The DHS Control Systems Security Program

Contributing Authors: John Hammer, Jeffrey Hahn, Trent Nelson, Julio Rodriguez, Jeffrey Tebbe

At the 2006 UTC conference, representatives of the Department of Homeland Security (DHS) National Cyber Security Division provided an overview of the Control Systems Security Program. The presentations provided a demonstration of the Program's cyber security self-assessment tool for control systems as well as highlights of an industry and government collaborative effort to publish recommended practices. DHS recognizes the importance of cyber security and uses a variety of examples to raise control systems security awareness.

The example used at the 2006 UTC SCADA Security session was a demonstration of an adversary gaining access to an industrial control or Supervisory Control and Data Acquisition (SCADA) system. This article provides a brief summary of these presentations.

Brief overview of the DHS Control Systems Security Program

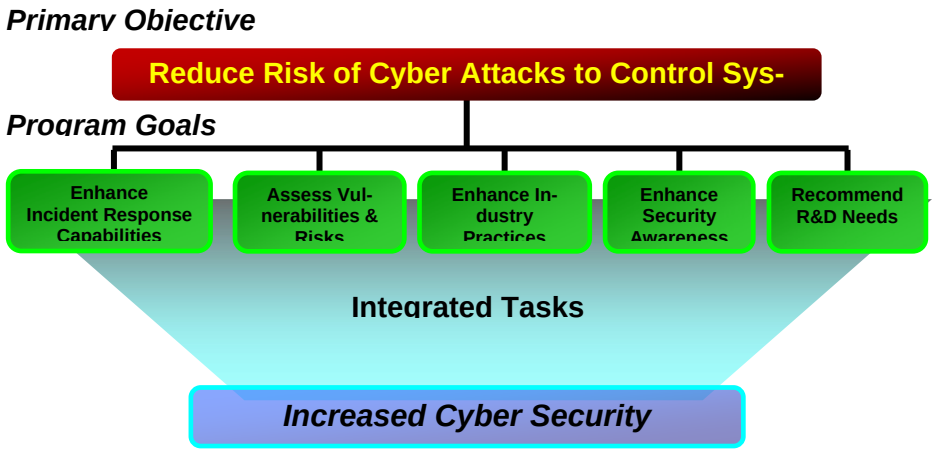
The primary objective of the DHS CSSP is to reduce the risk of cyber attacks to control systems within critical infrastructures and to identify and mitigate cyber vulnerabilities. The CSSP is supporting the control system community by enhancing incident response capabilities, developing cyber assessment tools, disseminating control systems security recommended practices, and providing awareness training. (See Figure 1.)

The CSSP utilizes the expertise and resources from other federal agencies, national laboratories, academia, and industry to reduce control system vulnerabilities.

A subset of the tasks being performed to increase cyber security includes--

- Identifying, analyzing, and informing the control systems community of emerging cyber threats and developing mitigation strategies.
- Conducting vulnerability assessments of vendor systems.
- Working with critical infrastructure sectors to identify vulnerabilities and risks.
- Participating as the cyber team member for the comprehensive reviews that are sponsored by the DHS.
- Validating a self-assessment tool for control systems that utilizes a database of control systems security requirements and associated recommendations.
- Working with control systems stakeholders in developing and generating recommended security practices.
- Working with standards bodies to enhance industry standards for control systems.
- Providing awareness training for control systems security.

Figure 1



Self-Assessment Tool for Control Systems

The cyber security Self-Assessment Tool was developed as a security tool to assist control system users to asses the cyber security posture of their control system networks. The Self-Assessment Tool assists users to identify the cyber security parameters of their control system networks and provides security objectives, in the form of specific actionable requirements, for improving security. Each requirement is linked to a series of associated recommendations for compliance - dependent upon the users desired level of security protection. The tool provides a repeatable and systematic approach for assessing the cyber security posture of industrial control systems.

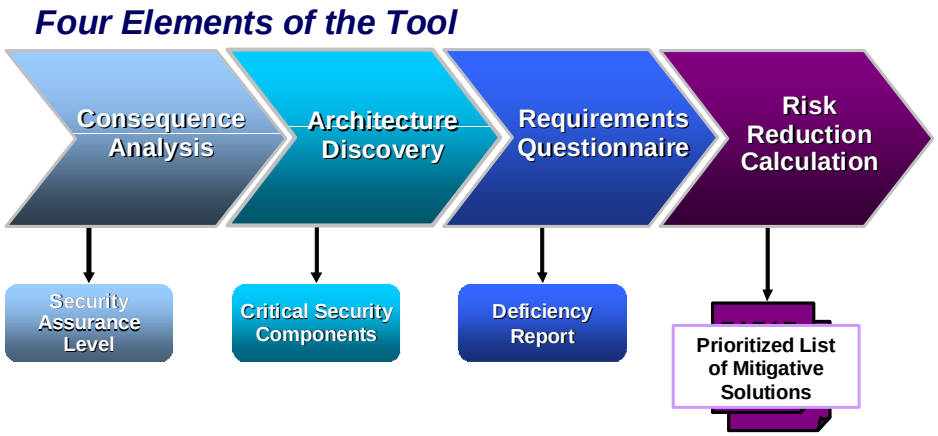
Industry Involvement

The CSSP recently began pilot testing the assessment tool with critical infrastructure asset owners across multiple sectors. The pilot tests include an on-site visit by the CSSP assessment team to assist asset owners in using the tool to identify security vulnerabilities in their system. The CSSP benefits from these tests by learning how to improve the tool and the asset owner benefits from the recommendations for improving their security posture that are generated by the tool.

How it Works

The tool is operated as a desk-top or lap-top application. The tool has four elements that function independently, but interface with appropriate information to provide an integrated result (see figure 2). As of June 2006, the first three elements (Consequence Analysis, Architecture Discovery, and the Requirements Questionnaire) are in beta testing. The Risk Reduction Calculation element is under development and is schedule to begin testing by the end of 2006.

Figure 2



The first element, Consequence Analysis, assists the user in analyzing the criticality of a site or facility - as it relates to the potential negative consequences of a successful cyber attack. This allows the user to determine how much rigor should be applied to reduce the risk of such a consequence. This element contains a questionnaire about the potential economic, loss of life (or injury), environmental, and/or cascading impacts of a successful cyber attack. Once the user has entered the responses, the tool calculates a recommended Security Assurance Level (SAL) for the facility or subsystem. The SAL provides a gauge of how much security rigor might be needed to reduce cyber vulnerabilities. The SAL also determines which set of security strategies (or level of rigor) will be recommended to meet the security requirements (i.e., the more severe the potential consequence, the more rigorous the recommendations).

The next element, Architecture Discovery, assists the user to identify the network topology that is critical to the system's security boundary. The tool's software contains a graphical user interface to assist the user in determining the cyber security boundaries and connectivity of the control system network. The network topology may be loaded manually or it may be interfaced to a non-intrusive network scanning capability that produces an XML file for uploading. Identifying the critical security components of the network topology is crucial to the selection of appropriate requirements and mitigation strategies.

Once the network topology has been established, the tool generates a set of questions specific to the critical components of the system and their connectivity. This is the Requirements Questionnaire element of the tool. The user selects the appropriate answer to the security questions that articulate the system's cyber security features. The answers are then compared to the requirements of the selected SAL. Upon completion of the questionnaire, the tool provides a list of deficiencies along with a graphical interpretation, to assist in identifying weak areas of the control system.

The results of the questionnaire are organized in charts and provide a series of scores to represent a level of confidence in compliance to the control systems security requirements. These scores will be a quantitative measure and allow the asset owner to prioritize efforts for improvement, as well as providing a baseline for measuring performance improvement over time.

The final element of the tool is the Risk Reduction Calculation. When completed, this component will identify the potential for risk reduction as security measures are implemented. Work on this module is continuing with an alpha version, scheduled to be available for testing by the end of 2006.

Recommended Practices

Recommended practices are used by control systems stakeholders in developing and implementing security solutions to their networks. These recommended practices are based on understanding the cyber threats, control systems vulnerabilities and attack paths, and control systems engineering. The CSSP and the control systems community are working together in order to make publicly available, recommended practices that have been vetted by subject-matter experts in industry.

The recommended practices working group has developed white papers on defense in depth and mitigations strategies for control system vulnerabilities, and has developed an interactive web site that discusses secure network architectures. More topics are planned to be published on a continuing basis. To learn more about the Recommended Practices working group and to review their products, follow the "Recommended Practices" web link at www.us-cert.gov/control_systems.

Understanding Control System Cyber Vulnerabilities

Control systems can be vulnerable to cyber attack from inside and outside the control system network. To understand the vulnerabilities associated with control systems it is necessary to know the types of communications and operations associated with the control system. Having an understanding of the how an adversary might use these system vulnerabilities to their advantage is also essential. There are many ways to communicate with an industrial control systems network and with the components that constitute the network. An individual who is knowledgeable in process equipment, networks, operating systems, and software applications can exploit cyber vulnerabilities to gain access to the industrial control systems.

Access to the Control System LAN

The first thing an adversary needs to gain access to a control system LAN, is the ability to bypass the network's perimeter defenses. However, common practice in most industrial control environments is to separate the business LAN from the control system LAN using a firewall. This not only helps keep intruders out, it also isolates the control system network from business network outages, worms, and other malicious code that can be present on the business LAN. Following are a number of common ways an adversary might penetrate these security measures and gain access to the control LAN. It is important to note, however, there are many other ways for an adversary to gain access.

One of the most common routes of malicious entry is directly dialing modems attached to the field equipment. Modems are used as backup communications pathways if the primary high-speed lines fail. In order to find the modem, the attacker could dial every phone number in a city looking for modems, or the attacker may dial every extension in the company looking for modems connected to the corporate phone system. Most Remote Terminal Units (RTUs) identify themselves and the vendor who made them. Many RTUs do not require authentication and it is common to find RTUs with the default passwords still enabled in the field.

Most control systems come with a vendor support agreement, since there is a need for support during upgrades or when a system is malfunctioning. The most common means of vendor support used to be through a dial-up modem connection. In recent years, that has transitioned to Virtual Private Network (VPN) access to the control system LAN. An attacker might attempt to gain access to the control system LAN via a "piggyback" connection to an internal vendor resource or field laptop.

Often it is the responsibility of the corporate IT department to negotiate and maintain long-distance communication lines. In this case, it is common to find one or more pieces of the communications pathways controlled and administered from the business LAN. Multiplexers for microwave links and fiber runs are the most common ways. A skilled attacker can reconfigure or compromise those pieces of communi-

cations gear to control field communications.

Most control systems have some mechanism for engineers on the business LAN to access the control system LAN. The most common mechanism is through a VPN connection to the control firewall. An attacker can then attempt to take over a machine by waiting for the legitimate user to VPN into the control system LAN and then piggyback onto the connection.

Nearly every production control system logs to a database on the control system LAN, which is then mirrored into the business LAN. Often administrators go to great lengths to configure firewall rules, but spend no time securing the database environment. A skilled attacker can gain access to the database on the business LAN and use specially crafted SQL statements to take over the database server on the control system LAN. Many databases are prone to this type of attack due to the perceived legitimate nature of the traffic A knowledgeable administrator can prevent this attack by implementing proper configuration rules.

Firewalls are often poorly configured due to historical or political reasons. Common firewall flaws include passing Microsoft Windows networking packets, passing "RServices", and having trusted hosts on the business LAN. The most common configuration problem is not providing outbound data rules. Improper outbound data rules may allow an attacker who can sneak a payload onto any control system machine to call back out of the control system LAN to the business LAN or to the Internet without detection.

Often the easiest way onto a control system LAN is to take over a neighboring utility or manufacturing partner. Historically, links from partners or peers have been trusted. In that case, the security of the system is only as strong as the weakest member. It is recommended that peer links be restricted behind firewalls to specific hosts and ports.

Control of the Process

When a cyber attacker gains a foothold on the control system LAN, the attacker needs little information about the process to shut it down. However, the attacker must discover the details of how the process is implemented to surgically attack it. A surgical attack can make specific changes to the control equipment or instrumentation, such as modifying quantities in a mixture, turning equipment on or off, or modifying the instrumentation output. An attacker that wants to be surgical needs detailed information about the process or system.

The two most valuable items to an attacker are the points in the data acquisition server database and the Human Machine Interface (HMI) or the operators display screens. Each control system vendor calls the database something different, but nearly every control system assigns each sensor, pump, breaker, etc., a unique number. On the communications protocol level, the devices are simply referred to by number. A surgical attacker needs the list of the point reference numbers in use and the information required to assign meaning to each of those numbers.

The operator's HMI screens generally provide the easiest method for understanding the process and assignment of meaning to each of the point reference numbers. Each control system vendor is unique in where it stores the operator HMI screens and the points database. Rules added to the Intrusion Detection System (IDS) looking for those files are effective in spotting attackers.

The easiest way to control the process is to send commands directly to the data acquisition equipment. Most Program Logic Controlers (PLCs), protocol converters, or data acquisition servers lack even basic authentication. They generally accept any properly formatted command. An attacker can simply establish a connection with the data acquisition equipment and issue the appropriate commands.

An effective attack is to export the screen of the operator's HMI console back to the attacker. Off-the-shelf tools can perform this function in both Microsoft Windows and Unix environments. The operator will see a "voodoo mouse" clicking around on the screen unless the attacker blanks the screen. The attacker is also limited to the commands allowed for the currently logged-in operator.

Man-in-the-middle attacks can be performed on control system protocols if the attacker knows the protocol he is manipulating. An attacker can modify packets in transit, providing both a full spoof of the operator HMI displays and full control of the system. By inserting commands into the command stream the attacker can issue arbitrary or targeted commands. By modifying replies, the operator can be presented with a modified picture of the process, which could cause the operator to take inappropriate actions.

Having an understanding of how an adversary can gain control or manipulate the data of a process control system, will help to

identify ways to block, detect and mitigate the consequences of a cyber attack. The DHS CSSP is working to provide information, product, and tools that will help industry increase the security of its control systems. For more information about the DHS CSSP visit www.us-cert.gov/controlsystems.

Laboratory. Jeff Hahn is an industry liason and can be reached at Jeffrey.Hahn@inl.gov. Jeff Tebbe, Self-Assesment Tool lead, can be reached at Jeffrey.Tebbe@inl.gov. Trent Nelson is Cyber Testing lead and his email is Trent.Nelson@inl.gov. John Hammer, cyber researcher, can be contacted using John.Hammer@inl.gov. Finally, Julio Rodriguez, program advisor and DHS liaison can be reached at Julio.Rodriguez@inl.gov.