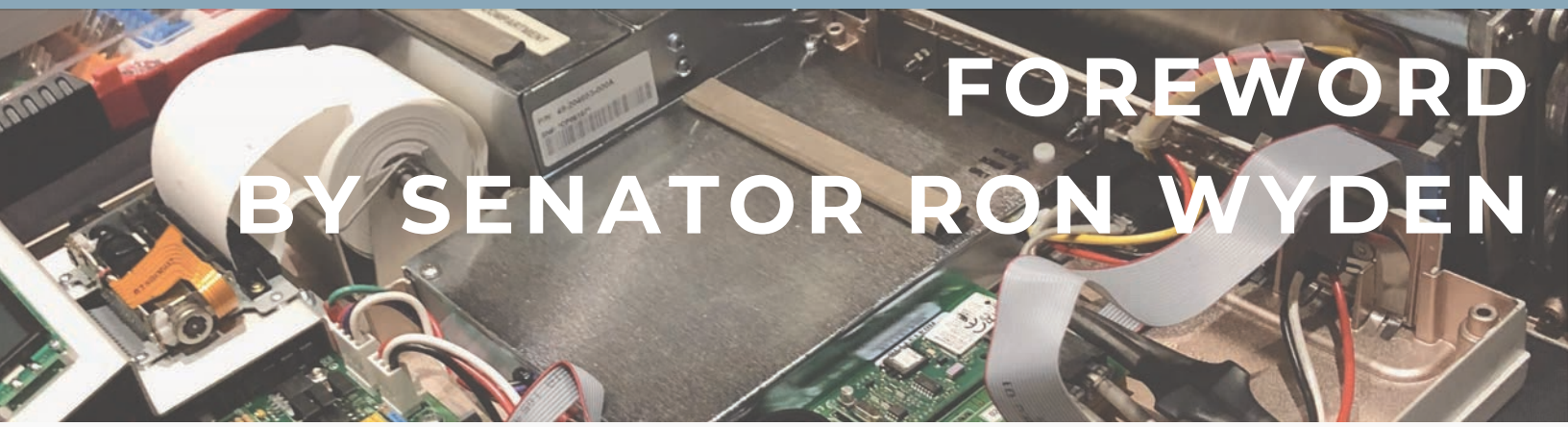
DEF CON 27 VOTING MACHINE HACKING VILLAGE

AUGUST 2019

REPORT CO-AUTHORED BY:

MATT BLAZE, GEORGETOWN UNIVERSITY
HARRI HURSTI, NORDIC INNOVATION LABS
MARGARET MACALPINE, NORDIC INNOVATION LABS
MARY HANLEY, UNIVERSITY OF CHICAGO
JEFF MOSS, DEF CON
RACHEL WEHR, GEORGETOWN UNIVERSITY
KENDALL SPENCER, GEORGETOWN UNIVERSITY
CHRISTOPHER FERRIS, GEORGETOWN UNIVERSITY

Table of Contents



FOREWORD BY SENATOR RON WYDEN

As one of the longest-tenured members of the Senate Select Committee on Intelligence, I've seen a staggering array of threats to the United States. I don't know that any threat poses more of a menace to the core of American democracy than an attack against our election system.

American democracy depends on the notion that elected representatives are chosen in elections that are free and fair, so that the government reflects the will of the people. Anything that undermines confidence in that principle strikes at the heart of our national security and identity.

And yet, nearly three years after Russia showed it was willing and able to penetrate our election systems, the hacking community at this year's Voting Village again demonstrated, our election infrastructure is still far too vulnerable to attacks.

The volunteer hackers and security researchers at the Voting Village are contributing tremendously to public understanding of how easy it is to hack our elections. Whether it is e-poll books, paperless voting machines, or ballot marking devices that print unverifiable barcode ballots, far too much of the equipment that American democracy depends is fundamentally insecure.

It doesn't have to be that way.

Congress needs to set mandatory federal security standards for our election infrastructure, from voter registration databases, to election day equipment, to election-night reporting websites. Otherwise, we're leaving state and county officials on their own against the full might of foreign government hackers. That's not a fight they should be expected to win.

In the short term, there are a handful of steps we can take to vastly improve election security. The first is reducing our dependence on insecure election equipment. Maybe, someday, there will be electronic voting machines that can stand up against dedicated hacking campaigns. That day certainly won't arrive in time for the 2020 elections, or the 2022 elections, for that matter.

As I said during my Voting Village visit last month, "We need paper ballots, guys."

Experts agree that handmarked paper ballots and post-election, risk-limiting audits provide the foundations of a secure election system. If our government takes action in the coming months,

there will still be time to dramatically improve our election security by 2020. The House has already passed a bill to ensure every voter can vote with a hand-marked paper ballot. And the Senate companion to the SAFE Act does even more to secure every aspect of our election infrastructure.

The danger is real. The solutions are well-known and overwhelmingly supported by the public. And yet the Trump Administration and Senate Majority Leader Mitch McConnell refused to take any meaningful steps to secure our elections. It's an appalling dereliction of duty that leaves American democracy at risk. These politicians need to hear the message that Americans won't accept doing nothing as the response to the serious threat of foreign interference in our elections.

The hackers at DEF CON's Voting Village did their job. Now it's time for the Senate and the president to do theirs.

INTRODUCTION

The Voting Machine Hacking Village (Voting Village) returned to DEF CON in August 2019 with a dramatic expansion in election equipment research and evaluation. DEF CON, the world's largest and best-known hacker conference, brings together a wide range of attendees including hackers; cybersecurity professionals; journalists; academics; lawyers; and local, state and federal government leaders. The Voting Village, now in its third year, saw a dramatic increase in attendance and participation, particularly from state, local, and federal government officials.

Since its launch in 2017, the Voting Village has served as an open forum to identify vulnerabilities within the U.S. election infrastructure and to consider solutions to mitigate these vulnerabilities. This year, the Voting Village demonstrated the role that hackers and other cybersecurity experts can, and should, have in the national endeavor to improve election security.

Over the course of two and a half days, hackers, technologists, academics, and other experts had full access to over 100 Voting-Village-owned voting machines to study, as well as the opportunity to attend talks and panels on topics ranging from the challenges involved in reporting on election security to the types of risk-limiting audits.

The clear conclusion of the Voting Village in 2019 is that independent security experts and hackers are stepping into the breach - providing expertise, answers, and solutions to election administrators, policymakers, and ordinary citizens where few others can.

While the discovery and replication of voting system security vulnerabilities are critical tasks for which the Voting Village plays an important role, that is not, in our view, its main contribution. Hundreds of security experts passed through the doors over the course of the weekend, many of whom had no previous experience with the particular problems and risks inherent to election technology. It is vital that we expand the pool of security experts equipped with the specialized knowledge required to evaluate, and ultimately improve, voting system security. We are especially proud of the success of the Voting Village in this essential education and outreach role.

From the outset, the mission of the Voting Village has been to highlight vulnerabilities in election equipment used in the United States and throughout the world and to serve as a resource for those whose goal is to improve the state of election security. As Voting Village organizer Harri Hursti emphasized, "As always we welcome everyone, but especially we welcome officials. We are here to help and get everyone informed - and let everyone experiment to verify the facts."

EXECUTIVE SUMMARY

1. Commercially-Available Voting System Hardware Used in the U.S. Remains Vulnerable to Attack

As in previous years, the 2019 Voting Village presented a range of currently marketed touch-screen direct recording electronic (DRE), optical scan paper voting devices, paper ballot marking devices (BMDs) and electronic poll books (e-poll books). While the Village did not attempt to (and could not) provide samples of every piece of voting equipment currently in use throughout the United States, every piece of equipment at the Village is currently certified for use in at least one U.S. jurisdiction.

And once again, Voting Village participants were able to find new ways, or replicate previously published methods, of compromising every one of the devices in the room in ways that could alter stored vote tallies, change ballots displayed to voters, or alter the internal software that controls the machines. In many cases, the DEF CON participants tested equipment they had no prior knowledge of or experience with, and worked with any tools they could find - in a challenging setting with far fewer resources (and far less time) than a professional lab (or even the most casual attacker) would typically have. In most cases, vulnerabilities could be exploited under election conditions surreptitiously by means of exposed external interfaces accessible to voters or precinct poll workers (or to any other individual with brief physical access to the machines). In particular, many vectors for so called “Advanced Persistent Threat (APT)” attacks continue to be found or replicated. This means that an attack that could compromise an entire jurisdiction could be injected in any of multiple places during the lifetime of the system.

As disturbing as this outcome is, we note that it is at this point an unsurprising result. It is well known that current voting systems, like any hardware and software running on conventional general-purpose platforms can be compromised in practice. However, it is notable - and especially disappointing - that many of the specific vulnerabilities reported over a decade earlier (in the California and Ohio studies, for example), are still present in these systems today.*

* See California Top-to-Bottom Review (2007): “Top-to-Bottom Review.” California Secretary of State. Accessed September 26, 2019. https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review/. and
Ohio EVEREST (2007): McDaniel, Patrick, Matt Blaze, Giovanni Vigna, Joseph Lorenzo Hall, Laura Quilter, Kevin Butler, William Enck, et al. “EVEREST: Evaluation and Validation of Election- Related Equipment, Standards, and Testing.” Secretary of State of Ohio, December 7, 2007. https://www.eac.gov/assets/1/28/EVEREST.pdf.

2. There is an Urgent Need for Paper Ballots and Risk-Limiting Audits

It is beyond the current and foreseeable state of the art to construct computerized (software and hardware based) voting devices that effectively resist known, practical forms of malicious tampering. However, this need not mean that elections must forever be vulnerable to compromise. Certain classes of voting equipment, including some (but not all) of the devices displayed at the Voting Village, can still be used to conduct high-integrity elections— in spite of their vulnerabilities — by conducting statistically rigorous post-election audits. Whether this is possible depends on the specific category of voting technology in use and, critically, whether a properly designed post-election audit process is routinely performed as a part of every election.

Systems that use paper ballots, such as optical scan voting devices, are physically designed to preserve a voter-marked record of each voter's intended choices (the original paper ballots themselves) which cannot be altered by even the most maliciously compromised software. These paper ballots are a prerequisite for the use of routine post-election Risk Limiting Audits (RLAs), which are a state-of-the-art, statistically rigorous technique for comparing (by human eye) a sample of ballots with how they were recorded by machine. This allows us to reliably determine the correct outcome of even an election conducted with compromised machines.

In particular, we emphasize that these audits can only be performed on paper-ballot-based systems. DRE ("touchscreen") voting devices cannot be used to conduct reliable or auditable elections in this way, because the stored vote tallies (as well as the ballot display) are under the control of precinct voting machine software that can be maliciously altered (in both theory and practice). The experience of the Voting Village strongly reinforces the widely understood risk that these machines might be compromised under election conditions in practice. The authors strongly endorse the recommendations of the National Academies 2018 consensus report, Securing the Vote,** that DRE voting machines, which do not have the capacity for independent auditing, be phased out as quickly as possible. This is an increasingly urgent matter, especially as foreign state actors (which may be highly motivated to disrupt our elections and which enjoy especially rich resources) are recognized as part of the threat to U.S. election integrity.

Unfortunately, the recommended practice of auditable paper ballots coupled with routine post-election risk limiting audits remains the exception, rather than the rule, in U.S. elections. While a growing number of states are already implementing paper ballots, legislation requiring routine risk-limiting audits has so far been advanced in only a few states.*** We strongly urge all states to adopt legislation mandating routine post-election risk-limiting audits. This is especially important because current optical scan paper ballot scanners (including those at the Voting Village) are known to be vulnerable in practice to compromise. Post-election audits are the only known way to secure elections conducted with imperfect hardware and software (as all modern computer-based hardware ultimately is).

** National Academies of Sciences, Engineering, and Medicine, Securing the Vote: Protecting American Democracy (Washington, DC: The National Academies Press, 2018). https://doi.org/10.17226/25120.
*** "Post-Election Audits." National Conference of State Legislatures, August 5, 2019. http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

3. New Ballot Marking Device (BMD) Products are Vulnerable

One of the most vigorously debated voting technology issues in 2019 is the appropriate role of paper ballot marking devices (BMDs) and how they relate to widely recognized requirements for software independence and compatibility with meaningful risk-limiting audits. Originally, BMDs were conceived of narrowly, specifically for use by voters with disabilities to assist them in marking optical scan paper ballots, bringing such systems into compliance with Help America Vote Act (HAVA) requirements for accessible voting. However, certain recent voting products greatly expand the use of BMD technology, integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

As a relatively new technology, ballot marking devices have not been widely studied by independent researchers and have been largely absent from practical election security research studies. In the Voting Village this year, we had two ballot marking devices, representing two commercial models of this technology: a traditional ballot-marking device and a hybrid device. The findings only underscore the need for more comprehensive studies.

Participants in the Voting Village found that both BMD models were vulnerable to practical attack. In particular:

1. The hybrid machine outwardly appears to be a separate ballot-marking device and ballot optical scanner as two units physically integrated but architecturally separate. However, it was found that the ballot-marking device was connected to the ballot-scanning device over an internal network, and in fact was an active device in vote processing. This means that hacking the ballot marking device enables altering votes at the scanning stage.
2. Both devices stored information that could allow an attacker to compromise the secrecy of individual ballots.

The weaknesses in the current generation of ballot marking devices raises broad questions about their security and impact on overall election integrity if they were to be put into general use in elections. Aside from their potential to be maliciously configured to subtly mis-record voter choices, current ballot marking devices also offer potential avenues for election disruption via denial-of-service attacks. Voting Village participants observed that clearing many simple error situations (including those that could be deliberately induced by an attacker) required rebooting the device. This can easily create long lines at a polling place, since, as we also observed, it can take up to 15-20 minutes for these devices to complete a reboot cycle.

4. Infrastructure and Supply Chain Issues Continue to Pose Significant Security Risks

The Voting Village explored threats to election security from the supply chain. Participants continued to observe a wide array of hardware component parts of foreign origin, as well as other aspects of the supply chains for software and operational software maintenance. For example, participants found in one machine a hard-wired IP address pointing to an overseas address block.

The exact purpose and nature of whatever underlying feature used this address remains undetermined, but it underscores questions about foreign control over voting system supply chains, which should be understood to include not just the sourcing of physical hardware, but also of software and cloud-based and other remote services.

There are also significant practical issues of local election administration and resources. Local election offices are, overwhelmingly, under-resourced and under-funded, especially relative to the threats they face. Many county and local voting jurisdictions have no full-time IT staff, and many rely on outside contractors for election system configuration and maintenance. This reliance on outsourcing means that election officials often lack internal tools and other capabilities to effectively manage, understand and control their election infrastructure and as a consequence are without direct control over the security of their IT environment. With rapid deployment of new IT technology into the election infrastructure, election offices are especially exposed to remote attack (including by hostile state actors). Unfortunately, very few election offices have the resources to effectively counter this increasingly serious type of threat.

It is important to recognize that IT and cybersecurity are distinct disciplines with only a partial overlap in expertise. To promote discussion and collaboration between election officials and security specialists, the Voting Village conducted the first “Unhack the Ballot” initiative to create an opportunity for election officials to connect with, ask questions, and find answers from security specialists. This “off the record session” was held for the first time in a private room at the Voting Village.

EQUIPMENT AVAILABLE AT THE VOTING VILLAGE

Direct-Recording Electronic Voting Machines

A direct-recording electronic (DRE) voting machine allows voters to electronically cast their ballots by manually touching their choice of candidate on a screen, monitor, or other similar device. The DRE records and tallies the votes directly into its computer memory, without a paper ballot. Only some DRE models feature a Voter-Verified Paper Audit Trail (VVPAT).

Dominion: Premier/Diebold AccuVote TSx

The AccuVote TSx is a DRE voting machine manufactured by Premier Voting Solutions, later acquired by Dominion Voting Systems. The product line currently belongs to ES&S.

As of 2018, the AccuVote TSx was in use in 18 states.*

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 transmitted to election headquarters.

As of 2018, the AVC Edge was in use in 10 states.**

ES&S: iVotronic DRE

The iVotronic DRE is an electronic voting system that allows voters to make their choices on a touch screen interface and records and tabulates votes in internal memory.

As of 2018, the iVotronic DRE was in use in 16 states.***

* "Polling Place Equipment - November 2018." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/#year/2018/.

** According to survey of publicly available information conducted by DEF CON Voting Village.

*** "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.

Electronic Poll Books

An electronic poll book, also commonly called an e-poll book, is typically either a dedicated device with embedded software or a standard commercial laptop/tablet with a software application that allows election officials to review, maintain, and/or enter voter register information for an election, functions that had traditionally been handled using a paper-based system. These systems are limited to the check-in process and do not participate in counting the votes. The usual functions of an e-poll book include voter lookup, verification, identification, precinct assignment, ballot assignment, voter history update and other registry maintaining functions such as name change, address change and/or redirecting voters to correct voting location. In the states that allow same-day registration, e-poll books are also used to enter new voter information and interact with statewide voter registration systems.

ES&S: Diebold ExpressPoll-5000

The Diebold ExpressPoll-5000 is an e-poll book, designed for use by individual poll workers. 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/Premier-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.

ES&S: ExpressPoll Pollbook Tablet with Integrated Pollbook Stand

ExpressPoll Pollbook Tablet is an e-poll book designed for use by individual poll workers and is used in precincts to check voters in before they are permitted to vote. This product was introduced to the market in 2015 and consists of a Toshiba Encore 2 standard 10-inch tablet running Windows 8.1 operating system. It is mounted to an integrated stand which has an internal USB hub for connected peripheral devices like a printer, smart card reader, ethernet, extra battery and magnetic stripe reader.

Ballot Marking Devices

Ballot marking devices (BMDs) are machines that allow voters to make choices on a screen and then print out a paper ballot with the voter's choices, which is the ballot of record. The paper ballot is then hand counted or tabulated using an optical scanner (see description below). In general, BMDs should neither store nor tabulate votes, but only allow the voter to record votes on ballots that are then stored and tabulated elsewhere. Some BMDs produce paper print-outs of barcodes or QR codes instead of a voter-verifiable paper ballot, which has become a source of much controversy.

The first ballot marking devices emerged in the late 19th century, but were only widely used in the last few decades. Today, electronic BMDs have come into widespread use as assistive devices in the context of optical scan voting systems to provide compliance with HAVA, though in recent years vendors have proposed that the devices be used by all voters.

ES&S AutoMARK

The AutoMARK is an optical scan ballot marker that is designed for use by voters who are unable to personally mark an optical scan ballot. The AutoMARK works in conjunction with an optical scanner. It was developed by Vogue Election Systems and the product line was purchased by ES&S. The machine features several features to enhance accessibility for voters with physical impairments or language barriers.

As of 2018, the AutoMARK was in use in 28 states.^

Optical Scanners

Optical scanners are digital scanning devices that tabulate paper ballots that have been marked by the voter. Ballots are either scanned at the precinct (in a precinct count system) or at a central location (in a central count system).

Diebold AccuVote OS

The AccuVote OS is an optical scan voting system. It can be used by precinct count systems and central count systems. Voters cast their ballots by inserting them into the AccuVote OS system, where votes are digitally tabulated, recorded, and stored. Originally marketed as the Unisys ES-2000, the machine later became known as the Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. In recent years, the machine has also been marketed and/or supported under the brands Diebold, Premier, ES&S, and Dominion.

As of 2018, the AccuVote OS was in use in 26 states.^

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.

As of 2018, the M650 was in use in 23 states.^

Hybrid Systems

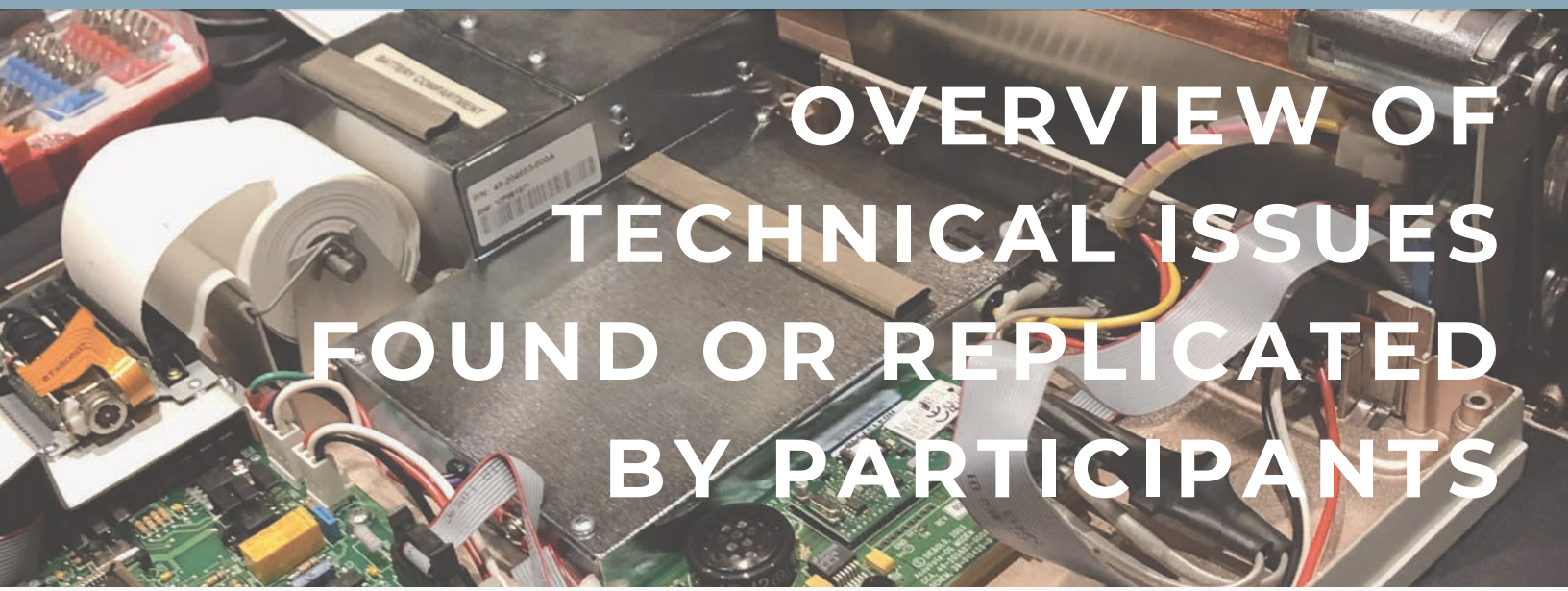
Dominion: ImageCast Precinct

The Dominion ImageCast Precinct is an optical scanner paper integrated with DRE ballot marking device. It scans human-marked ballots, allows voters with disabilities and other voters requiring assistance to use the ballot-marking device to mark and review their ballots, and stores ballots for tabulation after the election period.

As of 2018, the ImageCast Precinct was in use in 10 states.^^

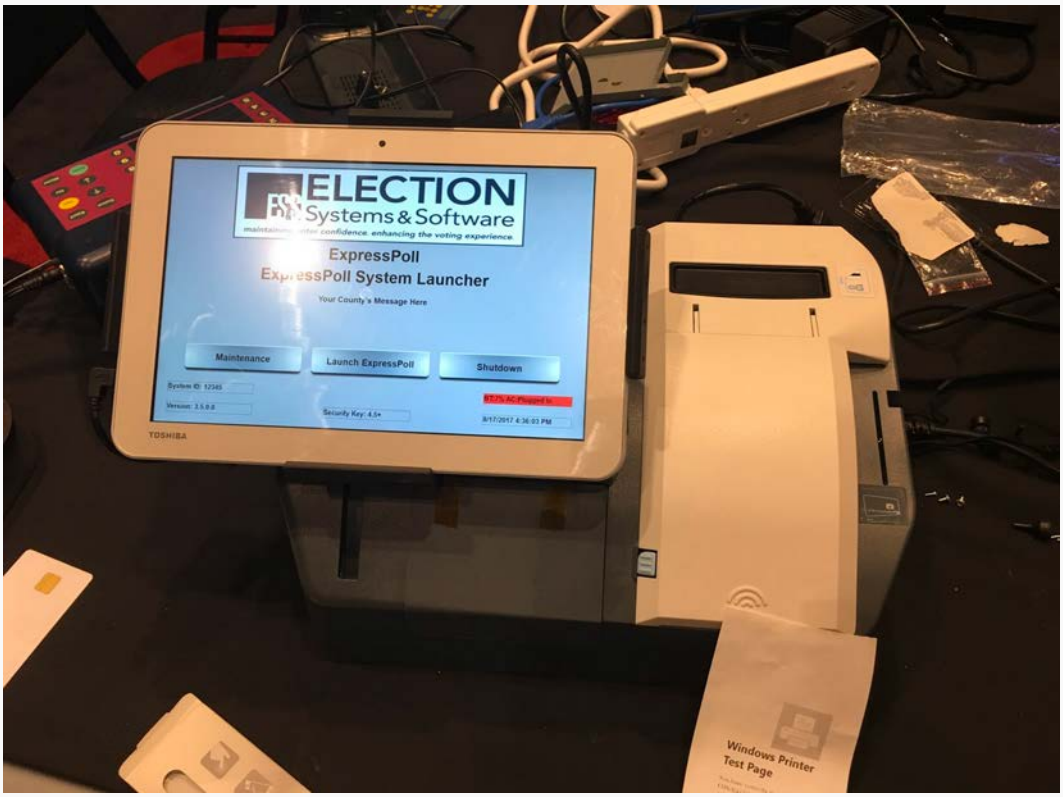
^ "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.

^^ According to survey of publicly available information conducted by DEF CON Voting Village.



OVERVIEW OF TECHNICAL ISSUES FOUND OR REPLICATED BY PARTICIPANTS

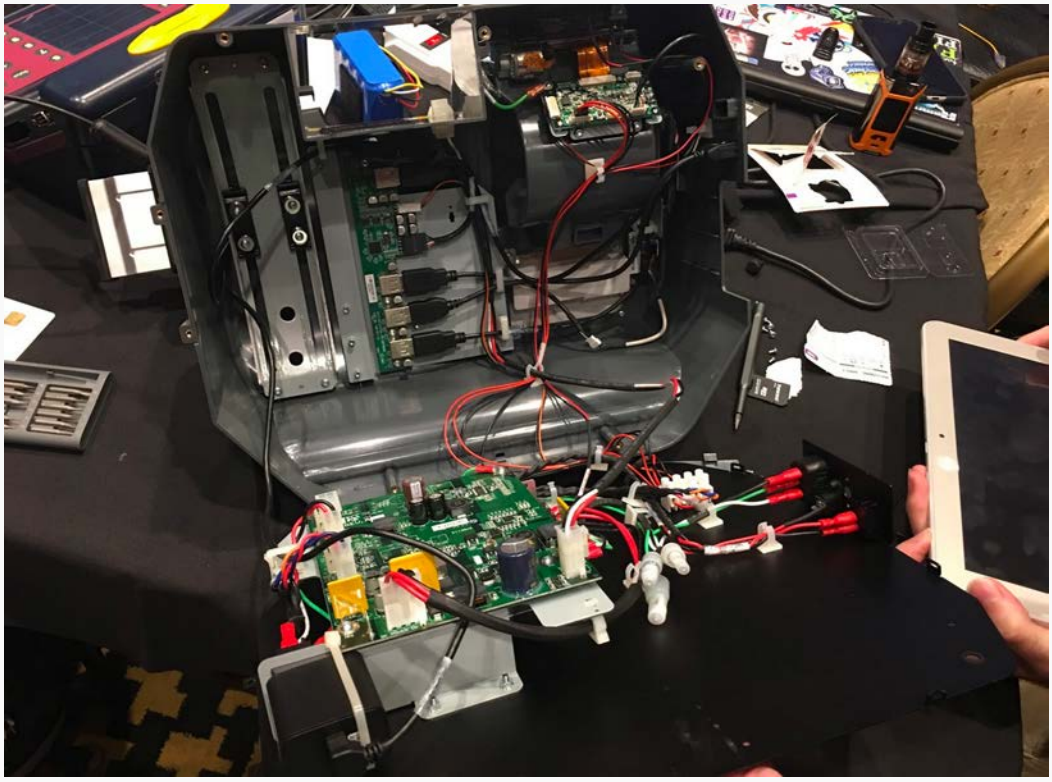
ES&S: ExpressPoll Tablet Electronic Pollbook



Picture: ES&S Electronic Pollbook System on an integrated stand with built-in printer, smart card reader, and other integrated peripheral devices.

The ES&S ExpressPoll Tablet Electronic Pollbook is an e-poll book which uses a standard commercial unencrypted Toshiba tablet held in place to a dock by a rubber locking mechanism. The specific model of the tablet was a Toshiba Encore 2 with Intel Atom CPU and running Windows 8.1 32-bit operating system.

The tablet can be popped out of its dock, exposing an SD port and a USB port of the tablet itself. Additionally, a USB hub is built into the mounting stand, which exposes additional USB ports. All these ports are active. The ports outside the mount are accessible to voters and poll workers without any physical locks or mechanical support for tamper-evident seals.



Picture: Internal electronics of the e-poll book stand. Internal USB hub visible is also directly connected to externally exposed USB connector. The researchers in the Village were able to print out with the voter permission slip directly by connecting into external USB.

While the SD card, which contains voter data, is encrypted, all keys are stored in plain text in a standard xml file allowing all data to be easily accessed and modified, thereby rendering encryption meaningless.

A card or USB device may be placed into the machine directly even when the dock is locked; the locking mechanism does not prevent access to the externally exposed ports on either on the tablet or on the stand.

None of the BIOS passwords were set. This allows unrestricted access to all system settings. By default, the device booted from a USB first without any password required.

The supervisor maintenance password is stored in plaintext on this device. In this case, the password for the tablet was “ESS”.

Security features supported by the underlying commercial hardware were turned off or not activated. The tablet supported Secureboot, a common security feature designed to check to see if the system has been tampered with and prevent the machine from running code of unknown origin. This was disabled by default on the tablet, allowing the e-poll book to load unsigned code from any source.

Picture: Externally exposed USB port on the side of the Electronic Pollbook Stand. The port does not get locked when the stand is locked and it does not have a lid or hook on which to place a seal.

As the Toshiba tablet is a standard off-the-shelf 'PC compatible' general-purpose device, it is supported by a wide range of general-purpose operating systems. This machine can be booted from a version of Linux using, for example, the external USB port and USB memory stick. Booting from Linux allows an attacker to access data on the device without encountering any Windows operating system-based defenses. Voting Village participants confirmed that an attacker would then be able to freely access data and run custom software, including software that would allow extraction of voter data. An attacker could also change or delete any voter registration data (like party registration) stored on the machine once the machine has been accessed.

The e-poll book operating system stack lacked any attempt to perform even the most rudimentary platform hardening. In fact, none of the bloatware that would come with a standard Toshiba tablet was removed. Apps for Netflix, Hulu, and Amazont were present in the e-poll book.

The lack of hardening is especially dangerous given that for one of the recommended deployments the system is intended to communicate over WiFi with wireless internet access to either Amazon Web Services or Microsoft Azure-based cloud services. Given that the operating system is unhardened and given that the standard bloatware provided by the vendor is present on the machine, there is an extremely wide, unprotectable, exposed attack surface.

ES&S AutoMARK

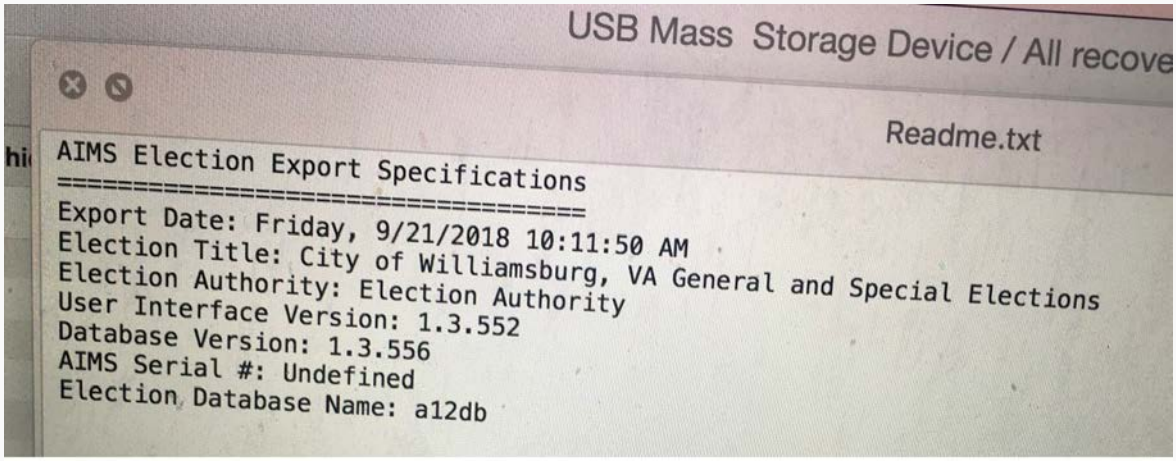
Picture: ES&S AutoMARK Ballot-Marking Device

The ES&S Automark is a ballot marking device that allows keyboard and ethernet ports to be plugged in after removing the top of the machine's case. The casing is closed only by 3 screws and does not include any tamper-evident seals. Immediate root access to the device was available simply by hitting the Windows key on the keyboard.

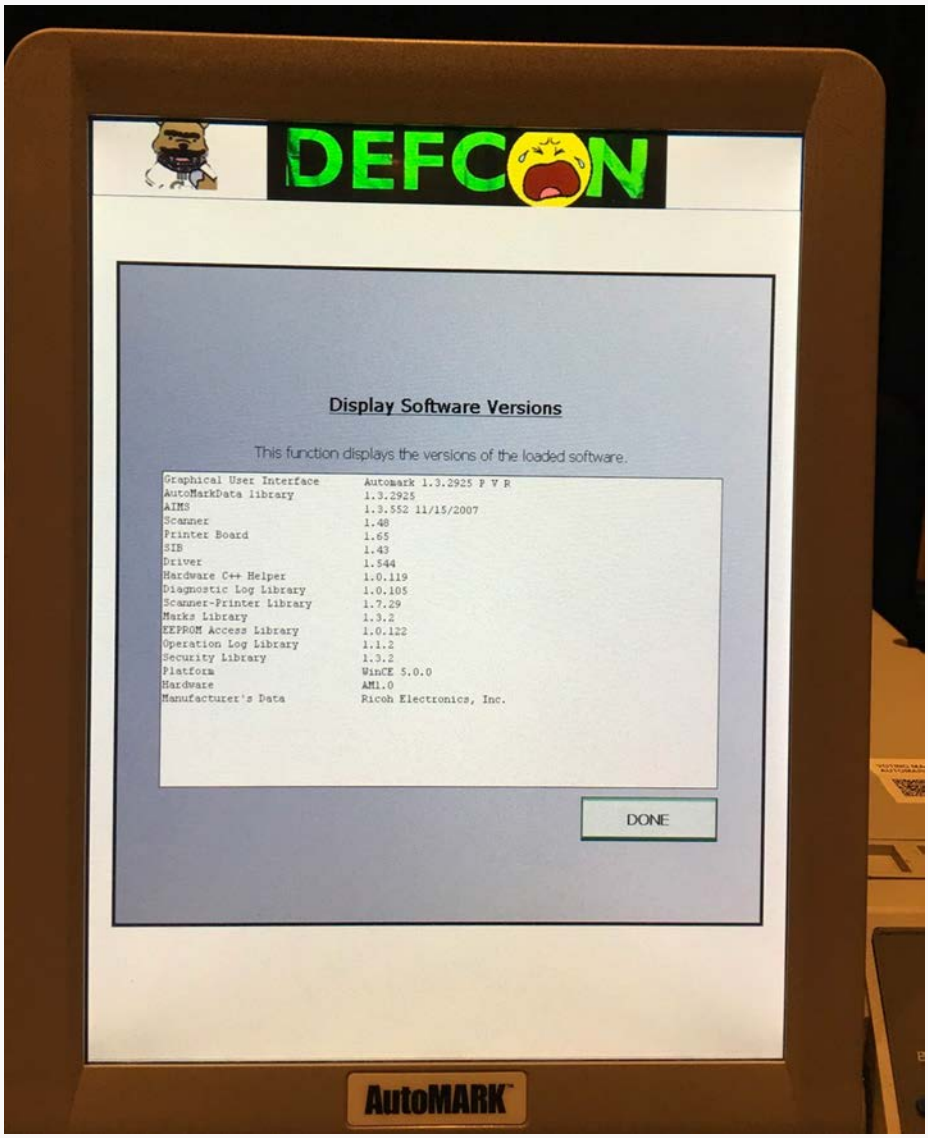
The lock to this device can be picked manually, allowing root and physical access to the unencrypted drive.

A RJ45 jack appears to be hidden behind a sticker on the front of the machine, accessible by removing the sticker without any tools.

The ES&S AutoMARK runs Windows CE Embedded Operating System 5.0. The application software in the machine appears to be last updated around the end of 2007, and the system appears to have been last used in a special election in late 2018.



Picture: Election database manifest file from the AutoMARK showing details of the last election for which it was used.



Picture: AutoMARK software version screen.

Operating system implementation has not been hardened or unneeded elements removed to minimize attacking surface. For example, Internet Explorer is present on this device.

Because the operating system is not hardened, an attacker can, before the machine boots up, drop malware onto the device after holding the “screen” button for five seconds.

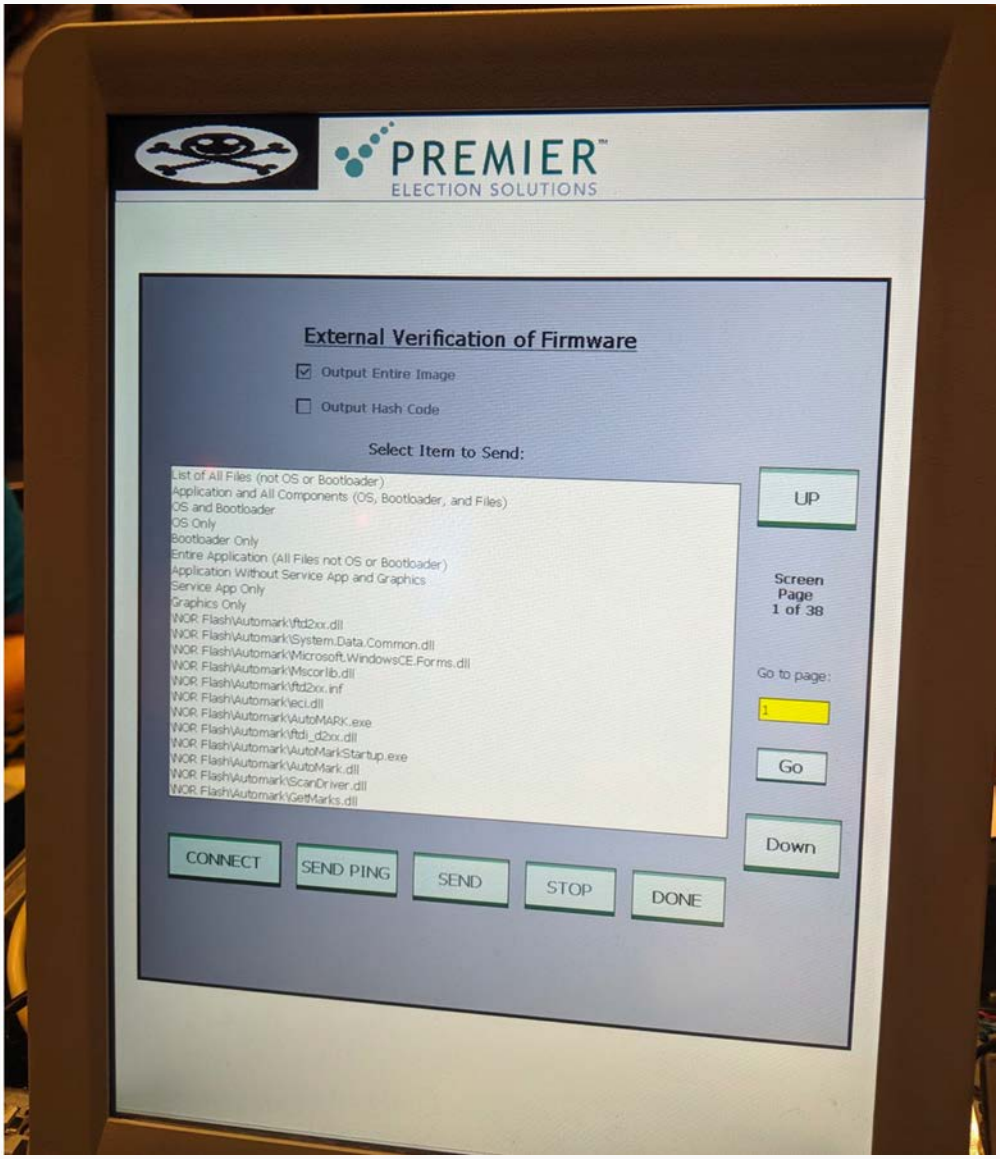
Collectively, a few people were able to change the group IDs of political parties still stored in the device from the previous election. However, this triggered a warning screen, indicating some form of integrity-checking for the stored data.

The embedded Windows operating system has special feature "Allow data connections on device when connected to PC" to enable Windows Mobile Device Center to allow the general purpose Windows version communicate with embedded windows. This feature was turned on.

The machine used several passwords/pins which were very simple, including passwords listed as default passwords in online manuals. These codes include “1111” as the pin code to replace the entire firmware of the device.

Participants were able to adjust the load address which caused the voting applications software to consistently crash. In this instance, the reason for the machine crashing would not be obvious to nontechnical people, such as the volunteers helping to run the polls, thereby creating an effective denial of service attack which would be hard to remotely diagnose.

Additionally, the administrator password was stored in the clear in the configuration file and participants were able to use it to enter admin mode. This enabled them to look at the binaries and replace the header on the voting machine with one of their choosing. Nick Bishop was one of the participants responsible for these discoveries, and has willingly identified himself.



Picture: AutoMARK firmware function enabling automated extraction of the whole system image.

Participants managed to place the DEF CON logo in the header portion of the screen and were able to edit the registry. Using a screwdriver to open up the machine, participants were able to plug a keyboard into an exposed USB port and operate the voting machine as a standard Windows CE machine after exiting the specialized voting software.

Participants Minoo Hamilton and William Baggett also discovered the default system maintenance password by searching on Google, revealing “admin” as the identification name and “vogue” as the password. This allowed both of them to gain access to the securities section on the machine, enabling them to make changes and access vital information. From the securities section they were able to run a remote integrity check that displayed the files and the integrity of each file. Mr. Baggett discussed potential implications for these risks for issues involving a forensic change of evidence. Depending on the protocol adopted by an election office, it is possible that if an attacker modified the access database or central tabulator after hacking their way in, the integrity of the modified data would not be checked against the centralized system.

Dominion Imagecast Precinct

Picture: Dominion ImageCast Precinct with Ballot-Marking Device screen turned to face the scanner (back) side of the machine.

The Dominion ImageCast Precinct is an integrated hybrid voting equipment. It combines an optical paper ballot scanner and ballot marking device and allows for nonvisual accessibility for the blind and visually impaired, in compliance with HAVA. This machine provides voters with disabilities the same opportunities for access and participation as other voters.

This device integrates the devices and the ballot box to store the cast ballots into one unit, but has a single locking mechanism that holds the entire ballot box together. If picked, ballots could easily be stolen using common items such as a standard trash picker.

Participants were able to access USB, RJ45, and CF slots on this machine without using destructive force.

The system also runs Busybox Linux 1.7.4, which has twenty currently known medium to high level vulnerabilities including the ability to allow remote attackers to allow a DNS through CPU/bandwidth consumption via a forged NTP packet which triggers a communication loop with the effect of Denial-of-Service attacks.*

* Search Results. Common Vulnerabilities and Exposures. Accessed September 26, 2019. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=busybox.

Boot settings also allow for the system to be booted from an external USB on startup.

Importantly, the CF card and card readers on the front and back of the machine are physically exposed, and could be replaced.

Additionally there is an internal USB port that is not exposed and an external CF slot that is covered by a tiny door. Either slot can be used to load the OS. Boot order is USB then CF.

The door opens by unscrewing one of the screws. The screws in question were so-called secure screws. Participants made a quick run to a nearby electronics store to purchase “Security Bits Set with Ratchet Driver” for under $28 which was used to open all ‘security screws’ used in any of the machines.

Picture: Small unmarked lid on the side of the machine for accessing CF card slot inside of the machine. So-called “secure screw” tips can be commonly purchased from any electronic store.

When participants removed the CF card on the front of the machine, they found scanned ballots and the configuration file in the clear. In the absence of other protections, modifying configuration data could allow an attacker to edit which X/Y locations on the scanned ballots matched with which candidate. Participants found no digital signing or encryption protecting those digital files.

Participants responsible for much of the work on this machine identified themselves willingly: Zander Work, Lyell Read, Cody Holiday, Andrew Quach, Steven Crane, Henry Meng, and Nakul Bajaj. As a group, they were able to boot an operating system of their choice and play video games on the voting machine, including a popular game called “Pong”. These participants averred that by bringing a simple screwdriver and CF card into the voting area, an attacker could use a screwdriver to access the machine’s intended CF card and swap it with the card they brought, allowing the attacker to boot an arbitrary operating system and take control over the machine.

The group was able to browse the file system on the CF card, proving that the filesystem was unencrypted and unprotected.

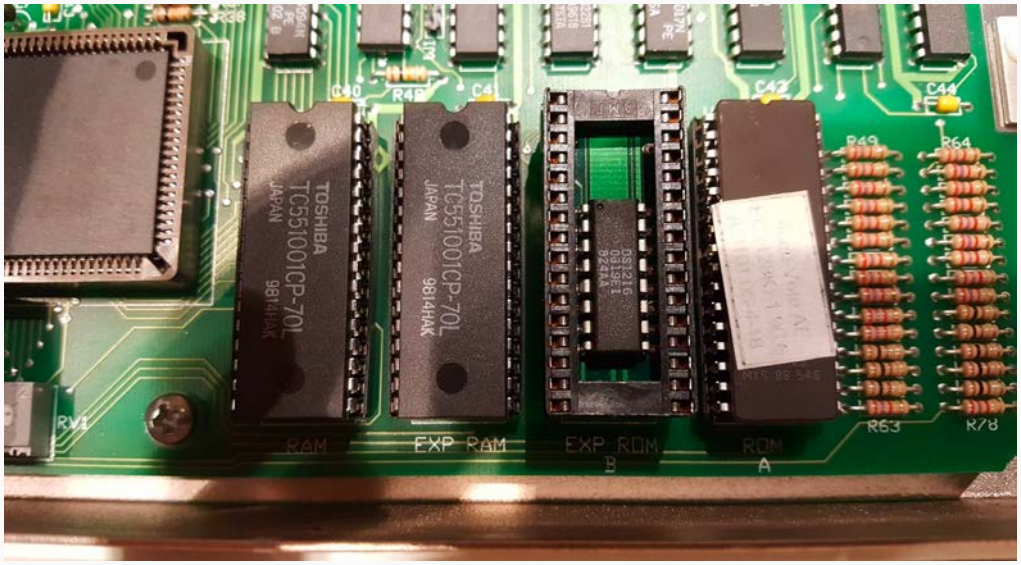
AccuVote-OS Precinct Count

Picture: Originally marketed as Unisys ES-2000 later become Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. Later also marketed/supported under brands Diebold, Premier, ES&S and Dominion.

Participants also discovered a set of previously undocumented functions in the Dominion/Diebold/Premier/ES&S AccuVote, enabling remote manipulation of the machine's memory card when the machine is connected to a network — without any physical access to the memory card, and without breaking or circumventing any physical seals. Researchers confirmed the existence of these features with a person who has previously been involved with the maintenance of these machines, and an election official who had encountered the feature before. The investigation of these functions and possible mitigations is ongoing at the time of this report.

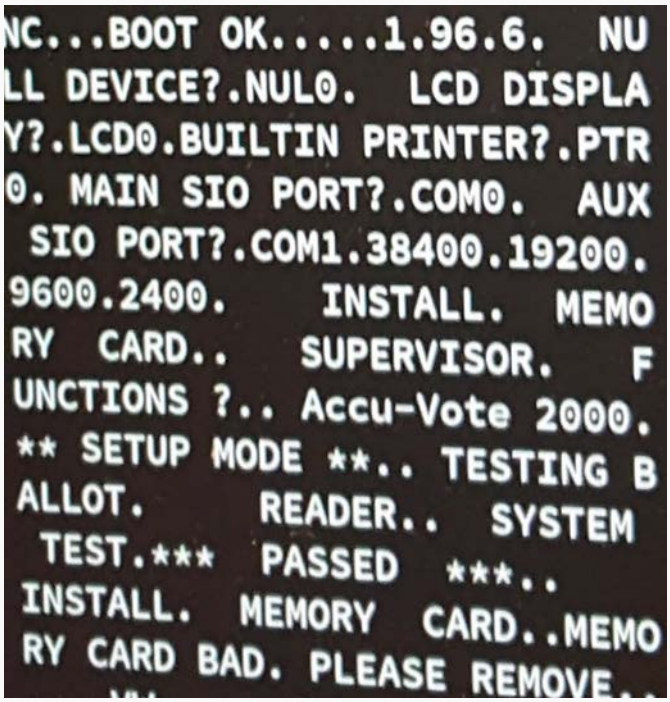
The Voting Village acquired two dozen devices from the same jurisdiction. From the circumstantial evidence of documents in the travel cases, it appears that the machines were put in use and subsequently retired together. However, the devices did not have the same software version installed. Despite possibly having been used in the same elections, some of the machines had software version 1.96.6, whereas others were running 1.96.4, an older version.

In this device, the software is installed on a socketed EPROM microchip. EPROM stands for Erasable Programmable Read-Only Memory and it is a type of programmable read-only memory (programmable ROM) that can be erased and reused. This type of chip has to be physically removed from the circuit board, placed into a separate programmer device, and completely erased before it can be reprogrammed. Erasing the chip is done by shining an intense ultraviolet light through a window through which the silicon chip is visible. The erasing window must be kept covered with an opaque label to prevent accidental partial or unstable erasure by the UV by sunlight or camera flashes and therefore the window is always covered by a sticker as seen in the picture.



Picture: AVOS circuit board with socketed EPROM chip containing election software. Software upgrades to this machine are installed by physically replacing the chip; as the chip is socketed, this can be done in a matter of seconds. The chip inside a socket is a SmartWatch CMOS real time clock with an NVRAM controller circuit and an embedded lithium energy source.

This machine was originally developed in 1986 and first introduced to market in 1989, and it is believed to have been used for the first time in U.S. general elections in Minnesota in 1990. The CPU of the system is NEC V25, which was the microcontroller version of the NEC V20 processor. The V20 was a processor made by NEC that was a reverse-engineered, pin-compatible version of the Intel 8088 with an instruction set compatible with the Intel 80186. It has 16-bit internal architecture and 8-bit external data bus. The V20 was introduced in 1982 and V25 was officially phased out in early 2003. The EPROM containing the programming was 128KBytes in size and the system had two RAM chips 128KBytes each.



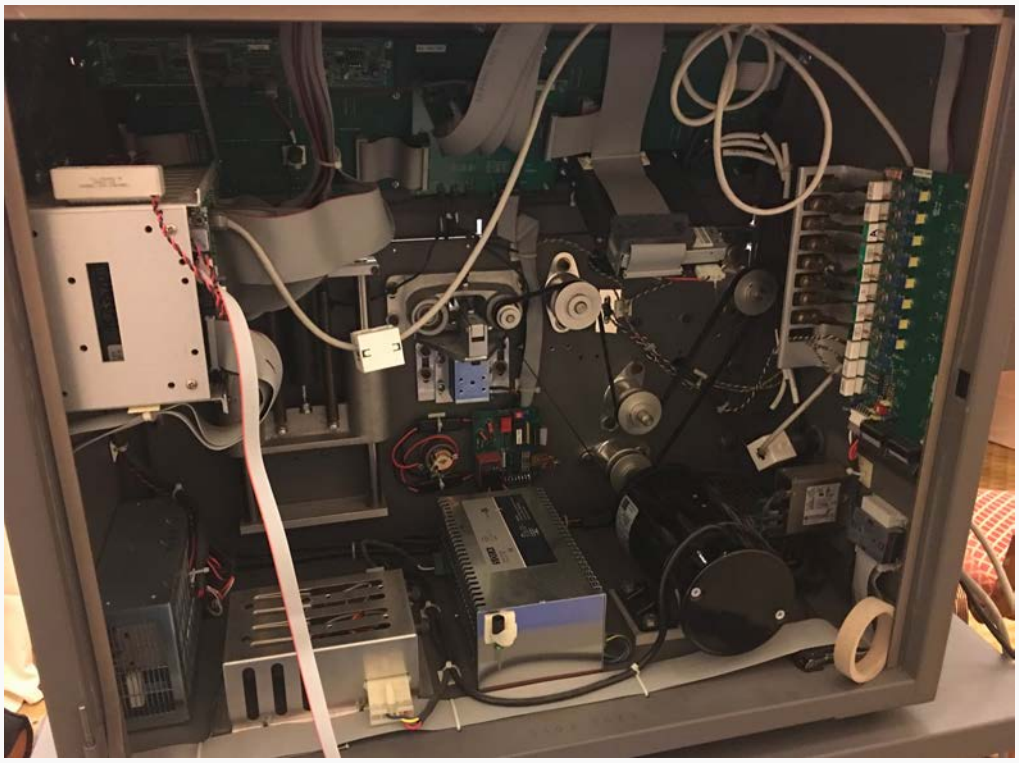
Picture: Human readable strings from the chip contained in the programming. As is typical for embedded systems of the era, the programming contains a lot of clear text strings. In this era of technology, compression and encryption were things of the future.

EVID

Picture: VR System EViD electronic poll book system.

Participants confirmed that the hardware for this machine is a normal general purpose PC hardware which is very low-end by today's standards. There was no BIOS password set on the machine. Consequently, participants were able to boot an arbitrary operating system off a live CD, which had the ability to run on 32-bit and limited to 128M RAM. Ultimately, the device was used as an entertainment device, amusing visitors with Nyan Cat.

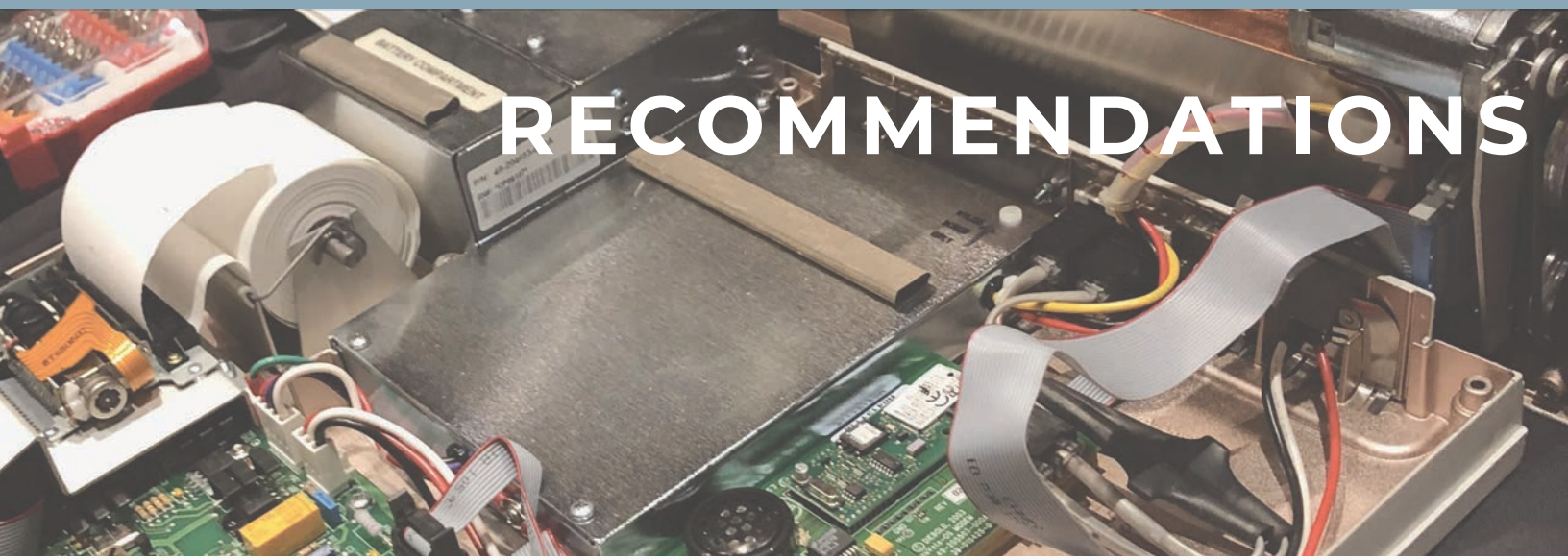
ES&S M650



Picture: Inside of ES&S M650 Optical Paper Ballot scanner. Storage devices and other electronics are quick and easy to replace in a card rack in the upper left. Note the overpowered for the purpose electric motor for moving the paper ballots.

Last year, the Village made accessible to participants two M650 units which had been used in Oregon. This year, the Voting VIllage acquired an additional unit used in the state of Washington. Based on documentation, all three devices were from the same year and same hardware revision. Based on that, the researchers were surprised to discover that the hardware and the features between the devices were not identical. It is unclear who had carried out the modifications.

The paper maintenance log inside the machine did not answer that question, but showed that maintenance personnel periodically have physical access to the inside of the machine. With physical access, this type of machine has no security protections against any kind of modifications.



RECOMMENDATIONS

While the DEF CON Voting Village is heavily focused on the technical aspects of the election infrastructure, the Unhack the Ballot initiative underlined the importance of all levels of the human factor aspects in an election ecosystem. Election officials need more training and better access to parties who can help them to navigate the consequences of technological choices around them. Bearing in mind that at the moment many of those choices take place in the long out-sourcing supply chains of the ecosystem and election officials are left into the tail-end of the process to design mitigation strategies into deployments which they were not participating in design. Election officials also need help to train their own staff to be more security-minded and to gain the 'muscle memory' instincts to protect day-to-day operations, both during election cycles and between them.

The security implications of ballot marking devices should be further studied. This calls for multi-disciplined research looking into the various aspects of the election process from integrity and security to usability and reliability. Current and proposed next-generation ballot marking devices have not been designed with security considerations in mind. They open the door for various methods to attack the election process. In the simplest end are denial-of-service attacks and attacks to compromise the secrecy of the ballot. Depending on the deployment strategy, the ballot-marking device will know a lot about the voter and therefore ballot-marking devices can be hacked specifically to, for example, disenfranchise vulnerable populations: voters who use audio interface, sip-and-puff, large fonts, non-English language ballots, or who take a long time to vote. The discussion about 'detecting' hacked devices is dangerous, because in the absence of remedies even if irregularities are reported there is almost no way to properly investigate. Ballot-marking devices as currently deployed have an insurmountable security design and delegation flaw: the protocols make voters responsible for checking whether devices are performing correctly, and voters cannot get any evidence to prove to others that a malfunction occurred and therefore even if voter detects and reports an error, it would often be the only remaining course of action for poll workers to assume a mistake on the voter's part.

The use of barcodes should be carefully analyzed from various security aspects. Malicious fraudulent advanced barcodes have been causing a lot of problems to Point-of-Sale systems and utilizing bar codes in elections opens a new avenue for injection and scripting type of attacks. The

election integrity, auditability and transparency aspects of using barcodes are even more important. Paper ballots have been promoted because they make those various methods of audits possible. This is true only if the significant record of the vote is human readable. At this point in time, we have to recognize that there are two aspects: technological soundness and the public trust. In elections, it is important that the losing parties and their supporters accept the results as fair. Any method of voting which is not completely transparent and understandable by everyone can be contested in the court of public opinion.

Hybrid machines, which offer users the option of inspecting their ballot before printing, should be avoided because they increase the risk of undetectable attacks. Because the machine knows which ballots are inspected and which are not, it can modify only those that are not inspected — essentially undermining the purpose of voter-verifiable ballots. Such attacks would be very hard to detect exactly because the attacked ballots are those not inspected. With today's razor-thin margins of victory in elections, even the ability to modify a small percentage of the votes undetectably can have a huge impact.

Inspection of newer models of e-poll books further underlines the absence of security design both in software, hardware and physical security aspects. E-poll books are inherently networked devices to synchronize across all devices at a polling place and to avoid cabling, which is often done wirelessly. Furthermore, many new makes and models of the e-poll books actively communicate in real-time over the Internet to back-end servers hosted in commodity cloud services. So far, the e-poll books studied in the Voting Village have been utilizing general-purpose operating systems on commercial off-the-shelf hardware with no special hardening or security measures.

Historically, security measures provided by the hardware / low-level programming have been systematically turned off in all classes of devices used as part of the election infrastructure. Unfortunately, this was found to be true also with newer generations of voting equipment in the Village. These practices greatly simplify paths to attack the machines and also place increased to unbearable burdens to physical security and chain-of-custody management of the machines over the entire lifetime of the devices.

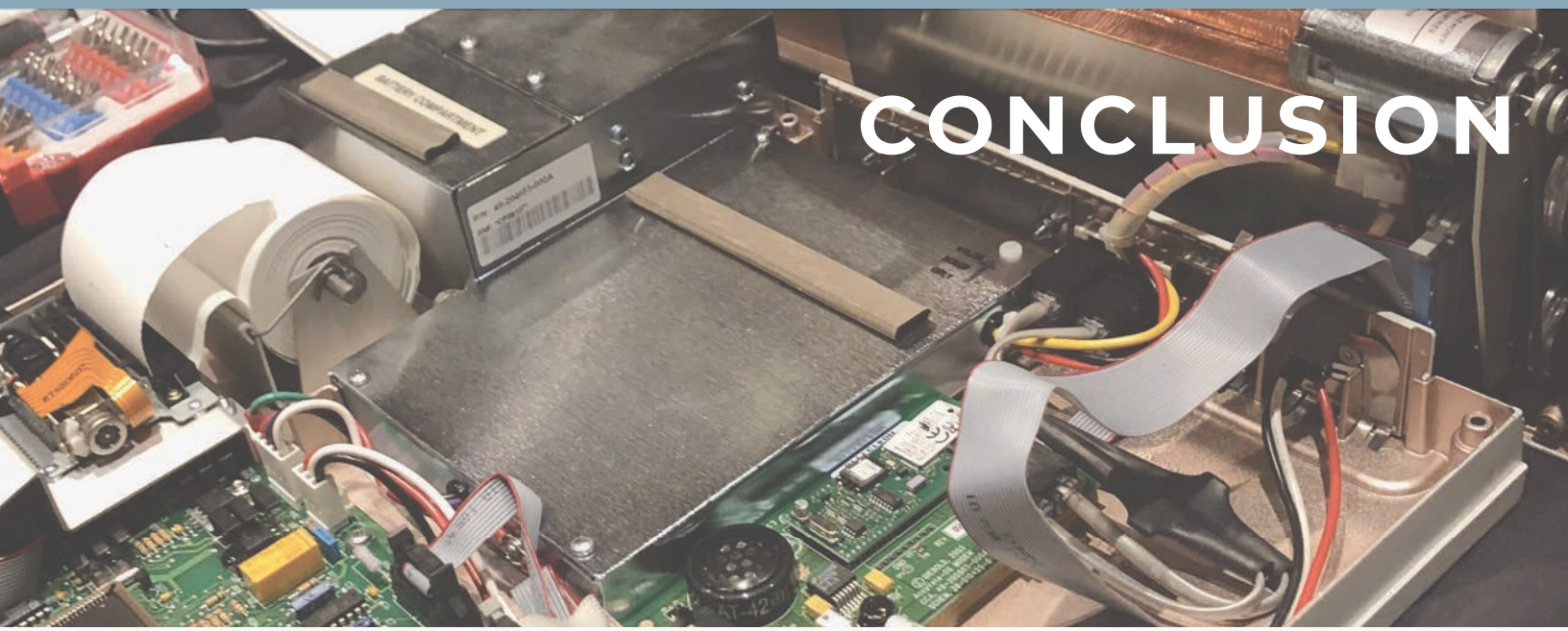
Election reporting was increasingly an area of concern in the Village discussions. With the election night beginning of the process happening over the internet as well as the end of the process as reporting happening over the Internet, discussions in the Village were drawn into similar information flow designs in other industries and how irregularities in those setting had managed to go unnoticed when the ends of the process are seemingly matching. There needs to be a process in place to verify that the reporting truly is sum-of-its-parts.

DARPA SECURE HARDWARE TECHNOLOGY DEMONSTRATOR

Since December 2017, DARPA has been working to build next-generation secure hardware through its System Security Integrated Through Hardware and Firmware (SSITH) program. This new hardware was unveiled for the first time to the public in the Voting Village.

The SSITH program develops methodologies and designs tools that enable the use of hardware advances to protect systems against software exploitation of hardware vulnerabilities. To evaluate progress on the program, DARPA has incorporated the secure processors researchers are developing into a very early prototype application of a secure voting ballot box. At the Voting Village this year, they turned the system loose for public review by thousands of hackers and DEF CON community members. The purpose of this application is solely to provide a demonstration system that facilitates open challenges. To be clear, the SSITH program will not produce a voting system, nor will it provide a specific solution to election system security issues for use during elections.

During DEF CON 2019, the SSITH system demonstrator consisted of a set of RISC-V processors that the research teams will modify to include their SSITH security features. Since SSITH's research is still in the early stages, only one prototype version of the 15 processors in development was available for evaluation. DEFCON 27 was the first small step on a path to evaluate the hardware design. In 2020, DARPA plans to return to DEF CON with an entire demonstrator system, which will incorporate fixes to the issues discovered during this year's evaluation efforts.



CONCLUSION

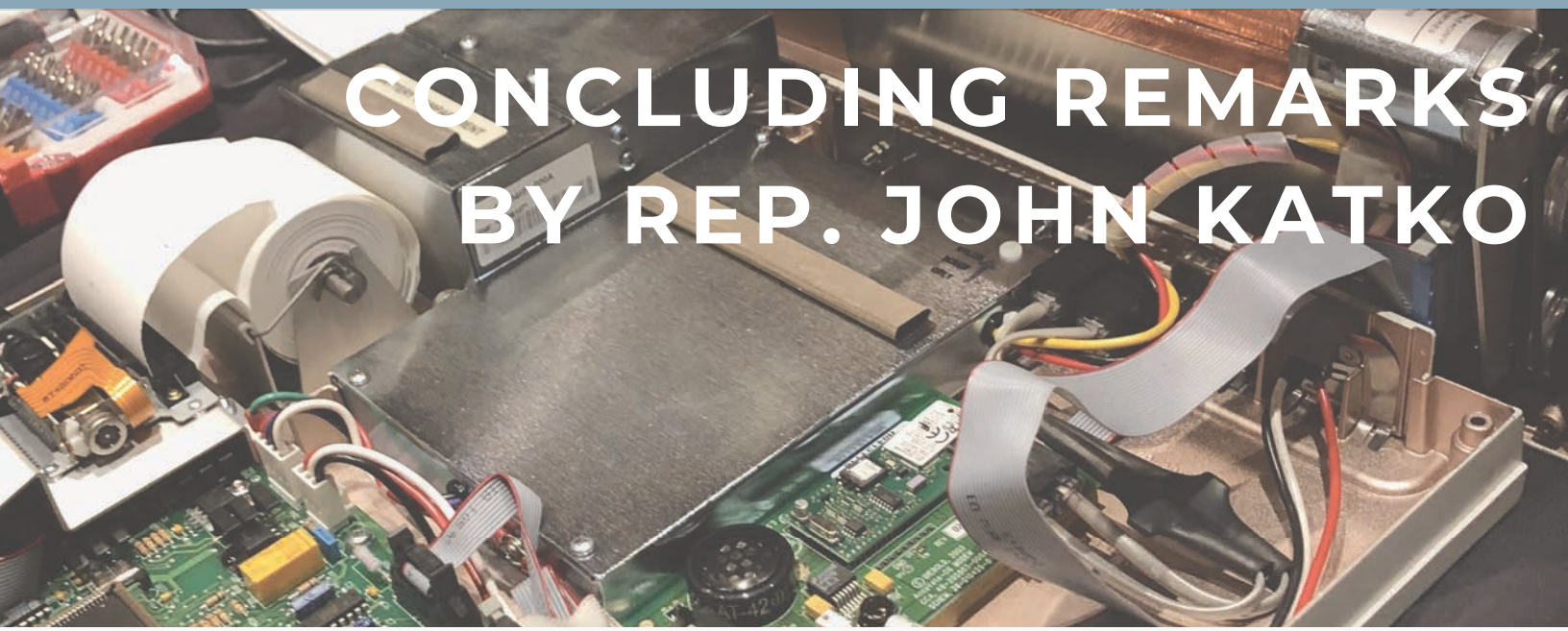
As in previous years, this year's Voting Village demonstrated vulnerabilities inherent in the election environment and highlighted the enormity of the task of securing our nation's elections. Among the many issues highlighted at the Voting Village this year, particularly on machines previously unavailable to the hacker community, three serious vulnerabilities stood out:

1. Widespread use of current ballot-marking device architectures poses new systemic security risks
2. Previously studied commercial election equipment continues to surprise with new weaknesses
3. Many systems are shipped with basic security features disabled

If we as a nation are serious, as we must be, about improving election security in the United States, particularly ahead of the 2020 presidential election, the Voting Village recommends that the following as urgent priorities:

I. Nationwide deployment of mandatory post-election risk-limiting audits
II. Nationwide deployment of voter-marked paper ballot systems
III. Dramatically increased funding and other resources to help local election officials protect their IT infrastructure from foreign state actors and other threats.

Without taking these steps to support election administrators at the frontlines of this clear national security threat, we fear that the 2020 presidential elections will realize the worst fears only hinted at during the 2016 elections: insecure, attacked, and ultimately distrusted.



CONCLUDING REMARKS BY REP. JOHN KATKO

The following is a transcript from Representative John Katko's remarks at the Voting Village Report release on September 26, 2019.

Good afternoon, everybody. Oh wake up, come on, I know it's not bad. Good afternoon. *[Audience responds: Good afternoon]*

Thank you for being here and, I never thought I would be saying this, I know the media is here and some others, but for those of you who are hackers, I guess I say 'welcome.' And I know there's a few here and you definitely serve an important part of this endeavor we're trying to work on.

I want to thank Congresswoman Speier for inviting me to speak, I really appreciate that, so thank you, Jackie.

I want to thank Matt Blaze for helping start the Voting Village and for discussing election security with me last week. We had a great discussion.

You know, as chair of the - or ranking member of the Homeland Security Cyber subcommittee you are trying to keep up with the pace of the bad guys and you are trying to keep up with the pace of our vulnerabilities. And that is a very daunting task.

It's clear from my discussion with Matt, it's clear from my time on the subcommittee, that it is, this is probably the number one threat to our country right now, is our cyber vulnerabilities.

And everything from cyber hygiene to offensive cyber capabilities if necessary, has to be discussed and has to be examined.

Election - elections are at the, strike at the fundamental heart of our democratic system. Elections are what we, we as a people founded our democracy upon. And it's clear that the bad guys are trying to hit our elections.

So, some things I figured out by talking to Matt and talking to many others, that are fundamentally clear to me: we are not gonna be able to do a system that is 100% fool proof no matter what we do. And that's a sobering reminder of the vulnerabilities, but we have to accept that.

So what do we do?

There's really kind of three pillars that I see, that we can do.

Is, number one, the voting machines themselves. And, number two, is the infrastructure that surrounds the voting machines, within it, like board of elections in New York State, for example.

And then what can we do to probe the systems to make sure they're good, and that's called risk limiting audits.

So, the voting machines themselves. After the 2000 debacle, the hanging chads and everything, we kind of tended to drift away from paper ballots, but now they're back. And they're back for a reason. Because we have to have a paper back-up to the electronic voting mechanisms that we have, just in case there's, something happens. I think it's critically important.

In New York state where I am it took 'em forever to get to that change but now we have a, a very good system where you fill out a sheet of paper and they scan it into the machine. And I remember it well because when I first ran for reelection I filled my ballot out wrong. I had to be reminded with the cameras all there that I filled my ballot out wrong.

So, maybe I was nervous, I don't know, but we have that now. It's not everywhere across this country, so we have to have those stand alone machines Those machines cannot be connected to the internet. They have to be stand alone machines.

Then you talk about the infrastructure around that. You talk about the board of elections, you talk about how they get the information from the machine and then tabulate all the votes. How do you do that? And how do you make sure you don't affect those machines themselves.

I think that's very important. That's going to take money. A lot of these states and municipalities, they have terrible decisions to make. Do we fix the potholes, or do we fix our election machines? And what's more tangible looking to them?

So it's hard and I think there's a role the government can play in providing that funding. And we need to do that.

And then the third thing is, and perhaps, I think, the most important thing, that Matt and Harri told me, and others, is doing the risk based auditing, if you will. And taking the machines even though you don't know there's anything wrong, go back over every once and a while and make sure by spot checks, I'll just give some background, in spot checking they have a hand recount,

retabulate - make sure that what's being reported is actually accurate. And that takes money, too. Those are the things, I think, the roles the federal government can play in election security.

And obviously getting the counties the best practices, but also getting them the money, so they can get the right machines, get the right security procedures in place, and get the right risk-limiting auditing procedures in place.

Those are the three biggest things that I see and everything that Matt's been doing here with the Voting Village and the DEF CON, all that stuff's really important because it helps us expose the vulnerabilities. We can never ever let our guard down, but if we can do those three things that I articulated and, believe me, I have other ideas but I am not going to articulate them here, that will go a long way toward it.

So whatever legislation that we come up with, it should most definitely deal with all three of those things. And anything I can do to help that, the Congresswoman or others, I would absolutely do.

And as always, I need input from you. Matt knows I listen to him and I will listen to others because you know I by far am not the expert on this.

One thing I have learned in homeland security is, as we get our defenses better, the bad guys get their offensive capabilities in that much more in tune.

I'll tell you because when I started out it took much more than something like this to take out an airplane and now this is all you need. *[holding up cell phone]*

So the bad guys are trying to perfect bombs, they're trying to perfect offensive terrorist capabilities, and they're trying to perfect offensive cyber terrorism capabilities. We have to be - never let our guard down. So that's why what you're doing here is so important.

We appreciate it very much and I'll just close with, get the information to us. Please, if you have ideas, no idea is outlandish. The only idea that is a bad idea is one I don't hear about. We can sift through what we think is good.

But the pillars that I think of are the stand alone machines, spot checking them, and having good infrastructure around them and good people around them is critically important and we can play a role in that.

So with that I'll say thank you very much and God bless. Have a good afternoon.

AFTERWORD
BY REP. JACKIE SPEIER

In 2016, we faced an unprecedented attack on our election by the Russian government, with criminal interference and disinformation poisoning our public discourse. Fortunately, the nuts-and-bolts administration of the election, from registering voters to tallying their ballots, was not, as far as we know, demonstrably affected.

This was not for lack of effort, however, and we must not breathe a sigh of relief.

I felt fear in my heart when I heard Special Counsel Mueller, testifying before me and the House Intelligence Committee in July, state without any equivocation:

"It wasn't a single attempt, they're doing it as we sit here, and they expect to do it during the next campaign. … Many more countries are developing capabilities to replicate what the Russians have done."

To my question about the ultimate takeaway, Special Counsel Mueller told us to focus on "that aspect of [his] investigation that would have long-term damage to the United States that we need to move quickly to address," and that his report was a "living message . . . for those of us who have some responsibility."

As citizens, we all bear this responsibility. The call to action has been answered by the grassroots efforts of the Voting Village and the patriotic hackers that have dedicated their talents to improving our election infrastructure. It is time for Congress to answer that call as well.

Former FBI Director Mueller's alarm joined a chorus of alarms that have been blaring loudly about the security of our elections for over three years. Just recently, the Senate Committee on Intelligence released a redacted report that found that "[t]he Russian government directed extensive activity . . . against U.S. election infrastructure."

In response to this terrifying threat, the House of Representatives passed two landmark bills that would guard our elections from malevolent interference. H.R. 1, the For the People Act, would harden our election security by enhancing federal support for the most secure voting systems, such as paper ballots, increase oversight over vendors, and develop a national strategy to protect democracy. H.R. 2722, the Securing America's Federal Elections (SAFE) Act, would provide financial support and enhanced security for election infrastructure, including $600 million for paper ballots and paper auditing systems and a commitment to future funding for election infrastructure.

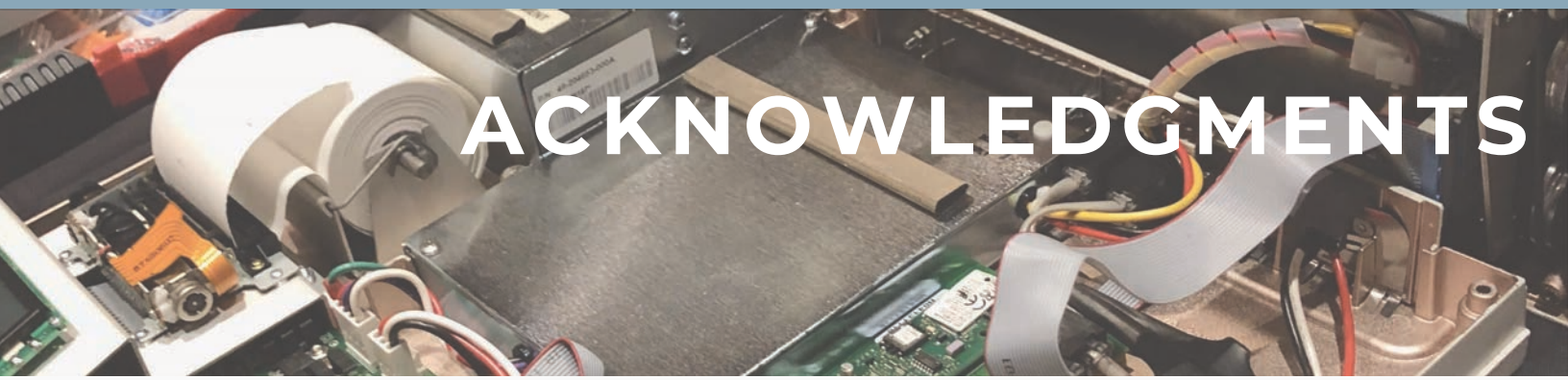
Yet Republicans in the Senate and this Administration have not taken up these crucial House bills or done much of anything to address this ongoing threat. Instead, they seek to undermine our intelligence communities and any efforts to fortify our election security. One has to ask oneself why that is—what could they possibly gain?

Having represented Silicon Valley for decades, I appreciate that the spirit of exploration and innovation, which can be used to disrupt and interfere, can also lead to a more vibrant and resilient society.

I believe that American ingenuity is up to the task of addressing the enormity of the problems we face. There are many vulnerabilities from a voter's registration to the tally. Voter rolls that are used to verify voters' identities as they enter the polls could be manipulated. The apparent technological ease of direct-recorded, entry touchscreen systems has been warmly embraced by many. But these systems also open up new avenues for interference.

Vulnerabilities in election systems strike not only at the infrastructure itself. Public awareness of these vulnerabilities also undermines confidence in elections and erodes trust in our system of government. Elections are the core of citizen participation, and when people feel their voice is silenced, increased apathy threatens to hollow out our government. It is a nightmare scenario – our votes – a sacred right which women and people of color in particular have had to fight and even die for – could be stolen from us. This is not an esoteric issue of ones and zeros, this is the frontline in what makes us Americans.

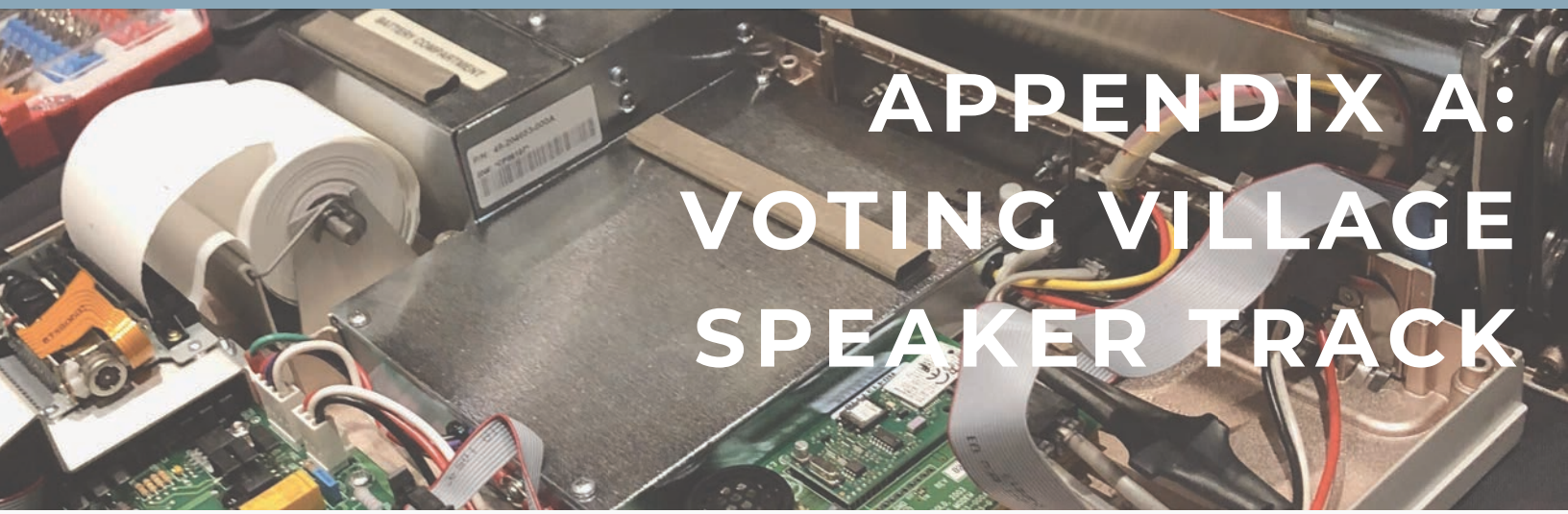
Voting Village's engagement with Congress has been a bright spot in the twilight zone of inactive agitation that typifies Capitol Hill. I urge my colleagues to join me and embrace engagement with election officials, security experts, and our patriot citizens who have answered the call to action for the benefit of us all.



ACKNOWLEDGMENTS

A number of individuals contributed to the success of the DEF CON Voting VIllage and the production of this report. A special thanks to:

- The organizers, subject matter experts, and partners who collaborated to make the Voting Village concept a reality and helped to author this report;
- The speakers and moderators of the Voting Village speaker track, including Senator Wyden, Representative Eric Swalwell, representatives of the U.S. Department of Homeland Security, the Defense Advanced Research Projects Agency (DARPA), and many others;
- The state and local election administrators who attended the Voting Village to share their wealth of experience and learn from the hacker community about the latest election system security concerns;
- The outstanding support and contributions of Jake Braun, Phil Stupak, Morgan Ryan, Jaclyn Houser, Analiese Wagner, Casey Dolen, Claire Martin, and Caroline Hymel;
- The indispensable legal advice and guidance provided by Kendra Albert, Sunoo Park, and Thomas Hopkins of the Cyberlaw Clinic at the Berkman Klein Center for Internet & Society, Harvard Law School; and
- Verified Voting and the Michael and Paula Rantz Foundation, for their generous support of this work.



APPENDIX A: VOTING VILLAGE SPEAKER TRACK

This year's Voting Village speaker track spanned all three days of the conference and featured members of Congress, representatives from the Department of Homeland Security and the Department of Defense, private sector pioneers, academics, researchers, and hackers of all stripes. Below is an overview of each day's talks, as well as each speaker's biographical information.

Friday, August 9, 2019

Welcome and Voting Village Kick-off Remarks

- **Harri Hursti, *Co-Founder, DEF CON Voting Village; Founding Partner, 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.

- **Matt Blaze, *Co-Founder, DEF CON Voting Village; Professor of Law and McDevitt Chair for the Department of Computer Science, Georgetown University***

  Matt Blaze holds the McDevitt Chair of Computer Science and Law at Georgetown University. His research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and on the intersection of computing and communication technology and public policy. In addition to his position at Georgetown University, he sits on the board of directors of the Tor Project. Blaze received his PhD in Computer Science from Princeton University.

- **Jake Braun, *Co-Founder, DEF CON Voting Village; Executive Director, University of Chicago Harris Cyber Policy Initiative***

  Jake Braun serves as the Executive Director for the University of Chicago Harris School of Public Policy's Cyber Policy Initiative where he works at the center of politics, technology and national

security to advance the field of cyber policy. Prior to joining CPI, Braun was appointed White House Liaison to the Department of Homeland Security (DHS) by President Obama where he was instrumental in the passage of the unprecedented Passenger Name Record (PNR) Agreement, one of the largest big data agreements in history. In addition, he worked on the development and implementation of the Homeland Security Advisory Council's Task Force on CyberSkills. Braun is also a fellow at the Council on CyberSecurity and is a strategic advisor to DHS and the Pentagon on cybersecurity.

Remarks by CISA Director Chris Krebs

- **Christopher Krebs, *Director, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency***
  Christopher Krebs serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

DARPA SSITH Program at DEF CON

- **Linton Salmon, *Program Manager, Defense Advanced Research Projects Agency (DARPA)***
  Dr. Linton Salmon joined the Defense Advanced Research Projects Agency as a program manager in September 2014. Prior to joining DARPA, Dr. Salmon spent 15 years in executive roles directing development of CMOS technology at GlobalFoundries, Texas Instruments and Advanced Micro Devices. Before joining Advanced Micro Devices, Dr. Salmon was vice president for Research and Technology Transfer at Case Western Reserve University and an associate professor of electrical engineering and physics at Brigham Young University (BYU), where his research areas included CMOS processes, micro-battery research, packaging and MEMS.

What Role Can Journalists Play in Securing Elections?

- **Maggie MacAlpine *(moderator), Co-Founder, Nordic Innovation Labs***
  Margaret MacAlpine is an election auditing specialist and system testing technologist. She has worked on a variety of projects that include electronic testing of voting registration systems, election security and election fraud for a variety of countries, states and counties. Ms. MacAlpine has served as an advisor for the office of the Secretary of State of California for the Risk Limiting Audit Pilot Program 2011-2012, and is widely regarded as an expert on the use of high-speed scanners for conducting post-election audits.

- **Kevin Collier, *Reporter, CNN***
  Kevin Collier is a reporter who covers the intersection of cybersecurity and national security, including efforts to safeguard election integrity. He has previously worked for BuzzFeed News, Vocativ, and the Daily Dot.

- **Kim Zetter, *Longtime cybersecurity/national security reporter for various publications including WIRED, Politico and The New York Times Magazine and author of the book* Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**
  Kim Zetter is a longtime cybersecurity and national security reporter for various publications including Wired, Politico and the New York Times Magazine and author of the book Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. She has broken numerous national stories over the years about NSA surveillance, digital warfare, Wikileaks and the hacker underground, and has been one of the nation's leading journalists covering voting machine and election security since 2003.

- **Eric Geller, *Cybersecurity Reporter, Politico***
  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

While the Bots Distracted You: Hacking the Electorate

Omelas and White Ops provide the most comprehensive ever look at the day to day tactics of Russian disinformation campaigns against elections. Using Omelas' subject matter expertise and AI, we show the extent of Russian propaganda shared on Reddit in the lead up to an election, the performance of different narratives and different domains, and the sentiment expressed in articles compared to the sentiment induced in the audience in comments. White Ops's state-of- the-art bot detection demonstrates how Russia has automated the process of spreading these narratives, the added reach attributable to bots, and the techniques employed by bots.

- **Evanna Hu, *CEO and Partner, Omelas***
  Evanna Hu is CEO and Partner of Omelas and non-resident Senior Fellow at the Atlantic Council. Omelas is a cutting edge technology company that exposes imminent risks among digital data. By utilizing machine learning/ artificial intelligence and data analytics, Omelas focuses on physical threats and identifies online campaigns of adversarial state and non-state actors. Evanna is also an expert in Counter-terrorism and Countering Violent Extremism, with fieldwork in Syria, Iraq, Afghanistan, Gaza, and Sweden, working on Neo-Nazi and Islamist violent extremists.

- **Ben Dubow, *CTO and President, Omelas***
  Ben Dubow is the CTO and President of Omelas. Ben began his career tracking the online propaganda of jihadists, Shiite extremists, white supremacists, and the militia movement before joining Google where he aided YouTube in detecting ISIS content, helped to develop Project SHIELD, and provided subject matter expertise for the Redirect Method. In 2017, Ben co-founded Omelas with the mission to stop the weaponization of the internet by providing precise data and analysis on how state actors and foreign terrorist organizations manipulate the web to achieve their geopolitical goals.

Trustworthy Elections: Evidence and Dispute Resolution

Suitably designed and operated paper-based voting systems can be strongly software independent, contestable, and defensible, and they can make risk-limiting audits and evidence-based elections possible. (These terms will be defined.) Not all paper-based voting systems have these properties. Systems that rely on ballot-marking devices and voter verifiable paper audit trails produced by electronic voting machines generally do not, because they cannot provide appropriate evidence for dispute resolution, which has received scant attention. An ideal system allows voters, auditors, and election officials to provide public evidence of any problems they observe--and can provide convincing public evidence that the reported electoral outcomes are correct despite any problems that might have occurred, if they are correct.

- **Philip Stark, *Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley***

  Philip B. Stark is Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley. He works on inference and uncertainty quantification in many applications including the census, elections, information retrieval, and Internet filters. He also studies foundational questions in the philosophy of science and statistics. He developed "risk limiting audits" as a method to check election results, which are now in law in six states and required by pending federal legislation. Stark currently serves on the Board of Advisors of the U.S. Election Assistance Commission. He has testified as an expert witness in a range of civil and criminal cases on issues including antitrust, elections, employment, equal protection, food safety, intellectual property, product liability, and vaccines.

Keynote Remarks: Senator Ron Wyden (D-OR)

- **Senator Ron Wyden**

  Senator Ron Wyden is the foremost defender of Americans' civil liberties in the U.S. Senate, and a tireless advocate for smart tech policies. Years before Edward Snowden blew the whistle on the dragnet surveillance of Americans, Wyden warned that the Patriot Act was being used in ways that would leave Americans shocked and angry, and his questioning of NSA Director James Clapper in 2013 served as a turning point in the secret surveillance of Americans' communications.

  Since then, Wyden has fought to protect Americans' privacy and security against unwanted intrusion from the government, criminals and foreign hackers alike. He has opposed the government's efforts to undermine strong encryption, proposed legislation to hold companies accountable for protecting their users' data, and authored legislation with Rand Paul to protect Americans' Fourth Amendment rights at the border.

  Wyden is a senior member of the Senate Select Committee on Intelligence and the top Democrat on the Senate Finance Committee. He lives in Portland, Oregon.

If the Voting Machines are Insecure, Let's Just Vote on Our Phones!

Despite the consensus that Russian actors targeted multiple points of U.S. election infrastructure, there are persistent calls for voting over internet-connected devices. This is not new: 31 states and

the District of Columbia allow military and overseas voters to send voted materials to their home counties via the internet, including by fax and email. Now, several jurisdictions are piloting another internet system that allows voters to send their votes via a mobile application which stores those votes in a blockchain. Such programs undermine the efforts made since 2016 to secure the election administration offices from attacks. Our military and overseas voters need to successfully cast their ballots on time – but we owe it to them to find ways that do not increase the security risk.
This talk will take a look at the current landscape of election security leading into 2020, examining the implications that technologies like blockchain could have on our elections and what the role of responsible technology looks like on our voting infrastructure.

- **Marian Schneider, *President, Verified Voting***
  Marian Schneider is the president of Verified Voting, a role to which she brings a strong grounding in the legal and constitutional elements governing voting rights and elections, as well as experience in election administration at the state level. Immediately before becoming President of Verified Voting, Marian served as Special Advisor to Pennsylvania Governor Tom Wolf on Election Policy. Previously, Governor Wolf appointed her as the Deputy Secretary for Elections and Administration in the Pennsylvania Department of State where she served from February 2015 until May 2017.
  Throughout her legal career, Marian has focused on the intersection of civil rights and election law. Formerly, she was a Senior Attorney with Advancement Project's Voter Protection program and was trial counsel in Applewhite v. Commonwealth, successfully challenging Pennsylvania's restrictive photo ID law on behalf of voters as an unconstitutional infringement on the fundamental right to vote.
  Marian received her J.D. from The George Washington University, where she was a member of the Law Review, and earned her B.A. degree cum laude from the University of Pennsylvania.

State and Local Preparations on Election Security in the Aftermath of the Mueller Report

- **Eric Geller *(moderator), Cybersecurity Reporter, Politico***
  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

- **Alex Padilla, *Secretary of State of California***
  Alex Padilla was sworn in as California's 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 from 2006 to 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. 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, *Election Consultant; former Director of Elections, Cook County, Illinois***

  Noah is an election consultant and the former Director of Elections for Cook County, Illinois. In this capacity he was responsible for the overall management of elections in one of the largest election jurisdictions in the country.

  Noah is an adjunct professor at DePaul University College of Law teaching Election Law and sits on the advisory board of the University of Chicago Harris Cyber Policy Initiative. Noah has presented extensively on Election Security, Sustainability, Election Day Management, Voter Registration Modernization and other Election Related items. He has also published articles on cyber security, election day administration and referendum law in Illinois.

- **Barb Byrum, Ingham County Clerk, Ingham County, Michigan**

  Barb Byrum is currently in her second term as Ingham County Clerk, serving as the county's chief elections official. As Clerk of one of the most populous counties in the State of Michigan, Byrum has successfully conducted 21 elections, 4 union elections, and the 2016 Presidential Recount. Byrum currently serves on Michigan's Election Security Commission, the Secretary of State's team of advisors tasked with strengthening and better securing elections in the state.

  Byrum has been a consistent advocate for the voting rights of qualified registered voters, with a focus on voting rights of military and overseas voters. Byrum serves on the Overseas Voting Initiative, which is a joint effort by the Federal Voting Assistance Program and Council of State Governments.

  Byrum graduated from Michigan State University with a Bachelor of Science degree in agribusiness management. She also holds a law degree from the MSU College of Law. Byrum previously served three terms as a Michigan State Representative. During her time in the Legislature, Byrum served as the ranking Democrat on the House Committee on Redistricting and Elections.

- **Amber McReynolds, Executive Director, National Vote at Home Institute**

  Amber McReynolds is the Executive Director for the National Vote At Home Institute and is the former Director of Elections for the City and County of Denver, Colorado. As one of the country's leading experts on election administration and policy, she has proven that designing pro-voter policies, voter-centric processes, and implementing technical innovations will improve the voting process for all voters. During her time in Denver, the Elections office was transformed into a national and international award-winning election office. Amber was also recognized as a 2018 Top Public Official of the Year by Governing Magazine for her transformational work to improve the voting experience in Denver and across Colorado. She is now focused on improving the voting experience across the country.

2020: Ready? Or Not?

- **Sherri Ramsay, *Senior Advisor, CyberPoint International; Senior Advisor: Cyber & NSA, Cambridge Global Advisors; former Director of the National Security Agency/Central Security Service Threat Operations Center (NTOC)***

  Sherri Ramsay is a consultant, engaged in cybersecurity strategy development and planning, cyber assessments, leadership, partnership development, and marketing & development of cybersecurity tools and security operations centers.

  Ms. Ramsay is the former Director of the National Security Agency's (NSA) Threat Operations Center. She led discovery and characterization of threats to national security systems, provided situational awareness for those threats, and coordinated actionable information to counter those threats with the Department of Defense, Department of Homeland Security, and Federal Bureau of Investigation. She also served as a senior leader in NSA's Signals Intelligence Directorate, Technology Directorate, and Information Assurance Directorate.

  Ms. Ramsay holds a Bachelor of Science degree from the University of Georgia, a Master of Science Degree from Johns Hopkins University, and Master's Degree from the Industrial College of the Armed Forces, National Defense University. She is on the Board of Advisors for Virginia Tech's Hume Research Center, the University of Chicago Cyber Policy Initiative, and TruSTAR Technology.

Beyond the Voting Machine: Other High Value Targets in Today's Election System

Since the U.S. Presidential election in 2016, there has been a heightened interest in election hacking. While electronic voting machines have been the primary focus, there are other high value targets could topple our election system if they were manipulated or compromised.

Brian will share his years of research into election systems to give you an insider's view of these high value targets and how and why they could be used by an adversary. In addition to a technical analysis of the components of an electronic voting machine, he will discuss the potential weaknesses of other key pieces of today's election system that many have overlooked.

- **Brian Varner, *Special Projects Researcher, Symantec Cyber Security Services***

  Since 2010 Brian Varner has been a special projects researcher on Symantec's Cyber Security Services team, leading the company's CyberWar Games and emerging technologies development. He previously worked at the National Security Agency as a tactical analyst.

  Brian holds a bachelor's degree in Computer Science from Florida Southern and master's degree in Information Assurance from Norwich University. Since early 2016, Brian has researched electronic voting machines and campaign security issues and is often called on by peers and media for his unique perspective on the potential threats facing today's election systems.

Putting Voters First: Expanding Options to Vote

- **Amber McReynolds, *Executive Director, National Vote at Home Institute***

  Amber McReynolds is the Executive Director for the National Vote At Home Institute and is the former Director of Elections for the City and County of Denver, Colorado. As one of the country's

leading experts on election administration and policy, she has proven that designing pro-voter policies, voter-centric processes, and implementing technical innovations will improve the voting process for all voters. During her time in Denver, the Elections office was transformed into a national and international award-winning election office. Amber was also recognized as a 2018 Top Public Official of the Year by Governing Magazine for her transformational work to improve the voting experience in Denver and across Colorado. She is now focused on improving the voting experience across the country.

Thirty Years Behind the Ballot Box: A firsthand look at the multiple factors preventing fair, effective and secure elections in America

- **Ion Sancho, *former Supervisor of Elections, Leon County, Florida***

  Ion Sancho served 28 years as Supervisor of Elections of Leon County, Florida. Elected in November of 1988, Sancho was sensitized to problems in elections when 5,000 voters were disenfranchised in a 1986 state and local primary election due to the misprogramming of the voting machines. Sancho was candidate in that election, and since then has dedicated his professional career to properly administering elections in Leon County, working for fair, accessible and verifiable elections nationwide.

  Concerned by voting machine security, Supervisor Sancho sanctioned a number of red team attacks on his voting system in the spring and summer of 2005, captured in HBO's 2007 Emmy-nominated documentary "Hacking Democracy", showing how the system could be hacked to alter the outcome of any election without being detected unless the paper ballots themselves were audited.

  Ion Sancho retired after the 2016 presidential election. He has remained active in the elections field, appearing as an expert witness in election cases and working with public and private entities heightening awareness to the threat of foreign intrusion to the American voting process, particularly the critical need for audits.

UnclearBallot: Automated Ballot Image Manipulation

As paper ballots and post-election audits gain increased adoption in the United States, election technology vendors are offering products that allow jurisdictions to review ballot images---digital scans produced by optical-scan voting machines---in their post-election audit procedures. Jurisdictions including the state of Maryland rely on such image audits as an alternative to inspecting the physical paper ballots.We show that image audits can be reliably defeated by an attacker who can run malicious code on the voting machines or election management system. Using computer vision techniques, we develop an algorithm that automatically and seamlessly manipulates ballot images, moving voters' marks so that they appear to be votes for the attacker's preferred candidate. Our implementation is compatible with many widely used ballot styles, and we show that it is effective using a large corpus of ballot images from a real election. We also show that the attack can be delivered in the form of a malicious Windows scanner driver, which we test with a scanner that has been certified for use in vote tabulation by the U.S. Election Assistance Commission. These results demonstrate that post-election audits must inspect physical ballots, not merely ballot images, if they are to strongly defend against computer-based attacks on widely used voting systems.

- **Kart Kandula, *Graduate Student, University of Michigan***
  Kart Kandula received his B.S.E. degree in computer science engineering from the University of Michigan in 2019 and is currently pursuing an M.S.E in the same area. He conducts research in the UM-Security lab under the supervision of Professor J. Alex Halderman. Currently, his research interest lies in problems affecting society and public policy, specifically election security. He has held internships at Microsoft and J.P. Morgan in the past.

- **Jeremy Wink, *Undergraduate Student, University of Michigan***
  Jeremy Wink is an undergraduate student at the University of Michigan currently pursuing a BSE in Computer Science. He has taken multiple security courses and has spent time researching topics surrounding election cybersecurity under J. Alex Halderman.

Saturday, August 10, 2019

Organizational Cybernetics: A Key to Resilience for the Digital Village

- **Kimberly Young-McLear, *Assistant Professor, U.S. Coast Guard Academy***
  Lieutenant Commander Kimberly Young-McLear is currently an Assistant Professor at the U.S. Coast Guard Academy. She holds engineering and technical degrees from Florida A & M, Purdue, and The George Washington University, including a Ph.D in Systems Engineering. She has taught a breadth of courses including Operations and Project Management, Crisis Mapping & Cybernetics, and Cybersecurity Risk Management. She has been instrumental in enhancing the inclusion of cybersecurity training and education program at the Academy for cadets and faculty. Lieutenant Commander Young-McLear was a key thought leader for the development of the Coast Guard Academy's first cyber undergraduate major. Furthermore as Vice Chair, she leads a multidisciplinary faculty Cyber Council to advance cyber curriculum and research at the Academy. Her research niche is focused on protecting critical infrastructure from cyber threats in the Maritime Domain. LCDR Young-McLear is also the program developer for NET21, a middle school outreach program, designed to systematically close STEM gaps amongst underrepresented students and teachers of color in the field of cybersecurity.

Ideas Whose Time Has Come: CVD, SBOM, and SOTA

From their origins in general purpose computing, Coordinated Vulnerability Disclosure (CVD), Software Bill of Materials (SBoM), and Secure Over-The-Air (SOTA) updates have been implemented or considered in safety sectors including industrial control systems, medical device manufacturing, and ground transportation. These common software security practices are becoming widespread global norms, turning up in public policy, international standards, and national law (often in sector-specific safety regulation). This talk will briefly review the practices (what), provide examples of successful implementations and supporting information (how), and (why).

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***
  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and

Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). In that capacity, she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism & force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

- **Art Manion, *Vulnerability Analysis Technical Manager, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University***

  Art Manion is the Vulnerability Analysis Technical Manager at the CERT Coordination Center, part of the Software Engineering Institute at Carnegie Mellon University. He has studied software security and coordinated responsible disclosure efforts since joining CERT in 2001. Having gaining mild notoriety for saying "Don't use Internet Explorer" and "Replace CPU hardware" in public, Manion now focuses on policy, advocacy, and rational tinkering approaches to software security, including standards development in ISO, OASIS, and FIRST. Prior to joining CERT, Manion was the Director of Network Infrastructure at Juniata College.

Incident Lifecycle and Incident Response Management Planning

In the past few years, the volume, types, and quality of cybersecurity - related attacks in elections have become more damaging and disruptive, and new types of security-related incidents have emerged. This white paper describes the best-known method for analyzing the stages of cybersecurity incidents and identifies actions that can be taken to avoid or minimize impacts at each incident lifecycle stage. We discuss the overarching workflow for elections security incident response and management and describe the Point and Line analysis approach, which considers factors such as attack vectors, motives, probability, and imp act to develop a set of Incident Response Templates in this paper. In addition, we include reusable templates for analyzing cybersecurity Incident Lifecycle and Incident Response Management, which can be customized for specific needs of any election jurisdiction in this paper.

- **Rahul K. Patel, *Elections Information Security Officer, Office of the Cook County Clerk and Chicago Board of Elections Commissioners***

  Rahul Patel is a seasoned Cyber & Information Security professional with over 25 years of experience defending the availability, confidentiality, and integrity of information assets. He is presently leading elections information security and risk management efforts at the office of the Cook County Clerk and Chicago Board of Elections Commissioners as an Elections Information Security Officer. Patel holds a PhD from Northcentral University, an M.B.A. from DePaul University, and an M.S. from Illinois Institute of Technology

- **Tonya Rice, *Director of Elections, Cook County, Illinois***

  Tonya Rice was appointed Director of Elections by Cook County Clerk Karen A. Yarbrough in 2019,

in which capacity she supports operations for one of the largest election jurisdictions in the country. Rice began her career in elections in 2005 as a political science graduate student at the University of Michigan, where she was a National Science Foundation Graduate Research Fellow, specializing in public opinion on voting technology and post-election audits, as well as the political participation of language minority citizens. Rice holds a J.D. from Northwestern University School of Law and B.A. from Northwestern University.

Assessing Election Infrastructure

- **Jason Hill, *Chief, National Cybersecurity Assessments and Technical Services (NCATS)***
  Jason Hill is the Chief of the National Cybersecurity Assessment and Technical Services (NCATS) Branch of the Cybersecurity and Infrastructure Security Agency (CISA). In this capacity Jason has primary responsibility to deliver quality security testing and analysis to customers that include the Federal government, State, Local, Tribal and Territorial governments, as well as Private Sector/Critical Infrastructure stakeholders. Mr. Hill has worked with several tech companies creating and teaching red team course work and conducting penetration testing in the commercial industry and DOD. Jason also spent 22 years as a US Army National Guardsmen for the Commonwealth of Virginia. As Master Sergeant of the 91st Cyber Brigade he led the Cyber Opposition Forces which provides red team & pen testing capabilities. He has achieved certifications for the Offensive Security Certified Professional and the Certified Ethical Hacker trainings.

- **Genevieve Marquardt, *IT Specialist, National Cybersecurity Assessments and Technical Services (NCATS)***
  Genevieve Marquardt serves as a member of the National Cybersecurity Assessments and Technical Services (NCATS) Cyber Hygiene team which is responsible for continuously assessing the "health" of external stakeholders' endpoints reachable via the internet and maintaining an updated enterprise view of the cyber security posture of their systems to drive proactive mitigation of vulnerabilities and reduce risk. Genevieve provides technical support pertaining to public IP scans and testing of .gov public facing networks for stakeholders.

- **Derrick Thornton, *Federal Lead, National Cybersecurity Assessments and Technical Services (NCATS)***
  Derrick Thornton joined the National Cybersecurity Assessments and Technical Services (NCATS) team in June 2017 as an Information Security Specialist. Derrick serves as a Federal Lead leading NCATS RVA teams conducting two week penetration tests. An 11-year veteran of the U.S. Air Force, Derrick was stationed at Robins Air Force Base, Georgia and at White Sands Missile Range, New Mexico while also serving 2 tours in the Middle East. The 4 years of military service at White Sands Missile Range was an assignment to the National Reconnaissance Office, which led to a 21-year career within the NRO. Derrick has a Bachelor of Science in Technical Management from DeVry University.

Securing America: How DHS, States, and Cybersecurity Startups are Working Together Before the 2020 Presidential Election

In 2016, 50 states' election systems were targeted by Russian nation-state hackers. Russian actors visited election websites, tested vulnerabilities by trying to exploit SQL database vulnerabilities, and even managed to access voter registration files and a county ballot. DHS deemed US election infrastructure "critical" and now CISA, DHS' critical infrastructure office, is actively providing scanning technology and technical assistance to states. States, which have direct authority over the issue, are doing a great job with their own efforts including working with the National Guard, looking public-private partnerships to provide DDoS mitigation and in some cases trying bug bounties and working with ethical hackers to keep elections secure. However, there is still much to be done to secure our democratic/election systems before 2020 - we need YOU. Election security will require a united effort with the scale and vigilance of a crowd of top talent. How are states innovating before the 2020 Presidential Election? How can hackers help?

- **Joseph Marks *(moderator), Reporter, The Washington Post***
  Joe Marks is a reporter for The Washington Post, where he writes The Cybersecurity 202 newsletter focused on the policy and politics of cybersecurity. Before joining The Washington Post, Marks covered cybersecurity for Politico and Nextgov. He also covered patent and copyright trends for Bloomberg BNA and federal litigation for Law360. Marks began his career at Midwestern newspapers covering city and county governments, crime, fires and features. He spent two years at the Grand Forks Herald in North Dakota and is originally from Iowa City.

- **Rita Gass, *CIO, California Secretary of State's Office***
  Rita established her career and progressed throughout the roles to become a chief information officer in 2008 with CCC. Remaining in this role for eight years, she eventually moved to the same role with California Secretary of State (SOS), where she continues to work now.

- **Wayne Thorley, *Deputy Secretary for Elections, Nevada Secretary of State's Office***
  Wayne Thorley is the Deputy Secretary of State for Elections for the Nevada Secretary of State's office and is responsible for administering the Nevada's election process including enforcing state and federal election laws and procedures and the Help America Vote Act.

- **Trevor Timmons, *CIO, Colorado Secretary of State's Office***
  Trevor Timmons has served the Colorado Secretary of State as Chief Information Officer since 2007, after eight years as Deputy CIO and Director of Software Development. Mr. Timmons has served under several Secretaries of State, during which time Colorado has gained a national reputation in several areas, including elections administration and cybersecurity operations.

- **Alex Joves, *Regional Director, Region V, Cybersecurity and Infrastructure Security Agency***
  Alex Joves is the Regional Director for Region V of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. He has served in various roles for DHS since 2007, including Regional Supervisor of Chemical Facility Anti-Terrorism Standards and Director of the National Infrastructure Coordinating Center. Prior to joining DHS, Mr. Joves was an

Associate Attorney at Perkins Coie LLP. He has a JD from The George Washington University Law School and a Bachelor of Science in Government from the U.S. Coast Guard Academy.

- **Josh Benaloh, *Senior Cryptographer, Microsoft Research***
  Josh Benaloh is a Senior Cryptographer at Microsoft Research and has worked on verifiable election technologies for more than thirty years. His 1987 doctoral dissertation at Yale University, entitled "Verifiable Secret-Ballot Elections", introduced the use of homomorphic encryption as a means to enable public verifiability in elections.
  Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has published and spoken extensively and testified before Congress on election technologies and was an author of the 2018 National Academies of Science, Engineering, and Medicine report "Securing the Vote – Protecting American Democracy".

- **Alissa Starzak, *Head of Policy, Cloudflare***
  Alissa Starzak is the Head of Public Policy at Cloudflare, an Internet performance and security company that is on a mission to help build a better Internet.

- **Jay Kaplan, *Co-Founder and CEO, Synack***
  Jay co-founded Synack after serving in several security-related capacities at the Department of Defense, including the DoD's Incident Response and Red Team.

Bootstrapping Vulnerability Disclosure for Election Systems

Seven months. It look seven months to make contact with a major city after discovering a critical vulnerability in their election registration website, which could have exposed (or worse, modified) information of millions of voters. As seen in the Mueller report, election systems are under active attack by foreign adversaries. Yet while vulnerability disclosure policies are becoming the norm in most industries, exactly zero states or election vendors have established vulnerability disclosure policies to allow reporting vulnerabilities in election systems. In a time where accepting feedback from the public is the best defense against these attacks, the lack of vulnerability disclosure policies hinders improvements in securing systems. In a talk by security researcher Jack Cable and Katie Trimble from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, learn industry best practices for vulnerability disclosure and how election systems can benefit from additional public scrutiny. Hear Jack's experiences disclosing critical vulnerabilities in several major election registration systems, and how this can be channeled to protect our nation ahead of the 2020 elections.

- **Jack Cable, *Security Researcher and Student, Stanford University***
  Jack Cable is a coder turned white hat hacker and a rising sophomore at Stanford University. Jack is a top ranked hacker on the HackerOne bug bounty platform, having identified over 350 vulnerabilities in companies including Google, Facebook, Uber, Yahoo, and the U.S. Department of Defense. After placing first in the Hack the Air Force challenge, Jack began working this past summer at the Pentagon's Defense Digital Service. At Stanford, Jack studies computer science and launched Stanford's bug bounty program, one of the first in higher education.

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***
  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). In that capacity, she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism & force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

- **Trevor Timmons, *CIO, Colorado Secretary of State's Office***
  Trevor Timmons has served the Colorado Secretary of State as Chief Information Officer since 2007, after eight years as Deputy CIO and Director of Software Development. Mr. Timmons has served under several Secretaries of State, during which time Colorado has gained a national reputation in several areas, including elections administration and cybersecurity operations.

"The Election System: Can We Fix It?" "YES WE CAN!"

As the previous DEF CON Voting Villages have proved, our voting equipment and infrastructure are very vulnerable to multiple types of attacks. Instead of focusing on problems and broken things, this talk will focus on simple fixes that vendors and governments can put into action right now.

Starting with the machines themselves, then moving through parts of the entire system, BiaSciLab will offer suggestions on how simple practices and changes in thinking and hiring can improve the security of the entire system.

Last year at r00tz BiaSciLab was one of the first to hack the mock election reporting system set up by the Voting Village. Some have pointed out that this was a purposely flawed system designed for the the kids to break. However, as outlined in the Mueller report, Russian hackers used the same SQL injection technique to break into an election reporting system. If our systems are so secure, how was this able to happen? Lack of secure coding practices and both peer and outside review. If proper coding review and application testing had happened, this SQL injection vulnerability would have been found and fixed.

Breaking down these flaws and offering real solutions for each one, BiaSciLab will bring hope in the face of this daunting and complex security problem.

- **BiaSciLab, *Founder and CEO, Girls Who Hack***
  BiaSciLab is a 12 year old hacker and maker. She was the youngest speaker at the Hackers on Planet Earth conference and has spoken at DEF CON previously in both the Bio Hacking Village and the r00tz Asylum kids con. She received national attention when she hacked the voting reporting system at DEF CON 26. BiaSciLab is alsothe Founder and CEO of Girls Who Hack, an organization focused on teaching girls the skills of hacking so that they can change the future.

Securing Voting Systems (Beyond Paper Ballots!)

While much "headline hacking" is devoted to exposing vulnerabilities on voting machines themselves, there is more to election systems security than simply popping shells on old, unsupported kiosks. In this session, attendees will learn what real world IT personnel in the 3071 counties and parishes across the U.S. face on and around Election Day, beyond the voting machine.

- **Tod Beardsley, *Director of Research, Rapid7***

  Tod Beardsley is the Director of Research at Rapid7. He has over 30 years of hands-on security experience, stretching from in-band telephony switching to modern Internet of Things implementations. He has held IT Operations and Security positions in large organizations such as 3Com, Dell, and Westinghouse, as both an offensive and defensive practitioner.

Machine Voting: The Bulgarian Experience

First machine voting experiments in Bulgaria started in 2009. Since then machine voting found its place in legislation with the usage of offline DRE kiosks with VVPAT. Latest developments in information security and the rising threads require flexible technical approach with still lagging legislation. The talk will pass through our machine voting experience, problems and solutions we came up with. We'll share detailed security requirements for voting machines and their implementation in practice. Special emphasis will be put on latest European parliament elections, held in May 2019 and upcoming municipal elections in October 2019.

- **Alex Stanev, *CTO, Information Services JSC***

  Alex started as a software developer in late 90s working on a wide range of projects – from specialized hardware drivers to large scale information systems for private and public sectors, including e-government services, elections management and smart cities.

  Since 2003 Alex has been leading computer processing of all election results and referendum projects in Bulgaria. As a consultant for the Central Election Commission of Bulgaria Alex is the primary author of technical and security requirements for election machines used in Bulgaria. As a security consultant, Alex has lead penetration test audits in Europe, America and Africa for financial and government institutions.

  Currently Alex serves as CTO in the largest Bulgarian systems integrator - Information Services JSC.

Addressing the election security threats posed by Very Small Jurisdictions

While most election administrators in the US are working in jurisdictions with populations in the tens or hundreds of thousands, there are states with jurisdictions as small as a dozen or so voters. In these Very Small Jurisdictions, the local interface with the state election system can be as crude as a Windows XP computer directly connected to an ISP and used by an Election Administrator with little computer experience or understanding of anti-social engineering practices. These are administrators with direct user access to statewide election systems containing voter roles and responsible for posting official election results. And while there are creative approaches to improving election worker training to offset social engineering threats underway in several states, they are virtually all designed for the more typical "macro" jurisdiction level (country-level

jurisdictions) and are not scaleable to these "micro" levels, leaving secretaries of state to run generalized safety trainings with little follow-up and few options for addressing these vulnerabilities. The talk will briefly explore the threat and why creating public logical network structures are best suited not just to mitigate the problem, but to potentially make these jurisdictions even more secure than their larger counterparts.

- **John Odum, *CMC, CEH, CNDA, MCP, CIW; City Clerk, Montpelier, Vermont***
  John Odum has been the elected City Clerk of Vermont's Capital, Montpelier, for 7 years. In this capacity he also serves as the the Election Administrator for Montpelier. Prior to being elected clerk, John worked in communications and IT for non-profits and political campaigns. His work has been published on websites of The Guardian, Governing, Huffington Post, as well as numerous Vermont area publications.

The Devil Went Down to Georgia. Did He Steal Souls? (Georgia's Electronic Voting Saga)

- **Marilyn Marks, *Executive Director, Coalition for Good Governance***
  In 2009, after a narrow loss to become the Mayor of Aspen, Marilyn Marks recognized the vulnerabilities in Colorado's election systems and chose to devote herself full time to election integrity litigation and lobbying efforts for more transparent and verifiable elections. She successfully litigated the effort to make Colorado ballots open public records for postelection reviews, followed by more than 25 election-related cases involving election transparency or voter privacy. She is currently the driving force behind the legal challenge to Georgia's unverifiable electronic voting system.

- **Rich DeMillo, *Professor of Computer Science and Executive Director, Center for 21st Century Universities, Georgia Tech***
  Richard DeMillo is the Charlotte B. and Roger C. Warren Chair of Computer Science and Professor of Management at Georgia Tech, where he founded and now directs the Center for 21st Century Universities. The Center is Georgia Tech's living laboratory for fundamental change in higher education. He is responsible for educational innovation at Georgia Tech and is a national leader and spokesman in the online revolution in higher education. Under his leadership, Georgia Tech has developed a pipeline of 50 Massive Open Online Courses that together enroll a million learners.

- **Logan Lamb, *Cybersecurity researcher***
  Logan Lamb is a Senior Security Engineer at Bird. Previously he has served as a Cyber Security Researcher at Bastille Networks and Oak Ridge National Laboratory. He has Master of Science and Bachelor of Science degrees in Computer Engineering, both from the University of Tennessee, Knoxville.

- **Jordan Wilkie, *Freelance journalist covering election integrity***
  Jordan Wilkie is pursuing a career as an investigative journalist covering criminal and social justice by combining data-driven reporting with long-form, narrative storytelling. My expertise to-date is in incarcerated juvenile and LGBTQ populations.

- **Robert McGuire, *Attorney for Coalition plaintiffs***

  Robert McGuire is the attorney for the National Election Defense Coalition plaintiffs in their current legal challenge to Georgia's unverifiable electronic voting system. His previous experience includes serving as a Senior Associate at Allen & Overy LLP, as a lecturer at the University of Denver's Sturm College of Law, and as a law clerk for the U.S. Court of Appeals for the Eighth Circuit. He earned his JD from Yale Law School.

- **Susan Greenhalgh *(moderator), Vice President of Policy and Programs, National Election Defense Coalition***

  Susan Greenhalgh is Vice President for Programs at National Election Defense Coalition. Susan performs extensive research, assembling and reviewing documents that may influence and impact state and federal policy regarding election verifiability and security. She also works with cyber security experts and advisors on the federal level to bridge the gap between national cyber security policy and election administration. Susan has a bachelor's degree from the University of Vermont in chemistry.

Sunday, August 11, 2019

Exploring Voter Roll Manipulation and Fraud Detection with Voter Files

Qualified Voter Files are published by states and contain information on registered voters. These files are used by political campaigns and analysts to gather data on registered voters. The public nature of these files also makes it easier for the public to detect voter fraud and can be used by third parties to help detect large scale voter registration attacks. The data contained in these files, however, could be used by attackers to impersonate voters and update or delete a voter's registration information and subsequently prevent the targeted voters from exercising their right to vote. Use of Qualified Voter Files could also inform attackers on what scale voters' information could be changed without raising suspicion.

- **Nakul Bajaj, *High School Researcher, University of Michigan***

  Nakul Bajaj is a rising high school senior at The Harker School. He is interested in computer science and public policy, and frequently participates in hackathons and debate competitions to learning more about each of these fields. Previously, he has done analysis on election datasets, finding patterns between race and income and voter turnout. In addition, he has worked on projects dealing with a combination of law and computer science, having built an expert system that helps inventors file their own patents. This summer, he is helping conduct research in Professor J. Alex Halderman's lab at the University of Michigan regarding electronic voting machines and other election security topics with help from PhD candidate Matthew Bernhard.

Defending Democracy: Working with Election Officials to Improve Election Security

Four years after documented foreign interference in the 2016 presidential election put election security in the headlines, cybersecurity experts and election officials still face challenges in working together. The need for collaboration is clear - especially in smaller and less well-resourced jurisdictions - so how can we bridge the gap? Hear from current and former election officials and election security advocates about how successful partnerships have moved the needle, and what to do if you want to engage your local election office.

- **Liz Howard, Counsel, *Democracy Program, Brennan Center for Justice***
  Liz Howard currently serves as Counsel for the Brennan Center's Democracy Program, with a focus on cybersecurity and elections. Prior to joining the Brennan Center, Ms. Howard was Deputy Commissioner for the Virginia Department of Elections. During her tenure overseeing election modernization projects in Virginia, she coordinated the state's decertification of all paperless voting systems, implementation of the e-Motor Voter program, and adoption of online, paperless absentee ballot applications. Ms. Howard earned her J.D. from the William & Mary School of Law in 2009.

- **Justin Burns, *Chief Information Security Officer, Washington Secretary of State***
  Justin Burns joined the elections security community in January, as CISO for the Washington Secretary of State. Prior to this, he served as a Solutions Architect and Technical Assistant to the Washington State CIO.

- **Trevor Timmons, *Chief Information Officer, Colorado Secretary of State***
  Trevor Timmons became Chief Information Officer for the Colorado Secretary of State in 2007, after eight years as Deputy CIO and Director of Software Development. During this time, Mr. Timmons served under several Secretaries of State and Colorado gained a national reputation in several areas, including elections administration and cybersecurity operations.

- **Jared Dearing, *Executive Director, Kentucky State Board of Elections***
  Jared Dearing is the Executive Director of the Kentucky State Board of Elections and has worked in the elections space for over ten years. Jared has public and private sector experience working both at the local and state level, including working for the City of Louisville as well as the Office of California Governor Jerry Brown. His private sector work includes several tech startups located in the Bay Area and Boston. He is a graduate of the University of California, Berkeley where he studied public policy and engineering.

- **Monica Childers *(moderator), Product Manager for Risk-Limiting Audits, VotingWorks***
  Monica Childers is a civic technologist with a background in digital product design and project management. As Product Manager at the VotingWorks she champions collaborative design, partnering with state and local election officials to build low cost, flexible tools for election administration. Over the past decade she has designed online voter engagement platforms, vote-by-mail ballot tracking systems, text & email election reminders, and a national trouble-ticket system for reporting problems with election mail. Having served as the project manager for Colorado's post-election audit software for the past year, she is currently working with election officials implementing risk-limiting audits (RLAs) and is helping shepherd the development of nationwide RLA software.

Securing Your Election Infrastructure: Plan and Prepare to Defend Your Election Systems, People, and Processes

Robert Anderson will provide some background of Election Security and the threat research that is on-going for Election Security. An overview for election teams to plan and prepare to defend their

Election Systems, People, and Processes. Provide guidance to update your Security Policies and Incident Response Plan. Help election teams understand their Attack Surface and where your election systems are most vulnerable. Review the primary Threat Actors poised to attack your election systems. Then review several approaches that could be deployed to protect Election Security Assets, and direct to some organizations that could support election teams.

- **Robert Anderson, *Chief Cyber Security Practitioner and President, Preying Mantis***
  Robert Anderson is a highly trained IT & Cyber Security professional with over 25 years of experience in a variety of cybersecurity domains. As a former Intelligence Officer working in the Middle East, he brings a unique perspective to security operations and incident response. Robert has deployed and led over 500 security programs and projects to Fortune 500 companies, federal, state, and local governments, and NATO. Robert has over 15 years hacking experience and is a Certified Ethical Hacker. He is an expert in Cyber Threat Intelligence and Information Warfare and has led Incident Response Teams during many high-profile breaches.

Keynote Remarks: Representative Eric Swalwell (CA-15)

- **Representative Eric Swalwell (CA-15)**
  In 2012 Eric Swalwell was elected to represent California's Fifteenth Congressional District, which includes a large part of the East Bay. Now in his fourth term, he's working hard to bring new energy, ideas, and a problem-solving spirit to Congress, with a focus on advancing policies that support equality, opportunity, and security.
  Congressman Swalwell serves on the House Permanent Select Committee on Intelligence, and believes protecting Americans is Congress' most solemn duty. He chairs the Intelligence Modernization and Readiness Subcommittee, which oversees overall management of the Intelligence Community: the policies and programs focused on making sure that all 17 U.S. intelligence agencies have the workforce, infrastructure and services they need to succeed. This involves fostering greater collaboration and better use of resources across the entire Intelligence Community in personnel management, security clearance reform, information technology modernization, and other areas.