ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Hacking Elections is Easy!

Part 1: Tactics, Techniques, and Procedures

September 2016

Authors

James Scott (Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

Thought Leadership Contributions from the Following Experts:

Rob Roy (ICIT Fellow & CTO, HPE Federal)

Underwritten by:

Hewlett Packard Enterprise

Join ICIT at HPE Protect 2016

Gaylord National Resort and Convention Center
National Harbor, MD
September 13-16, 2016

http://h41382.www4.hpe.com/hpe_protect/

www.ICITGala.org

Publication Alert

"Hacking Elections is Easy! Part Two" will be available for download the week of September 5th:

http://icitech.org/icit-analysis-hacking-elections-is-easy-part-two/

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Contents

Introduction

To hack an election, the adversary does not need to exploit a national network of election technology. By focusing on the machines in swing regions of swing states, an election can be hacked without drawing considerable notice. Voter machines, technically, are so riddled with vulnerabilities that even an upstart script kiddie could wreak havoc on a regional election, a hacktivist group could easily exploit a state election, an APT could effortlessly exploit a national election and any corrupt element with nothing more than the ability to describe the desired outcome could order layers of exploits on any of the multitude of deep web forums and marketplaces. Yes, hacking elections is easy.

Manufacturers and voting officials have constructed an illusion of security based on the semblance of complexity when, in reality, voting machines are neither secure or complex. In general, these stripped down computers utilizing outdated operating systems possess virtually every conceivable vulnerability that a device can have. Security researchers have been leveraging easy to find and easy to exploit vulnerabilities in every electronic voting system, since before their widespread adoption in the early 2000s. Attackers' ability to exploit vulnerabilities in the systems that support the American democratic process is not exclusive to election machines. Catastrophically disrupting the campaign of just about any political candidate can be done with little more than a DDoS attack on fundraising links and web properties, spam widgets on social media platforms, an insider threat who delivers a malicious payload on a USB drive or unsuspectingly by clicking a link in a spear phishing email, and a ransomware variant to encrypt important donor lists to further cripple fundraising. A pseudo tech savvy adversary could create a network of spoofed sites to confuse voters and this is just the beginning. By combining attack vectors and layering attacks, an adversary can manipulate the democratic process by inciting chaos, imbuing suspicion, or altering results.

Breached Trust

The electronic voting systems popularized in the United States in the early 2000s have been repeatedly proven vulnerable and susceptible to attacks that are so unsophisticated, an eighteen-year-old high school student could compromise a crucial county election in a pivotal swing state with equipment purchased for less than $100, potentially altering the distribution of the state's electoral votes and thereby influencing the results of the Presidential election. In the security community, the conventional opinion of attacks against electronic voting machines is that the impact of the successful attack and the likelihood of a successful attack achieving the desired impact are inversely proportional. Therefore, a successful attack against the Presidential election is extremely high impact, extremely low likelihood of desired impact, while a successful attack against a local election is low impact, high likelihood. This opinion is mostly valid; however, it naively dismisses realistic scenarios where an entire election is decided on the results of a swing state or a single county, which could be as little as 400 votes. As demonstrated in the 2000

election, manual recounts of paper ballots can have a margin of error greater than 400 votes. Attacks that influence local, State, and Congressional elections may still be valuable to attackers, and are discussed less frequently in the media. These attacks require less of a success rate and are more likely to succeed without notice.

The need for cybersecurity in electronic voting systems should not be dismissed under the assumption that attackers cannot have a meaningful impact. It may be equally naïve to believe that attackers are not motivated to compromise these systems. Motivated attackers will achieve some impact. White hat hackers and black hat hackers share some, though definitely not all, of the same opinions, interests, and mentalities. If security researchers have been interested in whether electronic voting machines were hackable since their widespread adoption, chances are reasonable that malicious adversaries have considered the same question. The security and cyber hygiene surrounding electronic voting machines has not drastically changed in over a decade. Consequently, security researchers and attackers alike have had plenty of time to discover, and potentially exploit, vulnerabilities in the systems and processes that support United States democracy.

Electronic voting systems were proven to be vulnerable to simple attacks before they were installed in most states; nevertheless, the convenience of digital voting superseded security researchers' concerns and the nation exchanged paper ballot systems for electronic voting systems. Many e-voting systems, such as those manufactured by Diebold, ES&S, or Sequoia, are nothing more than stripped down embedded PCs without so much as perimeter security. In the decade and a half since their widespread adoption, the systems have not become more secure or more dependable. In fact, most of the systems implemented in the early 2000s remain operational despite the informed opinion that they are less secure than a modern children's toy. Critical vulnerabilities discovered at least a decade ago remain unresolved. Every four years, during the presidential election, the same stories reemerge acknowledging that the e-voting systems are vulnerable to the same old attacks, without any change in the security or oversight of the systems. Despite the vigilance of a dedicated niche of security researchers, manufacturers and election officials do not prioritize security because election officials lack the technical expertise to identify vulnerabilities and manufacturers have a keen interest in profit before security and disclosure. In truth, many of the e-voting systems in operation have outlived their manufacturers and most election volunteers and officials lack any form of cyber-hygiene education or training. Elections are held in the same churches and schools that are regularly victimized by malware and run by the same retirees and secretaries who regularly fall prey to phishing emails. The remaining manufacturers still see security as an unnecessary cost and are under no pressure to assume the expenditure. The remaining election officials lack any form of authority or budget to secure the systems.

Election personnel fail to realize that any easy target is a valid target for a cyber-adversary. Why wouldn't an enemy nation state try to corrupt the United States elections if all it cost were a few hundred dollars and a few hours of work? Even if they failed, the seed of chaos, discord, and distrust planted in the population would serve numerous adversarial agendas [1]. There is no evidence to prove that a cyber adversary has hacked or attempted to hack an election at the local, state, or federal level; however, there is absolutely no evidence or assurance process in place to demonstrate beyond a reasonable doubt that adversaries have not hacked e-voting machines [2]. Americans trust their votes to be reliably cast, to be counted as cast, and to be secret to anyone but themselves. If manufacturers and election authorities cannot validate that electronic voting systems have not been compromised any more confidently than they could guess that systems have been compromised, then there is a recognizable on-going systemic problem. True democracy relies on the reliability of the democratic process. Like other forms of critical infrastructure, trust in voting systems should be assured according to a transparent and comprehensive methodology.

A Global Target

Despite the recurring discussion on electronic voting vulnerabilities that occurs every four years, only limited attention is given to the systemic problem undermining American democracy. On Twitter, security researcher Matt Blaze, comments "We tend to have this discussion a few months before general elections, when it's too late to make substantive changes to voting tech [….] basically, public concern about e-voting integrity peaks at roughly the point when the choice is use existing tech or postpone election." Most US citizens, including some security researchers dismiss the possibility of cyber-physical election fraud as an unlikely scenario because they naively believe that cyberattacks must have a significant fiscal motivation. In reality, cyber adversaries attack any vulnerable system for a variety of reasons. As discussed in brief throughout the paper, there have been numerous examples of compromised systems and potential election tampering already. It's time for a complete overhaul in electoral process cyber, technical and physical security.

External parties have a vested interest in the American political system. For example, China may want to influence elections to dissuade voters from electing a Presidential candidate who might pass economic sanctions, from electing a Congressional candidate who promotes anti-China legislation, or from electing a local candidate who opposes regional tongs or espionage associations. China has a history of undermining the democratic processes of nations that it views as malleable. Similarly, Russia may attempt to influence elections to increase public distrust in democracy over time or to oppose a candidate who poses a significant threat to Russian attempts to amass regional dominance [2]. Russia already interferes in the elections of nations that it deems weak. A June 2014 report detailed how Russian hackers attempted to alter the election outcomes in Ukraine by targeting vote aggregation software [3].

Given how easy it is to impact election results, as discussed below, a hacktivist, mercenary threat, or a lone-wolf threat actor could easily alter election results based on conspiracy theory, financial, or geopolitical motivations respectively. Again, the threat actor does not need sophisticated methods, significant resources, or an expansive operational network. The United States e-voting system is so vulnerable that a small group of one or a few dedicated individuals could target a lynchpin district of a swing state, and sway the entire Presidential election. Those who doubt the potential impact should consider that in 1960, John F. Kennedy only had 112,727 more votes than Richard Nixon. The 2000 election between George W. Bush and Al Gore was similarly contentious and it may have depended on as few as 400 votes [4]. A single unsophisticated attacker who spoofs a few hundred votes or who disrupts voting operations at a few key locations could have a similar impact on a future election, if they have not done so already. Imagine what a dedicated advanced persistent threat could accomplish. The long-term goals of an APT are heavily focused on disrupting the belief that America is a legitimate democracy and that one's vote truly matters. The reduction in voter confidence in the system is a victory within itself. Rather than discussing and subsequently forgetting the vulnerabilities of e-voting machines once every four years, in the months preceding the Presidential election, without responding to the known threat vectors and security vulnerabilities inherent in the machines, America's electronic voting systems deserves the attention of every citizen and every candidate in every political party.

Hacking Campaigns and Candidates

The democratic process can be negatively impacted along a number of attack vectors. In a broad overview, an attacker's goal is to compromise the confidentiality, availability, and integrity of the election process. Adversaries could launch or pay to launch denial-of-service attacks against a candidate or party's networks and websites. Free tools on Deepweb can be used to launch such attacks or the adversary could contact a DDoS-as-a-service site on Deepweb to disrupt a candidate's operations for a few dollars per day. Similarly, disrupting election agencies and regulatory officials' operations can interrupt reporting, interrupt record management, or prevent coordination between agencies. Public defacement of election agency sites or the public disruption of services reduces citizens' trust in the electoral process. The attacker could begin by targeting campaign workers and donors to dissuade them from participating in the election process. Phishing, DDoS, and other attacks that target donors using social engineering and public information, such as donor lists, may decrease political participation. Alternately, an SQL injection attack against a candidate's website can be used to steal credit card information or identities. Lax security and high employee churn make candidate sites easy targets for Dox, DDoS, watering hole, and other attacks. Using social engineering, a brute force attack, or by exploiting poor cyber-hygiene, a hacker could publicly embarrass a candidate by hijacking their

websites and social media accounts. Finally, and most importantly, electronic voting machines can be manipulated by exploiting unpatched vulnerabilities in their antiquated systems.

An unskilled threat actor may begin a campaign by sending phishing emails or using free script kiddie tools to remotely attack undefended local networks to compromise email and exfiltrate internal documents that reveal the types of systems used in an election as well as their storage conditions. The threat actor could access Deepweb, navigate to a forum or market and solicit a custom malware based on their knowledge of the systems that they wanted to infect. If necessary, a purchase could be made through anonymous chat clients such as IRC, with the assistance of a trusted intermediary to verify the malware, and paid for with an anonymous digital currency such as Bitcoin. The actor could compromise the employee network to uncover operational information, steal passwords, preemptively infect employee machines, alter or delete records, compromise or delete registration forms, or disrupt access to the polls with the help of ransomware, an attack on the backend server, or otherwise compromise e-voting machines [2], [4]. The actor could physically infect machines by gaining access to machines as an employee or contractor or by illegally accessing the machines at their storage site. For instance, at the time of this writing, ES&S has open positions available for interns and contractors. The listings do not specify any requirement of a clearance or in depth background check to work in close proximity to electronic voting systems [20].

Donors can forgive unsolicited emails and supporters can ignore hacked social media accounts. However, cyber-physical attacks against the systems supporting the electoral process have the greatest potential to undermine the democratic process because their impacts cannot be ignored. In all likelihood, cyber-physical attacks against electronic voting systems may continue to go unnoticed due to a lack of cyber-hygiene culture, a lack of verifiable and thoroughly tested security mechanisms, a lack of standardization, and a lack of public attention. The discussion on even minimally securing e-voting systems does not capture the public's attention. Despite irreconcilable proof of systemic vulnerability throughout the infrastructure adopted in 2006, all attention on the possibility of tampering falls with each elected official's celebratory balloons. When an attacker breaches a candidate's website or social media account, voters lose trust in the capabilities of the candidate. When an attacker compromises a United States election because the process has been left notoriously vulnerable for over a decade due to a non-transparent culture and a lack of public interest in securing the electronic voting computers that are currently less secure than a decade old laptop, some voters may lose faith in the democratic process.

Attacks on the democratic process are not difficult or sophisticated. Any hacker with enough time, a basic ability to navigate Deepweb, and access to YouTube, can impact public perceptions, control political conversations, and undermine the democratic process. For example, consider how effortlessly a dedicated, but ultimately unsophisticated, cyber adversary, such as a script kiddie, a hacktivist, or a lone wolf threat, can target a political campaign and inflict

devastating damage. First, the attacker navigates the Deepweb and downloads or purchases a malware with a Remote Access Trojan (RAT) component, such as BlackEnergy, Sofacy, Gh0stRAT, or numerous other, widely available malware. The attacker researches the campaign and targets low-mid level staff, such as interns and social media coordinators, with spear-phishing emails. Statistically, about a quarter of targets fall prey to well-crafted spear-phishing emails. When an unsuspecting staffer clicks on a malicious email attachment, the chosen malware installs on their system and the attacker begins to log keystrokes, capture screenshots, and even capture sound or video. The threat actor may exfiltrate documents, capture credentials, or, in the case of a malicious lone wolf threat, capture the candidate's private schedule, for use in further attacks. They might seize control of social media accounts and websites using captured credentials, or if the spear-phishing email failed, they can rely on freeware defacement tools, known exploits, or other forms of social engineering.

Alternatively, a spoofed candidate website can be created and used to capture a legitimate user's credentials if they accidentally navigate to the site via a malicious link. Likewise, spoofed banner ads promoting or refuting a given candidate can be deployed to redirect victims to either a spoofed website or a watering hole site. Compromised social media accounts can be used to embarrass the candidate or to distribute drive-by-download links that distribute malware onto supporters' systems. Man-in-the-middle attacks on the website can capture supporters' financial information. A compromised website could be used as a watering hole to distribute malware to supporters' systems. If the attacker distributed botnet malware, then they could use the resulting network to conduct distributed denial of service (DDoS) attacks against the remainder of the candidate's cyber assets or they could distribute ransomware to raise funds. The funds raised from stolen contributions, stolen supporter information, or from ransomware attacks, can be directly applied to leverage additional cyber-opposition against the candidate or their supporters. Alternatively, an adversary may dedicate the funds in opposition of the candidate's opinions, they could channel the funds to the candidate's political opponent, or they could use the money to fund terrorism and other nefarious activity with the bitcoins purchased from stolen campaign contributions. This is neither a complex nor a difficult scenario. Attacks such as the one described can hobble or cripple a campaign. Candidates of each party have publicly fallen victim to website defacement, email hacks, and system compromises in the last 6 months alone. Every stage of these attacks undermines the democratic process by reducing trust in the officials who are vying for public office. The main deterrent to attacks of this magnitude is their limited profitability compared to other dedicated attacks and the amount of time necessary to implement the stages of the attack chain. While financially motivated threat actors are the dominant majority, politically motivated actors exist and are increasingly more common as attacks become easier to launch thanks to widely available information and tools. Further, mercenary attackers can be hired in layers and as dedicated services for part or all of an attack. The obvious

precaution to prevent public incident is to invest in cybersecurity controls and to increase cyber-hygiene within the political process.

Now, consider that it may be even easier and even more anonymous to attack vulnerable electronic voting machines, but there is no foundational cybersecurity or culture of cyber-hygiene to build upon. Polling places are swamped with pseudo-anonymous voters and polling staff that make the locations ripe for insider threat and malicious activity. Combine this with the all-to-often dismissals of the threat as unlikely "because different states use different machines" or "because elections are not profitable", and a manufacturer industry devoid of transparency, cybersecurity regulation, or proper oversight, and one can begin to understand why security researchers throughout the industry have been anxiously attempting to dissuade electronic voting adoption for the past decade.

The Black Box Legacy

The U.S. has relied on known vulnerable electronic voting systems for nearly 15 years. In 2000, controversies surrounding "hanging chads" in paper punch cards used for the Presidential election in Florida inspired a will to move away from a paper ballot election system [7]. In 2002, Congress passed the Help America Vote Act, which provided a $4 billion federal fund to incentivize all 50 states into upgrading voting machines to e-voting systems of one form or another. The majority of the systems adopted were the digital touchscreen optical scan and DRE systems such as the Diebold TSx, Advanced WINVote, ES&S iVotronic, and the Sequoia Edge. Since the 2006 HAVA cutoff, all of these systems (some of which are still in use) have been repeatedly proven vulnerable by cybersecurity experts and academics [1]. These machines are antiquated and ill-maintained. In fact, because e-voting machines are essentially stripped, embedded computers with minimal proprietary systems, there is a reasonable likelihood that the systems that America depends upon to verify the election of the most powerful official in the world, are less secure than even the "Frankensteined" legacy systems compromised in the OPM breach. At least the latter systems had minimal perimeter security and were not physically accessible to thousands of citizens during operation.

In 2007, 42 security researchers conducted red team penetration testing of machines manufactured by Diebold, Hart Intercivic, and Sequoia, on behalf of the State of California. A subgroup of the researchers, including Matt Blaze conducted testing on the source code of a Sequoia system. Shortly after publishing their findings, Blaze recounted on his blog that:

> "I was especially struck by the utter banality of most of the flaws we discovered. Exploitable vulnerabilities arose not so much from esoteric weaknesses that taxed our ingenuity, but rather from the garden-variety design and implementation blunders that plague any system not built with security as a central requirement. There was a pervasive lack of good security engineering across all three systems, and I'm at a loss to explain how any of them survived whatever process

> certified them as secure in the first place. Our hard work notwithstanding, unearthing exploitable deficiencies was surprisingly -- and disturbingly -- easy.
>
> Much of the controversy around electronic voting concerns the possibility of hidden "backdoors" incorporated by a nefarious vendor. Properly obfuscated, such mischief would be almost impossible to detect. Yet our reports chronicle software weakened not by apparent malice but by a litany of elementary mistakes: static cryptographic keys, unsecured interfaces, poorly validated inputs, buffer overflows, and basic programming errors in security-critical modules. Deliberate backdoors in these systems, if any existed, would be largely superfluous.
>
> Unfortunately, while finding many of the vulnerabilities may have been straightforward enough, fixing them won't be.
>
> The root problems are architectural. All three reviewed products are, in effect, large-scale distributed systems that have many of their security-critical functions performed by equipment sent out into the field. In particular, the integrity of the vote tallies depends not only on the central computers at the county elections offices, but also on the voting machines (and software) at the polling places, removable media that pass through multiple hands, and complex human processes whose security implications may not be clear to the people who perform them. In other words, the designs of these systems expose generously wide "attack surfaces" to anyone who seeks to compromise them. And the defenses are dangerously fragile -- almost any bug, anywhere, has potential security implications [18].”

Systems by other manufacturers were found to be equally vulnerable. Electronic voting systems lack even the basic security that comes preinstalled on a home computer. Many electronic voting systems have not been patched for almost a decade because officials falsely believe that an airgap equates to security [1]. In 2016, 43 states relied on voting machines that were at least 10 years old and that relied on antiquated proprietary operating systems such as Windows CE, Windows XP, Windows 2000, Linux, and others. Vulnerabilities for these operating systems are widely available for free download on Deepnet. Alternately, some GUI based script kiddies tools can automatically scan for Windows XP and Windows 2000 and exploit known vulnerabilities to deliver malicious payloads. Even if the officials did their due diligence and practiced moderate cyber-hygiene, Microsoft has not released a patch for Windows CE since 2013 or Windows XP since 2014. Further, some of the manufacturers of older systems have gone out of business despite their products continued use [7]. Aside from cybersecurity vulnerabilities, these systems pose significant risk to the voter process due to their lack of replacement parts, continued service, or calibrated hardware [13].

The industry relies on security through obscurity. Independent Testing Authorities (ITAs), who certify electronic voting machines, are notorious for their lack of transparency. ITAs often lack the technical capabilities sufficient to assert that electronic voting systems can be trusted. Their purpose is not to test or secure the e-voting systems. ITAs just check that e-voting systems

mostly adhere to state guidelines and regulations. These accreditation authorities are actually paid by manufactures and often required to sign nondisclosure agreements. Consistently, when security researchers and academics investigate systems on their own and report vulnerabilities, manufacturers have threated them with lawsuits for breaching the confidentiality of proprietary systems. This litigation-based response is highly suspect and could indicate known operational negligence on behalf of the manufacturers and a systemic problem on behalf of the government that depends on them [1].

A Voluntary False Sense of Security

Election systems remain vulnerable despite oversight, in part, because the system depends on federal, state, and local authorities, who each possess their own systems, software, hardware, and security protocols [4]. In the United States, more than 9,000 voting districts all use different election processes, procedures and machines. Though an estimated 70% of the 9,000 United States precincts rely on electronic voting, only 60% of states require any form of post-election audit according to paper trails. Georgia, Delaware, Louisiana, South Carolina and New Jersey use electronic voting machines that leave no way to audit results after the fact. Swing states, such as Pennsylvania and Virginia do not rely on machines that generate a paper trail [5]. According to Verified Voting, 47 of Pennsylvania's 67 counties rely on digital voting machines without a verifiable paper auditing trail.

Election security is regulated state by state, mostly according to technical standards developed by NIST and the Election Assistance Commission (EAC). However, these guidelines are voluntary and policy on voting is decided by each state and in some cases, each county [1]. Denise Merrill, President of the National Association of Secretaries of State, said that though lack of funding keeps most precincts from updating their systems, all machines have to meet specific government standards. She continues, ""The idea of a national hack of some sort is almost ridiculous because there is no national system." She adds "Our voting systems are heavily regulated. They're tested both before and after. There are paper trails everywhere...by in large, I would say the American election system works very well." To their credit, the Election Assistance Commission (EAC) issues guidelines that suggest that all voting systems are vigorously tested against security standards and that systems certified by the EAC are not connected to the Internet. Given that the EAC guidelines are voluntary and that some counties lack the knowledge and expertise to follow the guidelines, electronic voting systems are generally in far worse condition than the EAC asserts. Further, the testing mechanisms may not detect all types of attacks. Of particular note, are forms of malware that automatically delete their components after a certain amount of time and the risk of insider threats. Though machine testing should be done in observer-tester pairs, some counties with limited personnel may be at exceptional risk of a malicious insider who can freely access machines due to lack of supervision.

For instance, of the 24,000 outdated e-voting systems used in Pennsylvania in the 2016 Presidential election, 4,600 are stored in two rooms in a warehouse near Pittsburgh. These machines are tested for malware and are secured with temper-evident seals in the months preceding the election [19]. This large time window provides an insider weeks or months to compromise a machine after it has been checked. An insider could isolate a machine, remove the security seals with acetone and a razor blade, bypass any physical lock with a key or picks, install malware or a compromised internal component, and then reapply the security seal when the acetone dries. The entire attack takes less than 5-7 minutes for an untrained attacker. A professional may be able to reduce that time to less than a minute or two. Poll workers are not trained to recognize insider threats. Since the attack requires so little time, poll workers may not even suspect that a fellow worker, who departs on a restroom break, may be actually compromising electronic voting systems.

So Easy, a Script Kiddie Could Do It…

Attacking voting machines is easy at every stage of their lifecycle. After all, e-voting machines are just computers, with reduced functionality, proprietary code, and limited or no endpoint security. If attackers can compromise something as complex as an iPhone or laptop, compromising e-voting machines is a trivial task. The same threats of insider threat, exploited vulnerabilities, malware, etc. apply to e-voting machines.

Script kiddies, the most unsophisticated category of hackers, are not as motivated to disrupt elections as the vastly more sophisticated nation-state APTs; however, hacking the insecure voting machines is trivial, even for them. Script kiddies, or their more motivated hacktivist brethren, might oppose a candidate, and manipulate the systems containing votes for that candidate, through cyberattacks. Prior to an election, the attacker might use the tools built into Kali Linux'' or they might purchase an exploit kit or malware on Deepweb, to compromise or deface a website, server, or database. A dedicated threat actor might conduct layers of trivial attacks to overwhelm a candidate's redundancy and security resources. For instance, an attacker can simultaneously and trivially conduct SQL injection, brute force cracking, cross-site scripting, and DDoS attacks against a given webpage, using only the basic features available in the free Kali Linux operating system and a few short YouTube tutorials. Conducting these types of attacks on a candidate or on media outlets on Election Day can influence the public and have a dramatic impact on the election. Election Day is tense for both political administrations and for the public. Because different regions of the country vote at different times and in different time zones, there is a certain level of information leakage that influences undecided voters to choose one candidate over the other. By controlling the spout of information, an attacker gains some control over dispersion of information and can thereby leverage it to influence the election. Access to honest representations of candidates can be disrupted through website defacements or DDoS attacks to prevent undecided voters from making informed decisions. Media outlets can be

similarly attacked to prevent exit poll predictions or election results from reaching the public. If news of the attacks supersedes news of the elections, then coverage is derailed entirely. In any case, a percent of voters may lose trust in the electoral system and either pick candidates in last-minute uninformed decisions or decide not to vote altogether. Worse, if local polling places depend on an internet connection for voter authentication, then a remote script kiddie can DDoS the polling place, compromise the voter database or server, or otherwise directly disrupt voters' ability to cast their ballot. If lynchpin regions of swing states are targeted with any of the aforementioned attacks, then an unsophisticated script kiddie could potentially shift the balance of votes in a critical swing state. Worse yet, though the attacker's actions are illegal, the results of the elections, based on the valid, misinformed votes of a disenfranchised population, may be upheld.

Humans: Security's Glass Heel

Some manufacturers do not require an extensive background check for employees, contractors, or interns. Any employee, contractor, or intern could be an insider threat capable of altering the hardware, firmware, or software of e-voting systems. Similarly, extensive background checks are not required in most states for election officials or those with preemptive access to the machines. In 2012, Argonne National Laboratory conducted a wide review of e-voting machines and found most widely used models were trivial to hack if the attacker has physically access the machine [4]. In recent interviews, Symantec researchers Brian Varner and Kevin Haley echoed a similar attack vector. With physical access to a machine for less than a minute and for less than $15, a system can be compromised by replacing the ROM module with an infected unit (provided prior access) or by repeatedly rewriting a voter access card and casting multiple votes (without prior access). In the latter attack, Varner estimates that up to 400 extra votes can be cast in the amount of time that a typical voter spends in the booth [5]. Even easier, some Sequoia voting machines have a yellow button on the back of the unit that overrides the voter access card and allows a user to cast a vote as many times as they press the button [14]. Changing the ROM module could alter how votes are tallied, received, and transmitted. Worse, a compromised voter access card loaded with custom malware could be plugged into a machine without drawing any attention at the polling station [16]. In either case, the attacker has used physical access to the device and limited knowledge, if any of the actual system, to redistribute the proportion of votes.

The primary difficulty in launching physical attacks is discrete access to the system. Election officials will notice a threat who starts dismantling a voting system to install a compromised ROM module in the middle of an election. Instead, a threat might gain access to the system as an insider threat at the manufacturer or storage facility, by volunteering to run the elections, or by posing as a repairman or auditing authority. With no technical skill whatsoever, a threat actor could pose on a college campus or street corner as a campaign volunteer offering to help register new young voters. The attacker could socially engineer a student into providing personal

information. In all likelihood, if asked to fill out a form or laptop survey, the student will provide the necessary information such as name, date of birth, social security number, last known address, and other data. Additional information can be drawn from social media accounts linked to the provided name or email address. The stolen identity can be used to volunteer for a political campaign or to volunteer to help at a polling center. The insider can gather information about what machines are used, where they are stored, what the actual chain-of-custody on administrative smart cards of PBEs looks like, and other operational details. Afterward, the adversary can either attack the machines where they are stored, or compromise the media, such as PBEs, USBs, and smart cards, that are connected to the voting systems, all while masquerading as a helpful volunteer [15].

Plug and Play USB Exploits

Newer e-voting units have accessible USB ports that officials use to install updates. Rather than reprogram a ROM module or rewrite an access card, the port can be used to install a trojan or ransomware. Malware affecting Windows systems such as CE, XP, and Windows 2000 can be obtained on Deepnet for little or no payment, and loaded onto a USB drive. Malicious USB drives could be mailed to election officials with spoofed letters detailing instructions to update systems. Many election officials, such as county clerks, lack the information security training and awareness necessary to recognize the threat. Accessing the ROM or USB drive might require an attacker to bypass a physical lock and a security seal. Cyber-physical attackers, without training, may not be able to pick a lock in an innocuous amount of time; however, in a demonstration of substantially insecure design, some manufactures use standardized keys that can be purchased online, acquired from other units such as minibars, or carved from a key blank according to online photos as in the case of the Diebold AccuVote TS and TSx. As of 2016, the TS/ TSx are still used in 26 states, including Pennsylvania, Ohio, Missouri, and Colorado. Security seals can be bypassed in numerous ways, such as by slowly dispensing a syringe of acetone (household nail-polish remover) on the adhesive coating of the seal. The seal can be slowly peeled back before the acetone dries and the reapplied after the attack. Attackers and security researchers alike, who are searching for vulnerabilities can also purchase voting machines such as the Sequoia AVC Advantage and the Diebold AccuVote TS online [1]. Security researchers report critical vulnerability discovery times ranging from 2-24 hours. Afterward, attacks were developed that took 15-60 seconds to execute by bypassing the physical controls and implanting a device such as a ROM module or a logic analyzer. Because voting machines often sit undisturbed and poorly secured in basements and warehouses, the attacker may have considerably more time to compromise the device.

Voting machines made by Diebold, Hart, and other manufacturers often have hardcoded encryption keys that are shared across their machines. Attackers can use the key to inject code or otherwise alter a system or it can be loaded into malware to bypass security and deliver a

malicious dropper or payload. Malware delivered via spoofed PBE, USB, ROM, or any other mechanism can be installed on the system and it can obfuscate its presence by exploiting administrative access.

Manipulating the Memory of an Election

The most convenient attack vector is to alter votes after they have been collected. Machine smart cards, PBEs, or other media, which function as electronic ballot boxes, can be reprogrammed to miscount or redistribute votes. Voter records are unencrypted and easily manipulated, and the black-box code could be altered by an insider threat to reorder ballot definition files, to alter vote tallies, or to disrupt the democratic process in numerous other subtle, but devastating ways [1]. One attack involves switching the memory card used to collect the votes with a compromised duplicate that alters the distribution of votes. This attack, known as a "Hursti hack", may have first arose in the case of the 2000 Presidential election in Volusia County Florida, where Al Gore mistakenly received negative 16,022 votes. It was also the basis for the 2006 documentary "Hacking Democracy" which brought electronic voting machine hacking to light.

In "Hacking Democracy", writer and stay-at-home-wife Bev Harris inadvertently gained access to Diebold TS operating system files that were leaked from an insecure FTP site. Harris, who had no knowledge or training in computer science or cybersecurity at the time, was able to download the files and eventually learn the inner workings of Diebold systems, with the assistance of security researchers and academics [12]. Electronic voting machine manufacturers keep their systems black-box proprietary because they rely on the outdated notion of security through obscurity. If Bev Harris, who had no knowledge of cybersecurity, was able to obtain operating system files, then a hacker probably can do so as well. Even now, when the internet has reshaped modern society and where (hopefully) cybersecurity at vendor organizations has improved, a skilled and dedicated adversary can remotely breach servers or airgaps and exfiltrate the proprietary system files upon which United States elections depend. In the case of systems that are older than 5 years, the attacker, like numerous security researchers before them, can probably purchase a fully functional electronic voting system online, and dedicate as much time as necessary exploring its file system. According to Verified Voting, the United States uses 36 different systems from 15 manufacturers, though the majority of systems are made by Premier/ Diebold, Sequoia, ES&S, Microvote General Corporation, and Hart Intercivic. These manufactures' systems, as discussed in Part 2 of this paper, have been examined by security researchers and academics. Despite their findings, few, if any manufacturers have patched vulnerabilities or even minimally hardened their system. Ergo, the attack vectors, vulnerabilities, and information necessary to exploit these critical systems are in publically available white papers, online blogs, on non-profit groups' webpages, and in YouTube videos.

Even if no prior system information is known, each manufacturer reuses some or all of its proprietary software amongst its systems and the type of system used in a given state or district can be found online. Further, because the results of elections must be interoperable, there are some similarities between file types and system designs between systems. Therefore, by possessing knowledge of a specific system or operational function, an attacker can design malware that will target a host of systems, in a number of identifiable voting districts.

As previously mentioned, an attacker may attack systems by social engineering the undereducated personnel who operate most polling places. If an attacker gains access to an administrative smart card or other token or if the attacker infects the card or PBE writer/ encoder with malware, then they can infect systems without ever making physical contact. If the attacker has access to the administrative card or if they can infect a machine with malware that will spread onto the administrative card, then they can spread malware onto multiple machines and increase their sway over an election. Votes and results that are transferred via an internal or external network are subject to man-in-the-middle attacks during transmission [5], [6]. Researcher Jeremy Epstein notes "Whether it's an optical scanner or a DRE, the votes still get totaled on a memory card. And at the end of the election, you put that memory card into a central card system," Epstein continues. "You could use it to infect the tabulator system, and once you infect the tabulator system, it could transmit on." If an attacker or malware reached the central tabulator, it could alter the recorded results, regardless of whether or not the individual machines were infected. If the election was close enough, or if there is not a verifiable paper audit trail, then the results falsified in the central tabulator may not be noticed or contested. To demonstrate the vulnerability of machines, Princeton researchers Ed Felton and Andrew Appel photographed unguarded machines prior to elections (to demonstrate ease of access), and installed malware on some machines that only allowed users to play Pac-Man. In one 2006 attack, Appel purchased an administrator card and reprogrammed it with malware. Using Return-Oriented Programming, Appel installed self-replicating malware on a Diebold machine and allowed it to spread to other machines through the administrative card, which was in turn reprogrammed to alter an example election [1].

Capitalizing on Chaos

Attackers do not necessarily have to compromise results to impact an election. A ransomware attack against systems or a DDoS attack against registration back-end servers prevents citizens from voting and spreads distrust in the system. This increases the longer attacks persist but would also be increased if the ransom demands were paid. In a 2002 Florida election, voters had to endure hours long lines because a portion of the e-voting machines would not turn on. Discontent with the voting process was high. Imagine how disgruntled citizens would be if a ransomware attack compromised the majority of machines in particular counties across the country. Even if the officials did not pay the ransom, the effect of suspicion and distrust would

linger [1]. The socioeconomic costs of auditing an election are already significant without widespread panic. Even if an attack did not impact the result of an election, an overt attack, that captured public attention, could incite the losing side to contest results across the country. The public might demand additional auditing or proof that attacks did not compromise machines across the nation. It is nigh impossible to prove that a system has not been compromised; however, even if public fears were dissuaded, no amount of explanation or proof can prevent certain individuals from believing fiction over fact. If a large enough community polarizes, then in the coming weeks or years, more script kiddies, hacktivists, and reprobates might launch cyberattacks against political targets. The theorists do not need to possess technical knowledge or skill. With malware-as-a-service, DDoS-as-a-service, script kiddie tools, and other options, a dedicated disenfranchised voter could launch layered cyberattacks with minimal knowledge or effort. Essentially, one compromised voting system, if made public enough, could result in numerous compromised systems in the future. On the macroscopic scale, the United States may appear indecisive to foreign nations. National adversaries may act out while the United States' focus lies within.

What's the Wi-Fi Password?

At the moment, through the convenience-driven inclusion of remote access capabilities in some systems, a remote unsophisticated attacker is capable of altering digital databases by infecting a networked tabulation machine, of erasing voter registrations from databases, of infecting software at the point of development, of writing and distributing malicious ballot definition files to networked machines, or of distributing malicious code as a patch. Some systems remain remotely accessible, despite EAC's guidelines. For example, the WINVote e-voting machines ran a version of Windows from 2002 and were certified in 2003. However in 2002, computer scientist Jeremy Epstein found that the machines were accessible from Wi-Fi and they used the hardcoded encryption key "abcde". Further, the machines have not been updated since 2004. Nevertheless, the machines were not banned in Virginia until 2015, and it is possible that they remain operational in some other states. WINVote was a Windows XP embedded laptop with touchscreen. Earlier versions ran Win 2000. It was certified as meeting the Voting Systems Standards (VSS) of 2002, and was approved for use in Virginia, Pennsylvania, and Mississippi. The system was hackable within a few hundred feet of the polling place, such as the parking lot. The range could be extended to a half mile with a simple antenna, which could be purchased or built from a Pringles can. The system, like most e-voting systems does not log access or changes. The system was decertified because in November 2014, voting machines in one precinct were repeatedly crashing, and it was hypothesized to be due to some interference from someone trying to download music using their iPhone. The State Board of Elections invited the Virginia Information Technology Agency (VITA), which is charged with providing IT services to the state government, to investigate the problem. The report, which was released on Apr 14, 2015,

detailed a litany of problems. The systems had hardcoded passwords “admin” and “abcde”. WINVote systems had not been patched since 2004. WINVote systems had open ports with active services. The report specifically notes that ports 135/tcp, 139/tcp, 445/tcp, 3389/tcp, 6000/tcp and 16001/tcp were all running unpatched services. An obsolete version of Microsoft Access, with the default weak access key “shoup” was on the systems. There was no data loss prevention application or any controls to prevent changes to files, accesses, or user rights. Consequently, an attacker was free to copy, paste, or edit votes once inside the database by editing the underlying database file. USB and physical connections were only marginally protected and there were no access controls once a device was connected.

An attack on a WINVote machine would be simple. The attacker would need a laptop at a polling place, or outside in the parking lot. They could use a free sniffer to capture the traffic, and use that to figure out the WEP password (or use what VITA published). Next, they would connect to the voting machine over Wi-Fi. If asked for a password, the default administrator password “admin” would grant them unrestricted access to the system. From there, they could download the Microsoft Access database using Windows Explorer. They could use a free tool to extract the hardwired key (“shoup”). They add, delete, or change any of the votes in the Microsoft Access database. Afterward, they would upload the modified copy of the Microsoft Access database back to the voting machine and wait for the election results to be published [10].

Similar vulnerabilities as WINVote have been previously discovered in machines from Diebold / Premier Elections Solutions, Sequoia, Hart, ES&S and other manufacturers [9]. Part of the problem is that manufacturers are not sufficiently including security-by-design or testing systems before selling them to municipalities. Often the systems rely on off-the-shelf hardware and software with minimal, if any, security. Local government certification agencies seldom have the time, resources or knowledge to properly test machines for vulnerabilities and often just accept the manufacturer’s claims for security [9]. As discussed in Part 2 of this paper, a remote attack of a Hart system could spread to every Hart system across the country.

Systemic Failures

According to Ron Rivest of MIT, the purpose of an election is to discover who won an election and to provide convincing evidence that the winner legitimately won. True democracy requires an end-to-end verifiable voting system that guarantees the integrity of votes as they are cast, collected, and counted. The fundamental security requirements of the election process are not complicated. Only eligible voters may vote, and each eligible voter votes at most once. Votes are kept secret and the sale or dishonest casting of a vote is prohibited. No parties (including but not limited to vendors, voters, election officials, candidates, spouses, etc.) are considered trusted because anyone can be an intentional or circumstantial insider threat. Finally, the final outcome of the process must be verifiably correct. The current culture and regulation surrounding

electronic voting fails to meet every fundamental requirement. Attackers can manipulate machines to cast multiple votes. Because the proprietary systems lack transparency and have numerous open vulnerabilities, voters cannot be assured that the confidentiality or integrity of their vote are maintained. Even if the systems are not vulnerable to attack, the systems lack software independence and transparent quality assurance testing. As a result, vulnerabilities are not discovered and an innocuous undetected software error could alter the outcome of the election in numerous ways such as subtracting votes or misappropriating a citizen's vote to the wrong candidate. Though some e-voting machines have a verifiable paper trail, in many cases, the trail is generated by the untrusted machine or entrusted to staff that have not been verified. There is no trusted chain of custody. Paper ballots have first degree integrity because they can be manually recounted as necessary [11]. Paper trails depend on a trusted chain of custody. There are numerous reported cases of election officials altering ballots, removing ballot boxes, or otherwise compromising the paper trail. Recounting paper ballots is time consuming and tedious, especially when public attention is eagerly awaiting results. As a result, statistical audits of the results are done to verify that the results of a select sample of paper ballots corresponds to the reported result [12]. However, because neither the chain of custody, nor the system, nor the central tabulator can be trusted, an audit of paper ballots is a null and meaningless check. At the very least, there is no guarantee that the official selecting the sample will select a truly random and representative sample. At worst, an insider threat could manipulate every aforementioned stage of the chain of custody [11]. Similarly, Voter Verified Paper Audit Trails (VVPATs) are not a foolproof solution. VVPATs can be spoofed and manipulated. VVPATs increase costs, which local governments may not be able to afford. Finally, VVPATs can be difficult to install and manage. As a result of these factors, the final outcome of the elections that depend on electronic voting systems cannot be verified because voters can neither trust the votes collected or the system collecting the votes [11].

Conclusion

More often than not, electronic voting systems are nothing but bare-bone, decade old computer systems that lack even rudimentary endpoint security. As an exponential "security free" attack surface, compounded by the absence of cyber hygiene, black box technologies, and an expansive threat landscape, an adversary needs only to pick a target and exploit at will. Fundamental cybersecurity hygiene dictates that organizations assume their technology is vulnerable until proven otherwise. Despite proven vulnerabilities and a demonstrative lack of security, manufacturers and officials have not improved e-voting systems. Easily exploitable voting machines will continue to plague America's democratic process so long as manufacturers are able to profit from and covertly obfuscate the vulnerabilities inherent within electronic voting systems. A lack of penetration testing, security-by-design, and comprehensive physical access controls result in lackadaisical security, which enables, rather than hinders, an attack. The

antiquated black-box systems become easier to compromise as vulnerabilities are discovered and left unpatched, and as the ubiquity of technology and the internet introduces new attack vectors to the stagnant security posture of the expanding e-voting threat landscape. Nation states, hacktivists, cyber jihadists, insider threats or anyone with an interest in swinging a local, state, or federal election currently have carte blanch access for the manipulation of America's democratic process.

Contact Information

Legislative & Executive Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

[1] B. Wofford, "How to hack an election in 7 minutes," POLITICO Magazine, 2016. [Online]. Available: http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144. Accessed: Aug. 19, 2016.

[2] B. Schneier, "Hackers are putting U.S. Election at risk," in *CNN*, CNN, 2016. [Online]. Available: http://edition.cnn.com/2016/07/28/opinions/hackers-election-opinion-schneier/. Accessed: Aug. 19, 2016.

[3] M. Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers (+video)," in Passcode, The Christian Science Monitor, 2014. [Online]. Available: http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video. Accessed: Aug. 19, 2016.

[4] M. Gregg, "Top Six ways hackers could disrupt an election," in Huffington Post, The Huffington Post, 2015. [Online]. Available: http://www.huffingtonpost.com/michael-gregg/top-six-ways-hackers-coul_b_7832730.html. Accessed: Aug. 19, 2016.

[5] CBS. Inc, "Hacker demonstrates how voting machines can be compromised," https://www.facebook.com/CBSThisMorning, 2016. [Online]. Available: http://www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines/. Accessed: Aug. 19, 2016.

[6] L. Segall, "Just how secure are electronic voting machines?," in CNN, CNN, 2016. [Online]. Available: http://money.cnn.com/2016/08/09/technology/voting-machine-hack-election/. Accessed: Aug. 19, 2016.

[7] B. Barrett, "America's electronic voting machines are Scarily easy targets," in Security, WIRED, 2016. [Online]. Available: https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/. Accessed: Aug. 19, 2016.

[8] R. Johnston, "How I hacked an electronic voting machine," Popular Science. [Online]. Available: http://www.popsci.com/gadgets/article/2012-11/how-i-hacked-electronic-voting-machine. Accessed: Aug. 19, 2016.

[9] J. Epstein, "Decertifying the worst voting machine in the US," 2015. [Online]. Available: https://freedom-to-tinker.com/blog/jeremyepstein/decertifying-the-worst-voting-machine-in-the-us/. Accessed: Aug. 19, 2016.

[10] M. Zimmerman, "Hack the vote: Cyber experts say ballot machines easy targets," in Fox News, Fox News, 2015. [Online]. Available: http://www.foxnews.com/politics/2015/06/11/hack-vote-cyber-experts-say-ballot-machines-easy-targets.html. Accessed: Aug. 19, 2016.

[11] R. Rivest, "Auditability and Verifiability of Elections," 2016. [Online]. Available: https://people.csail.mit.edu/rivest/pubs/Riv16x.pdf. Accessed: Aug. 19, 2016.

[12] B. Harris, "Home," BlackBoxVoting.org, 2016. [Online]. Available: http://Blackboxvoting.org. Accessed: Aug. 19, 2016.

[13] L. Norden, "America's Voting Machines at Risk," in Brennan Center for Justice, 2015. [Online]. Available: https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf. Accessed: Aug. 19, 2016.

[14] B. Friedman, "Here we go again: 'Just push the yellow button and vote as many times as you want' on Sequoia touch-screen voting machines!," in Huffington Post, The Huffington Post, 2006. [Online]. Available: http://www.huffingtonpost.com/brad-friedman/here-we-go-again-just-pus_b_33109.html. Accessed: Aug. 19, 2016.

[15] S. Kirchheimer, "Voter registration fraud - 3 election season scams, identity theft - AARP eve..," in AARP, AARP, 2012. [Online]. Available: http://www.aarp.org/money/scams-fraud/info-09-2012/voter-registration-fraud.html. Accessed: Aug. 18, 2016.

[16] M. R. Alvarez, T. E. Hall, and S. D. Hyde, Election fraud: Detecting and deterring electoral manipulation. Brookings Institution Press, 2009. [Online]. Available: https://books.google.com/books?id=HeUyo5RcI7wC&pg=PA119&lpg=PA119&dq=malware+dre+system&source=bl&ots=n_r74ypqph&sig=hwTZruFRhdsK5eDEUZWa0rRjWJU&hl=en&sa=X&ved=0ahUKEwjv3vWco9DOAhUEGR4KHSlGBX8Q6AEISTAI#v=onepage&q&f=false. Accessed: Aug. 18, 2016.

[17] M. Blaze, "Matt blaze on Twitter," in Twitter, Twitter, 2009. [Online]. Available: https://twitter.com/mattblaze. Accessed: Aug. 24, 2016.

[18] M. Blaze, "Matt blaze: California voting systems code review now released," 2007. [Online]. Available: http://www.crypto.com/blog/ca_voting_report/. Accessed: Aug. 24, 2016.

[19] A. Aupperlee, "Election officials: Voting machines 'extensively' tested, can't be hacked," in News, TribLIVE.com, 2016. [Online]. Available: http://triblive.com/news/allegheny/11013043-74/machines-election-county. Accessed: Aug. 23, 2016.

[20] ES&S, "Election systems & software,". [Online]. Available: http://www.essvote.com/career-center/. Accessed: Aug. 31, 2016.