PREMIER, ES&S AND HART TESTING

MICROSOLVED, INC.

PROJECT 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

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, ES&S and Hart voting systems and attempted to identify attacks that could be exploited against the confidentiality, integrity and availability of the systems and/or the overall elections processes. This report details the methodology, findings and results of that testing.

This report summarizes all of the other reports generated during the testing. Each vendor system test was detailed in three specific reports ranging from the technical details of the findings to summary level information. The SoS has reviewed these additional reports and accepted them as the output of the testing process. These reports vary in their sensitivity, and may not be fully available to the public.

The MSI team tested the 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 systems and many of their components. These vulnerabilities demonstrate the capability for attackers who gain access to specific components of the system to influence and tamper with the confidentiality, integrity and availability of the elections process. 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 systems was conducted onsite at the facility provided by the SoS. Our testing process took place from October 5th, 2007 through November 30th, 2007. The MSI team was provided basic training on the systems from the vendors. 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.

Systems Information

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

Premier Components:

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

ES&S Components:

DEVICE	MODEL OR VERSION NUMBER
Unity Election Management Software	3.0.1.1
Automark	87000 with CF memory card media and paper ballots
3 iVotronic DRE units	90998-BL, 91057-BL & 93038-BL including CF memory card media, serial printers and PEB units
Precinct Optical Scanner	Model 100 with PCMCIA memory card media, paper ballots and ballot box
Central Optical Scanner	Model 650 with zip disk media and paper ballots
Windows 2003 Small Business Server	Dell hardware - used for additional storage of elections data
Windows XP Professional Workstation	Dell hardware - used to manage the election, host of the Unity software

Hart Components:

DEVICE	MODEL OR VERSION NUMBER
Hart Elections Management Software (HEMS)	Versions as provided by SoS: BOSS, Tally, Rally, Servo, Trans, Ballot on Demand, eCM Manager and eCM token
Windows 2000 Professional Desktop	Dell workstation used to host Tally and other applications (except Rally & Servo)
Windows 2000 Professional Laptop	Dell laptop used to host Rally & Servo
Judges Booth Controller (JBC)	For powering and administering the DRE units and generating voter access codes; included PCMCIA memory cards (Mobile Ballot Box - MBB)
eSlate 3000 DRE	Version 4.0.1.9 with PCMCIA memory cards and VVPAT
eScan Optical Scanner	Version 1.1.6 with paper ballots, PCMCIA memory cards, CF memory cards, and plastic ballot box

General System Operation

The elections process 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 memory cards and other media 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 relevant software used to calculate the election totals. These software applications and host computers that run them 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 Systems. 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

Each of the systems were compared against a common baseline of information security practices. This framework for comparison was based on the PCI DSS standard that has become an industry accepted form of guidance for security best practices. The framework was originally designed to be applied to credit card processing systems, but easily extends itself to any form or critical data. The additional positives for selecting it as a baseline for this review is that if a system meets the requirements derived from the PCI guidance, it will easily pass all of the other myriad of relevant standards often used for voting system reviews and this specific framework is easily understandable by the average non-IT reader.

Below is a summary table of the performance of each of the three reviewed systems as compared to the baseline.

	PREMIER	ES&S	HART
Are firewall technologies and configurations adequate to protect systems and data?	Fail	Fail	Fail
Are password implementations sufficient to provide basic security?	Fail	Fail	Fail
Is the core data protected during storage?	Fail	Fail	Fail

	PREMIER	ES&S	HART
Is the core data encrypted during transit?	Fail	Pass	Fail
Are anti-virus applications used and up to date?	Fail	Fail	Fail
Are the components of the system securely developed, configured and up to date?	Fail	Fail	Fail
Are access controls deployed to enforce "need to know" and/or "need to access" boundaries?	Fail	Fail	Fail
Are user authentication mechanisms unique enough to provide non-repudiation?	Fail	Fail	Fail
Is access to the system logged, monitored and audited?	Fail	Fail	Fail
Are the systems routinely audited and tested for new vulnerabilities?	Fail	Fail	Fail

	PREMIER	ES&S	HART
Are security policies and processes in place to adequately protect the system, its components and the core data?	Fail	Fail	Fail

The review identified three key weaknesses in the systems. 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 all three of the vendors 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, all of the tested voting systems fail to comply with these basic tenets of information security and as such, suffers from a myriad of common vulnerabilities ranging from improper passwords 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 lack of integrity controls that have been applied to the systems and their components. Some systems were missing properly implemented encryption of the election files, allowing them to be edited or destroyed by an attacker or malware. Some systems failed to identify even trivial manipulations of the components or the data, including attacks ranging from write protection of the memory cards and other media to direct modification of the voting databases. Many components lacked basic security controls such as firewalls, anti-virus and other mechanisms for providing protection for system integrity.

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

The first and primary step in improving the security of the systems 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 vendors 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, vendors must proceed to deploy proper integrity controls such as anti-virus software, firewalls, encryption and deeper techniques such as proper bounds checking on inputs and other security programming standards. Adoption of these basic and well known security processes would minimize the amount of risk these systems face. SoS should also assist in this effort to increase integrity assurance by leveraging its skills and knowledge with their chosen Digital Guardian tool across all PC components of the various systems. Currently, the tool is deployed only on the Premier systems, but if correctly configured and implemented, all systems could benefit from its use, especially on the primary components used to calculate vote totals and process the election results. Development, implementation and enforcement of system specific white lists for applications and other relevant rules would give the SoS a capability to audit, assess and ensure the integrity of these critical systems that they do not currently have.

Lastly, the vendors 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 accounts/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 voting systems 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 those tests.

None of the systems performed well when measured against the established industry standard best practices of the IT industry. All three vendor systems reviewed have serious gaps in compliance with even the most basic set of information security guidelines used by systems in industries such as finance, insurance, medical care, manufacturing, logistics and other global commerce. Given the extremely valuable data that these systems process and the fact that our very democracy and nation depend on the security of that data, much work remains to be done by all three vendors. Adoption of best practices and implementation of additional controls to create a defense-in-depth security posture are critical to enhance the security of these systems.

Reference Section

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