
- **Require DHS to institute a pre-election threat assessment plan** to bolster its technical support capacity to state and locals requesting assistance.

Citations:
Further Reading & Resources

This compilation of best practices draws upon and acknowledges the contributions of multiple best practices and policy-development sources.

Belfer Center for Science and International Affairs, Harvard Kennedy School, Defending Digital Democracy, *The State & Local Election Cybersecurity Playbook*, February 2018

Brennan Center for Justice at New York University, *America's Voting Machines at Risk*, 2015

Center for American Progress, *Nine Solutions to Secure America's Elections*, August 16, 2017

Center for Internet Security (CIS), *A Handbook for Elections Infrastructure Security*, Version 1.0, February 2018

Congressional Task Force on Election Security, *Preliminary Findings and Recommendations*, 2017

DEFCON, *Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017

Halderman, J. Alex, University of Michigan, Expert testimony to the U.S. Senate Select Committee on Intelligence, June 21, 2017

ICA: Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution,* January 2017

Praetz, Noah, Office of Cook County, IL Clerk David Orr, *2020 Vision: Election Security in the Age of Committed Foreign Threats*, December 7, 2017

Verified Voting Foundation, *Principles for New Voting Systems*, February 2015

Wharton School, University of Pennsylvania, *The Business of Voting: Market Structure and Innovation in the Election Technology Industry,* 2016

MEDIA CONTACT
Jaclyn Houser, Cambridge Global Advisors
jhouser@cambridgeglobal.com