



ABB SCADA/EMS System INEEL Baseline Summary Test Report

*J. R. Davidson
M. R. Permann
B. L. Rolston
S. J. Schaeffer*

November 2004



Idaho National Engineering and Environmental Laboratory

*Prepared by: Idaho National Engineering and Environmental
Laboratory*

**ABB SCADA/EMS System
INEEL Baseline Summary Test Report**

**J. R. Davidson
M. R. Permann
B. L. Rolston
S. J. Schaeffer**

November 2004

**Idaho National Engineering and Environmental Laboratory
INEEL National Security Division
Idaho Falls, Idaho 83415**

**Prepared for the
U.S. Department of Energy
Office of Energy Assurance
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727**

ABB SCADA/EMS System INEEL Baseline Summary Test Report

INEEL/EXT-04-02423

November 2004

Approved by:



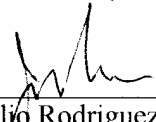
Jim Davidson, ABB Testing Principle Investigator

16-DEC-2004
Date



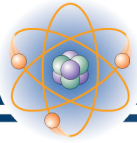
Alan M. Snyder, CITR Program Manager

16-Dec-04
Date



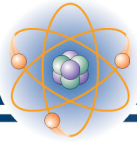
Julio Rodriguez, Critical Assurance Department
Manager

16-DEC-04
Date



ABSTRACT

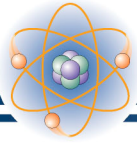
The Idaho National Engineering and Environmental Laboratory Supervisory Control and Data Acquisition (SCADA) Test Bed is a venue to test various SCADA systems with differing configurations to determine the security vulnerabilities of these systems. This SCADA test bed supports multiple programs sponsored by the U.S. Department of Energy, Department of Homeland Security, and other government and private sector clients. A portion of this testing consists of a baseline examination of the delivered system. This baseline must be performed to establish a starting point for subsequent testing. This document provides the baseline report for the ABB SCADA/Energy Management System as delivered to the Idaho National Engineering and Environmental Laboratory by ABB (software) and Hewlett Packard (hardware).



CONTENTS

ABSTRACT.....	vii
ACRONYMS.....	xi
1. INTRODUCTION.....	1
1.1 Scope.....	1
2. SYSTEM DESCRIPTION.....	3
2.1 Central Processing Server.....	3
2.2 Windows Resources Server.....	3
2.3 Inter-utility Control Center Protocol (ICCP) Server.....	3
2.4 Real-time Database and Communications Server.....	3
2.5 Historian Server.....	4
2.6 Consoles.....	4
2.7 Laptop Console.....	4
2.8 Network Switch.....	4
2.9 Network Router.....	4
2.10 Wireless Access Point.....	4
3. SECURITY PLAN.....	5
4. BASELINE TESTING TOOLS.....	7
4.1 Windows-based Tools.....	7
4.1.1 System Information.....	7
4.1.2 AIDA32.....	7
4.1.3 Net Diagnostics.....	7
4.1.4 Superscan 4.0.....	7
4.1.5 STAT Scanner.....	8
4.2 Unix-based Tools.....	8
4.2.1 Sys_check.....	8
4.2.2 Nessus Security Scanner.....	8
4.2.3 John the Ripper.....	9

4.3	Cisco Assessment Tools	9
4.4	Cyber Security Tools	9
5.	CYBER SECURITY TESTING	11
5.1	System Specifics	11
5.2	Attackers	11
5.3	The Local Network	11
5.4	Remotely Accessing the Local Network	11
6.	GENERAL RECOMMENDATIONS FOR SCADA SYSTEMS	13
6.1	Configuration Recommendations	13
6.2	Users and Passwords	13
6.3	Windows 2000 Server Platform	13
6.4	Windows XP Pro Platform	13
6.5	Open Ports	14
6.6	Microsoft Office	14
6.7	Cyber Security Recommendations for SCADA Systems	15
6.7.1	Passwords	15
6.7.2	Updates	15
6.7.3	Applications	15
6.7.4	Encryption	16
6.7.5	Services	16
6.7.6	Domain Name Services	16
6.7.7	Address Resolution Protocol	16
6.7.8	Windows Administrative Shares	17
6.7.9	Intrusion Detection	17
7.	CONCLUSIONS	19



ACRONYMS

ABB	Asea Brown Boveri
ARP	address resolution protocol
DNS	Domain Name Services
DOE/OEA	U.S. Department of Energy; Office of Energy Assurance
EMS	Energy Management System
HMI	Human Machine Interface
HP	Hewlett-Packard
ICCP	Inter-utility Control Center Protocol
INEEL	Idaho National Engineering and Environmental Laboratory
LAN	local area network
MSN	Microsoft Network
RTU	remote terminal unit
SCADA	Supervisory Control and Data Acquisition
WAN	wide area network

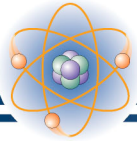


ABB SCADA/EMS System INEEL Baseline Summary Test Report

1. INTRODUCTION

The ABB Supervisory Control and Data Acquisition (SCADA)/Energy Management System (EMS) system consists of hardware and software that function as a SCADA system for the electrical power industry. The ABB system is connected to a local area network (LAN) via a Cisco WS-2924-XL switch. A Cisco 2611XM router connects this LAN to the SCADA test bed wide area network (WAN).

This document covers the security evaluation of the “baseline” or “as delivered” system performed in the Idaho National Engineering and Environmental Laboratory (INEEL) SCADA test bed as part of the Critical Infrastructure Test Range Development Program, which is funded by the U.S. Department of Energy; Office of Energy Assurance (DOE/OEA). This report is a nonproprietary version of the report sent to ABB that identified specific issues related to the security vulnerabilities in the ABB SCADA/EMS system. Work was performed by specialists in the fields of control system development, networking, software engineering, and cyber security. This report is the result of the team effort of these specialists to evaluate the ABB SCADA/EMS system baseline within the scope of the testing plan.

All testing and evaluation was performed by INEEL personnel at the Information and Operations Research Center located in Idaho Falls, Idaho.

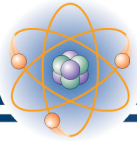
1.1 Scope

In this document, the term baseline refers to the configuration of the hardware and software as delivered to the INEEL. The INEEL ABB SCADA/EMS system consists of five server computers, two desktop consoles, a wireless access point, and one wireless enabled portable. These components are duplicated at ABB in Houston as a backup system that, when connected via WAN, will allow the testing of fail-over functions from the primary INEEL system to the backup ABB system, should the primary system fail.

At the time of testing, remote terminal units (RTU) capable of acquiring data or performing control functions to an external electrical power grid were unavailable. To fully evaluate performance and capabilities of the system, these external connections must be provided. Therefore, this baseline test did not include performance testing. Performance baseline testing will be implemented when external data points via RTU connections are available. This also limits testing the historian, the data acquisition system, and communication between the data acquisition system and the RTUs.

While the delivered system did include an Inter-utility Control Center Protocol (ICCP) server, the INEEL did not have access to another ICCP server to establish communications with the ABB system. This prevented testing of the ICCP services.

These two limitations focused the scope of the Cyber Security assessment, driving the testing primarily to operating system related vulnerabilities.



2. SYSTEM DESCRIPTION

The INEEL ABB system consists of a series of servers, consoles, and networking components to build a hardware platform on which to install the ABB Energy Management Software suite. This section identifies the individual components that make up the system tested at the INEEL.

2.1 Central Processing Server

The Central Processing server provides the central core for the SCADA system and includes database management, centralized communications, and other critical SCADA functions.

The Central Processing server consists of a Compaq Alphaserer running Tru64 release 5.1b. Disk storage is provided with six disk drives. A backup for these drives is provided in a split SCSI bus cage with 12 disk drives. Each set of six disk drives can be used as the primary drive system during boot. This allows a fully configured and functional backup copy of the central processing server to be available should testing crash the primary system.

2.2 Windows Resources Server

The Windows Resources server provides various centralized Windows services for the SCADA system. The Windows Resource server is an Hewlett-Packard (HP) Proliant computer with Xeon processors running a Windows 2000 server. Disk storage is provided by two disk drives configured as raid 1 (mirror). In this manner, one of the drives can be removed during testing to provide a fully functional backup drive.

2.3 Inter-utility Control Center Protocol Server

The ICCP server provides communication services for translation between different computers. The INEEL did not have a second ICCP server to allow a communications link with the ABB ICCP server. As a result, no evaluation of ICCP services was performed during this series of testing.

The ICCP server consists of a Compaq Alphaserer running Tru64 release 5.1b. Disk storage is provided by two disk drives acting as a primary and a secondary drive. The primary drive is mirrored via a manually run script to the secondary drive. During testing, the primary drive on the ICCP server was removed and the server was started using the secondary drive.

2.4 Real-time Database and Communications Server

This server supplies real time data acquisition and communications with RTUs for the acquisition of data and control of electrical power equipment. For the purposes of this test, the server was not connected to any external devices (e.g., RTUs). As a result, testing on this system was limited to operating system testing.

The Real-time Database and Communications server consists of a Compaq Alphaserer running Tru64 release 5.1b. Disk storage is provided by two disk drives acting as a primary and secondary drive. The primary drive is mirrored via a manually run script to the secondary drive. During testing, the primary drive on the server was removed and the server was started using the secondary drive.

2.5 Historian Server

The Historian server provides the historical database for long-term historical data used for evaluation, trending, and audit functions of the electrical grid under supervisory control by the SCADA system. The system was tested without input and hence the historian testing was limited to operating system tests.

The Historian server is an HP Proliant with Xeon processors running a Windows 2000 server. Disk storage is provided by six disk drives configured as Raid 1 (mirror). In this manner, one set of drives can be removed during testing to provide a fully functional drive set as a backup.

2.6 Consoles

The consoles provide the human machine interface (HMI) for the ABB SCADA/EMS system. In a typical system, there are many consoles, each providing control, analysis, and/or monitoring functions for the ABB system. All PCs on this system are HP Workstations with Xeon processors running Windows XP Professional. Disk storage is provided by a single disk drive. The NVIDIA Quadro NVS graphics system is capable of driving up to four computer displays.

2.7 Laptop Console

The portable console is a wireless laptop used for remote access to the ABB SCADA/EMS system via a wireless access point. While not in the ABB product line, it does represent a trend in the industry towards wireless technology. The laptop is a Compaq Evo with a Mobile Intel Pentium M running Windows XP Professional. Disk storage is provided by a single disk drive.

2.8 Network Switch

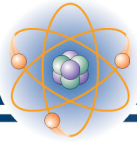
The network switch is a Cisco WS-2924-XL 24 Port 10/100UTP switch that provides for all LAN connections. The switch is configured direct from the factory with the exception of the network settings specific to the INEEL SCADA test bed WAN installation.

2.9 Network Router

A single Cisco 2611XM Router was used to provide for connectivity beyond the internal LAN connections to the SCADA test bed WAN. The router, like the switch, was configured at the factory with the exception of the network settings specific to the INEEL SCADA test bed WAN installation.

2.10 Wireless Access Point

A Compaq WL510 Wireless Access Point with 64-bit Wired Equivalent Privacy security was used by the ABB system. Little was tested on this item, as it is not a part of the normal installation of ABB SCADA/EMS system.



3. SECURITY PLAN

A typical system installation should include an extensive security plan covering cyber, physical, and personnel security.

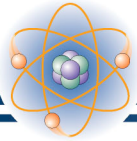
As part of this plan, policies, procedures, and methods are established to protect the SCADA assets. This includes how to deal with users, user groups, password management, password requirements, password expiration, data protection, data integrity, and disaster recovery. It should also include policies for virus management and individual system component use and recovery. The “use” portion is important to preclude the system component from being configured to perform functions beyond its intended use.

ABB’s SCADA/EMS product has three models for internal console security:

- Console Dependent
- User Dependent
- Console and User Dependent.

After reviewing these three security models, we believe that “Console and User Dependent” security is the best choice and should be used wherever practical. A combination of security mechanisms based on the authentication of authorized users for each console helps better control and track access.

For this phase of testing, a security plan was not used in configuring the system in order to establish ABB’s baseline system defaults. In this way, the system could be tested in its worst-case, most vulnerable state, and items that need to be changed in the default configuration could be identified. Future testing will implement a security plan that will be documented in subsequent report(s).



4. BASELINE TESTING TOOLS

A number of public domain and licensed software tools were used to facilitate documentation and evaluation of the INEEL ABB system baseline configuration. This section identifies these tools, their functions, and their applications relative to the ABB system. Where appropriate, links are provided to the Internet sites where further information about the tools can be obtained.

4.1 Windows-based Tools

The tools described in this section can only be run on a Windows operating system.

4.1.1 System Information

System Information (Msinfo32.exe) is a standard tool that comes with all presently supported Windows operating systems. It performs a hardware and software scan of the computer under test, providing an exportable file that can be reviewed.

This tool collects and displays system configuration information for local and remote computers. It contains information about hardware configurations, computer components, and software, including signed drivers and unsigned drivers.

The information acquired was exported as text and then converted to a Web page for incorporation into this report. The Web page link allows non-Windows based computers to view the reports.

4.1.2 AIDA32

AIDA32 is a freeware program similar to System Information. It provides information not supplied by Microsoft's System Information command. Its output is saved in a Web format, which allows for easy retrieval. This tool was selected from the suite of tools used based on this Web-based output and the addition of users and user groups to the report. The tool provides hot links to the vendors of some of the hardware and software installed on the system under scan. This tool works only on Windows systems.

For more information, visit <http://www.aida32.hu/>.

4.1.3 Net Diagnostics

Net Diagnostics administrative software, available only for Microsoft Windows XP, provides extensive testing of the network environment while the computer is running. This software is accessed from a menu within the System Information program. The tool is normally used as a diagnostic for a single system; however, the information provided is consistent with establishing the baseline of a system. For the purposes of this report, all scanning options were turned on to obtain a complete picture of the network configuration for the target computer. The software can also be accessed from a command prompt by typing: "netsh diag gui." This will launch the software with a graphical user interface for performing a scan. The final report is in html format and can be saved for future viewing.

4.1.4 Superscan 4.0

Superscan 4.0 is a freeware program for scanning ports and Internet provider (IP) addresses. It can scan a range of IP addresses to discover the valid IP addresses and perform a port scan on each of them.

The program scans the ports within a specified range and reports the results in a Web format. Since it is based on IP address, the software is capable of scanning any element of a system that has an assigned IP address. This includes Windows systems, Unix systems, routers, switches, and network printers. Hot links on some of the ports in the report allow the user to connect directly to those ports on the machine being tested.

For further information, visit <http://www.foundstone.com/resources/freetools.htm>.

4.1.5 STAT Scanner

STAT Scanner is a commercial product produced by Harris Corporation. This is the primary vulnerability scanner for Windows-based operating systems at the INEEL. The package provides excellent detection of vulnerabilities of the operating system, Microsoft applications, and the operating system components. It has a low rate of false positives, has excellent reporting capabilities, and is relatively inexpensive. The software requires access to the local administrative account on the host and requires that the following services be enabled: messenger, server, and remote registry in Microsoft Win2K and XP operating systems.

For further information, visit <http://www.statonline.harris.com/index.asp>.

4.2 Unix-based Tools

The tools described in this section were run from a Unix-based platform.

4.2.1 Sys_check

This TRU-64 version 5.1b utility performs a system scan for TRU-64 machines similar to Microsoft's System Information. The output from Sys_check is a Web-based report with hot links to the TRU-64 Web site for solutions to problems and answers to questions.

4.2.2 Nessus Security Scanner

The Nessus Security Scanner is an open source vulnerability assessment tool that consists of many plug-ins to check security configurations. It has the ability to perform over 1,200 remote security checks. Any subset of these plug-ins can be used in a security scan. All available plug-ins were used during the Nessus scan. They test for such vulnerabilities as a denial of service attack, backdoors, ability to gain root access remotely, and Windows user management. A range of IP addresses can be scanned for valid hosts, followed by a Nmap port scan of valid IP addresses. The results of these two scans provide the targets for plug-in tools to check for security flaws on system components.

The Nessus tool has been recommended as the best security scanner for Unix systems. It can also be used to scan Windows hosts. The Nessus report is useful in that it suggests solutions for security problems. Problems are ranked as security holes, warnings, and notes. This is helpful in determining which issues to address for different security levels.

For more information, visit <http://www.nessus.org/>.

4.2.3 John the Ripper

John the Ripper is a freeware password cracker with versions for most operating systems. Its main purpose is to quickly detect weak passwords, and is used by administrators and hackers alike for this purpose. Version 1.6 was used to test the ABB SCADA/EMS system.

John the Ripper cracks passwords from the password hashes in the Unix password or shadow file and the Windows SAM and SYSTEM files. Password hashes are a form of encryption. They are created by a one-way function to make them irreversible. John the Ripper hashes word lists of common passwords with the appropriate operating system's hashing functions and compares them to the hashed passwords in order to crack them.

For more information, visit <http://www.openwall.com/>.

4.3 Cisco Assessment Tools

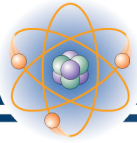
All Cisco systems come with some form of maintenance and technical reporting capability. This capability is used to determine the configuration of the hardware for troubleshooting purposes. Software and hardware configuration of the Cisco switch and router are documented using this tool.

For more information, visit <http://www.cisco.org/>.

4.4 Cyber Security Tools

The Cyber Security Research Department used a variety of readily available, open source tools to assess and penetrate the system. These tools allowed the team to complete the following assessments:

- Port scanning
- Vulnerability scanning
- Network mapping
- Password cracking.



5. CYBER SECURITY TESTING

5.1 System Specifics

Windows-based systems are ubiquitous and there are many tools available for securing these machines. Unfortunately, there are also many exploits available for them. The Tru64 machines are far less common, so there are a smaller number of exploits specific to these machines.

5.2 Attackers

Attackers, whose motives include widespread disruption, may want to get into systems, such as ABB SCADA/EMS system, to cause havoc in whatever sector can be breached.^a Industrial espionage or sabotage might also be a motive for attackers of an ABB SCADA/EMS system. Insiders also pose a significant threat, as in the case of the Australian disgruntled employee, Vitek Boden, who used a digital control system to leak hundreds of thousands of gallons of putrid sludge into parks, rivers, and the manicured grounds of the Maroochy Shire Hyatt Regency hotel.^b

5.3 The Local Network

The network switch was configured as delivered from the factory. This switch configuration affords no security. Using an address resolution protocol (ARP) backscattering technique, an attacker can easily see all of the traffic passing through the switch, and then pick targets for further monitoring or spoofing with a man-in-the-middle technique.

5.4 Remotely Accessing the Local Network

An attacker has several avenues for accessing the internal network, even with an appropriately configured firewall.

It is assumed that a firewall in the real world would be in place between the business or corporate network and the operations network, of which the ABB SCADA/EMS system is at least a player, if not the whole system. What is not assumed, is that the firewall would have the appropriate configuration to provide protection. It is also not assumed that the only possible path to communicate with the ABB SCADA/EMS system is through the firewall because many sites have either unauthorized devices that permit access around the firewall or communication paths that are erroneously deemed to be safe.

Perhaps the easiest way an attacker might penetrate the internal network is through a poorly configured firewall. If the rules in the firewall do not block undesirable traffic then there is little to prevent an attacker from walking through the front door.

E-mail attachments are a way to gain access to a system. Despite numerous warnings and examples of what can happen, people will open suspicious attachments that introduce malware onto their computers. There are several classes of payloads in these attachments, but the one of most concern here is

^a Article on terrorists using the internet for attack: <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>

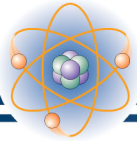
^b Article on Australian attack: http://www.news.com.au/common/story_page/0,4057,3161206%255E1702,00.html

the one that connects back to an attacker's computer, affording them a direct connection into an internal system. This is enough of a foothold to compromise the whole network.

Firewalls can be thwarted by these attacks because they are setup to allow outgoing traffic for certain functions. All an attacker needs to do is use one of the ports enabled for outbound connections by the firewall and his traffic will pass through.

Phishing is another approach that produces the same end as an e-mail attachment. The difference is that some form of communication, usually e-mail, is used to entice the recipient to visit the attacker's system and, in the process, the attacker's system downloads the malware via http, ftp, or any file sharing method.

Domain Name Services (DNS) is another point of attack. When an internal system makes a request for a look-up to a server that is outside of the internal network, the DNS request is subject to forgery. If an attacker can predict what name is in the resolution request, it can respond to the request with a forged reply that directs the following session to the attacker's system instead of the intended one. An attacker can either guess what names might be requested for resolution or "sniff" the traffic on the corporate network to gather a list of commonly used names. When the victim visits the attacker's site, they unwittingly download malware and execute it in their browser. There are other methods to accomplish this, but the browser is the most convenient for the attacker.



6. GENERAL RECOMMENDATIONS FOR SCADA SYSTEMS

This section covers both system and cyber specific recommendations for securing SCADA systems. Due to the proprietary nature of the ABB SCADA/EMS system, recommendations specific to this system are not included. The recommendations in this section are based on the operating systems and network configuration of the ABB SCADA/EMS system, but these recommendations also apply to systems with similar networking components and operating systems.

6.1 Configuration Recommendations

This section provides SCADA system users with general recommendations on configuring the operating systems and networking of a SCADA system.

6.2 Users and Passwords

While it is understood that the end user should establish a security profile for users and passwords, and should change all of the defaults, the baseline installation of operating systems and applications contain defaults that may be overlooked. Each SCADA vendor should guide the end user to establish the security profile and assure that all default passwords are changed as part of the deliverable.

6.3 Windows 2000 Server Platform

The Windows 2000 server operating system is commonly used in new SCADA systems. The high visibility of Windows-based systems increases the risk associated with an unpatched server. Therefore, it is important that these servers are kept up to date with patches.

6.4 Windows XP Pro Platform

The Windows XP Pro platform is another common operating system for SCADA vendor use. If the default install has been performed on the consoles, applications that are not required will be installed, services that are not needed will be automatically started, and options that should be considered will not be enabled.

Of primary concern are Outlook Express, MSN Messenger, Error Service Reporting, and Wireless Zero Configuration Services. These should not be installed during the build if they are not needed to perform the tasks assigned to the consoles. These programs are hard to keep patched and therefore place the consoles at risk.

Patches should be tested before they are applied to verify they will not damage the SCADA system. The Automatic Update service should be turned off to prevent untested patches from being installed.

The Remote Registry service should not be turned on automatically because it allows access to the registry from an external source. If needed during a security scan or vulnerability assessment, it should be turned on for the limited duration of the scan or assessment.

The Windows XP firewall should be turned on and configured to add security to the console.

These systems should not have direct access to the Internet, as this leaves them open to direct attack. Internet and corporate connectivity should be linked via primary servers. Patches, software loads, security profiles, and other items required for console configuration and maintenance should be pushed from a centralized server.

The delayed introduction of patches for known vulnerabilities leaves these systems open to attack. This can be somewhat mitigated if they are not connected to the Internet, but the system is only as secure as its weakest link.

All systems should be accessed with limited user accounts. These accounts should be created to allow software to run, but prohibit software installation and patches without being enabled by an administrator. This prevents unauthorized software from being installed, including many viruses, trojans, and spyware.

6.5 Open Ports

It is strongly advised that any unneeded ports be identified and disabled to improve security and reduce the number of patches required to maintain the system. Each machine should be evaluated and configured individually.

6.6 Microsoft Office

Microsoft Office provides another point of entry into these systems. As with the operating system, the Microsoft Office suite installation should not use the default install. Microsoft Office patching is a complex process that makes the patch testing process for critical security patches and component upgrades more difficult.

The Microsoft Data Engine used by Microsoft Access is difficult to keep patched and should not be installed unless absolutely necessary. The most secure solution is to leave Access out of the custom installation and use a database like Microsoft Structured Query Language hosted on a server.

The installation of Outlook and PowerPoint add to the vulnerability profile and should not be loaded. If needed, they should be used on a computer separate from the SCADA system.

For all Microsoft Office applications installed, a security policy (pushed from a centralized server) should be implemented that, at a minimum, requires the operator to accept macros prior to running them and to ensure that they are authenticated. If this capability is not required, then macros should be permanently disabled. Note, however, that disabling macros also locks out ActiveX controls used to initiate events and may disable the automated patching process.

When performing a custom installation, select only those items that are needed for the operation of the console to reduce the vulnerability profile. This installation should be pushed from a centralized server to provide a common install for all consoles. Where consoles have different functions and different requirements, a custom install based on the console function should be considered. For example, an operator's console will have different needs and a different security profile than a development console.

As Microsoft Office does not have a strong signature in the system, it can and should be patched more frequently than the Tru64 systems. Failure to maintain current patches opens the system to evolving threats from the highly visible Microsoft product.

6.7 Cyber Security Recommendations for SCADA Systems

6.7.1 Passwords

Most SCADA vendors instruct their customers to change the passwords during installation. However, experience shows that this instruction is only implemented about 50% of the time. Furthermore, it may not be obvious to all customers just what accounts are on the systems, and they may miss some even if they make this change. To alleviate these problems, each account should be given a unique, strong password and each system should be delivered with a different set of passwords. This way, each customer will have unique passwords on their systems, eliminating the possibility of a mass exploit through the use of default passwords.

Strong passwords mean a minimum of eight characters, including upper and lowercase letters, numbers, and special characters. The allowable special characters vary by operating system and application.

Because even the best passwords can be cracked given enough time, passwords need to be changed regularly. One hundred and eighty days should be the longest a password is in use for the least privileged accounts, and the frequency (and password length) should go up with the privilege level. Thirty days and 12 characters are good choices for the most privileged accounts. These recommendations are standard industry practice for cyber security policies.^c Use the operating system's features to enforce the policies.

The Windows systems default installation enables SYSKEY, which is good because it requires having both the SAM and SYSTEM files to crack the passwords. Unfortunately, getting copies of these files is possible from compromised accounts, and then a password-cracking tool does the rest.

While the Windows password schemes are weaker in general than most other systems, of particular concern is the LAN Manager password hashes (for compatibility with Windows versions prior to NT). These hashes, which are particularly weak, are parallel to Windows NT LAN Manager password hashes and should be disabled.^d

6.7.2 Updates

Many vulnerabilities can be eliminated by updating the operating systems and applications with the latest vendor patches. Key applications and operating system components will also need to be updated regularly in addition to the security patches. For instance, the Jet engine, MDAC, DirectX, and ActiveX components should be updated on Microsoft platforms even though they do not appear to be critical updates. Major changes to the operating system via low-level system patches often break these components, which are critical to application performance.

6.7.3 Applications

Do NOT install applications that are not essential to operations and install only the most limited of options if the applications must be installed. For instance, if Microsoft Office must be loaded, then load

^c SANS Password Policy: http://www.sans.org/resources/policies/Password_Policy.pdf

^d Microsoft article on disabling LAN Manager hashes:
<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q147/7/06.asp&NoWebContent=1>

only those components needed for control system management purposes, not the entire Office suite. Other applications that can be stripped down or not loaded at all during the installation process include databases, Web browsers, Web servers, e-mail clients and servers, games, chat clients, and remote administration tools. If needed only for business purposes rather than control system management, these applications should be loaded on a separate computer rather than on any of the SCADA components. If the applications are needed to manage the control system, each application should be reviewed for secure configuration and a plan for updating and managing the software should be included in any life-cycle management cycles.

NOTE: Applications typically do NOT uninstall cleanly from the Microsoft operating system. If any unnecessary, major applications such as Outlook or Access have been loaded on a computer, the operating system should be rebuilt and the applications loaded in a customized fashion.

6.7.4 Encryption

Replace necessary applications that use clear-text protocols with alternative applications that use encrypted protocols; for example, secure shell instead of telnet, and secure copy or secure ftp instead of FTP. Remote login (rlogin) can be directly replaced with secure shell, which was designed as a direct replacement for it.

When encryption is not used, messages between computers and other system components can be viewed, intercepted, and/or altered. Communication between components can be passively read for information gathering. A man in the middle attack could intercept and possibly change messages or commands going between the HMI and SCADA hardware. Included in the clear text information being intercepted could be user names and passwords. Once a user name and password pair has been “sniffed off the wire” the attacker can come back at any time to masquerade as that user until the password is changed. When all communications are encrypted, the attacker must be able to decipher the messages before reading or changing them.

6.7.5 Services

Services that are not needed should be disabled. Each of these offers another avenue of attack. As with other secure configuration techniques, turning off services may interfere with application or operating system performance and should be tested thoroughly on any platform.

6.7.6 Domain Name Services

As noted previously, DNS provides several opportunities for attackers, both in the applications themselves having vulnerabilities and in being able to forge answers to legitimate requests. In small, static networks, eliminating DNS entirely (clients and servers) and placing only the needed entries in each systems’ “hosts” file provides the necessary functionality and provides better protection.

6.7.7 Address Resolution Protocol

Similar to the DNS issues above, ARP is exploitable on a given network segment for a man-in-the-middle attack. If there are only a few systems on the network, hard coding the ARP tables on each computer will prevent these attacks. However, if there are more than a handful of systems, this quickly becomes a labor-intensive task and inhibits network troubleshooting.

There is a problem with the Windows 2000 systems in that gratuitous ARP's will override the static values. Windows XP and Tru64 are not subject to this problem, so a man-in-the-middle attack would have to be targeted at two Windows 2000 machines to be effective, if this recommendation is implemented.

6.7.8 Windows Administrative Shares

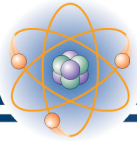
Windows enables “administrative shares” by default for the convenience of the administrator. Unfortunately, this is also for the attacker’s convenience and few administrators employ them anyway. These shares (C\$, D\$, ADMIN\$, etc.) should be disabled.^e As with other secure configuration techniques, locking down the administrative shares may interfere with application performance and should be tested thoroughly with any applications that will be loaded on the system.

6.7.9 Intrusion Detection

To quote information security expert, Eric Cole^f, “Prevention is ideal, but detection is essential!” New vulnerabilities are being found all the time. Furthermore, human errors cause once secure configurations to become less so. A problem cannot be addressed if no one knows it exists. For these reasons, SCADA vendors should strongly encourage their customers to install intrusion detection systems (IDS) on critical networks. Because of the lack of security logging inherent in most SCADA systems, particularly legacy technology, an IDS can provide information on network traffic, anomalous activity, and successful attacks that might not otherwise be available.

^e Microsoft article on disabling administrative shares: <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q314984&sd=tech>

^f Eric Cole is the best-selling author of *Hackers Beware*, and is the highest-rated speaker on the SANS training circuit, earning rave reviews for his ability to educate and train network security professionals worldwide.



7. CONCLUSIONS

Based on testing at the INEEL, the following recommendations have been developed for SCADA vendors using similar resources to the ABB system.

At a minimum, a guide should be provided to all end users listing the default accounts and passwords of the delivered systems. This should include specific procedures and recommendations on how to implement a security profile for each server and console type. The procedures should include information on best practices for users and groups as well as providing minimum password requirements.

Use of Microsoft's default installation for Microsoft products is not recommended. Microsoft's default installations leave the system wide open to attack. This includes installations of Microsoft Windows 2000 server, Microsoft Windows XP Pro, and Microsoft Office.

All systems should be examined independently for unneeded applications, open ports, services, groups, and users. Only those functions needed for SCADA/EMS operations should be implemented.

All network communications between the system components should be encrypted. Even though encryption can slow down the performance of the SCADA system, it prevents intruders from reading plain text messages that could contain user names, passwords, or other key information.

These guidelines allow the SCADA vendor to eliminate much of the "low-hanging fruit," as a first step in securing the power grid.

The specific results of this testing were reported directly to ABB for evaluation. Using these specifics and their own in-house resources, ABB has developed the next generation of their SCADA/EMS system. This system will be delivered to INEEL for testing to evaluate the success of these modifications and for subsequent vulnerability assessment. Through this pattern of testing, modification, and validation, ABB is assisting DOE/OEA and INEEL in evaluating SCADA systems for security with the goal of securing the nation's critical infrastructure.

