HART 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 Hart 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 Hart 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 Hart 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 Hart 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 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 Hart systems was conducted onsite at the facility provided by the SoS. Our testing process took place from November 20th, 2007 through November 30th, 2007. The MSI team was provided basic training on the systems from Hart. 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.

Hart System Information

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

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 Hart 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 Hart software called "Rally"(if multiple stations are being used) or "Tally" (if the main calculation computer is being used). The "Tally"software and its host computer 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 Hart 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 based upon the guidance of the SoS. 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 Tally computer became apparent. Since the Tally computer defines the election settings, creates 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 Hart system. Successful attacks against the integrity or availability of the Tally computer could have serious consequences. The Boards of Election around Ohio take established precautions during the elections cycle to protect the Tally computer, however, general questions and answers from other EVEREST project teams have indicated that protection of the Tally computer 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 Tally computer 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 Elections should take high levels of caution to protect the Tally computer 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 Hart 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 Hart 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 cascading failures identified in this assessment showed that failure to protect the memory cards from illicit access at any point in the elections cycle could have grave results on the integrity of the election. Hart has designed the PCMCIA memory cards that contain the ballot and vote data to be used and transported without the security of encryption. They wrongly believe the proprietary format of the card and data to be sufficient protection against tampering. However, in our testing, the MSI team easily copied, invalidated, edited and tampered with the contents of the memory cards, including disabling cards and preventing specific votes from being counted by the Tally system. The tools leveraged to perform these attacks were a normal Windows computer and a PCMCIA drive and software widely available for purchase on the Internet for under $100.00. This choice by Hart to not encrypt the data cascades throughout the system. None of the software components detect the tampering of the vote data, report that tampering has taken place or notify the user in any way (unless the card format is damaged in the tampering). The effect of this tampering capability is that attackers who gain access to the memory cards during an election could alter the vote files in many ways thus violating the integrity of the election and achieving one or more of the attacker goals.

Additionally, 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 many of the components in search of ways to exploit the system.
        - The system performed poorly in these tests. While the DRE and JBC units faired pretty well in this testing, physical access to the optical scanner device and the two computer systems hosting the Hart software was tantamount to complete compromise of the system. Attackers gaining physical access to these components would likely be able to achieve the attacker goals.
- 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 at an intermediate level in these tests. While remote exploitation of the optical scanner was not proven possible, it was identified as running insecure services and our scanning activities appeared to impact the device's performance in unpredictable ways. The network connection used to pass elections data between the Rally and Tally software components was found to be improperly passing data in plain text without encryption, and the computers hosting both applications (Rally and Tally) were easily compromised by enumerating a default account and quickly brute forcing the default password.

- 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 that 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. As described in previous sections, attackers gaining access to the memory cards could easily tamper with the core voting data. While the software components of the system seem to have been hardened against buffer overflows and other forms of input-based attacks, the capability to directly edit the voting database from within the Hart system was identified, as well as attack vectors for direct database editing either manually or via malware. These are critical issues.

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 DRE and JBC units performed very well. These precinct-located components are quite resistant to physical attack. All of the administrative functions are protected by passwords, which although weak, do provide a layer of defense against casual manipulation. The team could not identify a way to circumvent the operating modes of these units or achieve access to their underlying operating systems.

One physical vulnerability with the DRE unit was identified. The team found that by rocking the DRE back and forth in the cradle unit during the printing of the final ballot acceptance barcode, they could interfere with the printing of that barcode (and the DRE to printer connection) and cause it to be repeated over and over without alert or notice. This repetitious printing of the barcode could be a danger to barcode based automated recounts, but this process is not used in Ohio. In Ohio, currently, recounts of the printed paper tapes are performed manually - reducing this attack to from possible vote manipulation to simple confusion of recounting poll workers. This problem could be easily mitigated by providing proper training to poll workers about the issue and how it would be created so that they be vigilant for attempts to tamper with the system in this manner at the precincts. The vendor should implement changes in the system to prevent reprinting of bar codes and properly alert the poll workers to the issue - but the problem is not in need of urgent resolution for Ohio.

Physical attacks against the JBC also led to the discovery of a potential problem with the generation of voter access codes. By gathering as few as 25 voter access codes, our team was able to easily reconstruct the algorithm used to calculate them and begin predicting valid voter access codes. Exploitation of this vulnerability by an attacker could allow them to vote multiple times using the DRE device. While currently this device is used primarily for disabled voting in Ohio, keeping the user base quite small, future wide scale adoptions are possible. Expanded use of the current implementation would mean expanded risk that this vulnerability would be exploited. The solution for this problem lies in the random generation of the voter access codes rather than deriving them from a mathematical process. Hart should implement randomization of these access codes as soon as possible.

The optical scanner component performed less well against physical attack than the other precinct equipment. Compromise of the optical scanner can be easily gained by an attacker who achieves physical access to the scanner device in an unattended manner. Disassembly of the device revealed that the operating system (OS) of the scanner is directly loaded from a normal compact flash (CF) memory card that is secured inside the system only by tamper tape. An attacker with sufficient knowledge and resources could easily overcome the tamper seals and either modify or replace the operating system files or memory card. Highly resourced attackers could easily introduce malware that could impact the electronic counting processes or memory subsystems of the scanner device and affect the integrity of the elections process. The attacker could also leverage a second internal CF card slot to introduce malware or other code into the system as well. If that CF card were later removed prior to internal inspection, it would be nearly impossible to prove that it was or was not present at the time of an election. For Hart to mitigate the replacement and tampering potential of the OS CF card would require them to redesign the hardware of the system or introduce some other type of physical protection, such as an electronic case tampering sensor such as found on many PC systems. In fact, the MSI team encourages Hart to implement these electronic case sensors on all of their components. Since this is not practical in a timely manner, additional policy and process controls for ensuring that access to the optical scanner

units must be implemented and the replacement of the case screws with special screws that require more specialized tools than a phillips screwdriver should be put into place.

Other problems were also identified around the optical scanner unit. First, the ballot box that the scanner uses to hold the counted ballots was easily unlocked using common lockpicking techniques and tools. Attackers could leverage this problem to quickly gain access to the ballot box and add/remove or alter ballots. Further complicating this issue is the fact that duplication of ballots is not difficult. Some counties use specific watermarked ballot paper as a control, however, this is not required for proper system operation. Hart depends upon ballot sequence numbers for a large amount of ballot security. These serial numbers identify each ballot uniquely within the system - thus preventing ballot rescanning and simple photocopying of ballots. However, Hart's implementation of the algorithm to generate these ballot sequence numbers, just as with the JBC voter access codes, is easily predictable by gaining access to only a small number (under 25) of ballots and their sequence of creation. This means that attackers with the capability to predict valid ballot sequence numbers could introduce duplicate ballots into the process, making it nearly impossible to determine the true will of the voters from the impacted precincts. Such an event could have a large impact on the reputation of the Ohio elections process.

Lastly, at the physical layer of the precinct equipment, the security of the PCMCIA memory cards used to carry the elections data between the precincts and the central Board of Elections is inadequate. Attackers who gain access to the memory cards can easily tamper with the data and the integrity of the election as detailed previously. Protection of these cards is critical to the protection of the elections process in Ohio.

On the county Board of Elections side, the devices performed poorly in terms of physical security. Both the laptop Rally/Servo computer and the all important Tally desktop computer are easily compromised by attackers who gain physical access. Hart has taken some steps to begin to protect these devices by assigning BIOS passwords and preventing the introduction of other boot media, but they have failed to provide adequate security for the components in a meaningful way beyond that. The components lack firewalls, anti-virus software, critical patches and best practices-based logging and security configurations. Attackers with physical access to the system could easily circumvent the existing protections by resetting the BIOS or by introducing malware to the system during its normal operations. Hart should adopt a common security baseline for these components as suggested by SANS, the Center for Internet Security, NIST and others. Implementation of such a baseline would greatly enhance the security of these devices. Such implementations should include the addition of anti-virus and other relevant controls to protect the system from tampering and malware. While these would changes would not eliminate the need for physical security controls, they would at least raise the bar of prevention and detection for the casual attacker.

The penetration test then moved into exploitation of the communications processes used by the system. On the precinct equipment, the presence of a network jack on the back of the optical scanner was explored. The network presence of the optical scanner includes a Telnet server, which the team unsuccessfully attempted to compromise. Network traffic fuzzing and brute force attempts to identify a valid login and password combination failed. However, the team felt that a patient attacker with access to the device could eventually gain access. The result of this access would likely be a complete compromise of the component and its election data. The team reached this conclusion through the analysis of the previously identified operating system image on the internal CF card. Hart should disable the Telnet server in future versions of the product, as it represents a potential point of entry to the component. Boards of Election should cover the network jack with tamper tape during precinct deployments as an additional tamper control.

The centralized systems also utilize network communications to facilitate the transfer of voting data from the Rally laptops to the central Tally system. While these communications resisted attacks via network traffic fuzzing, interception and alteration of them is possible. The lack of proper encryption for these network transfers is an interesting issue, since Hart appears to have implemented some form of SSL to attempt to encrypt the connection between these components. However, full encryption of the connection is not performed, despite the certificate transfer that occurs when Rally units register with Tally. Throughout the elections data processing, Rally reads memory cards and waits for Tally to collect the data from the Rally components. These transfers of the actual vote totals contain plain text elements. While the MSI team was unable to identify the formatting of the transferred data due to time constraints, it appeared to be similar to the structure of the memory card files. Our estimation is that given the time and resources an attacker could likely learn to tamper with the vote data enough to manipulate the vote totals or invalidate some of the votes as we did when accessing the memory cards directly. Hart should immediately investigate this protocol implementation and ensure that it is operating as expected, as the presence of the plain text contents does not meet the best practices for a standard deployment of the SSL protocol.

Of most concern from the network exploitation was the identification and compromise of a default account on both of the Windows 2000 computers. The scanning process from the vulnerability assessment had identified the existence of a default account called [redacted] on both components. The account had administrative level access on both computers as well, making them a high priority target for attackers. In both cases, our penetration tools quickly identified the default password for these accounts to be [redacted]. Using these default login and password combinations, the components were quickly completely compromised from the network at the administrative level. This was made possible largely due to the lack of best practice compliant controls such as firewalls, logging mechanisms and proper password complexity settings. As a result of these default accounts, attackers who gain access to the network or who can introduce malware to any of the network accessible machines can easily gain administrative access to all of the other network components, including the mission critical Tally computer. Attackers could then tamper with the elections process and data as they desire. Hart should remove all default accounts prior to shipping any component. Additionally, as previously stated, all components should be deployed with their configurations in compliance with an established security baseline such as the industry standard best practices defined by NIST, SANS, the Center for Internet Security and others. Counties and the SoS should immediately remove these default accounts to prevent their exploitation.

Finally, while exploiting the file system level vulnerabilities identified in the system, the team identified two critical risks that immediately impact the integrity of the elections data. Of the highest risk is that the database storing the elections data within Tally is unencrypted. Again, Hart has chosen to forgo encryption of the core critical elections data in their system. Because of this lack of encryption, attackers or malware gaining access to the Tally computer could simply directly edit the database contents to modify the election results. Unless auditing is performed against the paper tapes from the precinct machines such editing would likely go undetected. The second mechanism that the team exploited to edit the database directly was Tally itself. The application includes the capability to directly edit the election results without the need for additional authentication or controls. While editing the database in this manner is logged by the application, those logs could be missed or deleted by the attacker. Hart should not only implement proper encryption controls for the elections database, but they should also remove or provide additional security for the editing functions built into Tally. If this process is required for recounts or the like, then additional security controls such as authentication of more than one user and/or the presence of a special eCM key should be required. Additionally, any reports or screen operations involving an edited database should alert the user to the fact that the data has been manually edited and should be manually verified. Such additional protections would minimize the risk of these issues to the elections process.

The SoS could also greatly enhance the security of the Windows 2000 components by implementing the Digital Guardian tool they use on other voting systems on the Hart system. When Digital Guardian is installed, configured and managed properly it would enhance the capability of the SoS to ensure the integrity of the operating system, database files and election management software. If a white list of allowed applications were also created and enforced, the operation of malware and other attacker tools would be much more difficult and detectable, thus reducing the risk levels of the existing Hart system.

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 any of the components, and the configurations of the Windows 2000 components is insufficient to protect the data
Are password implementations sufficient to provide basic security?	Fail	Passwords are generally weak and default administrative passwords exist on the two Windows components
Is the core data protected during storage?	Fail	The core data is not encrypted in the Tally database

BEST PRACTICE	PASS/FAIL	COMMENTS
Is the core data encrypted during transit?	Fail	The core elections data is unencrypted during physical transit on the memory cards, the network transactions between Rally and Tally are not properly encrypted
Are anti-virus applications used and up to date?	Fail	No anti-virus software was identified on any of the components
Are the components of the system securely developed, configured and up to date?	Fail	The DRE and JBC units would pass these requirements, as would the software itself - however, the optical scanner and the lack of secure configurations and patches on the Windows 2000 components cause the Hart system to fail this category
Are access controls deployed to enforce "need to know" and/or "need to access" boundaries?	Fail	Some role based controls are enabled in the software, however, the capability to edit the voting data without additional access controls fails to meet this criteria, default accounts exist
Are user authentication mechanisms unique enough to provide non-repudiation?	Fail	Operators of the components use common accounts, default accounts exist
Is access to the system logged, monitored and audited?	Fail	Logging is not configured in accordance with industry standard best practices on the Windows components
Are the systems routinely audited and tested for new vulnerabilities?	Fail	Critical patches are missing from component operating systems

BEST PRACTICE	PASS/FAIL	COMMENTS
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 Hart system fails to meet any of the twelve basic best practices requirements. If Hart would simply adopt a common set of best practices for system development, implementation and deployment, many of the underlying issues could be mitigated. If Hart 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 Tally computer and the protection of the core elections data. However, without a configuration to protect itself and the Tally computer/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 Hart 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, Hart should implement proper encryption of the elections data during both storage and transit. Databases and network communications should be protected using a strong security algorithm such as AES or the like. All existing memory cards (electronic ballot boxes) and any future media included in the system should only contain fully encrypted files. The proper implementation of strong cryptography would minimize the persistent and cascading risk of attacks against the integrity of the elections data processed by the system.

It would also be wise for Hart to randomize the ballot sequence numbers and voter access codes in use within the system. Proper (pseudo-)random number generation is a difficult process, but it would make the attacks currently available to perform "ballot box stuffing" much more unlikely to succeed. Existing application source code examples are available through various forums and trusted sources (such as programming language authors) to assist in the implementation of these changes.

Lastly, Hart 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 Hart 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 Hart system testing.

The MSI team identified several key threats to the security of the system. These threats range from lack of proper encryption to missing patches. 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 Hart system.

Definitions/Reference Section

Terms and Definitions:

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