Global Information Assurance Certification Paper

Auditing a FIX32 Supervisory Control and Data Acquisition System: An Administrator's Perspective

GSNA Practical Version 2.1

Author: Peter Tolen
April 4, 2003

Table of Contents

Figures

Abstract: This paper is an audit, from the perspective of a system administrator, of a supervisory control and data acquisition (SCADA) system running on a TCP/IP network on the Microsoft Windows 2000 operating system. The SCADA system software is Intellution FIX Version 7.0. This paper covers the system identification, evaluation of system risks, development of an audit checklist, and a discussion of the audit results.

Assignment 1 – Research in Audit, Measurement, Practice and Control

Identify the System to Be Audited

The subject of this audit is a supervisory control and data acquisition (SCADA) system used to provide supervisory control and monitoring capability for a number of physically dispersed processing plants. Due to the sensitive nature of information generated during the audit of production SCADA systems, the results shown in this audit were created by auditing a laboratory/test SCADA system using similar hardware and software as the production system. The SCADA system configuration and network topology of the laboratory/test system are similar enough to provide useful audit results, yet different enough to prevent the release of any information that could be used to compromise a production SCADA system.

The SCADA system being audited was broken down into distinct components and sub-components because of distinct differences in their security objectives. The major components are:

Control Network

The control network is an Ethernet network consisting of commercial-off-the-shelf routers, switches, dedicated serial modems, and software from various manufacturers. Communications is provided by a combination of private hard lines from 56K serial links to OC-3 fiber optic links, and dedicated leased T1 links. The SCADA nodes communicate using the Microsoft NetBEUI protocol. File access between nodes uses Microsoft file sharing. The only external connection to the control network is a one-way serial link to a data server owned by the company accounting department. The control network is otherwise not connected to the company wide area network or the Internet.

SCADA Servers and View Nodes

The SCADA servers and view nodes consist of variety of Intel x86 computers including Dell Dimension, Optiplex, and Poweredge computers. SCADA servers run the FIX data acquisition and management software and operate as Front-End-Processors (FEP's) directly communicating with the field devices described below. View nodes run the FIX Human-Machine Interface (HMI) and provide the interface between the plant operators and the plant equipment, and PlantTV

nodes provide a view-only capability to personnel who need to monitor the plants but do not have operator requirements. SCADA system application servers process data and provide input to the SCADA control programs.

The underlying operating system running the SCADA system software and applications is a combination of Windows 2000 server, Windows 2000 Professional, and Windows NT Workstation depending on the role of the node. Identification and Authentication to the OS is provided by Windows domains.

The SCADA system databases are housed on both the view nodes and the SCADA servers. The data bases on the SCADA nodes are the real-time database (RTDB) and the configuration database. The databases housed on the view nodes are the picture databases.

The real-time database is a distributed database system using a FIX proprietary file format. The RTDB is a distributed database that maintains the real-time status of the system, including real, analog, and Boolean records, engineering values, data generated by internal application programs, and data entered by operators. The RTDB is distributed in the sense that each plant houses a "sub-master" SCADA node that receives data from local RTU's and PLC's and provides local control logic for that plant. The RTDB is referred to in the FIX documentation as the process database.

The picture database is a set of proprietary FIX files that define the view screen designs used by the HMI to provide the user interface to the SCADA system. The picture database contains the graphical images (pictures) that SCADA system users interact with. The pictures contain graphic objects (buttons, scroll bars, progress indicators, etc.) used by the SCADA system to map operator actions to control and monitoring points and applications used by the SCADA system.

The configuration database is a set of configuration files stored on each SCADA node, with a master set stored on a central file server. The configuration database contains the SCADA system configuration information. It is queried by FIX at system startup and provides the data necessary to map applications, control points, logging files, names of equipment instances, names and numbers of RTU's and PLC's, and names and locations of external information.

The configuration and pictures files are stored on a central computer and accessed by the SCADA and View nodes. Access to shared FIX files between nodes is through Microsoft file sharing and is controlled by the security features of Windows NT/2000.

The Human-Machine-Interface (HMI) runs on the view nodes and is the interface between personnel who monitor and control the plant operations and the SCADA system. The HMI for the system being audited is the Intellution FIX32 Version 7.0

View module. Identification and authentication to the HMI is provided by a built-in FIX security module.

Field Devices

The field devices consist of transducers and sensors, remote terminal units (RTU's), and programmable logic controllers (PLC's) located in the plants being monitored and controlled. The sensors and transducers receive actual system values (e.g. pressure, current, voltage) over copper wire and convert those values into analog voltage or current signals which are communicated to the RTU's and PLC's over copper wire. The RTU's and PLC's convert the analog electrical signals into digital information and transform the information into engineering units that the SCADA system software uses for display, storage, and control logic. The RTU's and PLC's communicate with the front end processor (FEP) device drivers through serial links using the Modbus Serial communications protocol.

Evaluate Risk to the System

The primary threats to the SCADA system being audited are human-caused including internal hackers, careless operators, and disgruntled employees, environmental such as loss of power, loss of HVAC, or structure fire, and natural such as brush fires, lightning, or floods. The risks to the SCADA system being audited will be evaluated on a per component basis based on the Confidentiality, Integrity, and Availability requirements for those components, and the associated threats.

Control network

The confidentiality requirements of the data transmitted over the control network between SCADA nodes and View nodes ranges from Low to High. Data such as control commands and equipment status tend have low confidentiality requirements because such data is transitory in nature and knowledge of that data by unauthorized persons has little potential for impact. It can be argued that confidentiality of control data is critical because an attacker could monitor such signals and determine how the SCADA system works. In such a scenario the attacker could then insert false signals to try and perform his or her own operational action on the plant equipment. However, because the control network has no direct connection to any public network, the risks from such an attack are considered low. Since physical access to the control network infrastructure is necessary to perform such an attack, and that access would provide access to the plant equipment itself, it is more likely that physical damage to the plant equipment would be attempted.

The data with high confidentiality requirements are the credentials used to login to the domains and View nodes, and the SCADA network topology itself. The primary threat to the confidentiality of the control network data is internal, and

includes anyone with access to the SCADA network infrastructure (switches, nodes, etc.). Having access to the SCADA network infrastructure could allow someone to plug unauthorized computers or monitoring devices into the SCADA network in order to collect data or perform network discovery. The most likely insider threat is from operators and maintenance staff who have unrestricted access to the plants.

The Integrity requirements of the control network and the data transmitted on it are considered high. If control signals being transmitted from View nodes to SCADA nodes and from SCADA nodes to field devices becomes corrupt or are altered, mis-operation or non-operation of a device could occur. This could lead to personnel safety problems, equipment damage, or operational instabilities. The primary threats to the integrity of the data transmitted on the control network are noise, abraded cables, and mislabeling of connections. Another threat is intentional or unintentional corruption or modification of router information by employees or intruders.

Availability requirements of the control network are considered high. Although the plant equipment is generally capable of operating safely without the SCADA system, the financial and operational consequences of such operation can be significant. Long-term disruption of the SCADA network could cause additional personnel requirements for manual operation of the plant equipment. The major threats to the availability of the control network are deliberate damage to network infrastructure, equipment failure, flooding, fire, and power failures.

SCADA Servers and View Nodes

The confidentiality requirements of the data housed on the SCADA nodes varies with the type of data. Operational data in the RTDB has low confidentiality requirements because knowledge of that data provides no useful information to a potential attacker. The confidentiality requirements of the configuration database, picture database, and underlying operating system configuration files are high. Attackers or malicious employees could use that information to provide information required to gain further access into the SCADA system. The most likely threat to the information is from operators and maintenance personnel who through curiosity or malicious intent attempt to access the information in order to explore, modify, or damage the SCADA system.

The integrity requirement of all the data stored in the SCADA and view nodes is high. Corruption or alteration of data in the RTDB can result in equipment misoperation or non-operation and lack of knowledge of the true current state of the plant equipment leading to spurious alarms or alarms not occurring when they should. Either case could present personnel safety issues or cause equipment damage.

The accuracy of the configuration database information is critical to the operation of the entire SCADA system. Alteration or corruption of the configuration

database could cause parts of, or the entire, SCADA system to either not start at all, or to start in an unstable state. If the system did not start at all then manual operation of the plant would be required until a backup configuration database could be loaded and restarted. If the system started in an unstable state the potential exists for mis-operation of equipment or incorrect alarming leading to possible safety issues or equipment damage.

The availability requirement of the SCADA nodes and the associated data and information is considered high. The SCADA nodes are the "brains" of the SCADA system. Without the SCADA nodes operating, the front-end processors cannot communicate the information being transmitted to them from the field devices to the View nodes. In addition, the SCADA nodes control the I/O between the field devices and the SCADA applications so if the SCADA nodes are lost none of the SCADA applications will operate properly. Basically, loss of the availability of the SCADA nodes will bring down the system and operators must resort to manual means until the SCADA nodes are restarted. The major threats to the SCADA nodes are loss of power, loss of climate control, and physical damage to the building housing the SCADA nodes.

The availability requirement for the View nodes is considered low to medium. Although View nodes are used by operators to control the plant, in the case of the FIX system, SCADA nodes can be used as View nodes in an emergency. The risks to the plant is not high since the SCADA nodes will still be maintaining control over the system while View nodes are being restored. The main threats to View nodes are power failure, operator error, malicious actions such as rebooting the node from a floppy disk in order to gain access to the network, and failure of climate controls.

Field Devices

Except for the configuration settings on the RTU's and PLC's, the confidentiality requirement of the data processed by field devices is low. The data is transitory in nature and is only useful for a very limited time period. Because the field devices do not use Ethernet communications protocols, gaining access to the configuration files requires a local connection to the RS-232 configuration port on the devices. Protecting the confidentiality of the data on field devices is accomplished with appropriate physical security such as locking racks and limited access equipment rooms.

Integrity requirements for field devices are considered high because they are the primary link between the controlled process and the SCADA system. Corruption of the configuration settings on a field device could cause the device to stop responding, or worse, could cause the device to operate a piece of equipment in an unpredictable way. Such mis-operation has the potential to cause a threat to personnel safety and equipment damage.

Availability requirements for field devices are high. Loss of a single field device would not have devastating impacts unless that device is used to control a critical process or equipment instance. Total loss of a set of field devices would have significant impact and would require manual operation of the equipment those devices control.

Current State of Practice

Current state of practice:

There are currently very few resources available for developing security control objectives and audit checklists specific to SCADA systems. My research consisted of multiple web searches of many sites, including http://www.sans.org, FedCIRC, CERT, Department of Energy, the Institute of Electrical and Electronics Engineers, the National Institute of Standards and Technology, Usenet, and various SCADA vendor's web sites and user support groups. I also searched at amazon.com for books on SCADA systems. I was surprised at the lack of references for SCADA and in particular SCADA security. I joined the Process Control Security Requirements Forum in order to access information on their web site, and signed up on the Intellution web site in order to gain access to the FIX knowledge base. The best resources for developing security objectives for the SCADA system were the engineers and administrators who develop and maintain the SCADA system in the company being audited, and the FIX user manuals. The SCADA expert's average experience of over 20 years in SCADA operation, including design, development, and maintenance of SCADA software and hardware provided much valuable experience based information on the risks associated with securely operating the SCADA system. The suggestions for security settings found in the FIX documentation led to insights into how and why those settings were suggested and what risks they were meant to mitigate.

Most of the information that I did find was very general in nature and was applicable to most computer systems and networks, not SCADA in particular. One of the most discouraging aspects of the research I did on SCADA security objectives and controls was the sense that many of the white papers and presentations being written and given at conferences is self-serving. That is to say the people giving those presentations and writing those white papers tend to also be selling SCADA security audits. This bias may have a tendency to make those companies who should be considering security audits feel that the authors and presenters, instead of actually trying to raise awareness about security, are engaging in hype in order to increase sales.

There were, however, a number of white papers and presentations located on various web sites that contained enough general suggestions and corroboration that I was able to the general information from those sources along with internal documentation such as guidelines and security plans to develop a set of security objectives and a checklist for the particular system being audited. By combining

the general guidelines I found at http://www.oea.dis.anl.gov/documents/21StepsBooklet.pdf with the specific experiences of the SCADA experts, along with the suggestions for security settings found in the FIX documentation I was able to build a set of security objectives for general SCADA systems and a specific set of audit checklist items for the SCADA system being audited. Some of the references I used for this audit were either internal company documents, system documentation, or from web sites that required that I register or receive authorization. I had to register for the Intellution web site in order to get access to FIX White Papers, and I had to request a membership in the NIST Process Control Security Requirements Forum to get access to PCSRF papers. I did not include URL's for those web sites in the references section.

Improvements to Current Methods and Techniques

Until recently the prevailing wisdom regarding SCADA seems to have been that SCADA systems are secure because of their use of obscure or proprietary protocols, proprietary hardware and operating systems, and their isolation from external networks. Only in the last two or three years has the control industry and the SCADA user community recognized the importance of securing process control systems. As more companies have been linking their control systems to their accounting, inventory, and marketing systems in an effort to streamline business processes, interconnectivity to external networks has become more prevalent. In addition more and more SCADA vendors are using open communication protocols and commercial-off-the-shelf hardware and software components in their systems.

Because of a lack of awareness of the necessity of security in SCADA systems, or possibly a lack of interest, security auditing of SCADA systems appears to be in its infancy. Magazine articles and technical papers on SCADA security previous to the year 2000 are difficult to find. Consequently, there is very little solid information available regarding auditing techniques specific to SCADA systems. The current practice seems to be the use of standard network and operating system auditing tools such as network scanners, war dialers, and vulnerability scanners, and the application of "best practices" standards to SCADA systems. Some of these standards, such as keeping servers patched, and minimum password lengths, do not always apply to SCADA systems.

SCADA system vendors appear to have recognized the importance of some aspects of security in their systems for quite some time, especially in the areas of alarming, logging, and least privilege. However, the SCADA vendors do not seem to have recognized the importance of determining and establishing baseline security settings for the operating systems and communications protocols used by their systems. In addition, the use of scanning tools, especially vulnerability scanners, can cause very adverse impacts to SCADA system operations.

Suggested improvements to current auditing practices and techniques include:

- Research into the best automated tools, and their settings, to use on SCADA networks in order to cause no disruption to operations,
- SCADA system vendors determining and freely publishing appropriate security settings for the underlying OS used on their systems,
- SCADA system vendors implementing programs to test and validate security patches on their systems,
- More free exchange of SCADA system audit tools and techniques among the SCADA security consulting community.

Assignment 2 – Create an Audit Checklist

The checklist I developed is primarily based on high level security objectives found in the whitepaper 21 Steps to Improve Cyber Security of SCADA Networks. Each high level objective has one or more verification objectives used to assure that the high level objective has been met. This checklist is focused on the specific actions that can be taken to protect the SCADA network and underlying infrastructure.

Due to the broad scope of the general SCADA security guidelines that I found, including managerial, operational, and technical control guidance, I decided to limit the audit checklist to protecting the control network, limiting the ability of operators to SCADA functions only, and protecting the critical files and databases used by the SCADA system from unauthorized access.

Some of the subjective tests listed here require reviewing FIX configuration settings. Prior to commencing the audit, have the SCADA administrator print C:\FIX32\Local\View.ini and run a FIX Security Report from the Security Configuration Module.

Security Objective 1. Identify and remove or secure all connections to the SCADA network		
Audit Objective – Compliance Test – Reference	Expected Result	Risk
1-A. Verify that the system documentation includes identification of all necessary connections to the SCADA network. Subjective Test: Document Review of the SCADA System Security Plan Reference: 21 Steps to Improve Cyber Security of SCADA Networks	All external connections to the SCADA network should be documented, including: • Protocols used • Port numbers • Purpose of connections • Location of connection in the network topology	Connections to external networks cannot be adequately protected if SCADA admins and security staff are unaware of them.
1-B. Verify that only those connections that are documented exist. Objective Test: Use a laptop or handheld computer with a wireless card and a program such as NetStumbler to find undocumented wireless access points. Objective Test: Use a war-dialing tool against the phone exchange of the company to find undocumented dialup access points.	NetStumbler should report The war dialer should not find any modems on the system.	Undocumented and hence, unprotected external connections can be used for unauthorized access to the SCADA network and possibly used to cause malicious control actions or damage to the system.

Reference: 21 Steps to Improve Cyber Security of SCADA Networks		
1-C. Verify that all necessary connections to the SCADA system are protected by firewalls or other suitable means. Objective Test: Connect to the Corporate network and use a network scanner such as nmap to perform a SYN Stealth scan of the IP address space of the SCADA network. Objective Test: Connect a laptop to the network on the external interface of the firewall and use nmap SYN Stealth scan to scan the firewall for open ports. Verify that only necessary ports are open. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	The nmap scan from the corporate network should report: *Nmap run completed -- XX IP addresses (0 hosts up) scanned in XX seconds.* The nmap scan of the firewall should report: *Interesting ports on (XXX.XXX.XXX.XXX)* *(The X ports scanned but not shown below are in state: closed)* *Port State Service* *XXX Filtered XXX* *Nmap run completed -- 1 IP addresses (1 host up) scanned in XX seconds.* Note: Results of second scan should correspond to documented connection requirements. (IP addresses and port numbers deliberately obscured)	Business partner networks and the corporate WAN should be considered un-trusted networks. Those networks should not be given unrestricted access to the SCADA network because the SCADA admins and security staff do not have any control over their security. Compromise of an external network connected to the SCADA system through an unprotected connection could compromise the SCADA network. Note: This SCADA network did not have any external connections and a firewall scan was not required.

1-D Verify that policies and procedures exist for routinely checking the SCADA network for undocumented connections. Subjective Test: Document review of the SCADA SSP. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	System documentation should identify at least: • How often to check for connections, • Tools required, • Syntax or settings required, • Who is responsible for checking, • How to respond if undocumented connections are found.	Lack of documented policies and procedures can lead to ad hoc actions, or no actions, being taken by security personnel. Without procedures in place for conducting routine checks, undocumented connections could be introduced into the SCADA system.
1-E Verify that IDS systems are implemented (both internally and externally) to identify possible intrusions. Subjective Test: Physical verification of IDS built into the firewall or a standalone IDS system connected to the network. Objective Test: Connect a laptop to the segment the IDS is connected to and use nmap or a similar tool to scan the network. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	The SCADA admin or security admin should log into the IDS system and prove that it is operating. The IDS system should report a suspected intrusion. Actual report will vary depending on the IDS system implemented.	There is always the possibility of compromise to the SCADA network from either external or internal threat. If the system is compromised, or attempts are made to compromise the system, it is important to be able to identify such actions so that mitigation can proceed as quickly as possible. Lack of the ability to identify such actions can lead to a system being compromised or attempts being made without anyone knowing it is happening, and not responding in a timely manner.

Security Objective 2 – Harden SCADA network against insider attack		
2-A Verify that all necessary network services are identified and documented. Subjective Test: Document review of the SCADA SSP. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	The system documentation should identify: • Required service • Port number(s) that service uses • Purpose of service	If required services are not identified in the system documentation it is likely that default operating system configurations will be implemented because SCADA admins are not certain which services are necessary and may be unwilling to disable network services fearing loss of SCADA functionality.
2-B Identify network services running on SCADA servers and view nodes. Objective Test: Connect to the SCADA network and use a network scanner such as nmap to perform a TCP connect scan or a SYN stealth scan of the IP address space of the SCADA network. Make sure that OS detection is not enabled due to the possibility of crashing a SCADA device. If the SCADA administrators have a preferred scanning tool that they use regularly, have them use that tool.	Only those network services identified in the system documentation should be found running. The nmap scan should report for each node: *Interesting ports on (XXX.XXX.XXX.XXX)* *(The X ports scanned but not shown below are in state: closed)* *Port State Service* *XXX Open XXX* *Nmap run completed -- X IP addresses (X hosts up) scanned in XX seconds.*	Leaving unnecessary network services running exposes the system to the risk of someone using those services to compromise the system. It also imposes a greater burden on SCADA admins to apply appropriate patches since they must use a blanket patching policy in order to not miss anything.

Reference: 21 Steps to Improve Cyber Security of SCADA Networks	*Note: Results of scan should correspond to documented requirements.*	
2-C Verify that unauthorized equipment cannot be connected to the SCADA network. Objective Test: Plug a laptop computer into an open port on one of the SCADA network switches and use a packet analyzer (Windows 2000, Ethereal) set in promiscuous mode to "sniff" packets off the network. Or, use nmap to perform a ping sweep on the network. Reference: Ethernet Security, Safety Relies on Common Sense Networking, Jim Montague, Control Engineering, March 1, 2001	The nmap ping sweep should not show any results. The packet analyzer should not be able to see any network packets or communicate with the SCADA network in either case.	A malicious insider who can connect a computer to the SCADA network can use it to gain information about the system, modify files if they are not appropriately protected, and possibly shut down the system.
2-D Verify that SCADA view nodes cannot be booted from removable media such as CD or floppy disk. Objective Test: Attempt to boot a view node with a CD or a floppy disk. Reference: iFIX Whitepaper, The Fix Security System, 01/11/98, Al Chisholm	SCADA view nodes should not have removable media devices installed in them. If they do, they should be disabled as boot devices in the BIOS. The node should not boot from a floppy or CD, it should always boot from the hard disk.	Since view nodes are just Windows workstations, unauthorized use of a floppy or CD to reboot a view node can give a malicious user access to all files on the node. Those files include the SAM database and any SCADA configuration files on the view node. Such information can be used to gain further access into the SCADA system.

2-E Verify that Windows Null sessions are disabled. Objective Test: Use a tool such as Cerberus Internet Security scanner or attempt to initiate a null session by opening a Windows command prompt and using the command: `net use \\scadaserver\ipc$ "" /u:""` Reference: Hacking Exposed Windows 2000: Network Security Secrets and Solutions, J. Scambray and S. McClure.	Windows should generate the error message: "System error 5 has occurred. Access is denied"	In the event that an unauthorized person does gain access to the SCADA network, they should not be able to initiate null connections to SCADA servers. Such connections can be used to get information allowing further access into the network.
2-F Verify that NT authentication does not use NTLM authentication. Subjective Test: Review the settings in Control Panel->Administrative Tools->Local Security Settings->Security Options Reference: Hacking Exposed Windows 2000: Network Security Secrets and Solutions, J. Scambray and S. McClure.	The option "LAN Manager Authentication Level" should be set to: "Send NTLMv2 response only" on Windows 2000 Windows NT should have a REG_DWORD entry called "LMCompatibilityLevel" set to 2 in the registry key: HKLM\System\CurrentControlSet\control\LSA	LM uses a weak encryption mechanism. If someone gains access to the network, they can use L0PHTCrack to sniff password hashes and try to crack them. By having administrator passwords, a malicious person would have complete access to the SCADA system and could do anything they wanted to.

Security Objective 3 – Maintain proper configuration management		
3-A Verify that configuration and change control management policies and procedures are adequately documented. Subjective Test: Document review of the SCADA SSP Reference: Company IT Security Policy Memorandum, *Configuration Management if IT Systems*	Policies and procedures should be available for review in the System Security Plan or Configuration Management Procedure.	Configuration management and change control are critical in SCADA systems. Not having formal policies or procedures in place to document changes to the system can lead to changes being made on the fly and the potential for losing control of the configuration of the SCADA system. Lack of control of the configuration can lead to an inoperable or unstable system without the knowledge necessary to bring it back to a stable state.
3-B Verify that patches are tested prior to deployment to the SCADA network. Subjective Test: Review the CM procedures in the SSP or the SCADA SOP. Objective Test: Using a patch management tool such as Microsoft MBSA or Harris STAT, scan a representative set of the SCADA servers and view nodes to identify the patch levels installed. Reference: Process Control Security	Test procedures should be clearly stated in the CM documentation. Patch levels should be consistent across the SCADA nodes. It is not necessary that they be current, however each system should be at the same level.	Applying patches to a SCADA system without adequately testing them can cause the system to crash. In addition, since Windows servers must be restarted after applying a patch, system shutdowns need to be appropriately scheduled with process users.

Requirements Forum, Gas Industry Security Issues		
3-C Verify that only the equipment listed in the system description/inventory is connected to the SCADA network. Objective Test: Connect to the SCADA network and use a scanning tool such as nmap to perform a ping sweep of the network. Compare the results to the documented equipment list. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	The number of hosts and their IP addresses identified should match the system documentation. Nmap scan results should be: *Host (xxx.xxx.xxx.xxx) appears to be up*, for each piece of equipment listed in the documentation. The total list of responding hosts should equal the total listed in the documentation.	Undocumented equipment connected to the SCADA network should be considered un-trusted because the SCADA admins do not have any control over the security of the equipment. Un-trusted equipment can be used to gain information or potentially control of the SCADA system.

Security Objective 4 – Provide Adequate Backup, Restore, and Disaster Recovery Capability		
4-A Verify that adequate policy and procedures exist in the SCADA system documentation Subjective Test: Documentation review Reference: 21 Steps to Improve Cyber Security of SCADA Networks	Policies and procedures should be available for review in the System Security Plan or Contingency Plan.	Lack of formal policies for backup, restore, and disaster recovery can lead to incomplete or nonexistent backups.
4-B Verify that backup and restore procedures are followed according to		If critical system files are not backed up and a critical file becomes corrupt, it

existing policy. Subjective Test: Physically verify that backup media exists in locations stated in procedures Objective Test: Using a test/development server, have the SCADA admin perform a system restore of critical configuration files. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	CD or tape backups should be found in the location(s) listed in the documentation for backup media storage. Configuration files should be fully restored and the SCADA system on the test server should start successfully.	can be virtually impossible to rebuild from scratch. Complete loss of SCADA functionality can result.

Security Objective 5 - Limit SCADA system to a single dedicated use		
5-A Verify that all necessary applications and software are identified and documented in the system description or SSP. Subjective Test: Review system documentation. Reference: Microsoft Whitepaper, Implementing Common Desktop Management Scenarios	Documentation should include: • The name and version number of each program installed on each view node and SCADA node • The purpose of the program	If required programs are not identified in the system documentation it is likely that default operating system programs, or unnecessary programs will be installed.
5-B Verify that SCADA view nodes and	The Add/Remove Programs window	Unnecessary or undocumented

other computers on the SCADA network do not have unnecessary software installed. Objective Test: Perform a software inventory of a SCADA view node using Program->Control Panel->Add/Remove Programs and list the installed programs. Reference: Microsoft Whitepaper, Implementing Common Desktop Management Scenarios	listing should match what is documented.	programs can lead to burdensome patching requirements and possibly incomplete patches due to a lack of knowledge of patch requirements. Systems with incomplete patches may be vulnerable to exploitation.

Security Objective 6 – Provide Adequate Physical Security for SCADA System		
6-A Verify that field devices are protected according to the SSP. Objective Test: Visit the plant floor and look for secured cabinets or equipment rooms. Attempt to gain access to the equipment. Reference: Securing Supervisory Control & Data Acquisition Systems, Pipeline and Gas Journal, July 2002, Abo Y. Saad	Cabinets and equipment rooms should be locked and keys should be secured.	Uncontrolled access to field devices (RTU's and PLC's) provides someone the opportunity to use the configuration port to gain knowledge about the system or reconfigure the field device. Reconfiguring a field device could cause unpredictable or inadvertent control actions to take place and could endanger personnel and equipment.
6-B Verify that SCADA and application	The SCADA computer room should	Uncontrolled access to the SCADA

servers are housed in a physically secured, environmentally protected location. Objective Test: Visit the central SCADA computer room where servers are housed and attempt to gain access. If possible, attempt some type of social engineering. Reference: Securing Supervisory Control & Data Acquisition Systems, Pipeline and Gas Journal, July 2002, Abo Y. Saad	be locked and have access restrictions in place. Anyone asked to provide access should inquire as to the necessity and the authority for access. Such requests should be reported to a supervisor.	computer room or the cabinets where the sub-master stations are located provides someone the capability to take any number of damaging actions, including shutting down the system. The consequences of the actions that someone could perform include destruction of equipment, theft, and malicious control activity.

Security Objective 7 – Provide Adequate Incident Response Capability		
7-A Verify that policy and procedures exist for incident response. Subjective Test: Document review of the SCADA SSP. Reference: 21 Steps to Improve Cyber Security of SCADA Networks	Documentation should include at a minimum: • What is considered a security incident • How users are to respond to suspected security incidents • Who is responsible for assuming command of incidents • How admins and security staff are to handle incidents	Without documented incident handling procedures, delays and disorganization can occur with loss of evidence and the potential for not completely repairing any damages caused by an incident.
7-B Verify that personnel have	Operations staff and other SCADA	Lack of training in how to recognize

adequate training to recognize and respond to a security incident. Subjective Test: Interview operators and maintenance staff regarding incidents. Example questions to ask include: If the alarming log reported that a view node stopped responding, what would you do? If someone saying they are an engineer from Intellution called you on the phone and asked you for your system password, what would you do? If a controlled device in the plant changed state, and you did not initiate a change through a control action, what would you do? Reference: 21 Steps to Improve Cyber Security of SCADA Networks	system users should provide appropriate answers to the questions. The answers should basically match what is in the incident handling procedures.	and respond to security incidents can lead to a lack of understanding by operations staff about what they are and how to respond to them. This can result in incidents happening and not being recognized, especially social engineering incidents.

Security Objective 8 – Provide auditing and alarming capability, including provisions for traceability and accountability		
8-A Verify that the SCADA system logs	Events reported in the SCADA log	SCADA system controls equipment

all control events in such a way that actions are linked to program modules, applications, and recipes. Subjective Test: Review SCADA system event logs for such entries. Reference: Company SCADA System Experts	file or on the logging printer should show the name of the module, application, or recipe that caused an action to occur. Event logs should include: • Requested action • Name of module or program initiating the action • Result of the action • Exact date and time of the action and result	based on both SCADA recipes and custom applications. It is important to be able to trace control actions to initiating events so that if troubleshooting and/or process incident investigations can determine the causes of improper, accidental, or inappropriate control actions. Lack of capability to trace actions to specific components of the SCADA system can make it impossible to correct problems that may occur, or make it possible to determine the cause of an incident.
8-B Verify that the SCADA system logs all control actions taken by operations personnel. Objective Test: Have an operator initiate a safe control action such as changing a limit setting on a controlled device. Verify the log entry. Reference: Company SCADA System Experts	As the operator initiates the control action, the SCADA system log should immediately show an entry for that action. The entry should include: • Requested action • Name of user initiating the action • Result of the action • Exact date and time of the action and result	This is both a security and safety issue. Being able to track actions taken by operators provides the capability to determine if malicious activity is taking place or if inadvertent control actions are taking place due to operator error.
8-C Verify that security logging for the Windows OS is enabled. Minimum settings should include: • Unauthorized access to critical		Even though the underlying Windows operating system and network should be protected from unauthorized access, it is always possible that someone could gain that access. If someone gains unauthorized access to

SCADA and OS configuration files, • Fix and Windows System Stop/Start, • Failed and successful logins, including network logins Objective Test: Have someone with access to the Windows shell or with a network connection attempt to log into a SCADA server or view node from the network. Objective Test: Have an unprivileged user attempt to access a SCADA configuration file. Reference: iFIX Whitepaper, The Fix Security System, 01/11/98,Al Chisholm	The failed login attempt should be shown in the Windows Security Event Viewer as event number 529 "Unknown username or bad password" The access attempt should be shown in the Windows Security Event Viewer as event number 577, Privilege Use, Failure	the system and to the Windows operating system his or her actions can go undetected unless security logging is enabled.
8-D Verify that the SCADA system logs FIX security events. Objective Test: Attempt to log into FIX with a bad username/password pair. Objective Test: Attempt to access a FIX module that is not available on a view node. Reference: Intellution White paper, Validation Guide for SCADA/HMI Applications	FIX should log the event as "SECURITY VIOLATION: to login to FIX from node XXXX by user NNN" FIX should log the attempt in the day log as "SECURITY VIOLATION: XXX access to APPLICATION FEATURE XXX"	The SCADA system security logs are the first line of defense in detecting possible malicious activity. Not having security logging enabled could prevent the detection of authorized users attempting to gain unauthorized access to the SCADA system. By not detecting such activities it is not possible to stop it.

Security Objective 9 – Protect critical system files from unauthorized access.		
9-A Verify that access to critical system files is restricted to specific authorized users. Operators and maintenance staff should not have Read or Write access to critical files. Subjective Tests: Windows ACL's should be reviewed for appropriate settings. Right click on folder c:\FIX32\Local and select Properties->Security->Permissions and check the settings. Reference: Intellution White paper, Validation Guide for SCADA/HMI Applications	FIX operates in the context of the System so FIX files should be accessible to SCADA administrators and the System only.	Unauthorized access to critical system files either through curiosity or malicious intent can lead to corrupted or deleted system files. It can also lead to users with malicious intent gaining information necessary to gain further access to the system. If system files become corrupted or are deleted, the SCADA system could stop functioning.
9-B Verify that operators cannot use FIX database or recipe builder module. Subjective Test: Review the FIX security settings in C:\Program Files\FIX\view.ini for appropriate group settings. Reference: Intellution White paper, Validation Guide for SCADA/HMI	FIX should have three groups defined. Operators, Developers (or something equivalent), and Maintenance (or something equivalent) The Operators group should not have access to anything except Viewing, Alarm Acknowledge, and Set-point Control.	If operators have access to the FIX Recipe builder or Database builder modules, they can modify critical system files or create files that give them more access to the system than they should have.

Applications		

Security Objective 10 – Limit Personnel to Only Those Functions Required for Their Duties		
10-A Verify that operations and maintenance personnel cannot gain access to the Windows desktop. Subjective Test: Review the settings in the FIX view.ini file located in c:\FIX32\Local. Objective Test: Attempt to gain access to the desktop using CTRL-ALT-DEL. Reference: FIX System Documentation	view.ini should contain the following entry in section "Environment": Reboot=FALSE Nothing should happen. The FIX view screen should remain in place.	Accessing the Windows desktop at a view node provides a person with access to the file system and the Windows command prompt. Further access to the system can be gained, or information can be gathered about the network by using Windows network commands.
10-B Verify that the Windows task bar is disabled. Subjective Test: Review the settings in the FIX view.ini file located in c:\FIX32\Local. Objective Test: Attempt to access the Windows taskbar. Reference: FIX System Documentation	view.ini should contain the following entry in section "Environment": TitleBar =FALSE The taskbar should not display on the view node.	Having the taskbar enabled and/ displayed provides a means for operators to run programs on view nodes other than FIX. Running other programs has the potential to crash the view node or to obscure the view of the controlled process from the operator leading to the possibility of events occurring that require operator action that does not take place.
10-C Verify that the FIX menu bar is disabled in the default FIX view.	view.ini should contain the following entry in section "Environment":	If the FIX Menu Bar is displayed, operators can attempt to run other FIX modules, or shutdown FIX. Shutting

Subjective Test: Review the settings in the FIX view.ini file located in c:\FIX32\Local. Objective Test: Observe the view node default screen (view). Reference: FIX System Documentation	MenuBar=FALSE The FIX Menu Bar should not be displayed.	down FIX removes the operator's view of the controlled process and his or her ability to take control actions that could lead to possible unsafe conditions.
10-D Verify that non-operators cannot perform control actions. Subjective Test: Review the FIX Security Report access Objective Test: Have a non-operator attempt to perform a SAFE control action such as resetting a limit on a controlled device. Reference: FIX System Documentation.	The Operator group should be the only group with View, Alarm Acknowledge, and Set-Point Control functions allowed. FIX should not allow the action to take place.	Only trained operators should be allowed to take control actions on the controlled process. Actions taken by untrained persons could be potentially dangerous or destructive to personnel or equipment.

Security Objective 11 – Provide for unique Identification and Authentication of SCADA system users		
11- A Verify that FIX security is enabled. Objective test: Open the FIX security module and click on the "Key" icon. Verify that Enabled is checked.	The popup window will display two options for security Enabled and Disabled. Enabled should be checked.	None of the FIX security mechanisms, including I&A, limited access to FIX modules, or security logging will function properly unless FIX security is enabled.

Reference: FIX System Documentation		
11-B Verify that either Windows Domain I&A is integrated with FIX, or that FIX I&A is used and requires unique username/passwords. Subjective Test: Review FIX Security Report. Reference: FIX System Documentation	If security is enabled on the FIX system the security report will show all users who have valid accounts on the system.	Without unique I&A, provided by either Windows or FIX, it is not possible to tie security violations or control actions to a unique individual. Being able to tie actions to individuals provides the knowledge necessary to determine whether additional training is required, discipline is required, or if someone is maliciously attempting to perform actions outside their scope of duties.
11-C Verify that default FIX account for Admin is disabled. Objective Test: Attempt to log into FIX as Admin/Admin Reference: FIX System Documentation	FIX should display the error message: “User Admin not registered in Security”	The FIX Admin account is a default account that is enabled when FIX is installed. It is required for setting up the FIX security areas, users, and groups. FIX Admin has complete control over the FIX system and if the account is not disabled, it can be used to perform any action.
11-D Verify that company password policies are being followed. Subjective Test (Windows): Review the Local Security Settings->Password policies. Objective Test (Windows): Use L0PHTCrack to crack the Windows passwords if Domain Authentication is used and is integrated with FIX	Windows settings should be: Enforce password history: 5 passwords Maximum password age: 90 days Minimum password length: 8 characters Passwords must meet complexity requirements: Enabled	Weak passwords make it easier for someone to gain access to the system by either guessing passwords, or performing password cracking.

Security. Note: FIX does not have any technical means to enforce password policies or to allow users to change passwords. Reference: Company IT Security Policy Memorandum, *IT System Password Requirements*.		

Assignment 3 – Audit Evidence

The selection of checklist items to present was based on my evaluation of the criticality of those items to the overall security of the SCADA system. I felt that protecting the network from external access, protecting the network from insider attack, and protecting the underlying Windows OS and SCADA files were most critical. I also felt that in cases that protection might fail, detection of malicious activity was the next critical component of the SCADA system audit.

Checklist Item 1-A: Pass

Objective: Verify that the system documentation includes identification of all necessary connections to the SCADA network.

The SCADA network documentation indicated that no external TCP/IP connections exist either between third parties or the company wide-area network. The only connection that exists is a single serial connection used to "push" operations data from a data historian server to the company wide-area network. That link was protected by the use of custom software and by physically disabling the receive pins on the SCADA side of the RS-232 cable by cutting the pins off.

Checklist Item 1-B: Pass

Objective: Verify that only those connections that are documented exist.

I used NmapWin from the corporate WAN to perform a ping sweep of the IP space used by the SCADA network to locate connections to the corporate WAN. No undocumented connections were found. I also used a laptop computer and NetStumbler to attempt to locate undocumented wireless access points on the SCADA network. None were found.

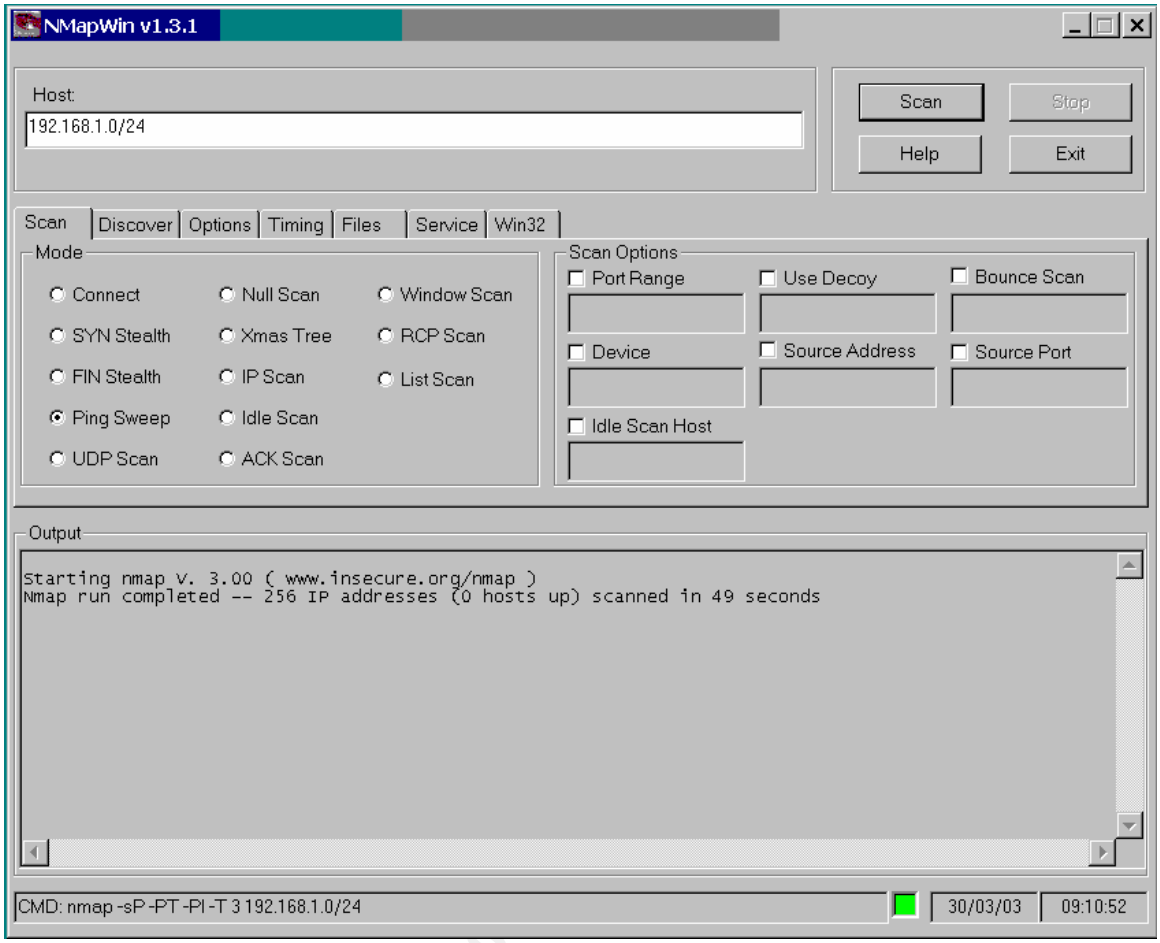

Figure 1 - NMapWin scan from company WAN

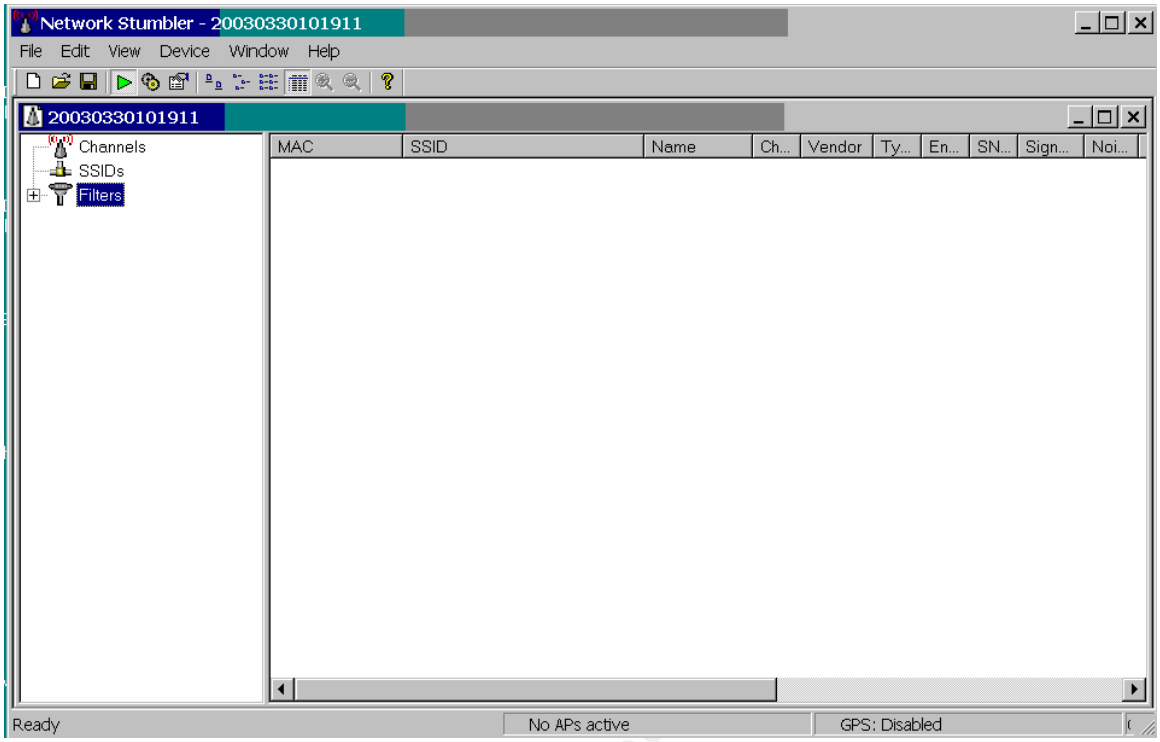

Figure 2 - NetStumbler Search

Checklist Item 2-A: Pass

Objective: Verify that all necessary network services are identified and documented.

The SCADA system documentation identified that Windows NetBIOS Session Service (TCP port 139), NetBIOS Name service (UDP port 137), and Windows locator service (TCP port 135) are required for FIX to operate properly. FIX uses those services and ports to provide communications between view and SCADA nodes. In addition, NT Domain Authentication is used so Microsoft-DS (port 445) is required on Windows 2000 nodes. In addition, the network time protocol (port 37) is required on each node to provide time synchronization. No other network services were identified as being required.

Checklist Item 2-B: Pass

Objective: Identify network services running on SCADA servers and view nodes.

A laptop computer was connected to the SCADA network and NmapWin was used to perform a SYN Stealth scan on the IP space of the network. The results were saved to a text file and are shown below. No unnecessary services were found.

```
# nmap (V. 3.00) scan initiated Mon Mar 03 08:33:55 2003 as: nmap -sS -PT -PI -T 3 -oN scada
net services.txt

192.168.1.1-46

Interesting ports on xxx.xxx.xxx (192.168.1.2):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open        time
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
1029/tcp   open         ms-lsa

Interesting ports on xxx.xxx.xxx (192.168.1.3):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open        time
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
1027/tcp   open         IIS

Interesting ports on xxx.xxx.xxx (192.168.1.4):
(The 1596 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open        time
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
427/tcp    open        svrloc
1031/tcp   open         iad2

Interesting ports on xxx.xxx.xxx (192.168.1.5):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State      Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
427/tcp    open        svrloc
1030/tcp   open         iad1

Interesting ports on xxx (192.168.1.7):
(The 1598 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open        time
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn

Interesting ports on xxx.xxx.xxx (192.168.1.8):
(The 1596 ports scanned but not shown below are in state: closed)
```

```
Port       State      Service
37/tcp     open       time
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
427/tcp    open       svrloc
1031/tcp   open       iad2

Interesting ports on xxx (192.168.1.10):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open       time
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
1030/tcp   open       iad1

Interesting ports on xxx.xxx.xxx (192.168.1.15):
(The 1598 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open       time
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn

Interesting ports on xxx.xxx.xxx (192.168.1.16):
(The 1596 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open       time
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
1027/tcp   open       IIS
2010/tcp   open       search

Interesting ports on xxx.xxx.xxx (192.168.1.19):
(The 1596 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open       time
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
427/tcp    open       svrloc
1030/tcp   open       iad1

Interesting ports on xxx.xxx.xxx (192.168.1.20):
(The 1598 ports scanned but not shown below are in state: closed)
Port       State      Service
37/tcp     open       time
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
```

Interesting ports on xxx.xxx.xxx (192.168.1.21):
(The 1597 ports scanned but not shown below are in state: closed)
Port State Service
37/tcp open time
135/tcp open loc-srv
139/tcp open netbios-ssn
427/tcp open svrloc

Interesting ports on xxx.xxx.xxx (192.168.1.24):
(The 1599 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp filtered ftp
139/tcp open netbios-ssn

Interesting ports on xxx (192.168.1.32):
(The 1597 ports scanned but not shown below are in state: closed)
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1029/tcp open ms-lsa

Interesting ports on xxx (192.168.1.35):
(The 1598 ports scanned but not shown below are in state: closed)
Port State Service
37/tcp open time
135/tcp open loc-srv
139/tcp open netbios-ssn

Interesting ports on xxx (192.168.1.42):
(The 1598 ports scanned but not shown below are in state: closed)
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds

Interesting ports on xxx (192.168.1.44):
(The 1596 ports scanned but not shown below are in state: closed)
Port State Service
37/tcp open time
135/tcp open loc-srv
139/tcp open netbios-ssn

Interesting ports on xxx (192.168.1.46):
(The 1596 ports scanned but not shown below are in state: closed)
Port State Service
135/tcp open loc-srv

139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS

Nmap run completed at Mon Mar 03 08:34:59 2003 -- 46 IP addresses (25 hosts up) scanned in 64 seconds

Figure 3 – TCP Scan

Checklist Item 2-C: Fail

Objective: Verify that unauthorized equipment cannot be connected to the SCADA network.

I connected my laptop computer, configured with the SCADA network IP address, netmask, and default gateway, to an open port on one of the Cisco Catalyst switches and attempted to ping sweep the SCADA network IP space. The results are shown below:

nmap (V. 3.00) scan initiated Mon Mar 03 08:38:27 2003 as: nmap -sP -PT -PI -T 3 -oN scada net ping.txt 192.168.1.1-46

Host (192.168.1.1) appears to be up.
Host xxx.xxx.xxx (192.168.1.2) appears to be up.
Host xxx.xxx.xxx (192.168.1.3) appears to be up.
Host xxx.xxx.xxx (192.168.1.4) appears to be up.
Host xxx.xxx.xxx (192.168.1.5) appears to be up.
Host xxx(192.168.1.7) appears to be up.
Host xxx.xxx.xxx (192.168.1.8) appears to be up.
Host xxx (192.168.1.10) appears to be up.
Host xxx.xxx.xxx (192.168.1.14) appears to be up.
Host xxx.xxx.xxx (192.168.1.15) appears to be up.
Host xxx.xxx.xxx (192.168.1.16) appears to be up.
Host xxx.xxx.xxx (192.168.1.19) appears to be up.
Host xxx.xxx.xxx (192.168.1.20) appears to be up.
Host xxx.xxx.xxx (192.168.1.21) appears to be up.
Host xxx.xxx.xxx (192.168.1.23) appears to be up.
Host xxx.xxx.xxx (192.168.1.24) appears to be up.
Host xxx (192.168.1.25) appears to be up.
Host xxx.xxx.xxx (192.168.1.28) appears to be up.
Host (192.168.1.29) appears to be up.
Host xxx (192.168.1.32) appears to be up.
Host xxx (192.168.1.35) appears to be up.
Host xxx (192.168.1.39) appears to be up.
Host xxx (192.168.1.42) appears to be up.
Host xxx (192.168.1.44) appears to be up.
Host xxx (192.168.1.46) appears to be up.

Nmap run completed at Mon Mar 03 08:38:39 2003 -- 46 IP addresses (25 hosts up) scanned in 12 seconds

Figure 4 - Network connection attempt

Checklist Item 2-E: Fail

Objective: Verify that Windows Null sessions are disabled.

I attempted to initiate a null session on one of the SCADA nodes and was successful:

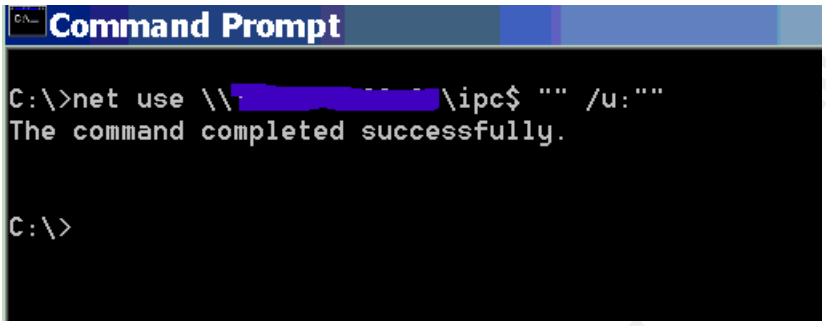

Figure 5 - Null session attempt

Checklist Item 8-C: Fail

Objective: Verify that security logging for the Windows OS is enabled.

Windows auditing was not enabled on the domain.

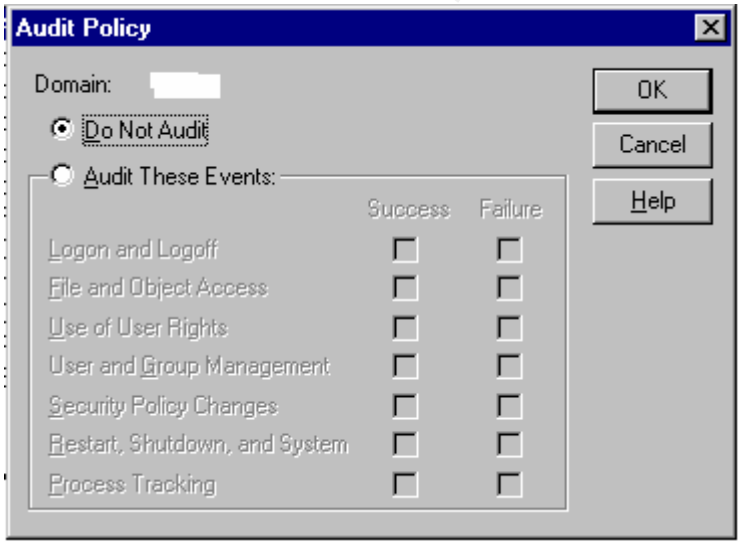

Figure 6 - Windows Security Audit Policy

Checklist Item 8-D: Pass

Objective: Verify that the SCADA system logs FIX security events.

I had the SCADA admin attempt to access FIX modules while logged in as guest. The log is below:

3/3/2003 08:41:47 XXXX logged out as Application User
3/3/2003 08:44:48 XXXX logged in as Application User
3/3/2003 08:46:02 XXXX logged out as Application User
3/3/2003 08:46:11 GUEST logged in as Application User
3/3/2003 10:56:26 XXXX logged out as Application User
3/3/2003 10:56:36 GUEST logged in as Application User
3/3/2003 10:57:55 xxx SECURITY VIOLATION: GUEST access to APPLICATION FEATURE WorkSpace Configure
3/3/2003 10:58:08 XXXX SECURITY VIOLATION: GUEST access to APPLICATION FEATURE Runtime Visual Basic Editor Access
3/3/2003 10:58:08 XXXX SECURITY VIOLATION: GUEST access to APPLICATION FEATURE Runtime Visual Basic Editor Access
3/3/2003 10:58:35 XXXX SECURITY VIOLATION: GUEST access to APPLICATION FEATURE WorkSpace Configure
3/3/2003 10:58:59 XXXX SECURITY VIOLATION: GUEST access to APPLICATION FEATURE System User Login
3/3/2003 10:59:02 GUEST logged out as Application User
3/3/2003 10:59:19 XXXX logged in as Application User

Figure 7 - FIX Security log of invalid access attempts

Checklist Item 10-A: Pass

Objective: Verify that operations and maintenance personnel cannot gain access to the Windows desktop.

I attempted to use CTRL-ALT-DEL to gain access to the Windows Task Manager so I could shutdown the FIX service through Task Manager. There was no response at all. The FIX view remained and no error was generated. An interesting thing did occur though, one of the view nodes we were testing on had a password protected screen saver that activated while a non-privileged user was logged into FIX. Since a CTRL-ALT-DEL key sequence is required to log back into a Windows workstation that is locked, and FIX had disabled CTRL-ALT-DEL for that user, we were unable to gain access to the view node. The only way to get back to the default view of the plant was to reboot the node. This is an indication that FIX users must be very careful when implementing this feature and verify that password protected screen savers are not used if CTRL-ALT-DEL is disabled.

Checklist Item 11-B: Fail

Objective: Verify that default FIX account for Admin is disabled.

I attempted to log into as Admin and was successful:

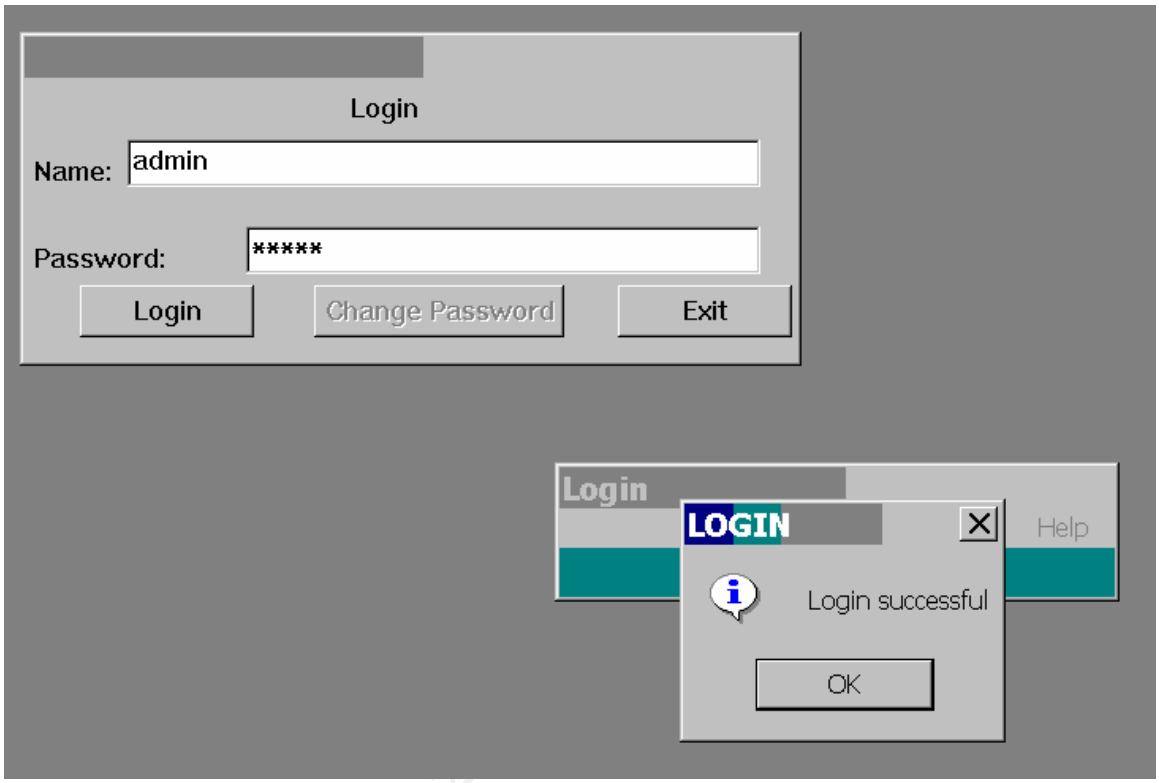

Figure 8 - FIX Admin login attempt

Residual Risk

The SCADA system audit demonstrated that the system is relatively secure. There is no access from outside the network and, except for the default account being active, good protection of the underlying operating system and network from normal user activity. The audit showed that good configuration management is utilized, system documentation is complete and up to date, and backup and restore capability is adequate. Areas of weakness are the ability to access the network and to perform intelligence gathering due to weak Windows security settings.

The only real threat to the system is from the insiders such as disgruntled, bored, or curious employees. Considering the fact that most operators and maintenance personnel are trusted not to cause damage and disruption to the system, this risk is low. This threat must be taken seriously though because it is always possible that such employees exist. With recent trends in the economy it is not unlikely that downsizing efforts could take place, or that contentious union negotiations could occur. These types of activities foster the atmosphere for resentment and

bitterness and can lead to situations of disgruntled employees trying to disrupt the system.

Is the System Auditable

From the perspective that the SCADA system is composed of network devices, Windows 2000 servers and workstations, and peripheral devices, and that it is therefore considered an IT system, then it is easy to state that it is auditable because many tools, techniques, and checklists exist to audits networks and systems. In addition, because the SCADA system, and SCADA systems in general, provide mission critical functionality they cannot be shutdown or caused to shutdown through the actions of an audit. Some of the tests I wanted to perform, including using nmap to scan the network for services, were at first blocked by the operations staff until they were performed on a test network to prove they did not cause harm. Even then there was skepticism regarding the safety of such scans. Auditors should be aware that if they are performing any type of scan on a SCADA system and something goes wrong, no matter the actual cause, the auditor will be blamed.

Because the system is, or should be, designed and deployed to perform only one function, and there are a number of ways to meet the security objectives of the system, I found it somewhat difficult to create and use a checklist that would apply equally to any FIX SCADA system. FIX itself provides a number of ways to configure security, including hardware keys for different functional requirements of SCADA nodes, and variations in configuration file settings. Each system requires a thorough review of how it is secured prior to conducting the audit, and adjustments should be made to the checklist.

Another area where it was difficult to determine appropriate security objectives and audit items was the field devices. Field devices are now being marketed that incorporate Ethernet communications capability and they lend themselves to typical network auditing practices. The field devices on the system that I audited use a serial communications protocol (Modbus) and serial communications lines. I could not find any information on techniques or tools to use for auditing field devices and protocols even though there are references to vulnerabilities in some of those devices. Obviously, I was not comfortable attempting to perform tests where I sent mangled information to the field devices because of unpredictable behavior of the controlled system.

Assignment 4 – Audit Report or Risk Assessment

Summary

In general the SCADA system audit results were mostly positive. The system is particularly strong in the areas of documentation, configuration management, and backup and restore capability. The main concerns found are related to weaknesses in the underlying operating system and network configuration that will allow an insider who bypasses the existing access controls to gain unauthorized access to system information. The weaknesses found are:

- The ability to connect unauthorized computers to the network,
- Being able to initiate a null session to a SCADA node,
- Lack of Windows security auditing,
- The FIX Admin account still being enabled,
- The password control mechanisms in FIX do not meet company policy.

Although company employees are considered trusted because they do have access to various parts of the plants, and the risk of such insider activity is somewhat low, there is always the possibility that recent downsizing activities or future union contract negotiations could lead to disgruntled employees.

Background/Risk

Finding 2-C: Connecting unauthorized computers to the network – (Figure 4) Being able to connect an unauthorized computer to the network would allow anyone who gains access to network switches to connect a laptop to the system. They could then use it to access configuration files, sniff packets for the purpose of cracking passwords, or configure it as a SCADA view node with admin privileges which would give them access to control capabilities. Someone with access to configuration files could also purposely change them, or accidentally corrupt them leading to mis-operation of equipment or an unstable system. Someone with access to the controlled process could cause significant harm to the system by disrupting the process.

Finding 2-E: Windows null sessions are allowed on SCADA nodes – (Figure 5) Windows null sessions allow someone who bypasses the first layer of protection and gains access to the Windows operating system to gain further knowledge about the SCADA nodes, including shares, security policies, and usernames. Such knowledge can be leveraged to provide further access into the system resulting in the same consequences as stated in the previous paragraph.

Finding 8-C: Windows Security Auditing was not enabled on the Domain - (Figure 6) Windows security auditing should be enabled as well as FIX security logging. By having Windows security auditing enabled administrators can be

alerted to attempts by insiders to gain unauthorized access to the SCADA system through normal logins, and to events related to someone already having access to the SCADA network. If all of the preventive security controls fail, logging provides the detection of security events and sufficient time to take corrective actions. Not enabling Windows security auditing removes the ability to detect unauthorized activities taking place on the SCADA network, and prevents administrators from taking corrective actions because they are not aware of the activities.

Finding 11-B: FIX Admin account not disabled – (Figure 8) The FIX Admin account is similar to the Windows administrator account. It is a default account that is set up when FIX is installed, and it is used for configuring the system. The first thing a SCADA administrator should do when setting up FIX users or groups is to create an account for themselves that has FIX Admin rights. They should then delete the user "Admin" from the FIX users. Having this account enabled on production SCADA nodes and view nodes is a very risky situation. Anyone with Admin rights to FIX can do anything they want and access any FIX module. Actions could include reconfiguring the system, taking inappropriate and potentially dangerous control actions, and shutting down the SCADA system. It would also be impossible to track the user who performed such actions.

Finding 11-D: FIX password policies do not conform to company IT security policies – (Not shown in audit results) FIX 7.0 does not provide any technical controls for assuring that passwords meet complexity, aging, or minimum length requirements. FIX 7.0 also does not allow users to change their own passwords. Although there are no known cracks for FIX passwords that I could find, the possibility of those being created due to the high profile of SCADA systems always exists. Having passwords that never expire, and are not complex makes brute force or dictionary cracking relatively easy if the necessary software is written. Even though the risk of that happening is low the possibility must be considered.

System Changes and Further Testing

All of the findings were fixed and retested on the system and are reported below. Even though all the findings were mitigated there is still some risk that is addressed in the next section.

Finding 2-C Connecting unauthorized computers to the network – To repair this finding the administrator opened a telnet session to the switch (192.168.0.1) and locked all of the unused ports. I then retested the system by using the same procedure as in checklist item 2-C and used nmap to perform a ping sweep of the network. The results are shown in Figure 9.

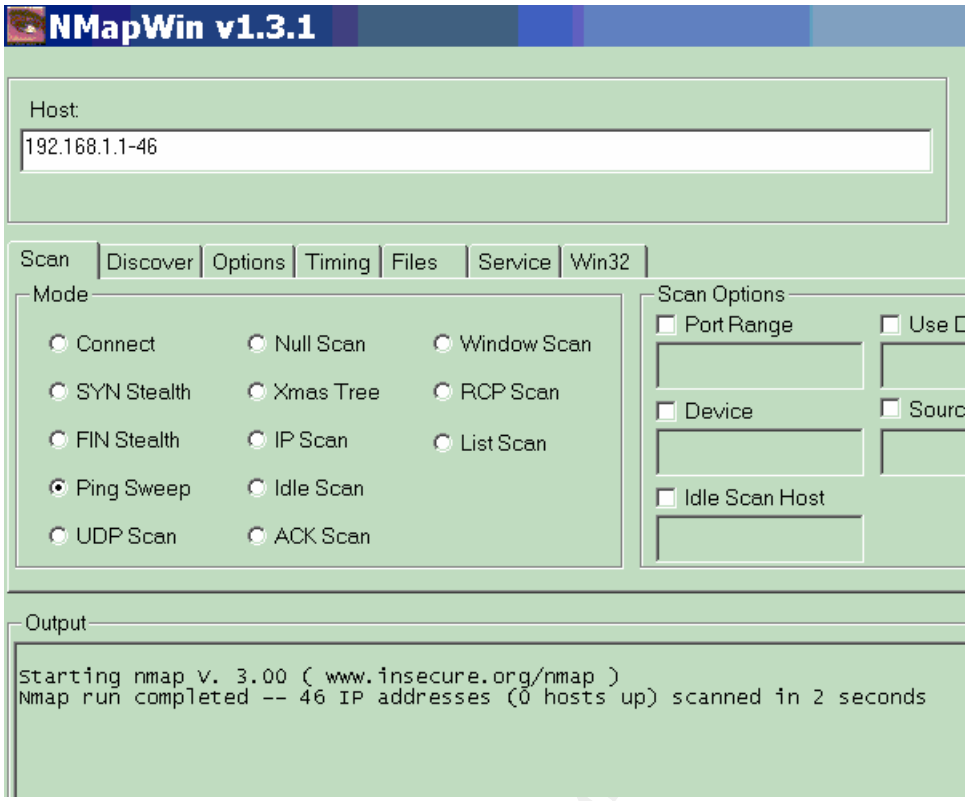

Figure 9 - Retest of connecting equipment to network

Finding 2-E Windows null session are allowed on SCADA nodes – To fix this weakness the administrator used the Control Panel->Administrative Tools->Local Security Policy->Local Policy->Security Options, and set the first entry "Additional restrictions for anonymous connections" to "No access without explicit anonymous permissions". I then attempted to initiate a null session to the SCADA node. The results of that test are shown in Figure 10 below.

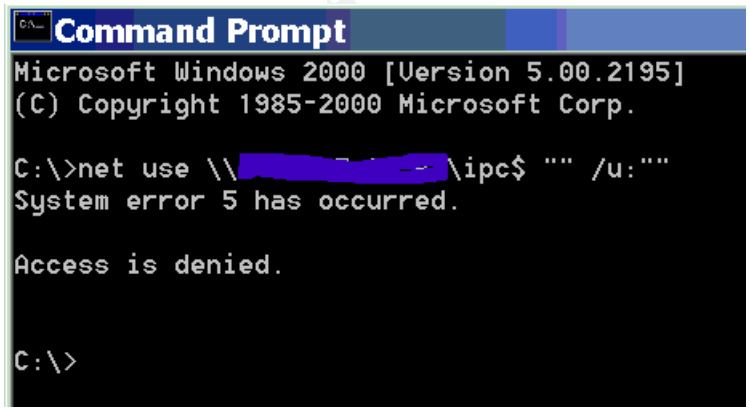

Figure 10 - Null session test after fix applied

Finding 8-C: Windows security auditing not enabled on SCADA or view nodes – Security auditing was enabled on the domain controller as shown in

Figure 11. The auditing was then tested by attempting to login with a bad username/password pair and the audit log, Figure 12, was reviewed to verify that logging was indeed enabled.

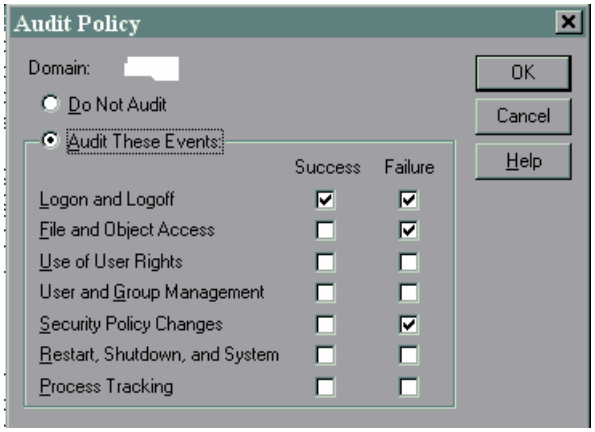

Figure 11 - Windows audit policy after fix applied

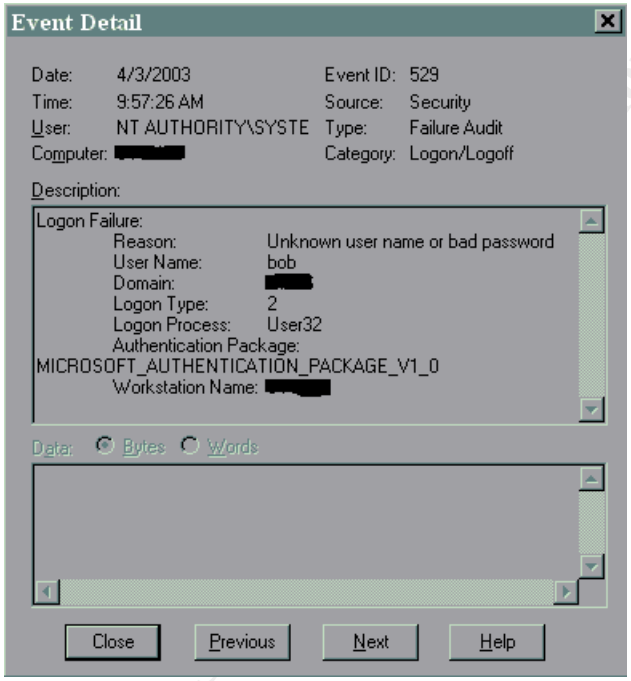

Figure 12 - Bad username/password login

Finding 11-B: FIX Admin account not disabled – This was corrected by using the Security Configuration Module for FIX to delete the Admin account after assuring that one of the SCADA administrators was given full access rights to the FIX system. I then tested the setting by attempting to log into FIX as Admin/Admin. Results are shown below in Figure 13.

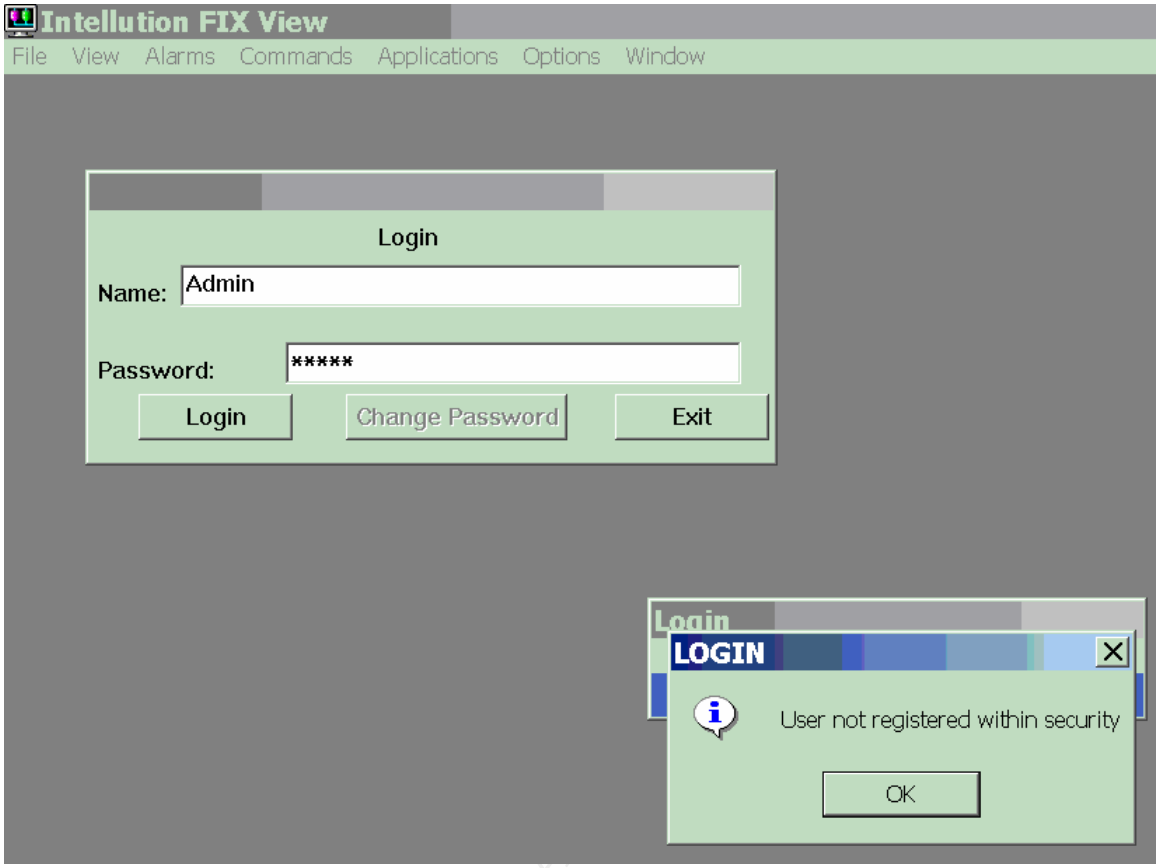

Figure 13 - FIX Admin login test, passed

System Justification

Based on the fixes applied and tested as shown in the previous section it appears that there are no remaining insecurities in the SCADA system. However, there are still some subtle problems that create some measure of risk to the system.

One of the problems, supported by audit finding 2-C, is the ability to connect unauthorized computers to the network. That risk was mitigated by disabling unused ports on the network switches. It is still possible, however, to disconnect a SCADA view node from the network, connect a small four-port hub or switch, and reconnect the SCADA view node. This would then leave two open ports for connecting unauthorized equipment to the network. One mitigating control for this possibility is that the SCADA nodes periodically poll the view nodes to verify that they are still communicating with the system. The polling takes place on a user specified interval and if a node is not responding, an alarm event is recorded in the FIX alarm file. At least the system operators will be alerted to someone disconnecting a SCADA view node and can make an appropriate response.

A potential correction to the problem of someone using an active port for connecting unauthorized equipment to the network is to purchase and install the

latest versions of network switches. The newer switches have the capability to assign specific MAC addresses to specific ports on the switch and would prevent someone from disconnecting and reconnecting equipment. The cost of the replacement switches for the system being audited is approximately $4,000 per switch.

The other problem with the system is the lack of password policy enforcement mechanisms in FIX, and the fact that FIX passwords do not meet the complexity requirement, being only six characters and not distinguishing between upper and lower case characters. Since two levels of authentication are used, Windows and FIX, the Windows password policy enforcement is used for the domain. However FIX does not have that capability. Currently SCADA users cannot change their passwords and rely on the administrators to assign passwords. Since the passwords chosen by the administrators are somewhat complex, but not necessarily related to anything of interest to the users, it is probable that those passwords will be written down and stored somewhere. Hopefully the users will keep them in a safe place, but they do run the risk of passwords being inadvertently disclosed to unauthorized users.

Technical controls for password policy enforcement do exist for Windows, and FIX includes the capability to integrate Windows I&A into the FIX environment. The attempt at that integration has not been successful however, and the current practice of having administrators assign passwords and set them in FIX will be continued. The latest release of FIX, iFIX Dynamics, supposedly integrates into Windows I&A easily, but the expense of migrating to the new product is considerable. Not only will the software upgrade costs have to be paid, the custom recipes and applications may have to be rewritten due to the latest product using Visual Basic instead of a FIX custom scripting language.

References:

- "21 Steps to Improve Cyber Security of SCADA Networks", U.S. Department of Energy, Argonne National Laboratory, http://www.oea.dis.anl.gov/documents/21StepsBooklet.pdf
- Jim Montague, "Ethernet Security, Safety Relies on Common Sense Networking", Control Engineering, March 1, 2001, http://www.manufacturing.net/ctl/index.asp?layout=articleWebzine&articleid=CA68320
- "Implementing Common Desktop Management Scenarios", Microsoft Whitepaper, http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp
- Al Chisholm, "The FIX Security System", iFIX Whitepaper, 01/11/98
- Abo Y. Saad, "Securing Supervisory Control & Data Acquisition Systems", Pipeline and Gas Journal, July 2002, http://www.undergroundinfo.com/PGJ/pgj_archive/July02articles/securingsupervisory.pdf
- "Security Guidance for Supervisory Control and Data Acquisition Systems", Internal Company Document
- FIX Electronic Books (FIX System Documentation)
- "Validation Guide for SCADA/HMI Applications", Intellution White paper
- Joel Scambray and Stuart McClure, Hacking Exposed, Windows 2000, Network Security Secrets and Solutions, Osborne/McGraw-Hill, 2001