A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)

Systems and Network Analysis Center

Released: August 20, 2010
Version: 1.1

Publisher's comments:

This publication is the first in a series intended to help Industrial Control System (ICS) owners and operators in need of improving the security posture of their systems. This document will focus the reader on aspects of network security and give them a framework for assessing their current operational risk. It will then offer the reader a quantifiable approach to help them make decisions for reducing risk and improving their systems security posture.

Table of Contents

1. Introduction

Industrial control systems (ICS) monitor and control complex industrial processes like petroleum refinement, chemical production, product manufacturing, and electric power generation and transmission. Modern ICS infrastructures consist of a variety of intelligent, microprocessor-based equipment communicating over potentially complex distributed network links.

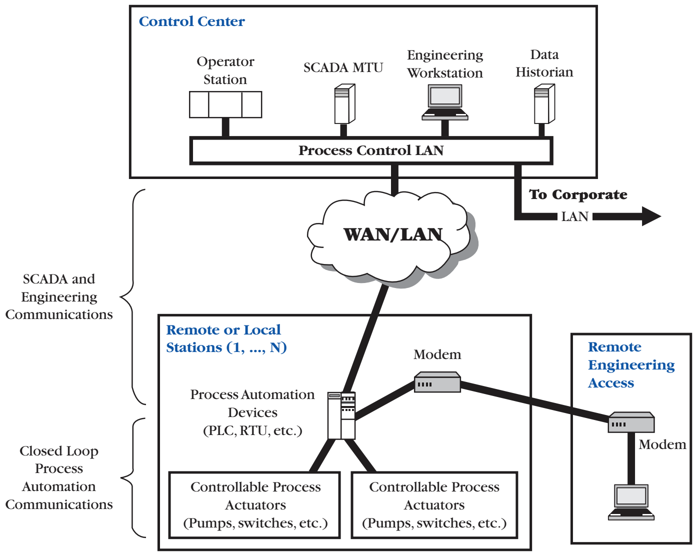

Figure 1: Overview of a Generic ICS Communications Network

Most ICS networks contain communications links similar to those shown in Figure 1, including:

- ***Communications for Closed Loop Process Automation:*** industrial processes are controlled by networked ICS equipment and by process automation devices[1] that gather process status (e.g. switch positions or motor RPM), run preconfigured process control algorithms, and send commands to implement the process changes dictated by the executed control algorithms (e.g. raise motor RPM, open a breaker, or turn a pump on). This cyclic, closed loop control cycle repeats as often as tens of milliseconds.
- ***Communications for Supervisory Control and Data Acquisition (SCADA):*** plant operations personnel in a control center monitor the status of processes on PC-based operator workstations and/or on large system mockup displays. One or more SCADA master terminal units (MTUs) located in or near the control center periodically gather process status from networked ICS equipment and make it available to operators and other personnel. Controls on the operators' screens allow them to manually alter the process if required. The MTUs then relay these commands from the operators to the networked ICS equipment for communicating the requested process changes. The communications between the MTUs and the networked ICS equipment are implemented using dedicated SCADA protocols like DNP3 or IEC 60870-5-101/104. For large ICS infrastructures, like those that control natural gas distribution or electric power transmission, the MTUs must communicate with many geographically dispersed process automation devices in remote stations.
- ***Communications for Configuration and System Engineering:*** engineering and management communications allow personnel to change settings or configurations in networked ICS devices to alter the behavior of the equipment. For example, ICS personnel may use a remote engineering access connection to make changes to the process control algorithm executing in a networked process automation device.
- ***Communications for Process Data Archiving and Retrieval:*** subsets of the process status values, executed commands, and received system alarms are typically

[1] Process automation devices include Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and digital protective relays that monitor and protect electric power system equipment (transmission lines, transformers, etc.)

stored in a database server for archiving and trending purposes. This data is often made available to system planners, billing departments, and other personnel on the control center SCADA network and/or corporate business network.

Much of the United States' critical infrastructure is dependent on industries that employ networked ICS systems. Sabotage or disruption of these industries can have wide-ranging negative effects including loss of life, economic damage, property destruction, or environmental pollution. Our reliance on ICS networks makes them attractive targets for electronic attack. Because of this, it is important for industrial control system owners and operators to systematically assess the threat of electronic attack against their critical networked assets and to apply defensive technologies to reduce the threat.

Cost-benefit analysis allows us to prioritize defensive efforts by identifying security improvements that provide the greatest benefit for a given cost. The "cost" is the expenditure required to implement and maintain the security improvement (financial, manpower, etc.) The "benefit" is the empirical savings gained by having the security improvement in place.

The process of deciding the value of the "benefit" of a security improvement involves assessing the impact or loss you are likely to incur in the event of a successful electronic attack, recognizing that security improvements reduce the chance of incurring these losses.

In this publication, we discuss the process of assessing the potential impact or loss incurred by successful compromise of networked ICS assets or network links. The loss potential is a direct function of two factors: the loss due to a single, successful cyber-incident and the expected frequency or likelihood of such incidents. Points in the ICS network that simultaneously exhibit a high loss potential and a high potential for electronic compromise (e.g. are highly vulnerable to cyber-attack) are high priority areas where application of security improvements are likely to yield the greatest benefit.

2. Network Connectivity Assessment

The first step in any electronic security assessment is to create an accurate map of all networked assets and the digital communication links that connect them. Accurate network maps are critical for identifying mission critical assets and the electronic attack avenues that may threaten their reliable operation. The network connectivity audit should produce written documentation that clearly and accurately records information about every networked asset, including:

- Unique identifier (serial number or assigned tag number)
- Description of functionality, mission/purpose, etc.
- Physical location
- Physical security mechanisms protecting the device (fences, locked cabinets, etc.)
- Network connections to/from the device
- Network addresses (MAC, IP, SCADA, etc.) assigned to the device
- All other available physical interfaces

2.1. Physical Network Audit

Most complex networks are at least partially documented during the design and planning phase. Such documents can serve as a starting point for a security-related network audit but must not replace a comprehensive, visual verification of all network connections. This process involves inspecting network media installations to trace all connections between networked assets and locate undocumented devices, data taps, etc. Undocumented connections to unauthorized and unmanaged assets can severely compromise the security of an ICS network. For example:

- Undocumented PCs may remain unpatched and vulnerable to known exploits
- Unauthorized wireless access points may provide direct access to critical network segments
- A PC with two network interfaces may provide an unsecured bridge between network segments
- A network tap in a communications cabinet can allow malicious data injection and interception
- A device or system modem connection previously used for maintenance purposes

A thorough physical audit should reveal the presence of all assets connected to the network and eliminate security "blind-spots" posed by undocumented/unmanaged assets. Tools, like the Sandia National Labs ANTFARM (see www.rubyforge.org), have been created to assist in mapping out the network topology.

2.2. Electronic Host Discovery

Electronic host discovery methods may be necessary to identify network connections where a visual media trace is not possible (e.g. point-to-multipoint wireless connections or physically obscured node connections). Active host discovery scans that send traffic onto the network must be used with extreme caution on critical ICS networks. Such scans can have adverse effects on network performance due to increased scan-related network traffic load. Network bandwidth degradation or adverse device reaction to scan traffic can cause loss of critical process control functionality, with potentially dangerous consequences.

The following list outlines several electronic host discovery techniques and provides guidance on their use in critical ICS network segments.

- ***TCP/IP Device Discovery:*** tools like nmap allow you to scan a wide range of IP addresses to discover attached hosts/devices. Execute a simple ping scan and avoid high traffic options like port scans and version or operating system discovery. Set the scan options to slow the scan down to a safer rate (e.g. one packet per second). Also, exclude all critical ICS equipment for which you know the IP address in order to reduce risk of unexpected reactions.
- ***Wireless 802.11x Device Discovery:*** handheld wireless audit devices are widely available that allow you to safely discover nearby 802.11x-based devices and IP network access points. Use a product with a highly directional antenna to help track down device location. Most wireless audit products do not send traffic directly to the network, though some traffic may be sent to the receiver itself. Because of this, such scans are fairly safe even on ICS networks. Because of the threat posed by undocumented 802.11x devices, wireless site audits should be performed during network security assessments.

Passive Traffic Analysis: traffic captured from a network tap or monitor port can be parsed to identify hosts communicating over the tapped or mirrored link. Passive traffic analysis does not directly affect the network once the tap point has been installed. TCP/IP parsers like Wireshark are widely available, but commercial, non-IP traffic parsers (e.g. serial SCADA protocol parsers) can be hard to find for ICS-specific protocols. Passive traffic analysis does not always produce high-confidence results because only actively-communicating hosts are detectable.

Most complex, hard to trace network segments are IP-based because the routing and addressing capabilities of TCP/IP allow for extremely large, interconnected network architectures. You will most likely not need to use electronic host discovery methods on simpler, non-IP, wired network segments (visual inspection will usually suffice).

3. Loss Assessment

The goal of a comprehensive loss assessment is to identify actions that can be performed by a motivated attacker via unauthorized electronic access to the device or network link that services it. Communications services[2] receive data from the network, process the data, and potentially send responses to the network. Any service that receives data from the network can potentially be manipulated or exercised by a motivated attacker. Malicious manipulation can come in the following forms:

- ***Unauthorized Use of the Intended Function of the Service:*** an attacker may use the intended function of the service to cause malicious actions. Examples include unauthorized operation of process control points via a SCADA service or unauthorized manipulation of device settings via an engineering access service.
- ***Exploiting Unintended Flaws in the Service:*** an attacker may discover flaws in the code that implements the communications service to cause actions that were not intended by the designers. Examples include execution of malicious code to take over the device or sending data to the service to cause an error in the code, causing the device to go offline or reboot.

A qualitative measure of the potential loss incurred by unauthorized access to a device or network link requires knowledge of the services available on the device or link and the actions that a motivated attacker could perform by manipulating the available services.

3.1. Identify Electronic Services Available on Device Interfaces over Network Links

Most embedded ICS devices are designed to implement a very limited, specific set of communications services. In general, the designed communications capabilities of these embedded devices are static and cannot be altered by installation of third party software. Product literature is a good place to start when trying to determine which services are running on an embedded ICS device's networked communications ports. Product documentation will almost always reveal details about the electronic communications services required for the device to perform its intended mission (e.g. where the dedicated SCADA port is and which process status and control points are available on it, or how a user can reconfigure the device via the engineering access service). Product literature should document product implementation details including:

- The number of physical interfaces, where they are located on the device chassis, and how they connect to other networked devices (e.g. Ethernet TCP/IP or RS-485 multi-drop serial)
- Functionality/services available via a given interface (e.g. what you can do via the interface)
- Configuration settings that control which services are available on a given port (e.g. a setting that specifies choice of Modbus or DNP3 SCADA protocols, or a setting that disables FTP)

[2] A service is any independent program or task running on a device that sends and/or receives data through a physical interface over an electronic communications link to perform some dedicated function.

- Configuration settings that control or limit functionality of a given service (e.g. settings that determine which process control command points are available on the SCADA interface)

Services selected when ordering a device can dramatically change a given device's communications capabilities, so it is important to have ordering information available when assessing a device's networked services. This information is often encoded in the device's order code found in the delivered literature or on the device itself (printed on an external label or available via the user interface). In addition, the active configuration/settings can change the communications profile of in-service devices (see the list above) and should be consulted to verify the current status of the device whenever applicable.

Some critical ICS devices, however, do not have static (or at least predicable), well-documented communications profiles. For example, PC-based ICS equipment and workstations are extensible in the sense that installed malicious software or planned, third party software packages can open additional communications services. In addition, modern PC operating systems are extremely complex and include standard services for file sharing, remote access, etc. that can be enabled by changing a few simple settings. For these complex, dynamic devices it may be necessary to conduct active scanning and analysis tests[3] to enumerate the services available on a given interface. Active scanning can also reveal undocumented functionality/services in "simpler" embedded devices (e.g. undocumented functionality for vendor calibration, testing, or servicing).

We have already discussed the potential consequences of conducting active testing on critical, in-service ICS network segments and equipment. Because of these dangers, it is always best to conduct active service scans of critical ICS devices by staging "cloned" devices on a test network. Embedded ICS devices can be "cloned" by using similar models with comparable settings/configuration. PCs can be "cloned" using hard drive duplication software like Norton/ Symantec Ghost.

TCP/IP scanning tools like nmap can be used to enumerate all TCP and UDP services running on any TCP/IP interface. We recommend scanning all valid TCP ports (1 through 65535), and all valid UDP ports (1 through 65535) to ensure that all available services are discovered. Such a scan sends tremendous amounts of scan frames onto the network and to the target device, and should only be conducted on a test network, or at a greatly reduced scan rate (set scan options to reduce the rate of transmissions).

3.2. Identify Consequences of Unauthorized Access to Devices or Network Links

Each communications service available on a given interface enables remote users or processes to perform some set of functions. Authorized use of these functions by trained ICS personnel and configured processes is an essential component of an ICS network. However, a motivated attacker may choose to exercise these functions to cause damage, incite confusion, or perform other malicious actions. It is the empirical cost of these malicious actions that we wish to assess and prioritize. With the services identified, we can assess the actions that can be performed via the network interface (e.g. via any and all services available on the interface). Examples include:

- ***Alter Process Status in Transit:*** process status points like flow rate, electrical breaker

[3] Active tests send traffic to the device via external software to identify and exercise services or functionality.

status, or fluid pressure may be observed and altered via a compromised SCADA or process automation link. The altered values may cause process automation equipment or monitoring personnel to react inappropriately and compromise the integrity or safety of the system/process.

- ***Exercise/Operate Process Control Points:*** an attacker may send process control commands that control pumps, open or close breakers, or change process set points via a SCADA or engineering access link. These actions may put the controlled process in an unsafe or unstable state.
- ***Reconfigure ICS Devices:*** an attacker may alter the active device configuration/settings to alter the behavior of the device. For example, an attacker may alter the control algorithm in a process automation device to damage critical equipment or injure personnel
- ***Steal or Intercept Sensitive Data:*** an attacker may intercept unencrypted sensitive data like passwords, intellectual property, or network documentation in transit, or access it directly via file sharing/transfer services or the user interface.
- ***Delete or Corrupt Data:*** unauthorized file system access or system destruction may lead to lost or corrupted data.
- ***Disable the Device:*** an attacker may be able to disable critical devices by sending malicious traffic to the device or by erasing/invalidating firmware or configuration files.
- ***Install Malicious Software:*** an attacker may install altered firmware or take advantage of known flaws in a communications service to execute malicious software on a target device. The installed software/firmware may open communications backdoors or otherwise alter the behavior of the target device.

With malicious actions identified, it is possible to at least subjectively assess the costs associated with a cyber-attack against a network interface or network link. This "value" is the cost or consequence of plausible, worst case scenarios for attacking the services available on the link. These costs can involve estimated dollar values, or more esoteric notions of cost. Following are some examples of potential costs or consequences associated with a successful cyber-attack:

- Value of damaged equipment or damaged product
- Human death or injury
- Environmental damage or cleanup costs
- Cost of lost production including those incurred by customers due to loss of supply
- Loss of customer confidence or company reputation
- Fines or penalties
- Cost of legal actions
- Costs associated with stolen or destroyed data

The process of assessing cyber attacks and their consequences will require direct involvement by personnel that are intimately familiar with the engineering and operation of the ICS and the processes that it monitors/controls. For example, personnel with knowledge of the control programs executing in a process automation device and how their manipulation or loss will affect the process, or personnel familiar with the system-wide effects of malicious operation of high voltage breakers in an electric power system.

3.3 Assign a Loss Metric to Each Networked Asset

It is extremely difficult to assign a fixed dollar amount to consequences of a cyber-attack against a network interface or device: how do you decide how many dollars a human life or polluted river is worth? It is usually sufficient, however, to use a graduated scale like [low, moderate, high] or [(least severe) 1-10 (most severe)]. The number of graduations in the scale is not critical, but it is important to formulate a set of rules governing the assignment of the levels (e.g. any potential for loss of human life necessitates a severity rating of "high", or any action that results in a loss of production of X percent of capacity for Y hours gets progressively higher severity rating as X and Y increase above predetermined levels).

FIPS Special Publication (SP) 800-82[4], Appendix E contains a summary of efforts by the National Institute of Standards and Technology (NIST) to apply federal risk assessment and security standards to ICS networks. The NIST methodology assigns three loss metrics to separately record the impact of losses due to compromise of:

- ***Confidentiality:*** a compromise of confidentiality is the unauthorized release or theft of sensitive information. Examples include theft of passwords in transit or intellectual property from a file server.
- ***Integrity:*** a compromise of integrity is the unauthorized alteration or manipulation of data. Examples include manipulation of billing information or alteration/injection of SCADA protocol commands.
- ***Availability:*** a compromise of availability is the loss of access to the primary mission of a networked asset. Examples include malicious corruption of device firmware to disable critical ICS functionality or deletion of important data from a file server or database.

For example, a critical SCADA MTU may receive the following loss metric:

1. ***Confidentiality loss metric = LOW:*** unauthorized disclosure of SCADA point maps, protocol details, etc. would not result in significant losses.
2. ***Integrity loss metric = HIGH:*** tampering with SCADA maps, alteration of process status information in transit, or injection of false commands can result in death and extreme loss.
3. ***Availability loss metric = MODERATE:*** loss of SCADA MTU availability would result in manual operation or shutdown and recovery of MTU functions, but no catastrophic losses.

Prioritizing the existing avenues of attack to the ICS (for the loss of confidentiality, integrity, and/or availability) will help us determine and choose the appropriate defensive technologies to integrate into the system. For example, preserving confidentiality may require encryption technologies or additional access controls, whereas preserving availability may require additional redundancy or disaster recovery planning.

One way to convert the three loss metric values to a single loss metric assigned to the network interface or device, is to simply use the highest assigned metric value from the confidentiality, integrity, and availability loss metrics (e.g. HIGH for our example above).

4. Threat Assessment

The potential loss due to a cyber-incident is a function of both the consequences of the achievable malicious actions, which are identified during a comprehensive loss analysis, and the expected frequency of such incidents. The frequency of cyber-attack rises when both the number of motivated attackers rise, and sufficient opportunity exists for attackers to gain a level of system or network access adequate enough to perform potentially-damaging actions: both motivation and opportunity must be present.

[4] FIPS Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, is available at the National Institute of Standards and Technology, Computer Security Resource Center website at csrc.nist.gov..

4.1 Identify Attack Sources and Potential Motivations

Knowing the identity of potential attackers and the motivation that drives them can be very useful in determining where attacks are likely to come from and what the most probable goal of the attack is likely to be. This knowledge, in turn can help prioritize and focus defensive efforts.

It is also possible to fall victim to unintended attack by automated tools and malicious software designed to propagate attacks against other targets. For example, worms and viruses are sometimes created by hackers to automate the takeover of Internet-connected PCs. A user may accidently transport a worm onto a closed ICS network via removable media, resulting in an untargeted attack by self-propagating software.

Threat Source	Description and Motivation
Insiders	An insider is a user for whom a list of authorized system access privileges are defined (e.g. physical access or partial electronic access to some system assets), but chooses to perform unauthorized actions against the system. An insider may be motivated by job dissatisfaction, revenge, or monetary gain. They can be an employee of the targeted company or a third party entity given system access for maintenance or contractual purposes. Their knowledge of the system and access privileges can greatly enhance their ability to conduct an effective attack.
Terrorists or Activists	A terrorist or activist is any individual or group motivated by ideology to perform targeted attacks that promote their philosophy or cause. For example, anti-Western terrorist organizations may be motivated to attack U.S. interests by executing attacks that result in mass casualties or damage to the U.S. economy. An environmental activist group may attack a nuclear power plant ICS to cause a televised incident and sway public opinion against nuclear generation.
Hackers or Cyber-Criminals	Hackers and cyber-criminals are motivated by financial gain, notoriety, or simply by the thrill of the challenge. Cyber-crime can be extremely lucrative. The sale of cyber-resources including credit card information, stolen intellectual property, or networks of compromised, Internet-connected servers has created a burgeoning black market economy. The tools created for these purposes are openly shared on the Internet, creating a large population of professional and "recreational" hackers.
Nation/State Sponsored Cyber-Warfare	Nation/State sponsored cyber-warfare programs can be well-funded and legally protected by the hosting nation. Such programs may concentrate on identifying electronic methods for harming the infrastructure and economy of target countries. ICS networks are used to monitor and control much of the world's critical infrastructure and may be a primary target of state sponsored warfare programs.
Competitors	ICS systems often control processes that produce marketable products. Competitors may be motivated by financial gain to steal intellectual property or to sabotage critical systems to reduce competition in the marketplace.

Table 1: Overview of Potential Attack Threats and Motivations

4.2. Identify Roles and Privileges of Authorized Users

Identifying and documenting the rights and privileges of all authorized system users is essential for enforcing the "principle of least privilege", and for assessing the threat posed by insider attacks. The principle of least privilege is the policy of employing physical and electronic access control technologies to ensure that users can only execute actions required to carry out their role or job duties.

Proper network segmentation is also largely driven by user roles: users with similar authority and requirements are typically grouped together and given electronic access only to network segments consistent with these requirements. Electronic connections between network segments populated by users and devices with dissimilar roles or authority can form an avenue of attack. Defining user roles and enforcing the principle of least privilege is an essential tool for limiting the insider threat and for restricting/ slowing attack propagation.

4.3. Identify Potential Electronic Attack Vectors

Electronic attack vectors are any vulnerable electronically accessible point within an ICS network. Of these points, any which are outward facing toward a hostile electronic network threat are the most likely entry points for an adversarial attack. Identifying these potential points, along with the entire electronic attack footprint[5] (if possible) into the defendable network, and quantifying the threat exposure posed by these entry points and footprints is an essential aspect of a network security assessment. Exposing a network interface to motivated attackers puts the attacker in a position to probe the device's interface for vulnerabilities that can result in the identification of entry points into your system.

A defendable network segment is a subset of a network that exhibits the following properties:

- Assets within the electronic perimeter of a defendable network segment operate within a secure physical perimeter (locked building, fence line, monitored multi-building facility etc.) and are physically accessible only by personnel with definable roles and authorities
- Users with local electronic access to devices and network access points within the defendable sub-network electronic perimeter have similar roles and authorities (e.g. similar trust and/or privilege profiles)

This definition assures that assets within the defendable electronic perimeter are physically isolated from outsiders[6] and can be effectively monitored. Also, they are not significantly exposed to electronic attack from users within the defined electronic perimeter due to their similar trust profiles. Because electronic attacks are more likely to come from outside the defendable electronic perimeter, the electronic access points into the perimeter represent the highest risk network connections.

Network connections that leave the *physical* perimeter of the defendable network may be susceptible to wiretapping or electronic intrusion by outsiders. Wide area network (WAN) connections exhibit a wide range of relative risk depending on the technology/media used to implement the connection. WAN infrastructures that are open to unfettered, global access by potential attackers are of particular concern. Following are some examples of common WAN technologies and the risk they pose to ICS network segments that use them:

- ***Internet:*** the Internet is a globally-accessible

[5] Electronic path through a system which characterize the attacker's successful attack path.

[6] Outsiders are unknown individuals with no definable role or authorization on the network.

mega-network that has become the primary avenue of attack for those wishing to conduct targeted or random cyber-attacks. Any device addressable via a public IP address can be directly attacked from anywhere in the world. Internet-born attacks may propagate through vulnerable systems and target indirectly-connected, critical ICS network segments.

- ***Dialup:*** dialup modems used for remote access into critical ICS devices or network segments are globally-accessible. Any attacker with the telephone number of the line can connect to the modem and directly attack the connected equipment. These modems often form direct backdoors into the heart of critical, "protected" ICS network segments.
- ***Leased Lines:*** lines leased from third-party bandwidth providers (e.g. a telephone company) are owned and managed by the provider, so you do not have direct control of the security of the media. For example leased lines implemented via the public switched telephone network may be susceptible to attacks that target remotely-accessible switching and routing equipment.
- ***802.11x Wireless:*** 802.11x wireless access points provide direct access to the TCP/IP network segment to which they are connected and can form backdoors into protected ICS networks. An unsecured WiFi access point can be easily located and penetrated from many miles away with a high-gain antenna using readily-available software and equipment.
- ***Non 802.11x Wireless:*** non-WiFi radio links (e.g. microwave) are not as likely to be randomly located as 802.11x-based implementations, but links can still be located using spectrum analysis tools or by visually locating antennas at target locations. Unsecured links are susceptible to data interception and injection, and may be jammed and disabled using commercial transmitters.
- ***Wholly-Owned Media:*** wholly-owned fiber or copper media can be very safe WAN alternatives, but should be physically managed and monitored to prevent wiretaps in communications breakout cabinets or accessible cable runs.

Links between defendable network segments may also be susceptible to remote electronic attacks by insiders. This risk is greatly increased if the principle of least privilege is poorly-enforced and these unauthorized actions are allowed to flow across the defendable electronic perimeter. It is important at this point to compare the defined roles and authorized actions of users on each of the connected, defendable network segments. As the trust or authorization discrepancy increases, the risk of insider attack increases.

Finally, connections between defendable network segments are conduits through which focused attack traffic and malicious software (e.g. worms and viruses) may propagate. Connections between critical, highly-managed network perimeters and "risky" network segments that cannot be adequately secured are of particular concern. A successful electronic attack against the less secured network segment can put the attacker in a position to launch attacks against the critical network segment through exposed electronic access points. Examples of risky network interconnections follow:

- ***Connection between ICS monitoring/control networks and corporate network segments:*** corporate or business network segments require connections to the Internet (usually indirect connections through firewalls or proxy servers) so users can send e-mail, access websites and perform other global communications functions. These services open corporate network segments up to global, Internet-born attacks that can propagate to connected ICS network segments.

- ***Connection between a critical SCADA database server and a third-party maintenance network:*** third party maintenance contractors often require access to critical ICS network segments to provide software and/or hardware support services. These third-party networks are not managed and controlled by the ICS owner so the security of the network cannot be trusted.

4.4. Assess Attack Difficulty

Attack exposure is greatly increased when critical actions can be executed with little effort by unauthorized individuals. The loss assessment process identifies the services that provide access to critical/costly actions and the first stages of the threat assessment identifies the exposure of these services to potential attackers. The final piece of the threat assessment is to more formally evaluate and determine the level of effort required to execute any of the actions identified in the loss assessment.

Firewalls and access control lists in routers are commonly used to block communication services from flowing through protected TCP/IP network connections. When assessing the difficulty of an electronic attack against a point on the network (e.g. via an identified attack vector), you must identify which services are available at the point of attack. As long as the firewall/router remains uncompromised and is configured correctly, the blocked services cannot be exploited at the point of attack. Tools similar to the Sandia National Labs ANTFARM can utilize the device configuration files to visually display all possible paths within the network infrastructure and help the analyst assess the device configuration correctness.

Any unfiltered communications service that receives attack data from the network may have flaws that make them susceptible to exploits that can cause malicious code execution or denial of service (e.g. remote take over or the disabling of a device). For services that commonly run on PCs, routers, and other IT infrastructure devices, known vulnerabilities are listed and documented on security websites (e.g. www.cert.org) or on vendor websites (e.g. www.microsoft.com). Vulnerabilities found in dedicated/embedded ICS equipment are not as publicly available. This is partly due to the sensitivity of the subject, but more so due to the fact that they have traditionally been isolated on protected networks and have not received as much scrutiny as other Internet-connected products. Using services with known vulnerabilities can greatly increase exposure to trivial attacks using "push-button" attack tools designed to exploit specific vulnerabilities.

Many electronic communications services have security mechanisms in place that impede unauthorized execution of the functions/actions offered by the service. Passwords/PIN-based authentication schemes and cryptographic services are common protective mechanisms. The effectiveness of such mechanisms depends on implementation specifics and minimum baseline constraints (e.g. minimum password length), and varies widely across services and vendors. Some examples of weak or non-existent security mechanisms common in ICS networks follow:

- ***SCADA Command Injection:*** lack of security mechanisms in SCADA and process automation protocols make them susceptible to trivial command spoofing and frame injection attacks that can execute/operate any process control points available via the interface. Almost every SCADA protocol in use in ICS networks is susceptible to such attacks unless the service is protected with external mechanisms (e.g. additional cryptographic protection protocols).

- ***Password Interception:*** authentication parameters (e.g. passwords) are often transmitted "in the clear" and are susceptible to interception via data taps or man-in-the-middle attacks (e.g. ARP cache manipulation). Examples include passwords protecting access to Telnet or serial terminal applications used for engineering access to critical ICS equipment, or FTP file access.
- ***Vulnerable Web Services:*** web browsers transmit data to/from the server in the clear unless SSL/TLS is used (e.g. https). Passwords and other sensitive information can be intercepted from the network via data taps or man-in-the-middle attacks. Even encrypted SSL/TLS connections are susceptible to man-in-the-middle data interception/manipulation attacks if the user ignores the security warnings posted by the client web browser. Finally, implementation flaws in the web services can allow attackers to input malicious command strings into user input fields that can be used to extract sensitive information from the server or execute malicious code (SQL injection attacks).
- ***Weak Authentication Mechanisms:*** ICS devices often use weak password or PIN entry authentication mechanisms to protect against unauthorized device configuration changes. For example, a scheme may not allow users to choose strong passwords (long, complex strings). Particularly simple passwords are highly susceptible to automated password guessing attacks.

Assessing the effectiveness of an implemented security mechanism often requires hands-on testing of a representative device (preferably on a safe test network). If at all possible, test the exact configuration of the device used in the operational network.

Weaknesses in user training or security policies and procedures can potentially subvert even the most effective security mechanisms. Unintended user actions can severely jeopardize the security of a network. For example, an authorized system user may accidently introduce a Trojan horse, virus, or worm onto a critical ICS network segment via an infected USB stick or CDROM, or be coerced by an attacker into revealing sensitive network details or passwords over the phone.

4.5. Assign a Threat Metric

The threat of successful cyber-attack increases as both exposure to motivated attackers increases and the ability to conduct damaging attacks increases. For example, a dialup engineering access link with a weak password-based security scheme (e.g. password set to the default value) is both exposed to a global collection of potential attackers, and vulnerable to trivial compromise.

It is important to assign a threat metric to each potential attack vector to quantify the risk of a successful cyber-attack occurring via that attack vector. Again, a graduated, scale should be sufficient to prioritize the threat levels at various points of the network.

5. Prioritizing Defensive Efforts

ICS networks can be complex and extensive. We must prioritize defensive efforts when securing these large networks in order to ensure that finite budgets and resources are allocated optimally, and to ensure that the most important security concerns are addressed early in the process.

Loss Metric	Threat Metric	Composite Priority Value
HIGH (3)	HIGH (3)	6
MODERATE (2)	HIGH (3)	5
HIGH (3)	MODERATE (2)	5
...	...	....
LOW (1)	LOW (1)	2

Table 2: Combining Loss and Threat Metric Contributions to form a Priority Value

Points in the ICS network that exhibit both a high potential loss metric and a high threat metric are high priority areas where application of security improvements are likely to yield the greatest benefit. It is sufficient to treat both metrics as equally-important and to add the contributions of the two metrics to form a composite priority metric. For example, assigning a numeric value of 1, 2, and 3 to metric values of low, moderate, and high, respectively, would result in the following composite priority values:

For the example in Table 2, we would place the highest priority on addressing security concerns for network interfaces or devices on the network exhibiting the highest priority values. Finite security resources should be allocated to securing these points on the network first. As the priority value decreases, the relative threat of a high-loss cyber-attack decreases.

In practice, you may apply a different method for combining the loss and threat metrics than the example shown in Table 2. For example, you may choose to weight the loss metric values higher than the threat metric values in order to reflect an elevated intolerance to loss.

6. Conclusions

Many current ICSes were not built to withstand networked cyber attacks. This paper has offered the reader a cost-benefit analysis approach which will allow them to prioritize their defensive efforts by identifying network security improvements that provide the greatest benefit for a given cost. It has discussed a process of assessing the potential impact or loss incurred by successful compromise of networked ICS assets or network links. Once a prioritized list has been created, a cost effective risk management approach to addressing system vulnerabilities may occur.

Systems and Network Analysis Center
410 854-6632 • DSN: 244-6632 • FAX: 410-854-6604