A Holistic Cyber Security Approach

Author: Rebecca Santos
Intuitive Research and Technology Corporation
becky.santos@irtc-hq.com
Advisor: Dr. Bruce Peters
Abstract
The objective of this paper is to educate its readers on the basics of various security assessment terminology, tools, and techniques as applicable to voting machines. The intended audience includes enablers within the election management process who may be getting pressure to ensure the electronic voting systems they oversee are adequately protected. This may include State Election Commission, Secretary of State, State Election Office, State Procurement, or County Election Officials. Additionally, security professionals unfamiliar with election administration and voting systems, may use it as a quick start to familiarize themselves with the unique security requirements of the voting domain. The intention within this whitepaper is to bridge the gap between these two sets of professionals in an attempt to promote secure and trustworthy electronically assisted voting systems. The origin of the topic was derived from knowledge gathered, observations made, lessons learned, and concerns established while collaborating with Pro V&V, an Independent Voting System Laboratory (VSTL), on a security vulnerability assessment of an election management solution. The target of evaluation during this assessment was a Commercial Off The Shelf (COTS) based electronic voting management system. Relevant cyber security terminology is defined and potential vulnerabilities to the voting systems are explored. Descriptions of select industry standard tools and tactics employed by security professionals during an assessment are provided. The case is presented for the importance of continuous security assessment and improvement. Parallels are drawn from other industries in an attempt to leverage lessons learned and to eliminate mistake recurrence. The overarching theme is to provide the reader with enough information towards approaching the problem with a practical holistic strategy to improve overall security within the electronically assisted voting domain.
Introduction

The cyber security challenge is unquestionably receiving an increase of attention these days. Daily media coverage of security breaches is affecting peoples’ trust in information technology and communication systems at large. Trust is, first and foremost, the ultimate element to protect within any security endeavor. Mechanisms of security enforcement, aimed to increase the level of confidence within a system, cannot be deployed or assessed without some level of trust. Furthermore, their failure ultimately leads to an unrecoverable decay of trust in the system. This concept is particularly significant with respect to the voting system as only a perceived failure in security could lead to the sentiment of disenfranchisement within a hard fought democracy. “Security is as important as reliability in guaranteeing the integrity of the voting process and public confidence in the system. Losing confidence in elections means losing confidence in our system of government” (Jefferson et al., 2004).

Current elevated attention is bringing security to decision makers’ forefront of priorities as they are more often being held directly accountable for the security of systems within their domain of control. The increased attention and pressure leads many of these enablers seeking service providers claiming to be able to secure their computing systems and environments. This claim is often made without the service purveyor having a full understanding in the domain of evaluation, or being allocated ample time for a thorough assessment. This combination results in an insufficient assessment based on compliance and leads to a false sense of security.

The recent cyber theft of millions of personnel records from the federal government was accomplished by sophisticated skilled individuals. If centralized government databases with extensive security precautions in place are vulnerable, how vulnerable are all of the voting machines dispersed around the nation? While some sort of voter fraud has been claimed in almost every past election, the potential of voter fraud or just the hint of irregularities could be dramatically compounded with the addition of different states using different electronic voting systems. In 2015, the State of Virginia Information Technologies Agency (VITA) reported in the Commonwealth Security and Risk Management Report that a security review of WINVote voting equipment, in use since 2002, determined that weak security controls were unable to prevent hackers from modifying the vote records [1].

While the tampering with the machines is unsettling on a technical level because clearly the deficient security controls created vulnerabilities that were not identified until anomalous behavior was occurring on devices in the midst of the polling, what is the damage done to the integrity of the voting process? To control costs, manufacturers often use off-the-shelf hardware and software which can be riddled with vulnerabilities. Because of schedule and cost constraints, manufacturers may not be able to sufficiently test systems before delivering them to local governments. Likewise, government certification agencies seldom have the time, resources, or knowledge to properly test machines for vulnerabilities. Some of the lost trust in the process can be recaptured through the involvement of the National Institute of Standards and Technology (NIST) and the Election Assistance Commission (EAC) which has a program to help municipalities certify election machines. Subject matter experts (SMEs) from NIST are more than capable of developing standards and providing guidance; but, these security features often add cost just as more involved testing will add cost and delay innovative products getting to the customers. Therefore, as good stewards of the public’s funds and trust, states and municipalities need to appreciate the nature of the cyber security risks, the complexity (and therefore the cost) associated with mitigating the risks, as well as the testing required to validate the successful implementation. Manufacturers are not unbiased and therefore cannot be relied on to fulfill this role. Certified testing firms are more than capable of doing the testing to certify the equipment, but do so in pristine laboratory environments. If there are issues
reported, how does the information get shared and most importantly how do the repairs get implemented without there being the possibility of conflicts of interest? Training is usually needed beyond just the deployment and operation of the equipment, but also how to be aware of and identify threats from hackers to more urgently respond to and recover from potential breaches in security. Finally, the threat environment is constantly evolving and changing as old threats are addressed and become less potent but new threats are discovered. An independent source of knowledge, skill, and experience is needed to support the process.

An independent company that understands all aspects of cyber security would be a benefit to the municipalities in generating requirements and evaluating the manufacturer’s claims. Such a company could support certification testing by providing and evaluating fixes to manufacturers when needed. The company could provide training to users and operators to demonstrate what security breaches look like so that issues would be more rapidly identified. Finally, the independent company can remain current on various threats and attack vectors in ways that government voting agencies cannot easily do. These same characteristics are what cyber security and information assurance companies provide to the Depart of Defense (DoD). The capabilities of these companies, along with their mission to remain independent and unbiased, is ideally suited to be applied to address these issues. These types of companies have individuals with all of the training, specialized certifications, and investigative tools needed to support the municipalities. By consulting early in the process and throughout the process, a cyber security company provides value added through:

- Writing more focused requirements that reduce system cost and testing time,
- Efficiently identify threats and rank their likelihood and severity to define the trades between risk and system complexity (which often leads to higher cost),
- Provide testing tools and write test plans that truly exercise the equipment in a realistic and efficient manner to remove unnecessary costs while documenting actual performance.

The electronically assisted voting system domain has unique terminology, characteristics, risks, challenges, and consequences. However, the knowledge, techniques, tools, and tactics used to evaluate and protect such systems can be leveraged from best practices utilized and proven within other industries. Security professionals possessing these assets can add significant value by leveraging the many lessons learned from supporting other industries.

Procurers of security services may be overwhelmed by a collection of unfamiliar terminology, tools, and tactics leaving them in a circumstance unable to make fiscally responsible decisions with an adequate amount of due diligence towards security. The intention within this whitepaper is to bridge the gap between these two sets of professionals in an attempt to support a secure and trustworthy electronically assisted voting system.

**Voting System Domain and Future Developments**

Domain knowledge is particularly important in any security assessment, as the threats, vulnerabilities, and risks differ between domains. The voting system domain information presented is not intended for the
subject matter expert who has dedicated their career to voting system security, yet one coming from a different industry needing a handle on the general scope. There is an abundance of information publicly available on the subject, and it is easy to get lost in the vastness or to be misguided by advocacy groups or false claims. The intention is to provide general understanding of the voting system landscape and to define the scope for the recommendations presented.

The Help America Vote Act of 2002 (HAVA) defines voting systems as: (1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used (A) to define ballots; (B) to cast and count votes; (C) to report or display election results; and (D) to maintain and produce any audit trail information [2]. The United States voting methods in use are currently a heterogeneous combination of methods which are not all electronic or technical in nature. Voting methods are dependent on the election district and include: paper ballots, paper ballot marking assisting devices, optical scanners to read paper ballots both at local precincts and central scanning locations, Direct Recording Electronic Devices (DRE), and any combinations of these. Each method has its own assortment vulnerabilities. Reliability and integrity has been improved by combining features from several methods.

DREs typically utilize electronic technologies to present a ballot to the voter assisting navigation through the voting process. DREs provide an advantage of eliminating ballot marking mistakes easily made by a manual marking process such as over and under voting. Many of the DREs currently in use are proprietary, single purpose machines. There have been many recommendations made and the trend seems to be moving towards the adoption of commodity COTS hardware and software components [3] [4]. In 2014, a report by The Presidential Commission on Election Administration made this recommendation to the President. They supported their argument by asserting the following:

“Jurisdictions that use electronic voting machines usually deploy machines for a few days per year and then lock them up in storage for the rest. For cash-strapped jurisdictions that wish to keep pace with evolving technology, the purchase of hundreds of expensive, specialized pieces of hardware good for only one purpose — elections — no longer makes sense” [4]. One specific technology adoption trend is the utilization of touch screen capabilities of COTS mobile devices as the end-point user input device. The output is a marked ballot that the voter can verify, scanners can tabulate, and which can be preserved for auditability. The key component here is the necessity to produce a Voter Verified Paper Trail (VVPT), although this is not a requirement in all districts at the current time.

The VVPT output is essential for auditing the electronic voting system’s accuracy and integrity as well as providing a backup in the event of a required recount challenging the electronic results. A 2012 Scientific American article provides a perfect argument for paper which is still relevant today, “The reason is simple and resonates with the contentious debate that has yet to be resolved after at least 15 years of wrangling over the issue of electronic voting. No one has yet figured out a straightforward method of ensuring that one of the most revered democratic institutions—in this case, electing a U.S. president—can be double-checked for fraud, particularly when paperless e-voting systems are used.” Since a purely electronic networked voting system cannot guarantee security or privacy, it seems evident that a marked ballot in paper form will remain relevant for the foreseeable future. This immediately eliminates internet based voting as an option. A great reference for the full understanding of this problem is presented by David Jefferson in a Google Tech Talks titled “Electronic and Internet Voting” [5]. A move towards risk-limiting audits provide great benefits to the process increasing trust by statistical evaluation ensuring the integrity of the systems [6].
A current primary concern, both by election management professionals and the well-informed public, is the age of the voting system equipment currently in use. In 2002, President George W. Bush signed the HAVA which provided the funds needed to upgrade the voting system infrastructure. Since then, the budgets needed to improve the system have been sparse, leaving the country reliant on obsolete technology. According to a report published by the Brennan Center for Justice in 2015, 43 states are using voting systems that will be at least 10 years old in 2016. In 14 States, machines will be more than 15 years old [3]. As a result, upgrades are inevitable. It is prudent and pragmatic to ensure that security is a primary concern during this renovation.

The current heterogeneity of voting systems across the country has provided some level of security by obscurity with protection against orchestrated large scale security attacks that could have affected the outcome of an election. If recommendations are heeded, many of these systems will be replaced with commercial or open source election management software and commodity hardware architectures. This strategy allows for incremental, more affordable, upgrades of the infrastructure in the future. A security benefit to consider is that a familiar architecture presents the opportunity to use tools, tactics and techniques from other industries. However, one consequence is that this strategy also introduces new security problems to consider. It is plausible to assert there will be some inherent standardization of technology in use. This standardization is potentially introduced by districts taking advantage of economies of scale coupled with the elimination of single purpose hardware equipment. This approach has the potential to homogenize larger areas. Entire states, or potentially regions spanning multiple states, may choose to integrate solutions from a common vendor. Even where separate and distinct vendors are used for election administration software, the underlying networks hosting the applications will be homogenized. New risks are exposed due to two simple concepts: 1) migration to commodity systems presents a more commonly known attack surface and 2) homogenizing technologies can lead to a larger area being affected by an attack. Therefore, security assurance is even more important and security professionals need to be prepared to assist in protecting this valued institution.

Voting System Security Requirements
In order to determine a defense strategy, one must first have a true understanding of what is to be protected. The Voting System Performance Guidelines [7] identifies the relevant security requirements that must be addressed in any voting system that will receive EAC certification. These are generic requirements whose implementation is left up to vendor interpretation. The requirements state that all systems must implement protection controls for the following:

- Unauthorized changes to system capabilities for
  - Defining ballot formats
  - Casting and recording votes
  - Calculating vote totals consistent with defined ballot formats
  - Reporting vote totals
- Alteration of voting system audit trails
- Changing or preventing the recoding of a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Preventing access to vote data – including individual votes and vote totals by unauthorized individuals
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes
A more explanatory list of technical requirements that directly map to these security tenets of the VVSG are offered in the presentation titled “Electronic and Internet Voting” by Dr. David Jefferson, computer scientist and subject matter expert in voting systems. In this presentation, Dr. Jefferson enumerates the following technical requirements of a voting system:

- **Voter Authentication:** All registered, eligible voters vote; unregisters and ineligible votes disallowed
- **Ballot Selection:** Voters are presented exactly the set of offices/measures they are eligible to vote on
- **Multiple Vote Prevention:** No one votes more than once
- **Accuracy of Capture:** Voter’s intent is accurately captured
- **Integrity:** Ballots are not lost, nor corrupted, nor are phony ballots inserted
- **Accuracy of Tally:** Votes are tallied and reported accurately, according to law
- **Privacy:** Votes cannot be associated with the voters who cast them (precinct level) no single or group leaks
- **Privacy2:** No way for voter to prove how s/he voted to 3rd party: hence votes cannot be coerced or sold
- **Software Integrity:** Object code must be derived from the certified source code, and distributed without modification
- **Availability:** System must be up to at least accept ballots for the entire period prescribe by law
- **Reliability:** All other properties hold even in the face of transient, or partial permanent system failures
- **Security:** All other properties hold even in the face of a (limited) conspiracy of election officials, programmers, 3rd parties and voters to undermine the election
- **Verifiability:** Each voter can verify that his/her own vote was captured properly
- **Auditability:** The system produces a tamper-resistant independent records or audit trail used as a basis of a statistically sound end-to-end audit
- **Mission Critical:** Elections must be held on a fixed day, and cannot be postponed or re-run. No 2nd chances. Strong design bias toward prevention of problems, rather than after-the-fact repairs.

These requirements are focused on the abstract voting system, and the capabilities and security restrictions it should enforce. It is important to note that the hosting platform and network infrastructure must also be evaluated to ensure that it can uphold these tenets. Voter privacy needs to be added to these requirements. The concept of voter privacy isn’t simply restricted to ballot secrecy, it also includes the database of voter registration information which contains personally identifiable information (PII). PII data can be used for identity theft and impersonation. Mexico and The Philippines both sustained breaches in 2016 [8] leading to data exfiltration of registered voter’s personal information. Furthermore, we have an obligation to ensure that voter registration systems and databases are protected as well.

A holistic security strategy takes all requirements and all system components into consideration for assessment. The strategy should encompass layers of defense consisting of physical, administrative, technical controls, applied to all aspects of a system and related processes in an effort to assure the requirements are enforced. Some of the system components that must be assured protection are:

- **People**
- **Network Infrastructure**
- **Voter Registration Software and Back End Databases**
- **Election Management/Administration Servers and Back End Databases**
- **Election Execution Software**
- **Tabulation Equipment**
• End Point / Polling Host
• End Point / Polling Accessibility Peripherals
• End Point / Poll Administration Host
• Repositories of Auditable Paper Trails

The new proposed COTS based voting systems are beginning to resemble that of an enterprise network architecture. As a consequence, many of the same vulnerabilities affecting enterprises will be introduced into the voting domain. There are few notable differences to mention that present additional challenges. First, their configuration and patch state remains static once certification is obtained. Second, systems are typically only locally networked, consisting of small separated networks that are assembled for the sole purpose of supporting Election Day. Third, systems must be absolutely, without question, be dependable with respect to availability, confidentiality, and integrity on this day.

Security professionals have a fiduciary duty to educate asset owners, facilitating their decision making process. They must take care not to present hyperbolic scenarios so that their recommendations are not discredited. Strategic implementation of mitigating controls combined with practicality with respect to budget is of extreme importance since these are commonly the greatest challenges encountered by the asset owner. Just as it is imperative that a security assessor understand the specific challenges associated with voting administration, it is important for election administration professionals to understand core concepts in security.

Security Assessment Terminology

Defining Vulnerabilities
A vulnerability is a threat or weakness that leaves a system in a state that could be exploited. A system, in the context used here and specifically with respect to voting, is not necessarily an individual computing device or a machine. Rather, it represents the collection of machines that serve particular roles, the people involved with them, and the processes surrounding both. A holistic security approach evaluates this entire ecosystem in its native state. While evaluating components independently in a laboratory environment is important, a true top down holistic assessment would involve evaluating the entire system in the state in which it will be on the day of election.

Vulnerabilities can be well known and documented, or undiscovered. Having a known vulnerability does not imply that a potential attacker is aware that the system has this weakness. Having an exposure is the condition when an attacker is aware of a vulnerability in the system that they know they can exploit. Vulnerabilities can be present due to poor design, mistakes in implementation, misconfiguration, disregard to manufacturer recommendation, or simply negligence. The ultimate goal is to prevent exploits by not introducing the vulnerabilities. From a holistic security perspective this is achievable by requiring vendors to continuously educate developers, adopting better coding practices, and performing more rigorous security testing. Security must be incorporated throughout the entire software development lifecycle. Security is enforced both through design and code implementation. Many seasoned, skilled, senior level developers of today were formally educated during an era when security, specifically secure coding practices, was not a distinct part of the curriculum. Design has been traditionally focused on functionality, reliability, and usability. A move towards baking security into earlier phases of the software development lifecycle facilitates reaching this goal, but it can never completely eliminate vulnerabilities.

Why Are There Vulnerabilities?
The best cyber security programs can only keep out the unmotivated or unskilled hacker. If a skilled and motivated hacker wants to gain access to a system, no security program would stop them, regardless of
the amount of budget spent. Within any electronic computing system, this is true due to the inherent existence of flaws in any system developed by human beings. Software and hardware systems will always be released with bugs. These bugs can be known or unknown. It is impossible for human beings to ensure that there are absolutely no errors in a system because it is impossible to prove that something does not exist. Therefore, at any point in time there are any number of unknown errors within a system that are potential vulnerabilities. There are many people performing research trying to discover such errors, not always with altruistic intentions.

Companies are often forced to accept the risk associated with the release of systems with known deficiencies. They often do so in order to remain competitive in the market and to meet release deadlines. This risk acceptance process can be problematic; such as the case when the company didn't realize how the known bug, which they chose to accept and release to the public, could be exploited.

Over and above having this assortment of flaws, known and unknown, we also have the human involved in the implementation, configuration, and maintenance of these systems. These less than perfect systems are combined, and new vulnerabilities are potentially introduced via misconfigurations. The combination results in a complex layered composition of technology, with the possibility of pinholes everywhere. If a potential attacker, outsider or insider, has knowledge of a specific target, ample motivation, and time, it is only a matter of time before they can connect through those pinholes to achieve their goal.

Protecting this delicate ecosystem is an on-going challenge. As previously stated, the ultimate goal is to eliminate the vulnerabilities, but a contingency is to harden what is known and to implement selective layers of defense around the architecture in order to lessen the possibility that the remaining vulnerabilities are exploited. In order to understand how security professionals protect these assets, it is important to be familiar with the way these vulnerabilities are exploited.

The Hacking Methodology
Ethical hackers are security professionals who utilize the same methodologies used by ill-willed hackers in order to identify vulnerabilities in a system, allowing them to be mitigated rather than exploited. Covering the complete methodology is beyond the scope of this paper, however a primary concern to consider, with respect to election systems, is reconnaissance and scanning. The scenario presented here is from the perspective of an outsiders’ attempt at exploiting a vulnerability in a system unknown to them. The scenario is presented in an effort to explain the reconnaissance and scanning phases of the hacking
process and to emphasize the need for operating system hardening and patch management in the voting system domain.

In the hacking methodology taught by institutions like SANS and EC Council, typically an initial target is selected and the bad actor performs open source reconnaissance to collect information. Open source reconnaissance or intelligence gathering is basically compiling publicly available information in order to discover a potential point for unauthorized entry. Information can be obtained from the internet or via social engineering tactics. Gathering information available via the internet is a passive activity that cannot be prevented or detected. Public disclosure of information related to hardware, operating systems, software, network addresses, procedures, or people can lead to opportunities for exploitation. The probability of discovering a vulnerability and architecting an exploit increases as more information is discovered.

The next step typically consists of scanning or “footprinting” the initial target system. This is often accomplished via the use of automated scanning tools in order to determine specific versions of operating systems, database systems, and application software in use by the system. The version information obtained by these scans proves the existence of known vulnerabilities on the target system. Automated configuration and vulnerability assessment tools scan targets to identify, analyze, and classify security weaknesses. Much like pattern based virus protection software, vulnerability scanners are only able to identify known issues. The automated tools search for misconfigurations or known software weaknesses in target systems based on a set of tests. Most automated scanners use the Common Vulnerability and Exposures (CVE) database. The CVE contains common ways to refer to information system security vulnerabilities and exposures with the purpose of providing a common taxonomy for publicly known cyber security issues. Although the goal of CVE is to make it easier to share data across tools, repositories, and services, and security professionals, the information is publicly available and can be used for nefarious activity.

This “footprinting” activity is performed in order to discover what “pinholes” are resident in the layered architecture discussed in the previous section. Finding a vulnerability in the system provides a skilled hacker with the information necessary to create a customized payload to exploit the vulnerability and perform the nefarious activity intended. A typical initial point of entry in an enterprise IT infrastructure is a publicly facing web application server. The main purpose of this target is to gain initial access, then to use this compromised system as a pivot point to scan and compromise other more valuable assets, all while covering one’s tracks to remain unnoticed. This process is repeated on other target systems until the mission or desired effect is accomplished.

With respect to voting system certification, the inherent transparency in the process of certification presents a problem to consider. The concerning aspect is that much of the information normally obtained during reconnaissance and scanning steps is already compiled and publically available. For example, with a few simple internet searches, one can determine which states use DRE without paper trails, the manufacturer of the voting systems in use, the manufacturer’s supporting documentation, and all details of the COTS or third party components in use by the voting system architecture. The specifications of the system architecture are openly available as part of the Voting System Certification Report. The vulnerabilities exposed by this transparency have the potential to introduce elevated risks. This will be especially important as the systems are upgraded to infrastructures resembling those of typical enterprise
networks simply because it provides a potential hacker with many of the details needed to prepare for an orchestrated attack without ever having access to the system. This portion of the process is the most difficult and time consuming. Delivering the exploit in some cases is the easy part.

Vulnerability Assessments, Penetration Testing, Red Team, and Software Analysis
The following analogy is presented in an effort to control the overuse of certain terms, and to educate the reader on different security assessment types. An uncomplicated analogy to describe the differences between Port Scanning, Vulnerability Assessment, and Penetration Testing is as follows. Port Scanning would be equivalent to going through and checking the windows of a house to see which ones are open giving easy access to a potential intruder. Vulnerability assessments are checking the closed windows in order to determine if they are locked and that the locks are performing correctly. Penetration Testing is analogous to actually exploiting those unsecured windows and gaining entry to the house, proving that entry is possible and the house is insecure. The exploitation is performed by taking advantage of the open or unlocked windows and possibly breaking or bypassing the locks, getting inside, and seeing what you can get. Red Team exercises can be described as a planned execution of such penetration testing. A Blue Team would typically, prior to and sometimes concurrent with the penetration test, try to lock the windows before and as the Red Team is trying to gain entry. These techniques are performed on networks, hosts, software, and processes involving people. These concepts only slightly overlap with application security assessments which is another layer, further down in the layers of details. Software assurance analysis involves analyzing the source code itself for vulnerabilities. This assessment may be conducted with automated code analyzers and by manual inspection of source code or compiled binaries, the latter being more commonly referred to as analysis via reverse engineering. Another technique is application security testing, sometimes called application fuzzing, which tries to exploit vulnerabilities in software via its typical inputs controls but providing it with anomalous, unexpected data. Adhering to the same theme, code analysis is somewhat analogous to inspecting the architectural blue prints of a house to determine where the windows and locks are or should be.
The Security Assessment

Performing a thorough security assessment takes a lot of time, determination, and patience. It is important that the scope of an assessment is defined because a security assessment can truly be inexhaustible. Typically an assessment will include recommendations for compensating controls, but implementation of correction is not included in the scope of the assessment. Understand what is included.

A true top down assessment would require the assessors to evaluate all layers of the entire system of systems, including policy, people, and procedures in addition to the electronic systems, in its native environment and on a recurring basis. As mentioned before, new software and firmware vulnerabilities are being discovered daily. Security professionals typically have areas of expertise as well. One well versed in network and infrastructure defense may not be able to perform code analysis or application vulnerability testing. Be sure to select a team with diverse experience.

A security professional is typically not allocated ample time to evaluate the entire set of software code within a system to look for vulnerabilities, nor do they typically have access to the source code to evaluate its content. Security professionals often use a combination of automated tools supplemented by manual inspection to perform their tasks. Much like the hacker methodology, security professionals often start with port and vulnerability scanning, but may move on to more through assessment if part of the scope.

Technical Recommendations

Although not a conclusive list, the following are some technical security recommendations to consider as part of a holistic security program. These recommendations are based on initial observations into the common practices within the voting domain.

OS Hardening and Patch Management

Best practices for mitigating vulnerabilities in an enterprise network include operating system hardening and routing patch maintenance. Routine hardening and patch management should be considered integral in a holistic security approach. Operating System hardening is the processes of ensuring the surface of vulnerabilities is reduced to the smallest area feasible. Hardening is performed through configuration settings patch installations, removal of unnecessary hardware, software, and default accounts to name a few. “Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Also, patches are usually the most effective way to mitigate software flaw vulnerabilities, and are often the only fully effective solution” [9]. Essentially patch management involves routinely assuring that the pinholes are plugged, limiting potential vulnerabilities that would expose unauthorized entry points.
As previously mentioned, the voting system state remains static once certified. The state of the system is published in the certification report. This implies that the applications and hosting operating system are not patched, therefore any vulnerabilities discovered post certification will be resident on the system while in storage and on election day. Dependency on secrecy for providing security should be avoided at all costs. Transparency in process and system actually affords many security advantages. The recommendation is not to lessen transparency, rather to focus on ensuring that vulnerabilities exposed by transparency are mitigated. Leaving systems unpatched for prolonged periods of time compounds exposures providing more opportunity for potential exploitation. Opportunities for nefarious activity increases proportionally with the combined increase in information available and time exposed.

Eliminate Dependency on Security by Network Isolation

A recommendation to consider is to implement a patch management process in conjunction with an expedited certification process. This is particularly important when the voting systems are hosted upon commercial operating systems and database servers because their vulnerabilities are published publically. A potential hacker does not need physical or remote access in order to discover an exploitable vulnerability or to develop an exploitation tailored to the target system. They simply need to determine a way to introduce the exploit code to the system which can happen in a matter of minutes.

It seems that a common compensating control in the election management industry is to deploy voting systems and their supporting components without internet connectivity isolating them via policy for security purposes. It is true that this prevents remote exploitation of a vulnerability. However, it does not prevent exploitation of a vulnerability in the event of the following 1) if the bad actor does somehow gain physical access, 2) if they use some form of deception to get an authorized user to introduce the crafted exploit, 3) if the bad actor is an insider that has access and authorization to the systems, or 4) if an innocent authorized user makes a mistake connecting the system via unapproved channels. Other industries have experienced security degradation by their reliance on network isolation. The only way security by isolation can be reliant is to completely remove external communication devices, such as network cards and USB drives, from the hardware. Isolation or air gapping without a supplemental patch management policy implies that known vulnerabilities are resident in the system for an extended duration. The easiest vulnerabilities to exploit are also the easiest to mitigate.

Continuous Security Assessment and Improvement

Security, just like quality, relies on continuous improvement. Information security and asset protection relies on management of risk via vulnerability and threat understanding, mitigation processes, and strategic budget allocations. This can only be performed through continuous self-reflection, assessment, education, and improvement. Security improvements can be of an administrative, physical, or technical nature. Technology is continuously evolving and thus the vulnerabilities it presents and those who take advantage of them are evolving as well. Continuous review is one of the most important aspects of risk
management, since the landscape is constantly changing, as it helps to ensure that the plan remains relevant and effective.

The number of capable adversaries aiming to exploit these vulnerabilities will continue to increase. As voting systems reach the end of their lifecycle and are replaced with COTS based systems, the change towards the more homogenous and familiar will present new security concerns. Adversaries' tool sets are increasing due to their increase and understanding of the technology or simply their access to exploitation tools. Information is ubiquitous. No longer are these skills and tools controlled by an elite few, as long as there are motives they will be trying. Therefore, the security of a system will always need to be to constantly monitored and evolving. The key take away is that there is no panacea, security is a process of continuous assessment and remediation which must evaluate the entire system of systems in its native environment to be effective. Security is not a box to check.

**Conclusion**

While many technical security recommendations can be presented, it is important to keep some level of focus on the bigger picture. A true practical holistic security approach implores a fine balance of cooperation between vendors, election officials, and security professionals all sharing a common goal to manage or mitigate risk all while adhering to a budget. Security and budget are always at odds in any industry. It is economically infeasible to exhaustively test security in any system. Budget consideration is vital to securing the election management process which is typically plagued with a lack of funding contradictorily coupled with its importance to democracy. Therefore security professionals need to approach the problem and provide solutions with practicality, strategy, and non-exaggeration. They need to be sure not to have a hyperbolic, “the sky-is-falling “, attitude that leads to discredit the profession. Of course, if you have a screw driver and physical access to the system you can hack it. Additionally they should feel compelled to help educate their patrons and help build a dependable defense against wrong doers. Election management system vendors need to promote solid education and awareness of secure coding practices and design within their development teams. They need to ensure that the system design, if unable to prevent, has the ability to detect and recover from an incident. They need to harden the underlying COTS operating systems. Election officials need to remain educated on security language in order to be able to build it into the vendor procurement language, to understand what they are buying, and to make security a priority. They need to take advantage of security professionals that come equipped with knowledge of best practices from other industries to help assure a secure process. Most importantly everyone needs to understand that there is no panacea, security is a continuous process of assessment, remediation, and improvements.
References


