wyle laboratories

7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411
Fax (256) 721-0144
www.wylelabs.com

SECURITY ASSESSMENT SUMMARY REPORT
FOR
UNISYN VOTING SOLUTIONS, INC.
OPENELECT VOTING SYSTEM (OVS), VERSION 1.0

Reviewed by:

Jack Cobb 12-30-04

Jack Cobb, Senior Project Engineer

ACCREDITED
Cert. No. 845.01

COPYRIGHT BY WYLE LABORATORIES. THE RIGHT TO REPRODUCE, COPY, EXHIBIT, OR OTHERWISE UTILIZE ANY OF THE MATERIAL CONTAINED HEREIN WITHOUT THE EXPRESS PRIOR PERMISSION OF WYLE LABORATORIES IS PROHIBITED. THE ACCEPTANCE OF A PURCHASE ORDER IN CONNECTION WITH THE MATERIAL CONTAINED HEREIN SHALL BE EQUIVALENT TO EXPRESS PRIOR PERMISSION. WYLE SHALL HAVE NO LIABILITIY FOR DAMAGES OF ANY KIND TO PERSON OR PROPERTY, INCLUDING SPECIAL CONSEQUENTIAL DAMAGES, RESULTING FROM WYLE'S PROVIDING THE SERVICES COVERED BY THIS REPORT.

TABLE OF CONTENTS

Page No.

1.0 INTRODUCTION 1

1.1 Objective 1
1.2 Scope 1
1.3 References 2
1.4 Terms and Abbreviations 2
1.5 Test Specimen Description 3

2.0 EXECUTIVE SUMMARY 4

3.0 TEST OBSERVATIONS AND RECOMMENDATIONS 5

3.1 Scans 5
3.2 Group 1 Tests 5
3.2.1 Group 1 Recommendation 7
3.3 Group 2 Tests 7
3.4 Other Tests 8

4.0 INITIAL FINDINGS 9

5.0 CONCLUSION 10

1.0 INTRODUCTION

1.1 Objective

The purpose of this Security Assessment Summary Report is to identify common vulnerabilities throughout the system as it relates to physical and technical security. This assessment documents the security assessment activities that were performed on the system and the results of those activities including Security Test & Evaluation (ST&E), vulnerability scans, audits, and any other risk assessment activities. This report provides the system's stakeholders with an assessment of the adequacy of the physical and technical controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits or processes.

1.2 Scope

This report includes the assessment of the system level physical, operational and technical controls and the components that directly support the Unisyn Voting Solutions, Inc OpenElect Voting Systems Release 1.0. The following system components were assessed in this report:

- OpenElect Voting Optical (OVO)
- OpenElect Voting Interface (OVI)
- OpenElect Central System (OCS)
- Central Scan System (OVCS)

The following components that directly support the system were also assessed in this report:

- Ballot Layout Manager (BLM)
- Election Manager (EM)
- Election Server (ES)
- Software Server (SS)
- Tabulator, Tabulator Client, Tabulator Reports (Tab Cluster)
- Transport Media (TM)

The following activities are within the scope of this project:

- Review of supplied documentation on administration, operations, system administration, and network management.
- Assess the physical security of the system.
- A series of network scans to enumerate addressable devices and to assess each systems available network services.
- A configuration and security assessment of the systems.
- Penetration testing of systems and networks.

The following activities were NOT part of this security assessment:

- Social Engineering to acquire sensitive information from manufacturers' members or suppliers.
- Testing that would physically destroy the system.

1.0 INTRODUCTION (continued)

1.3 References

- EAC 2005 Voluntary Voting System Guidelines, Volume I, Version 1.0, "Voting System Performance Guidelines", and Volume II, Version 1.0, "National Certification Testing Guidelines"
- NIST Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, February 2004
- Security Content Automation Protocol (SCAP): Guide to The Secure Configuration of Red Hat Enterprise Linux 5
- Unisyn Voting Solutions, Inc OpenElect Voting Systems Release 1.0 System Overview 04-00446
- Unisyn Voting Solutions, Inc OpenElect Voting Systems Release 1.0 System Security Specification 04-00447
- Unisyn Voting Solutions, Inc OpenElect Voting Systems Release 1.0 System Functionality Specification 04-00444

1.4 Terms and Abbreviations

Table 1-1 Terms and Abbreviations

Term	Abbreviation	Definition
Ballot Layout Manager	BLM	Unisyn OVS application used to lay out ballot information.
United States Election Assistance Commission	EAC	Commission created per the Help America Vote Act of 2002, assigned the responsibility for setting voting system standards and providing for the voluntary testing and certification of voting systems.
Election Manager	EM	Utilizes the election definition file from the Ballot Layout Manager, adds jurisdiction voting device specific options and produces the CD used to load the election onto the voting devices and OVCS.
Election Server	ES	A component of the OCS, the ES updates the system clock and downloads new Election data to the voting devices prior to each election, typically at the warehouse.
OpenElect Central Suite	OCS	Set of applications supplied by Unisyn to run at the Election Headquarters to support elections on the OVO, OVI, and OVCS systems. Includes: Ballot Layout Manager, Election Manager, Election Server, Tabulator Client, Tabulator Server and Tabulator Reports. In addition, the OCS includes the Software Server (SS) system for updating and validating OVO and OVI (voting device) software.
OpenElect Voting Central Scan	OVCS	A bulk scanner solution at the Central Site, used for casting provisional and mail-in ballots; can also be used to perform recounts.
OpenElect Voting Interface	OVI	Used as an ADA solution and early voting device.
OpenElect Voting Optical Scan	OVO	Scanning and tabulating voting device located at the precinct and used during early voting.
OpenElect Voting System	OVS	The Unisyn voting system submitted for certification testing.
Software Server	SS	Updates and validates voting device client software.
Tab Cluster	-	Tabulator, Tabulator Client, and Tabulator Reports applications and supporting hardware.
Transport Media	TM	USB device used by the system to transport election data.

1.0 INTRODUCTION (continued)

1.5 Test Specimen Description

The OVS is a paper ballot precinct voting system that uses touch screen and scan technology to scan and validate ballots, provides voter assisted ballots for special needs voters, and tabulates precinct results.

The OVS consists of 4 major components:

- OpenElect Central Suite (OCS) System with Ballot Layout Manager, Election Manager, Election Server, Tab Cluster and the Software Server.
- OpenElect Voting Optical (OVO)
- OpenElect Voting Interface (OVI)
- OpenElect Voting Central Scan (OVCS)

The following Linux OS versions were used during the penetration security scans:

- OVI Linux OS version 2.2
- OVO Linux OS version 0.6.01
- OVCS Linux OS version 0.1.8
- OCS Linux OS version 0.0.99

*All version numbers are pre-release versions used during testing. Any changes to these pre-release versions will be analyzed to determine the impact of the changes to the security testing and regression/retest will be performed if necessary.

The following application versions were used during the penetration security scans:

- OVI application version 0.3.9
- OVO application version 0.6.9
- OVCS application version 0.2.1
- OCS application version 0.5.10

*All version numbers are pre-release versions used during testing. Any changes to these pre-release versions will be analyzed to determine the impact of the changes to the security testing and regression/retest will be performed if necessary.

The equipment used during the penetration security scans is listed in Table 1-2.

1.0 INTRODUCTION (continued)

1.5 Test Specimen Description (continued)

Table 1-2 Security Scan Equipment

Equipment	Manufacturer / Model	Hardware Specifications	Service Tag	Soft ware used during scans
Laptop Used as the main scanning tool	Dell Latitude E5500	Processor: Intel Core2Duo T7250 2.0Ghz Memory: 2x 1GB 800Mhz RAM Hard Drive Capacity: 120GB	C9448J1	Backtrack Nmap/Zenmap Nessus
PC 1	Dell Optiplex 755	Processor: Intel Core2Duo E7200 2.53Ghz Memory: 4x 1GB 800Mhz RAM Hard Drive Capacity: 250GB (Mirrored)	G5HW3J1	All OCS applications
PC 3	Dell Optiplex 755	Processor: Intel Core2Duo E7200 2.53Ghz Memory: 4x 1GB 800Mhz RAM Hard Drive Capacity: 250GB (Mirrored)	D5HW3J1	OVCS
OVI	Unisyn	Security scans, bios resets, physical break-ins	UNI150004	
OVO	Unisyn	Security scans, bios resets, physical break-ins	UNI000003	

2.0 EXECUTIVE SUMMARY

The OpenElect Voting System (OVS) has been determined to be a “Minor System” and has been determined to have a security categorization of “High”. Wyle determined OVS to be “Minor System” based on the fact that it functions in a closed network with three major interfacing components that do not depend on any external systems. The determination of a “High” security category is based on the definitions published in FIPS PUB 199 for potential impact. “The potential impact is HIGH if – The loss of confidentiality, integrity, or availability could be expected to have severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.”

The Test Group team at Wyle Laboratories prepared this Security Assessment Report in accordance with U.S. Election Assistance Commission (EAC) and National Institute of Standards and Technology (NIST) guidance. The results captured within this report are intended to be an addition to any existing Risk Assessments performed outside of the certification process. It summarizes the risks associated with the vulnerabilities identified during the system’s Security Test & Evaluation (ST&E), vulnerability scans, audits, limited penetration testing and any other risk assessment activities. All results were analyzed to provide the certifier and system owner with an assessment of the physical, operational, and technical controls implemented to protect the confidentiality, integrity, and availability of the system.

The following are major security issues discovered during initial security testing:

- The BIOS on the OCS and OVCS are not password protected.
- Hard Drives on the OCS and OVCS are not encrypted.
- Although the files on the TM were encrypted, the TM drive itself was not encrypted

2.0 EXECUTIVE SUMMARY (continued)

NOTE: These issues were reported to Unisyn at the conclusion of the security test. Unisyn updated the user documentation to provide clear instructions on the BIOS configuration for both the laptop and desktop BIOS firmware used during testing. A regression test was performed on both the laptop and desktop configured as documented by Unisyn. Attempts were made to "backdoor", "by-pass" and defeat the BIOS password on both the laptop and desktop. Those attempts were unsuccessful. Additionally, new Linux OS builds were released after the security tests were complete. Linux OS version 0.7.0 was released and Wyle performed regression scans of the new builds and found no new issues to report.

3.0 TEST OBSERVATIONS AND RECOMMENDATIONS

3.1 Scans

The OCS, OVCS, OVI and OVO were each scanned multiple times using Nmap and Nessus. Every component of the system was initially scanned with Nmap to verify ports, protocols and services. The Nmap scans also provided verification for ports later discovered with Nessus scans. They also provided the testing team insight to any additional penetration tests that could be conducted. The Nessus scans provided vulnerability assessment for each component of the system. The components were scanned with both leveraged and unleveraged account information. Additionally, both 'root' and 'administrator' accounts were used to verify permissions and remote access.

The OCS scans included scans of the system with ES, SS, Tabulator and Tabulator Client. Unleveraged scans provided no pertinent information. Scans conducted with 'root' credentials resulted in the same findings as the unleveraged scans. The leveraged scans using 'administrator' credentials provided one (1) high and one (1) medium finding;

- **High** (CentOS: RHSA-2009-0256) The remote CentOS system is missing a security update which has been documented in Red Hat advisory RHSA-2009-0256.
- **Medium** (Apache Tomcat servlet/JSP container default files) Example JSPs and Servlets are installed in the remote Apache Tomcat servlet/JSP container.

The High finding deals with an incorrect browser package being installed (firefox-3.0-0.beta5.6.el5.centos). This vulnerability can be mitigated down because the system in normal operation would not be connected to an open network with external access.

Recommendation: This package should be uninstalled if not needed or appropriately updated.

The Medium finding could result in a cross scripting attack but this is not likely unless the system is connected to an open network. See the following section concerning ports for added reasoning of this exploit.

Recommendation: These files should be removed if unneeded. They may themselves contain vulnerabilities such as cross-site scripting issues.

3.0 TEST OBSERVATIONS AND RECOMMENDATIONS

3.1 Scans

Two minor findings were noted in the OCS Scans. These were the omission of two (2) ports from the ports and services list provided by the vendor, were discovered during scans. These were ports:

- ipp (631/udp) This is normally standard 'Internet Printing Protocol'. The only issue with this finding is the port is not documented by vendor.
- ajp13 (8009/tcp) This is the standard port for apache-tomcat Connector. Being the default port in conjunction with the medium finding could normally be an issue for a system. A system with this combination of findings on a network could face a cross scripting attack. The open network does not have to have access to the internet for this attack to take place.

NOTE: The scans of SS with 'root' credentials on the initial software version leveraged were successful. During regression testing of the new software version 'root' credentials could not complete the scans successfully.

The OVCS unleveraged scans provided no pertinent information. Scans conducted with 'root' credentials resulted in the same findings as the unleveraged scans. The leveraged scans using 'administrator' credentials provided one (1) high finding;

- High **(**CentOS : RHSA-2009-0256) The remote CentOS system is missing a security update which has been documented in Red Hat advisory RHSA-2009-0256.

One other minor finding was the omission of port ipp (631/udp) 'Internet Printing Protocol' from the documentation provided by the vendor.

The OVI and OVO scans were attempted while the system was in different stages of initialization. The first attempt was performed on system startup. The second scan was performed with the system in an operational state. Other scans were performed when an election was being loaded and software was being updated. All scans attempted failed to complete and did not provide any pertinent information. Scans performed while loading elections provided error messages and stopped the process.

3.2 Group 1 Tests

This group of tests was run on the OCS, OVCS, OVI and OVO. Both the desktop and laptop version of the OCS were tested. The following types of tests were run:

- File permission checks on critical files/apps/directories
- Account checks (privileges, password)
- Bios – order change, backdoor, potential MBR attack on crypto
- Xwindows – bypass/ short cut desktop
- Password policy enforcement
- Injection attacks (overflows)

These tests were done both manually and with the use of scripts. The ST&E scripts used were; unisyn_ste.sh (used on the OCS) and unisyn_ste_a.sh (used on the OVCS). Both systems passed all tests with the exception of the Bios test. The OCS and OVCS both did not have the Bios password enabled and to further complicate the issue the hard drives on both of the systems are not encrypted. This vulnerability allowed the systems to be fully compromised in less than 5 minutes.

3.0 TEST OBSERVATIONS AND RECOMMENDATIONS (continued)

3.2 Group 1 Tests (continued)

3.2.1 Group 1 Recommendation

Wyle recommends the BIOS password be enabled and the system boot straight to hard drive. If practical encrypt the OCS and OCVS hard drives. If implementing encryption of hard drives affects performance or causes issues with the software application then at a minimum the BIOS passwords need to be set, boot directly to hard drive, and ensure detection of physical tampering to system will be obvious.

NOTE: Unisyn did provide instructions to enable the BIOS password. Please see the Executive Summary of this document for more details.

The security test team attempted to perform a file permissions and account checks test by accessing the OVO and the OVI . Access could not be gained; therefore, the systems were given a "pass" rating for this test. The security team also spent several hours attempting to "bypass", "defeat", and "backdoor" the BIOS password. The time taken to attempt this and the risk analysis performed on this process deems it highly unlikely this type of attack would be successful. The Xwindows test was not scheduled for these two systems. The OVI and OVO passed all tests within this and other groups. The OVI and OVO are primarily assessed by review of the SCAP documentation provided by the vendor and other tests performed by Wyle.

3.3 Group 2 Tests

This group of tests was run on the OCS, OVCS, OVI, OVO and TM. Both the desktop and laptop version of the OCS were tested. The following types of tests were run:

- Attacks from TM
- File manipulation
- OCS installer
- Only Unisyn type hardware (TM only)
- Clean or cleared (TM only)

The OVI and OVO passed the Attacks from TM test. All attempts were ineffective. The OCS and OVCS failed on the Attacks from TM test based on the fact that the test script file could be copied into their home directory and ran. It is noted that the script could not be run from the TM or the Desktop. It should also be noted that the script could only run within the confines of the accounts' permissions. The assumption for failure is based on the opinion that a better written script could possibly be more effective and cause damage because of the lack of BIOS password protection.

OCS and OVCS passed the File Manipulation test with concern. The build and configuration of the system software protect against this in normal operation, but the BIOS password not being enabled could allow unlimited access for file manipulation. The TM passes with concern. The files on the TM are encrypted but the drive itself is not. Access to the TM itself can lead to several things (e.g. data corruption, data thief). The OVI and OVO were not scheduled to be subjected to this test because previous tests demonstrated the access at this level could not be gained within the scope of this testing.

NOTE: Unisyn did provide instructions to enable the BIOS password. Please see the Executive Summary of this document for more details.

3.0 TEST OBSERVATIONS AND RECOMMENDATIONS (continued)

3.3 Group 2 Tests (continued)

The OCS and OVCS pass with concern on the OCS Installer test. The OCS installer program normally functions properly but the unprotected BIOS could lead to manipulation of this program. Manipulation of the installer program could have devastating effects on the system.

NOTE: Unisyn did provide instructions to enable the BIOS password. Please see the Executive Summary of this document for more details.

The TM passes on the 'only Unisyn type' because the systems only recognize that specific hardware. On the clean or cleared test the TM passes with concern. The OVS components check and clean the TM and only allow it to function within the correct parameters. Example, adding a file to the TM after a closed election is loaded throws an exception. One issue does remain; hidden files bypass all checks by the OVS components. This is a minor point due to the fact that both OCS and OVCS implement adding drives by "mounting" only.

3.4 Other Tests

These tests were run on the OCS, OVCS, OVI and OVO. Both the desktop and laptop version of the OCS were tested. The following types of tests were run:

- Test Verification process
- Election day network connectivity
- Hardware connections (USB, LAN)
- Data corruption
- Data validation
- EM to OVCS control
- Hidden key check

All four components passed the Test Verification Process test. This test was a review of the process performed earlier by Wyle in another test area. The OVI and OVO were tested for Election Day Network Connectivity and passed. Both systems functioned properly and could not be manipulated. All four components passed the Hardware Connections test. This test was aimed at the USB interface and LAN connection.

The OCS and OVCS were tested for data corruption and passed with concern. Both the systems could not be manipulated under normal operations. However, with the unprotected BIOS could easily make data corruption possible. The OCS was tested for data validation and EM to OVCS communication control and passed both tests.

NOTE: The "Built on OS check" listed in the test matrix in Table 3-1 was not performed on the OVO and OVI. After risk analysis this test was deemed ineffective and was not attempted. Unisyn did provide instructions to enable the BIOS password. Please see the Executive Summary of this document for more details.

3.0 TEST OBSERVATIONS AND RECOMMENDATIONS (continued)

3.4 Other Tests (continued)

Table 3-1 Unisyn OVS Security Test Matrix

TEST	EM/ES	Tab Cluster	OVI	OVO	TM	EM/ES	Tab Cluster	OVI	OVO	TM
Ports, Protocols, Services Scan w/ Nmap	X	X	X	X		P	P	P	P	
Ports, Protocols, Services Scan w/ Nmap (leveraged)	X	X	X	X		P	P	P	P	
Vulnerability Scan w/Nessus	X	X	X	X		P	P	P	P	
Vulnerability Scan w/Nessus (leveraged)	X	X	X	X		P	P	P	P	
File permission checks on critical files/apps/directories	X	X	X	X		P	P	P	P	
Account checks (*privileges, password*)	X	X	X	X		P	P	P	P	
Test Verification Process	X	X	X	X		P	P	P	P	
Attacks from key - TM	X	X	X	X		F	F	P	P	
File manipulation	X	X			X	C	C			C
OS Tests										
Bios - order change, backdoor, potential mbr attack on crypto	X	X	X	X		F	F	P	P	
Xwindows - bypass/short cut desktop	X	X				P	P			
password policy enforcement	X	X	X	X		P	P	P	P	
election day network connectivity			X	X				P	P	
Hardware connections (usb, lan)	X	X	X	X		P	P	P	P	
Application Tests										
Injection attacks (overflows)	X	X	X	X		P	P	P	P	
OCS Installer	X	X				C	C			
Data corruption - view other election	X	X				C	C			
Data validation - Absentee ballots check -?	X					P				
EM to OVCS control	X					P				
Build on check, OS	X	X				X	X			
Hidden key check			X	X				P	P	
TM Tests										
Only Unisyn type					X					P
Clean or cleared					X					C

Legend

To be tested marked with X

Post test marked with grade

P - Passed

C - Pass with concern

F - Failed

4.0 INITIAL FINDINGS

This security assessment of the OpenElect Voting System (OVS) was performed in a hybrid Certification and Accreditation (C&A) / penetration test environment. Penetration tests were limited to plausible threats. Plausible threats were determined using three factors; access, time to perform, and difficulty. The test scenarios were created, times to execute actions were recorded as well as ease in which to execute the actions (i.e. action was complicated/hard to execute). The tools and knowledge needed to execute the attacks were also taken into account. A risk assessment was performed on each of the tests in order to quantify the value of test and likelihood of the actual attack being executed.

4.0 INITIAL FINDINGS (continued)

Our overall impression of the OVS is that the system's software is very secure, the system is well configured and functions according to EAC standards. The OVI and OVO are almost impenetrable within the scope of this test. The only way the security team could access or compromise those two components would be physically detectable and therefore useless to an attacker. There are however three major areas of concern. These areas are listed below:

1. Build documentation for the OCS and OVCS do not state to assign a password to the BIOS. There also currently is no instructions/documentation stating to provide banding or seals on the OCS and OVCS. The lack of a password on the BIOS allows an attacker to change the boot order and boot the system to live media. This coupled with the lack of encrypted hard drives allows these two components to be totally compromised in only a few minutes. Not implementing banding or seals on the systems prevents the detection of an attempt to physically access the system. Physical access is required in order to clear the CMOS and reset the BIOS password.

2. The security categorization of "High" was primarily given to the OVS because it processes and handles voting data where the loss of integrity and availability could be severe. Hard drives on the OCS and OVCS are not encrypted. Best practices dictate that a high security categorized system should implement encryption of data at rest. In some applications encryption puts data available at risk and cause performance issues. With an encrypted hard drive even if the boot order is manipulated and a live media device runs it is harder for an attacker to compromise the system.

3. Most of the files/data transported on the TM are very well encrypted. However, the TM itself does not implement encryption. This allows anyone access to the TM and could lead to data corruption or data thief. Data corruption is easily compensated by the OVS system but compensating for this would increase the election processing time. The likelihood of the encryption used by the OVS being cracked is minimal therefore data theft is minimal. The fact that election files/data, readable or not, could possibly be shown to be outside of the secure, controlled voting system is not good. The perception is more damaging than the reality regardless of whether the files can be manipulated or not. Additionally the components of the OVS do not check for hidden files on the TM when cleaning or loading data. The OVS does control the mounting and checks for only authorized data on the TM so this issue is minimal but, perception is sometimes worst than reality.

5.0 CONCLUSION

After the initial security test findings were reported to Unisyn, they supplied Wyle with updated instructions to enable the BIOS password on all OCS and OCVS hardware configurations. Wyle followed these instructions as written and a regression test was performed on both the laptop and desktop configured as documented by Unisyn. Attempts were made to "backdoor", "by-pass" and "defeat" the BIOS password on both the laptop and desktop. Those attempts were unsuccessful. Additionally new Linux OS builds were released after the security tests were completed. Wyle performed regression scans of the new builds and found no new issues to report. In addition, security tie straps were provided and documented for the OCS and OCVS hardware. The security tie straps and their documented installation were analyzed and found to be adequate.

Wyle has determined the Unisyn OVS, Version 1.0, to be compliant with the security requirements of the EAC 2005 VVSG.