EVEREST PROJECT

Ohio Secretary of State

PREMIER SYSTEM

MICROSOLVED, INC.

TECHNICAL MANAGER'S REPORT

CONFIDENTIAL[1]

[1] This report is released by Ohio Secretary of State Jennifer Brunner consistent with the Ohio Public Records Act, Ohio R.C. 149.43. The reader of this document is advised that any conduct intended to interfere with any election, including tampering with, defacing, impairing the use of, destroying, or otherwise changing a ballot, voting machine, marking device, or piece of tabulating equipment, is inconsistent with Ohio law and may result in a felony conviction under, among other sections, Ohio R.C. 3599.24 and 3599.27.

Table of Contents

Table of Contents

Overview

The Ohio Secretary of State (SoS) retained the services of MicroSolved, Inc. (MSI) as a part of the overall EVEREST project to examine the security of the electronic voting systems in use in Ohio. As a part of that study, the MSI team performed red team penetration tests against the Premier voting system and attempted to identify attacks that could be exploited against the confidentiality, integrity and availability of the system and/or the overall elections processes. This report details the methodology, findings and results of the Premier system testing.

This report is report number two in a series of three reports. This report is geared toward explaining the general processes undertaken to review the Premier system, explaining the various phases of the work, identifying the overall issues found and attempting to provide root causes for the problems. The report also contains general suggestions for improvement and mitigation of the discovered issues and comparison of the system against a twelve step framework of best practices. An executive summary of the process and findings (report #1) and a specific catalog of technical findings (report #3) were delivered alongside this report to the SoS. Please see the appropriate report if you seek more general or more specific information.

The MSI team tested the Premier systems without any access to the source code of the components. Attacks were performed by emulating both the common access of the voter at the precinct level and access that is available to various people who come into contact with the systems during their life-span - from deployment and implementation to the regular access members of the board of elections, etc.

The overall results of the testing showed serious vulnerabilities in the system and its components. These vulnerabilities demonstrate the capability for attackers to execute arbitrary code on many of the components given access to them. Further, specific scenarios were identified where attackers who successfully gained access to the systems and exploited identified vulnerabilities could likely impact the results of elections. Generally speaking, the vulnerabilities identified in the study stem largely from the lack of adoption of industry standard best practices that have been developed for the IT industry over the last several years. Adoption of the best practices for IT systems, networking, information security and application development as suggested by NIST, the Center for Internet Security, OWASP, SANS and other working groups would eliminate a large amount of the risk associated with the findings contained in this report.

General Testing Information

The testing of the Premier systems was conducted onsite at the facility provided by the SoS. Our testing process took place from October 5th, 2007 through October 25th, 2007. The MSI team was provided basic training on the systems from Premier. This training was roughly equivalent to the training provided to poll workers on the general use of the systems and their deployment in the polling place. MSI did not have access to the source code of the applications nor to any specific "insider information" other than data that was publicly available from the vendor and from the Internet. MSI was provided with access to the systems in an unrestricted manner for the purposes of testing. This access to the systems was used to identify the vulnerabilities of the system. Obviously, attackers would not be given such wide access to the systems in question, thus we take this into consideration when we discuss the identified issues. However, it should be noted that access could likely be obtained by determined and/or well-resourced attackers through a variety of means ranging from bribery and breaking-and-entering to social engineering and outright coercion. History has shown that determined attackers often find powerful ways to gain access to their targets.

Premier System Information

The following components were tested as a part of this study:

DEVICE	MODEL OR VERSION NUMBER
GEMS Election Management Software	1.18.24, Including the KeyCard Tool Software 4.6.1
GEMS Server	Dell Server with Windows 2000 Server Service Pack 4 and Applicable Software Including Sygate Firewall, Anti-Virus Software and Digital Guardian
TSX Voter DRE System	4.64
Accu-Vote 2000 Precinct Optical Scanner	1.96.6, Including Paper Ballots
Accu-Vote Central Optical Scanner	2.0.12, Including Paper Ballots
Digi Serial to Ethernet Gateway	PortServer II
VC Programmer	ST 100
Mobile Electronic Poll Worker Tablet System	Windows CE-based tablet PC for Poll Registration
Elections Media Processor System with Elections Media Drive Tower	Dell Workstation with Windows XP Professional Service Pack 2 and the Elections Media Processor Software
Generic Ethernet Switch	This device is generic in that each county selects their own hardware. This is a basic ethernet hub or switch and can be any vendor or model.

DEVICE	MODEL OR VERSION NUMBER
PCMCIA and CF memory cards	Various types
Smart Cards for Premier Component Access	Provided by Premier
Voter Card Encoder	Spyrus PAR2

General System Operation

The Premier system is a widely distributed system with groups of components located at each precinct (polling place) and another group of components located at the central Board of Elections. Communication between the decentralized components and the centralized components takes place in Ohio via the human movement of PCMCIA memory cards holding the election information and the individual voting machine recorded ballots. In Ohio, no network connection or modem use is permitted between the decentralized precincts and the centralized Boards of Election.

It should also be noted that the memory cards are not the legal and official ballot of record in Ohio. The paper tapes generated by each voting machine are, in fact, the ballot of record and are the legal representation of the ballots cast by the voters. This is especially important to remember as attacks against the electronic systems are discussed. Attacks that modify the electronic records but not the paper records, or disruption/destruction of the electronic records could likely be performed, but if auditing against the paper records showed inconsistencies or errors, or if the electronic records were unavailable, the election would be decided based upon the paper tape records of the machine.

Voters interact with the precinct voting systems and their information is returned to the Board of Elections to be processed, recorded and tallied to determine the election results. Each memory card is read into the central GEMS server that performs the tally and results reporting. The GEMS server can be thought of as the election system "brain".

Methodology Overview

The methodology used for the study was MSI's traditional application assessment process. It consists of the following phases: attack surface mapping, threat modeling, poor trust/cascading failure analysis, vulnerability assessment, penetration testing and reporting. As a convenience for comparing each of the three systems against one another, we also established a twelve step framework of industry standard best practices and assigned a pass/fail to each value. More information about this framework and process will be detailed in the specific section titled Baseline Comparison in this report. Each phase of the study is detailed in the sections below.

Attack Surface Mapping

The purpose of the attack surface mapping phase is to provide the team with a graphical representation of the areas of the holistic system that would be available for assault by an attacker. This process also presents a graphical format to the team for beginning to understand the relationship between the surfaces and is an excellent tool for helping the team identify bad assumptions on the part of the developers and possible areas where cascading failures of security mechanisms could carry through from component to component. The output of this phase of work is a set of graphical object maps that are intended for internal team use only.

The mapping of the Premier system was performed with broad approaches, mapping the many areas where the system inputs or outputs data and interacts with other objects or components. The attack surface mapping revealed to the team the importance of these paper tape records and their proper handling. However, in Ohio, each county Board of Elections creates their own policies and processes for handling the paper records and all other parts of the election. Throughout the testing, this circumstance would prove to be a seriously dangerous issue for the security of the elections data. Without a common, centrally managed, best-practices-compliant set of policies and processes it is difficult to ensure that elections data is handled with consistency and effective security across the 88 counties of Ohio. This problem is magnified by the fact that each Board of Election varies by size, capability, funding and staffing level. As such, the attack surface mapping phase helped the team identify that the security and management of the paper tape voting records is an area of the greatest importance, is a highly likely target for attackers and is likely to be an area where security controls will vary greatly in their adoption, effectiveness and use. Review of this attack surface is outside the scope of our assessment, but we highly recommend that other components of the EVEREST project explore this attack surface and identify any underlying security issues and possible mitigations.

The other issue identified in the attack surface mapping phase was that the need to protect the GEMS server became apparent. Since the GEMS server defines the election settings, is a key component for creating the electronic ballots and memory cards, acts as the centralized aggregator of results and performs the tally processes to determine the outcome of the election - it is THE key component to the Premier system. Successful attacks against the integrity or availability of the GEMS server could have serious consequences. The Boards of Election around Ohio take established precautions during the elections cycle to protect the GEMS server, however, general questions and answers from other EVEREST project teams have indicated that protection of the GEMS server may be less than satisfactory in some locations outside of the elections cycle. Again, analysis of this issue is outside of the scope of our assessment but has been turned over to other teams for exploration. Basically, the GEMS server must be protected physically and from network intrusion during its entire life. Illicit access, at any point from deployment to destruction, could have serious impact on the integrity and availability of any elections performed using the system going forward. Each Board of Election should take high levels of caution to protect the GEMS server at all times. Physical access must be restricted at all times using dual-person access controls to prevent anyone from being alone with the system, and it should be powered down with the hard disks relocated to a locked safe or physically secure location separate from the machine when not in use. Hopefully, other practices and processes will be identified by other EVEREST teams that will enhance the security of the Premier system during its life cycle including before, during, after and between election cycles.

Threat Modeling

The second phase of the study was to perform modeling of the potential threats against the Premier system. The SoS specifically requested that our assessment be based on the following attacker goals:

- Confidentiality - the attacker would like to breach the veil of ballot secrecy and identify how specific voters cast their ballot

- Integrity - the attacker would like to perform actions that impact the ability of the system to accurately reflect the will of the voters, the attacker would like to influence or modify the outcome of the election

- Availability - the attacker would like to perform actions that impact the capability for an election to be held or for the outcome to be determined in a timely fashion

- General Chaos - the attacker would like to introduce enough issues into the elections process that the general public would fail to have confidence in the Boards of Election, the Secretary of State and/or the election itself

If ANY of these capabilities are reached by the attacker, then they have successfully compromised the election or elections process. At the minimum, they would impact local races and political processes. At the maximum, they could impact the results of a national election or do severe damage to the state's reputation or public faith in the State of Ohio.

Our threat models were established using four broad ranges of threat agents or attackers. These include:

Note: Attackers may begin at one level of the threat agent model and move higher on the scale during the process of the attack. Threat agents should be classified as their highest achievement of capability.

THREAT AGENT	DETAILS
Casual External Attackers	These attackers are interested in exploration of the voting system and/or possibly performing attacks against the elections process. This group of attackers lacks any access to the systems beyond the normal interactions presented to the voting public. They do not have sufficient skills, motivation, resources or capabilities to gain access to non-public components of the system or system functions. An example of this threat agent might be an individual hacker attempting to breach the security of the elections process for personal gain or understanding. Generally, this group of attackers is unlikely to impact the elections process in any meaningful way given the extremely distributed nature of the system.

THREAT AGENT	DETAILS
Focused and/or Resourced External Attackers	These attackers are interested in performing attacks against the elections processes using larger amounts of skills, resources and capabilities. However, to fit this category, they must be unable to gain access to any components or system functions beyond those presented to the voting public. An example of this threat agent might be a group of attackers with a specific agenda who are attempting to attack the system on a wide scale. This group of threat agents has higher capabilities and may be able to inject enough issues into the elections processes to achieve the General Chaos attack goal. They are, however, unlikely to achieve any of the other goals defined in this study.
Casual Internal Attackers	These attackers have obtained the ability to access the system or components beyond those surfaces normally exposed to the general voting public. They may have gained access to core system components, software functions or other protected resources. This group of attackers holds moderate skill and no true agenda to cause harm. An example of this threat agent might be a poll worker or employee of the Board of Elections who is interested in exploring the system or components. Another example might be a hacker who uses social engineering to gain access to the system or components for the purposes of exploration, personal gain or understanding. This group of threat agents have a higher capability to achieve attacker goals. Even without a harmful agenda, they present a risk to the system based upon mistakes, inadvertent or dangerous disclosures and exposure of the system to potential threats from malware and other attack vectors. They are likely to be capable of meaningful attacks against the elections process.

THREAT AGENT	DETAILS
Focused and/or Resourced Internal Attackers	These attackers are the highest threat to the system. They have achieved access to non-public system functions or components and have great capability and desire to perform malicious activity to achieve the attacker goals. These attackers are likely highly skilled, highly resourceful and capable of creating a myriad of scenarios for gaining access to the system. An example of this threat agent might be the agents of a foreign nation state or other well-resourced organization with specific political intent. They may use bribery, coercion or social engineering to gain access to the non-public functions of the system. They are likely capable of subtle attacks that can be leveraged to achieve the attacker goals, even on a wide scale. Attackers in this threat agent group are highly likely to achieve the attacker goals with meaningful impact on the elections processes. In many cases, given specific scenarios, detection and response to these attacks may be difficult. Again, these attackers form the most significant risk to the system.

The team also utilized the STRIDE method for performing threat modeling against each of the attack surfaces. Those surfaces found to be open to exploitation (exposure nodes) were evaluated for specific forms of testing. The STRIDE method evaluates each attack surface of the system for the following types of threats:

- Spoofing
- Tampering of inputs
- Repudiation attacks
- Information leakage or disclosure
- Denial of service attacks
- Escalation of privileges

The outcome of this analysis generated our test cases for the vulnerability assessment phase of the engagement.

Poor Trusts/Cascading Failures Analysis

In this phase of the process the team begins to examine the surface maps for areas where compromise could be spread from one component to the other or be leveraged for access from external-facing components or functions to the core of the system. In this case, the team reviewed research conducted by other testing teams and reviewed the relationships of the surface maps generated in phase one. Any identified issues are added to the test cases and help the team to focus on important exposure nodes during the vulnerability assessment phase.

The team quickly identified several cases where exploitation of vulnerabilities in the attack surfaces of components could lead to the introduction of malicious code (malware) into the system. Earlier testing by other teams had flagged potential exposures within the DRE component that could lead to the introduction of malware. Further, the earlier team had concluded that compromise of the DRE via malware could also spread to the GEMS server. As previously stated, compromise of the GEMS server could allow attackers an opportunity to impact the integrity and/or availability of the elections process - thus achieving attacker goals. This made the testing of mechanisms to introduce malware into the DRE a critical priority for the assessment.

In addition to the DRE, the team also identified that compromise of the Elections Media Processor (EMP) system also looked like a feasible platform for attack and compromise of the GEMS server. Testing of the security of the EMP system was also determined to be a critical task.

Lastly, given the high amounts of human access to the system components given to insiders, the team identified that best-practice-based security policies and processes were a critical component as well. Human failures, dishonesty, incompetence or malicious behaviors from poll workers, members of the Boards of Elections or other key people could likely greatly influence the achievement of attacker goals. Again, given that this finding is outside of the scope of our assessment, we urge the SoS, Boards of Election and other key elements of the elections process to expend resources to study, compile, approve and implement a series of best-practice-focused security policies and processes across all counties. If needed, the Boards of Election, should create an advisory council or steering committee of various membership with a defined charter of creating these policies and processes, working with the SoS to audit their adoption and implementation and to periodically update them as threats, controls and technology continue to evolve.

Vulnerability Assessment

Now that the attack surfaces of the components had been identified and analyzed, the vulnerability assessment phase was undertaken. In this phase we performed systematic testing of the surfaces to identify the presence of any known or unknown vulnerabilities.

It should be noted that the vulnerability assessment phase emulated the various groups of threat agents and performed testing as appropriate for each group. That is to say that components and functions were tested repeatedly with various levels of access and capability.

Generally, our vulnerability assessment covered the following attack vectors:

- Physical access
    - The team tested the components for vulnerabilities through physical access. The team probed the lock mechanisms, the accessible ports of the devices and any of the input/output subsystems that were available on the components. They also disassembled some of the components in search of ways to exploit the system.
        - The system performed poorly in these tests. Various methods of introducing malware into the system were identified. Physical locks were found to be inadequate to protect against common picking attacks and keys were found to be non-unique across components. Basic physical security best practices failed to be implemented in several cases, leaving the system dependent on the need for policies and processes external to the system for physical protection from compromise.
- Network and communication access

    - The team tested the components for networking and communications for vulnerabilities. The team used network scanners, serial port probes, sniffing tools and exploit code to probe for exposed vulnerabilities in the communications processes of the system.

        - The system performed well in these tests. Manipulation of the communications streams and network traffic failed to yield any significant vulnerabilities. However, weaknesses in the protection mechanisms installed on the GEMS server were identified in this phase. These weaknesses expose the GEMS server to possible network compromise from the EMP workstation or other network devices by an attacker or malware with access to the network during a GEMS server boot process.

- File system access

    - The team tested the components for vulnerabilities in the processing of elections data or in the way that the underlying operating system or applications interact with the file system. The team used a technique called "fuzzing" to mutate the files used in the input/output processes of the system. Fuzzing essentially tests the system by creating files with contents known to likely cause problems in applications and with random data of various types including strings, integers and binary data.

        - The system performed poorly in these tests. Several components were found to be vulnerable to input manipulation attacks that could introduce arbitrary code to the system. These vulnerabilities are typically leveraged by attackers to inject malware or to take control of the components themselves.

Penetration Testing

In the penetration phase, our team explored the damage of exploiting the vulnerabilities identified in the previous phase. We attempted to gain access to the components and influence the underlying performance of the components and applications. We also leveraged the security weaknesses to cascade the failures and create verified paths to the system core.

At the physical layer, the team was extremely successful. Physical vulnerabilities existed in several forms across several of the components. Generally speaking, for devices whose intended deployments are to be public-facing and whose purpose is to serve a critical function such as government elections, the systems seemed woefully inadequate from physical attacks.

Locks on the optical scanners and plastic ballot sorting/storage bins were easily circumvented using common lockpicking tools. In the case of the plastic ballot unit, the locks on all of the entries were opened in moments with a minimum of effort. While lockpicking is a common attack and difficult to defend against, steps to improve the security of locks should be taken. In both cases, tamper tape seals could be used to assist in minimizing the effects of these attacks, but such an effort should be undertaken by the Boards of Election in unison to identify and adopt the best practices for placement of the tamper tape seals to achieve the maximum protection. Such placement should be with the largest amount of seal contact along the opening as possible.

Keys to the physical locks of the devices are also non-unique. The keys to the DRE system covers are easily obtainable over the Internet. Attackers gaining access to keys to a component could open the locks across a wide number of the same units (all the locks that we tested were keyed the same across the units - for example, all DRE's can be opened with the same key). This could potentially expose many systems to tampering. Premier should create unique keys for each device.

Physical attacks on the DRE unit were also identified that would cause the unit to boot into administrative mode. By disabling the printer or causing errors with the smart card reader during the boot process, attackers could gain access to reconfigure the DRE device, change election settings and possibly even delete electronic ballot results previously cast on the specific DRE unit under their control. These errors are possible to exploit using only a common credit card or the voter smart cards and a strong, thin piece of material to cycle the power button. As previously determined by other researchers, the door that is supposed to protect the power button and primary memory slot on the DRE can be easily circumvented, even when locked and with tamper tape seals in place. Premier should implement stronger tabs that are closer together and positioned to prevent power manipulation. Premier should also reduce the capability of the boot modes presented when errors occur to include only the specific functions needed to troubleshoot and repair the error. General access to administrative functions should not be the normal response to errors.

The tamper tape seals themselves also create a policy/process vulnerability in that they can be simply manipulated to make it appear as if tampering has happened whether or not it truly has occurred. Threat agents working in teams could possibly cause enough tampering evidence to cause issues in local races, or perhaps even larger scale elections if they manipulated the media properly. The tamper tape seals are checked only at the beginning and end of an election cycle in most precincts and because there is no generally accepted process for handling the tampered systems, the Board of Elections in each county determines how the situation is managed. Attackers could leverage this issue to cause General Chaos in the election process and achieve the goal of disrupting public confidence in the election. Again, a common policy should be created and adopted by the counties at large for the handling of tampered systems.

The worst physical security issues in the system revolve around the two PC based components. Both the GEMS server and the EMP workstation are poorly configured and protected against physical access attacks. On both systems, attackers are very likely to be able to deploy malware or other malicious code if they gain physical access to the systems for even a short time. On both systems, the USB connections, optical disc (CD/DVD) drives and floppy disk drives are all active. Further, the EMP workstation does not have anti-virus software installed and the anti-virus software on the GEMS server had not had signature updates for approximately two years. These lack of basic security mechanisms further reduces the effort and skills required by an attacker with physical access to successfully compromise the system. In addition, it generally lowers the ability of the system to defend itself and detect malicious activity.

Much of the physical defense for the GEMS server seemed to be centered on the Digital Guardian (DG) security tool. DG is installed on the servers by the SoS to overcome known weaknesses in the GEMS software that have been publicly identified in other tests. DG is tasked with protecting the GEMS software from replacement, tampering and direct editing of the database. However, in our testing, once access to the GEMS server is gained, either via physical access or network compromise, the protections offered by DG are easily circumvented. In fact, the DG applications themselves can easily be detected and disabled using common anti-root kit or hidden process elimination tools from the Internet. Once these processes are terminated, the attacker or malware is free to attack GEMS directly with any of the known security vulnerabilities or other techniques. When the attack is complete, the processes for DG can simply be restarted without any notice that tampering has occurred.

The DG application, as deployed by the Ohio SoS, is also configured to not enforce many of the rules that it is programmed for. Instead of actually blocking the actions of the user recognized as malicious, DG alerts the user that the actions have been detected, will be logged and have been blocked - but then allows the actions to occur anyway. Even worse, DG is deployed with logging disabled, so no logs of the detected events are created. This allows attackers with access to the system to perform many types of attacks against GEMS without any resistance or chance of detection. To further complicate matters, DG applies its protective capabilities based upon the user context attempting the action. Three users exist on the GEMS server system: Administrator, gemsadmin and gemsuser. Attempts have been made to relegate specific functions to specific accounts (though they could be refined even more). However, the SYSTEM context also exists on Windows systems. The SYSTEM context is used by Windows to perform system functions and operating system level transactions. However, the SYSTEM context is also the most common level at which attackers compromise the system. Attackers generally seek this level of access and most popular exploits are geared to yield this level of access. DG's rules, however, are not applied to the SYSTEM context leaving attackers running in this mode free to assault GEMS directly without interference from DG.

The Ohio SoS should implement new configurations of DG to allow the tool to enforce the rules of the system. DG should also be configured to log all suspicious activity and to apply its rules to all users, regardless of context. In addition, SoS should configure DG with a white list of approved applications that may be executed on the system. Applications outside of this white list should not be allowed to execute. This would provide a greater level of protections for the system, the applications and data and even for DG itself. Boards of Election should adopt a policy for reviewing the DG logs and ensuring that no suspicious activity have been detected. The SoS should adopt a policy and process for updating DG rules and configurations over time as the applications and technology of the voting system changes.

Windows primarily depends upon proper password configurations for protection from attackers with physical access. However, the password policies in place on the EMP workstation and GEMS server are not in compliance with industry standard best practices, thus leaving passwords vulnerable to trivial attack. The default password of [redacted]" is likely to yield access to a significant number of GEMS server systems as no Windows configurations require password changes or rotation. Premier should adopt common and standard Windows configurations for the EMP workstation and GEMS server that are in compliance with industry standard best practices as published by NIST, the Center for Internet Security and others. Adoption of these common best practice configurations would greatly enhance the security of the components.

Lastly, physical access to the paper ballots themselves could be a danger to the integrity and availability of the system. The Premier system does not serialize the ballots, so they are not unique. The implications of this implementation are that paper ballots can be re-processed through the optical scanner without notice. Essentially, this allows some votes to be counted more than once. While policies and audit processes have been implemented to protect against this attack, a risk remains that those processes could fail or be circumvented, thus allowing vote duplication to occur. This is yet another item that Boards of Election should collaborate on to define best practices for prevention and detection of these issues and then implement those practices consistently throughout the state. Further, another physical risk was identified with the paper ballots. Attackers could modify regular paper ballots using pen, ink and white out or the like to mutate ballots into diagnostic or election ending ballot cards. These malicious ballots, in large enough quantity could impact the availability of the election data and cause high levels of frustration among elections staff. Such modifications can be difficult to detect with the human eye, and could be used to attempt to gain the General Chaos attacker goal, especially if media coverage were also manipulated by the attacker.

When the MSI team moved into pen-testing the networks and communications mechanisms, the components performed slightly better than in the physical testing. We tampered with the network and communications mechanisms between the components and focused on the events that occur when GEMS is pushing data to the EMP workstation, DRE and central optical scan units. Tampering with this data, regardless of the state of the SSL encryption used between some components did not identify any successful means of attack. The GEMS software ignored attempts to replay session data as well as attempts to mutate the transmitted data. In this resistance to common attack vectors, the GEMS software performed well.

However, the team did identify a few specific issues in the network testing. The first and most serious being a vulnerability in the firewall software used to protect the GEMS server from network compromise. In this issue, the team identified a window of opportunity to attack the GEMS server during its boot process. There exists a window of several seconds where the Windows 2000 operating system has loaded the network capability of the OS and the network is functional before the system loads the Sygate firewall. Attackers or malware with access to the network could exploit the GEMS server via the network using zero-day attacks, password exploits or other mechanisms to compromise the system before the firewall loads. Essentially, this means that the other devices, such as the DRE and EMP workstation (which lacks meaningful firewall and anti-virus protections) could be used as a staging platform for such attacks. This makes the suggestion that Premier effectively harden and secure these other network devices even more important.

Secondly, the team identified poor password policies on the Digi ethernet converter. Using a common brute force password tool, the team easily and quickly determined the default password for the root account of the device to be "[redacted]". This allowed an attacker or malware with network access to take control of the device and change the configuration. Given the criticality of the device in the elections process as the gateway mechanism for collecting and transferring data from the precinct optical scanners and the absentee ballots, loss of this device could impact the availability and timeliness of the elections processing, thus causing issues that could meet the attacker's goals.

In the last section of the pen-testing phase, the MSI team exploited file system related issues and the vulnerabilities that dealt with mutated or "fuzzed" files in the system. Here, the system performed quite poorly. Several issues with file handling and common vulnerabilities were identified. Some of these vulnerabilities could lead to the execution of arbitrary code, others to denial of service attacks and one led to a situation where GEMS data could be manipulated in such a way as to impact the integrity of the election.

The first finding in this phase involved the DRE component. Just as in the physical phase, the MSI team was able to create an error condition that caused the DRE to boot into administrative mode. In this case, the attack was performed by filling the memory card with enough files or directories that the DRE was unable to successfully write the files it uses when in boots. When this occurs, the DRE unit boots to administrative mode. Again, attackers could exploit this situation to gain access to administrative functions of the machine including configuration, encryption keys and management of data on memory cards inserted into the machine.

The file system testing also identified a plethora of buffer overflow exploits that could be performed by modifying the "[redacted]" file on the memory cards. This file, which is unencrypted plain text, appears to be related to the ASSURE security platform in use by Premier on the DRE and other components. Basically, the file tells the various components which of the files on the memory cards are currently being used in the elections process. Introducing common buffer overflow techniques into the fields of this file found exploitable buffer overflows in the EMP software and the DRE applications. Exploiting these vulnerabilities allows attackers to perform denial of service attacks against the system and could be used to execute arbitrary code, such as malware, on the system. Again, this is an alarming issue, as it again reinforces that access to the memory cards or other system components could allow attackers to introduce malware into the system that could make its way to the GEMS server and given the right capabilities affect the integrity and availability of the electronic components of the elections processes. Premier should take immediate steps to mitigate these basic flaws and perform proper bounds checking on all operations throughout the entire system code base. Additional levels of security source code review should be performed to verify that all basic application security issues have been mitigated.

Further testing of the file system attacks against the DRE and the Mobile Electronic Poll Worker devices revealed that issues with known file names being able to introduce malicious code to the systems remains a problem. As identified in other tests, the files "[redacted]", "[redacted]" and "[redacted]", if present on the memory card during boot, automatically and blindly install applications and other code onto the DRE, overwriting the current software loads. "[redacted] also performs on Poll Worker device. As shown in other tests, attackers with knowledge of the issue and proper formatting of the files, could introduce malware or other arbitrary code into the system if they can gain access to memory cards or inject illicit memory cards into the elections process. Again, given the vulnerabilities to malware, this remains a serious and grave risk to the system. Premier should modify these devices to either use code signing of applications or remove this capability for field upgrades in its entirety. Given the security posture of the overall system and the weaknesses present in the other components, this is simply too dangerous of an operation to be allowed without proper controls being implemented.

Given the work of other studies on the cryptography of the file systems, where present, primarily on the PCMCIA memory cards, our team performed only basic testing of the cryptographic mechanisms. In doing so, we found that they were capable of resisting attacks by the casual threat agents, but that as shown in other studies, they remain vulnerable to well-resourced attackers. Given this issue, our team attempted to manipulate the encrypted files without breaking their encryption using the fuzzing techniques previously described. The results of this testing revealed a significant issue in the integrity of the system.

Our team mutated the ballot box files of the election that are contained on the PCMCIA memory cards. Specific cases were identified where subtle changes in the file (in its encrypted state) would not be detected by the EMP component. These specially mutated files would be deemed valid by the EMP and would be sent to the GEMS server for processing. Once on the GEMS server, the GEMS application would mark the precinct of the tampered ballot file as having reported, but when attempting to process the actual ballot data in the file would encounter an error. In this case, no message was provided to the operator of the GEMS system, and no log entries were created by GEMS in its internal audit logs. Essentially, this means that attackers could manipulate files processed by the EMP workstations to cause GEMS to report the affected precincts as having been completed, but the votes from those precincts would not be added to the tally of the results. It should be noted that specific forms of mutation caused this error, and that the memory cards processed into GEMS by the DRE component detected the files as being invalid before processing them. As such, the capability of the attacker to leverage this vulnerability is greatly reduced, but the issue remains nonetheless. It is also entirely possible, though not proven in our testing, that other manipulations of the ballot box files may also exist that would allow this problem to be exploited on the DRE or other mechanisms. Premier should undertake a careful review of the GEMS code to ensure that any issues encountered by the GEMS application always present the operator with knowledge of the problem, create proper audit log entries and never mark precincts as reported if their voting data can not be fully processed.

In fact, our team found that the GEMS application lacked any type of basic integrity checking for its database files. Mutated database files were loaded by the GEMS application, causing internal database errors and such. Obviously, given the importance of the data in the GEMS database, it should be performing some sort of integrity checking and validation. In other parts of the system, such as on the memory cards, Premier uses encryption techniques for this very purpose. However, they fail to leverage encryption or authentication of the database within the GEMS application in any way. The effects of this problem are grave. In addition to causing the GEMS applications to encounter exceptions, it also allows attacks such as replacing or modifying the GEMS database to be easily performed by attackers or malware who gain access to the system. In the State of Ohio, the SoS, has deployed Digital Guardian to prevent these attacks, but as shown above, this is incomplete protection. The best solution would be for Premier to implement appropriate, strong encryption of the database and authentication of the database before processing in the GEMS application. Such controls would greatly strengthen the security posture of the entire system.

Another type of input attack was identified on the Poll Worker device that created a buffer overflow. In this case, the team identified that the application first called during the boot process of the device had input validation issues. The application itself is a simple placeholder style application that displays information about the Poll Worker machine such as time/date, version information, etc. The application appears to have a single purpose of launching the real Poll Worker application once the appropriate media are loaded on the component. However, our team found that by attaching a USB keyboard to the device, an attacker could actually insert text into the edit field intended for displaying information to the operator. By doing so, and injecting large numbers of characters, a buffer overflow would actually be trigged in the application causing denial of service to the application and possibly allowing the execution of arbitrary code. This is yet another example of source code that should be analyzed by Premier and hardened against the common forms of application attack in accordance with industry standard best practices.

Lastly, The MSI team also attempted to exploit and modify the contents of “files” located on the smart cards used throughout the system. Though interactions with the smart cards were possible with common tools, the team was unable to identify any changes that impacted the system beyond making the cards unusable. No vulnerabilities were identified in the processing of the smart cards or their contents.

Baseline Comparison

In order to provide an easy means of understanding the security posture of the voting system in use in Ohio, the MSI team created a simple framework for the baselining of each system against industry standard best practices. The framework created was adapted from the PCI standards, of which our team has deep knowledge, and we felt gave an easily grasped way to concisely aggregate the various standards and practices guidelines being reviewed by the EVEREST project. We feel that this framework incorporates all of the existing standards associated with both general information security and specifically with the security of electronic voting systems.

To ensure ease of communications and to create a level playing field for all the systems to be compared against, we chose to implement a system of pass/fail grading for each of the twelve requirements of the framework. Passing a category means that the system meets the best practices requirements for that area, while failing indicates that the system does not meet industry standard best practices in the mind of our team.

Below are the specific twelve areas of the framework and the score assigned to the system for each one, along with our reasoning for the score:

BEST PRACTICE	PASS/FAIL	COMMENTS
Are firewall technologies and configurations adequate to protect systems and data?	Fail	Firewalls are not deployed on the EMP system, Vulnerabilities exist in the GEMS firewall implementation
Are password implementations sufficient to provide basic security?	Fail	Passwords across the components are poorly implemented and configurations are not sufficient to enforce complex password use
Is the core data protected during storage?	Fail	The data is vulnerable to compromise by attackers and malware at various stages of its existence, including on the DRE, at the EMP workstation and on the GEMS server itself
Is the core data encrypted during transit?	Fail	While the data on the PCMCIA memory cards is encrypted, the contents of the memory cards used in the optical scanners is not

BEST PRACTICE	PASS/FAIL	COMMENTS
Are anti-virus applications used and up to date?	Fail	The EMP workstation, DRE and Poll Worker device lack anti-virus applications, the GEMS server anti-virus software is out of date
Are the components of the system securely developed, configured and up to date?	Fail	Common programming flaws are present on many system components including exploitable buffer overflows
Are access controls deployed to enforce "need to know" and/or "need to access" boundaries?	Fail	While the SoS has deployed Digital Guardian to assist in this role, it has failed to provide adequate security to meet best practices
Are user authentication mechanisms unique enough to provide non-repudiation?	Fail	Operators of the components use common accounts
Is access to the system logged, monitored and audited?	Fail	Logging across the components is woefully inadequate to provide meaningful audit capabilities, intrusion detection or basic forensic analysis
Are the systems routinely audited and tested for new vulnerabilities?	Fail	While no operating system flaws were found, patches and updates to the applications were not present, No meaningful process for ongoing assessment or mitigation of emerging threats was identified
Are security policies and processes in place to adequately protect the system, its components and the core data?	Fail	Given the lack of consistency across the deployments of the system throughout the counties of Ohio, meaningful security policies and processes remain to be identified and adopted

Framework Comparison Summary:

Score (Pass/Fail): 0/12

Root Cause Determination

Review of the various vulnerabilities in the system identifies a couple of specific root causes. First and most importantly, the vulnerabilities demonstrate a lack of adoption of industry standard best practices with regards to general IT functions, networking, system and information security and secure application development. The Premier system fails to meet any of the twelve basic best practices requirements. If Premier would simply adopt a common set of best practices for system development, implementation and deployment, many of the underlying issues could be mitigated. If Premier would take the best practice steps of hardening the systems in accordance with Center for Internet Security, NIST, SANS, OWASP and/or other frameworks of best practices, they could greatly enhance the security posture of the system as a whole.

The SoS implementation of Digital Guardian may also be able to assist in the efforts to better secure the system. If the Digital Guardian tool were properly configured and implemented to enforce best practices, it would likely greatly enhance the security of the GEMS server and the protection of the core elections data. However, without a configuration to protect itself and the GEMS server/application from common attacks, the tool does little to enhance the security of the overall system.

Lastly, a key root cause for much of the risk to the system is the lack of consistent, best practices-based security policies and processes surrounding the system. Given the roles of the SoS and the county Boards of Election, inconsistent management, implementation and handling are key reasons for concern. If the counties identified best practices for with regards to the system and implemented them consistently across the state, security improvements are likely to be gained. Further, a consistent set of policies and processes would simplify the oversight of elections security and provide the public with a verifiable set of auditable requirements that are likely to increase public trust in the elections process.

Suggestions for Improvement

The first and primary step in improving the security of the Premier system is for all parties involved to embrace industry standard best practices and enforce them through technology, policy and process and education throughout the entire system. If all of the major stake holders, from the vendor to the SoS and from the Boards of Election to the poll workers had a consistent and usable set of rules to enforce, the overall security of the system would be enhanced.

Secondly, immediate concern and mitigation of the malware risks are required. Additional controls such as updating existing anti-virus software, implementation of additional anti-virus tools and reconfiguration of the Digital Guardian package must be undertaken. Since the deeper solution of changing the various component application code to mitigate the vulnerabilities that could be leveraged by attackers to introduce malware into the system are likely to take considerable time and resources, additional layers of controls must be implemented to create a defense-in-depth approach within the existing system. In addition to the installation of new controls and the reconfiguration of existing ones, a key focus must be in identifying ways to protect the system components from tampering during their lifecycle. Careful examinations of the specific processes in which the way the equipment is handled, stored, maintained, setup, transported and managed must be performed. Processes must be created and enforced to ensure that no single point of exposure occurs where an individual could attack the systems without detection. Historically, controls such as dual-presence, where no one person is allowed to be alone with the equipment, have proven somewhat successful at minimizing risk. However, whatever solutions identified and adopted, they must be done so in a controlled, consistent manner across the State or little true mitigation is likely.

Lastly, Premier must undertake a systematic approach to mitigating the identified vulnerabilities in the system. This includes repair of the software, hardware configurations, basic deployment images, default passwords and general security posture of the system. Each issue mitigated by the vendor greatly reduces the amount of risk management that must be transferred to the counties by policy and process controls. Given the lack of resources many of the counties face, this is likely to have significant impact on the entire elections process.

Summary

The Ohio Secretary of State (SoS) retained the services of MicroSolved, Inc. (MSI) as a part of the overall EVEREST project to examine the security of the electronic voting systems in use in Ohio. As a part of that study, the MSI team performed red team penetration tests against the Premier voting system and attempted to identify attacks that could be exploited against the confidentiality, integrity and availability of the system and/or the overall elections processes. This report details the methodology, findings and results of the Premier system testing.

The MSI team identified several key threats to the security of the system. These threats range from common attacks such as buffer overflows and malware to the specific issues in how components of the system handle error conditions. Many of these issues stem from a lack of adoption of industry standard best practices across the spectrum of the elections system, from technical implementations to policies and processes in use at the county level. Adoption of best practices and implementation of additional controls to create a defense-in-depth security posture would enhance the security of the Premier system.

Definitions/Reference Section

Terms and Definitions:

Buffer Overflow - Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code. For more information, please see:
http://www.owasp.org/index.php/Buffer_Overflow

Fuzzing - Fuzz testing or Fuzzing is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion. For more information, please see: http://www.owasp.org/index.php/Fuzzing

Sites for Best Practices and Frameworks:

The Center for Internet Security - http://www.cisecurity.com/

NIST (National Institute of Standards and Technology) - http://www.nist.gov/

SANS (SANS Institute) - http://www.sans.org

OWASP (The Open Web Application Security Project) - http://www.owasp.org

PCI DSS (Payment Card Industry Data Security Standard) - http://www.pcisecuritystandards.org

EVEREST Project Information:

Ohio Secretary of State EVEREST Project - http://www.sos.state.oh.us/sos/info/everest.aspx