Control Systems Cyber Security Awareness

US-CERT
Informational Focus Paper

July 7, 2005

Produced by:
United States Computer Emergency Readiness Team

Focus Paper – Control Systems Cyber Security Awareness

I. Purpose

The Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) Control Systems Security Center (CSSC) is taking this opportunity to remind the control systems community of the importance of cyber security for control systems. This focus paper on "Control Systems Cyber Security Awareness" is the first installment in a series of papers intended to provide relevant cyber security information to the control systems community. The control systems community encompasses those entities that have a vested interest in the security of control systems to include critical infrastructure owners and operators; standards and regulatory bodies; federal, state, and local governments; associations; academia; control systems manufacturers; vendors; and various service providers.

This initial focus paper raises cyber security awareness through discussion of control system cyber security trends and provides information on DHS and federal partner programs designed to enhance the cyber security posture of control systems within critical infrastructures. It also provides contact information on where control systems owners and operators can report, and obtain assistance with, control systems cyber security incidents and vulnerabilities.

Future control systems cyber security focus papers will present information on topics covering control system cyber threats, indications and warnings of control systems cyber attacks, recommendations for improving control systems security, ongoing control system cyber security initiatives by government agencies and private industry, and other relevant control systems cyber security topics.

II. Background

Our Nation depends on the continuous and effective performance of a vast infrastructure to sustain our modern way of life. Control systems, which are integral components of this critical infrastructure, monitor and control sensitive processes and functions including electricity generation, transmission, and distribution; natural gas production and distribution; petroleum products refining; transportation systems monitoring and control; water supply; wastewater treatment; chemical processing; discrete manufacturing; and numerous other critical operations upon which our Nation depends.

A control system is defined as the combination of computers, process control equipment, process interface systems and associated applications which work in concert to monitor the variables of a technical process and manage the process of interest. Names often used to identify control systems are supervisory control and data

acquisition (SCADA), distributed control system (DCS), process control system (PCS), energy management system (EMS), safety instrumented system (SIS), and manufacturing and control system (M&CS).

III. Trends

Historically, control systems that monitored and controlled critical infrastructure processes were operated in an isolated or stand-alone environment where computer systems and devices communicated with each other exclusively, and typically did not communicate or share information with systems not directly connected to the control system network. These control systems were typically comprised of proprietary hardware, software, and protocols designed specifically for control system operations. Knowledge of these proprietary applications and protocols was limited to a small population. Proprietary control system protocols and data were not readily available to the general population and significant effort and resources would have been required to acquire the proprietary information, understand the control system, discover vulnerabilities in the control system, develop the tools to exploit the identified vulnerabilities, and gain sufficient access to the control system so that vulnerabilities could be exploited to carry out unauthorized or malicious activities. For the reasons presented, in particular because access to control systems was greatly limited, critical infrastructure control system security efforts were primarily focused on protecting control systems from physical attacks.

More recently, with the vast information technology expansion and the drive towards having information readily available from any location, many previously stand-alone control systems are being transitioned to the “always connected” world, where real-time control system information can be readily and easily accessed remotely by vendors, engineers, maintenance personnel, business managers, and others via corporate networks, the Internet, telephone lines, and various wireless devices.

To reduce operational costs and improve performance, control system vendors and critical infrastructure owners and operators have been transitioning from proprietary systems to less expensive standardized technologies, operating systems, and protocols currently prevalent on the Internet. These widely accepted technologies, protocols, and operating systems, such as Ethernet, IP, Microsoft Windows, and web technologies, have a large number of known cyber vulnerabilities, and new vulnerabilities are reported on a daily basis. Exploitation tools, worms, and how-to papers are often readily available shortly after the announcement of a new vulnerability. Significant information on control systems is now publicly available, including design and maintenance documents, technical standards for the component interconnections, and standards for communicating between devices. In addition, control system security concerns are

elevated because control systems are typically not up-to-date with the latest security patches, fixes and best practices due to concerns with taking real-time systems off-line and concerns over making system modifications, which might affect the time sensitive operations of the control system or potentially affect existing agreements with control system vendors or others.

In addition, the control systems commonly utilized in the United States are often sold and used in adversarial countries, providing adversaries an insider view of system components and software. Adversaries could dedicate time and resources to discovering vulnerabilities and developing exploits and then attempt to remotely gain access to critical U.S. control systems through an increasing number of potential control system access points.

IV. Supporting Data

The Group for Advanced Information Technology (GAIT) at the British Columbia Institute of Technology (BCIT) maintains a security incident tracking system, known as the Industrial Security Incident Database (ISID), designed to record incidents of a cyber security nature that directly affect control systems. This database contains events such as accidental cyber-related incidents, as well as deliberate events such as external hacks, denial-of-service (DOS) attacks, and virus/worm infiltrations. ISID data is collected through research into publicly known incidents and from private reporting. BCIT researchers ascertained the reliability of each reported control system incident by verifying its details using standard investigative techniques. Records for incidents with a reliability of “unknown or unlikely” were not used in the analysis. ISID data was collected for the period of 1982 through 2004.

One significant ISID finding identified from analysis of incident reports for the period between 1994 and 2004 was a five-fold increase in the annual control system incident rate (average 12 incidents per year) for 2002 to 2004, as compared to the period between 1994 and 2001 (average 2.4 incidents per year). It appears that sometime between 2001 and 2002 there was a significant increase in identified control system incidents. This finding could, to some extent, be due to an increase in reporting, an increase in the ability to identify and gather incident information, or an increase in the number of widespread worms and viruses.

The BCIT ISID data also indicated that a majority of identified incidents have occurred in North America (United States and Canada) and that the petroleum, transportation, power, and utilities industries represented the majority of incidents for the period 1982 through 2004. Industries that had lower numbers of incidents identified included chemical, pulp and paper, water/waste water, electronic manufacturing, food and

beverage, aerospace, metals, and others. BCIT reported that during 2005, chemical companies have contributed a number of control system incidents, balancing the list and adding them to the petroleum, transportation, power, and utilities industries as industries representing the majority of incidents.

Another significant area to highlight from analysis of the BCIT ISID data for the period 1982 through 2004 is incident type. The six incident-type categories identified for ISID data were external, accidental, internal, audit, other, and unknown. For the period between 1982 and 2001, 29% of incidents were labeled as external, 50% accidental, and 21% internal. For the period from 2002 to 2004, a dramatically different 66% were labeled as external, 22% accidental, 3% internal, and 9% fell into the audit, other, and unknown incident type categories. This finding represents a significant shift from a majority internal and accidental control system incident types to a majority of external incident types. Again, this may be partially due to exposure of control systems to worms and viruses as control systems migrate to an "accessible from anywhere" world.

The change in the Nation's critical infrastructure control systems environment has resulted in an increase in the number of vulnerabilities available to exploit, the available avenues for cyber attack, and the number of people capable of successfully executing a cyber attack. In other words, the attack tools (cyber weapons) are mature enough to cause significant harm, and are readily available to and usable by individuals with limited knowledge of control systems and associated architectures. Those with intent to cause harm have a ready-made selection of easy-to-use tools and exploits for execution.

The Department of Homeland Security and other federal partners understand the importance of control systems to our Nation and have acknowledged the increased risks presented to our Nation through control system changes that are taking place at plants and facilities throughout our Nation and around the world. A number of programs have been established by DHS, and its federal partners, to address and enhance the cyber security posture of control systems within our Nation's critical infrastructures. Some of these initiatives are presented below.

IV. Ongoing Programs to Secure Control Systems

United States Computer Emergency Readiness Team (US-CERT) Control System Security Center CSSC)

The DHS National Cyber Security Division (NCSD) established the US-CERT as a public-private partnership among DHS, government agencies, and academia to improve the Nation's cyber security posture. The US-CERT is charged with protecting our

Nation's Internet and critical infrastructures by coordinating defense against and response to cyber attacks.

To respond to the growing concerns over the cyber security of control systems within the national critical infrastructure and to address the *National Strategy to Secure Cyberspace*, the US-CERT Control Systems Security Center (CSSC) was established in June 2004. The US-CERT CSSC is a specialized US-CERT resource established to bring together control system owners, operators, Information Sharing and Analysis Centers (ISACs), vendors, industry associations, and subject matter experts to address control systems cyber vulnerabilities and to develop and implement programs aimed at reducing the likelihood of success and severity of impact of a cyber attack against a critical infrastructure. The US-CERT CSSC enhances the cyber security of the Nation's critical infrastructure by coordinating government and industry activities to identify and mitigate control systems vulnerabilities and perform vulnerability assessments; to build a security culture within the control system community through training, outreach, and awareness; and to provide a national response capability for control system threats, vulnerabilities, and incidents. The US-CERT CSSC utilizes DHS resources; Idaho National Laboratory; other relevant federal agencies and National Laboratories; and private sector control system entities and subject matter experts to ensure the best available facilities and minds are addressing the critical task of protecting our Nation's control systems used in critical infrastructure.

National SCADA Testbed (NSTB)

The Department of Energy (DOE) has launched a multi-laboratory partnership to implement the National SCADA Testbed (NSTB) to test control system vulnerabilities and security hardware and software. Working in conjunction with DHS, other federal agencies, and the private sector, the NSTB strives to identify and remediate SCADA vulnerabilities and recommend security standards to protect the critical energy infrastructure SCADA systems.

Together with the US-CERT CSSC, the NSTB offers the government and industry a full-scale infrastructure suite of facilities for assessing and validating control systems technologies, standards, and vulnerability reduction efforts across all critical infrastructure sectors.

Process Control Systems Forum

DHS has established the Process Control Systems Forum (PCSF). The PCSF is a unified DHS Science & Technology (S&T) Directorate and NCSD effort to form a natural bridge between government and industry. The stated purpose of the Process Control

Systems Forum is to accelerate the development of technology that will enhance the security, safety, and reliability of process control and SCADA systems by providing a single venue for technologists from all sectors, from all vendors, and from academia to work together in evaluating, developing, refining, specifying, and testing new technologies and improving the security of legacy control systems.

The PCSF is not a standards body and is not intended to replace any existing activities in the PCS and SCADA community. The PCSF builds upon the existing body of work in this subject area, and establishes links with others in industry and government to arrive at a common underlying architecture for process control systems that offers security, reliability, resiliency, and continuity in the face of disruptions and major incidents.

The PCSF serves as a channel for industry to engage with DHS and its various programs that promote control systems security. The success of the forum will help ensure that DHS and its federal partners are meeting the needs of the control systems community. To this end, DHS and DOE both encourage active industry participation in the PCSF. Please see www.pcsforum.org for more details.

V. Contacting US-CERT CSSC for Control System Incidents and Vulnerabilities

The US-CERT, through utilization of its CSSC resources, has the capability and subject matter expertise to assist control system owners and operators with control system cyber incidents and with managing control system vulnerabilities. The US-CERT web site (http://www.us-cert.gov) provides useful cyber security information for control system owners and operators. In the near future, the US-CERT will have web pages specifically dedicated to control systems security. These control system web pages will provide information about the CSSC program and will serve as the “one-stop” resource for information concerning control system cyber security.

Control system incidents and vulnerabilities can be reported to the US-CERT via its web site (http://www.us-cert.gov) by clicking on the “Report an Incident” or “Report a Vulnerability” buttons and then entering the requested information. Control system incidents and vulnerabilities can also be reported via telephone at (703) 235-5110. The US-CERT can also accept electronic submissions of protected critical infrastructure information (PCII). For more information on PCII or to gather additional information concerning the CSSC program, send an email to soc@us-cert.gov.