PREMIER SYSTEM

MICROSOLVED, INC.

EXECUTIVE SUMMARY 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 the first in a series of three reports. The report contains general suggestions for improvement and mitigation of the discovered issues. A technical manager's report of the process and findings in greater detail (report #2) and a specific catalog of technical findings (report #3) were delivered alongside this report to the SoS.

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

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.
PCMCIA and CF memory cards	Various types

DEVICE	MODEL OR VERSION NUMBER
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. Each of the phases build upon the insights gained from the previous phases to add to the team's understanding of the system, its operation and the risks, threats and vulnerabilities it faces.

Threat Models Reviewed

The study performed 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.
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.

THREAT AGENT	DETAILS
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.
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.

Results of the Review

The review identified three key weaknesses in the Premier system. Exploitation of any or all of these weaknesses could allow attackers to achieve the goals described above to varying degrees. Attackers leveraging these vulnerabilities could greatly impact the security and public trust of the elections process.

The primary finding of the review was that Premier had failed to adopt, implement and follow industry standard best practices in the development of the system. Basic best practices have emerged over the last several years to assist organizations with the development, configuration, deployment and management of IT infrastructures in a secure fashion. However, the Premier voting system fails to comply with these basic tenets of information security and as such, suffers from a myriad of common vulnerabilities ranging from buffer overflows to weak configuration of the components. In many cases, vulnerabilities and weaknesses that have been known for several years still exist in the system components.

The second key finding of the review was the apparent vulnerability of the system to malware infection and manipulation. If properly skilled and resourced attacker can gain access to any of several components in the system at any time during their life-cycle, there exists a large possibility that they could implement malicious programming (malware) into the system with little chance of detection. Once the malware was in place on the system, it could perform a variety of tampering and could likely spread from component to component throughout the system. The ability of malware to affect the integrity and availability of the elections process is profound and disturbing, but the lack of capability to detect and report potential malware attacks against the system makes it the single largest threat. Due to the inherent weaknesses of the system on these technical levels, the work of ensuring the protection of the elections data must be transfered from the systems to human processes.

This leads to the third key finding of the review. Given the nature of the elections process in Ohio and the distributed management of the process by the eighty-eight independent Boards of Election, no clear and effective security policies and processes have been established or adopted across the state. As such, each county Board of Elections establishes their own processes for management of the election systems and the handling of the elections data. Without a best practice-based, consistently implemented set of security policies and processes, security weaknesses are likely to abound. Further impacting this problem is the fact that many county Boards of Election face staff and budget shortfalls which largely prevent them from having enough resources to seek out and implement their own solutions.

Suggestions for Improvement

Obviously, given the lack of adoption of best practices as a key finding of the review, the first suggestion for improvement is for Premier to adopt these industry standard best practices and then apply them, en masse, to the system. The very applications themselves need to be hardened against known forms of attack, while the various other components should be configured to enforce the basic security rules of the best practices frameworks. Various organizations - NIST, the Center for Internet Security, SANS, OWASP and others have public frameworks that could be

leverage to provide security baselines for future versions of the systems. Given the importance of the elections processes to our democratic form of government, these basic security practices should be the bare minimums accepted from the vendors of the systems critical to elections.

Secondly, immediate attention to the configuration and deployment of additional controls to minimize the risk of malware infection must be implemented into the existing system. These additional controls should prevent the introduction of malware where possible, detect the presence of malware and attempts to inject malware into the system and provide a means of logging and auditing for these types of attacks. Any component that could be used as a potential gateway to introduce malware to the system should have additional controls created to protect it. These controls should include, but not be limited to, additional anti-virus software, reconfiguration and strengthening of the SoS's Digital Guardian implementation, additional human-based policy and process controls at all levels - including the county Boards of Elections and the volunteer poll workers themselves. Additional training on these controls should also be performed at all levels and awareness training focused on detecting potential attacks and social engineering scenarios should also be performed. In short, the controls to prevent malware infection should address all levels of the elections process and should include technical, policy and process safeguards and education for the people involved so that they can better safeguard the system against these threats.

Lastly, the county Boards of Election should form a working group to identify best practice policies and processes for the handling of these elections systems. Once identified, they should adopt and implement these policies and processes consistently across the state. This would greatly enhance the security of the system and give local Boards of Election clear and concrete goals as well as insight into the resource requirements of implementing these solutions. Further, the SoS should use these common guidelines as a basis for auditing and oversight of the county Boards of Election and use them as a basis for ongoing education, training and awareness.

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

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 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