THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 8

February 2009
SCADA

Contact: CIPP02@gmu.edu
703.993.4840

George Mason University
School of Law
CENTER for INFRASTRUCTURE PROTECTION

Featured in this month's issue of *The CIP Report* are Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems monitor and control the processes of many of our Nation's infrastructures. The security and safety of transportation, water, communications, and many other vital parts of our everyday lives all rely on SCADA systems. In this issue we look at some of the different SCADA systems and their applications.

The first article provides an overview of George Mason University's research on SCADA systems. This research focuses on railroad transportation and Positive Train Control systems. The second article discusses the Energy Sector's response to cyber threats and the efforts to secure their control systems. An article from Mississippi State University's Critical Infrastructure Protection Center explains their research on Human Machine Interface (HMI) systems. The next article presented discusses the security of SCADA systems, specifically cyber security and the difference between cyber and information technology security. *Legal Insights* also discusses cyber security in this issue.

This month we present the first article of *Cyber Conflict Perspectives*, a regular feature that Eneken Tikk will be contributing to. Ms. Tikk joins our staff from Estonia and heads the legal team for the NATO Cooperative Cyber Defence Centre of Excellence. We have also included information on the release of the 2009 National Infrastructure Protection Plan (NIPP) and information on the 9th Control System Cyber Security Conference, being held October 19-22, 2009.

We thank you for your support and feedback, both are very important. We hope you find this issue of *The CIP Report* informative and helpful to improving the security of our critical infrastructure.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

Mick Kicklighter

Critical Rail Infrastructure Protection Research at George Mason University

by Duminda Wijesekera, Ph.D., Associate Professor
Department of Computer Science

Critical Rail Infrastructure Protection is a vital infrastructure issue that George Mason University (GMU) is currently addressing through research. Critical Rail Infrastructure Protection focuses upon the protection of Supervisory Control and Data Acquisition (SCADA) wireless communications systems utilized by the railroad known as Positive Train Control Systems (PTC). PTC systems are specialized SCADA systems that provide positive train separation, over speed protection, and protection for roadway workers working within the limits of their authority. Public Law 110-432 mandated installation of these systems on all Class I intercity and commuter railroads, as well as railroads carrying Toxic by Inhalation (TIH) material by 2015.

Railroads are a critical transportation asset and play a significant role in the United States economy. They transport a diverse mixture of commodities that support all facets of the U.S. industrial base. Railroads operate in every state in the U.S., except Hawaii, and travel across a network that exceeds 140,000 miles while simultaneously moving over 1.7 trillion ton miles of freight. This equates to 25% of all intercity freight tonnage carried in the U.S. and 41% of all ton miles. Railroads also operate the 30,000 miles of the Department of Defense (DoD) Strategic Rail Corridor Network (STRACNET) for the movement of DoD munitions and other materials. The freight includes 1.7 to 1.8 million carloads of hazardous material, including TIH material. TIH materials are "gases or liquids that are known or presumed on the basis of test to be so toxic to humans as to pose a health hazard in the event of a release during transportation". While this material constitutes only 0.3% of all hazardous material shipments by rail, this still equates to more than 21.6 million ton miles of TIH movements per year. Railroads, hence, are a crucial yet sensitive component of the U.S. network.

Disruptions in railroad services can have a significant adverse impact on the U.S. economy as well as military preparedness. The geographic dispersion of the railroad infrastructure, the manner in which it is constructed, and the ease with which an adversary can disrupt or damage it precludes providing absolute security. Although the rail industry and the government have undertaken extensive efforts to protect the movement of freight and passengers, rail security remains an exercise in risk mitigation, as opposed to risk prevention. A determined adversary can exploit any one of a number of vulnerabilities, with potentially catastrophic consequences. These vulnerabilities are associated with the physical and communication components of infrastructure protection. While there are additional steps that can be taken to reduce exploitable vulnerabilities, the fact remains that the system, and the public that it serves, will always be exposed to a measurable level of risk.

Railroad accidents in the United States are relatively rare events. In 2006, the total accident/incident rate across all railroads was 16.25 incidents per million train miles. Although this rate is low in terms of absolute numbers, it equates to more than 13,100 separate incidents, 22.2% which were train related accidents (collisions or derailments) and highway grade crossing incidents. Service disruptions resulting from accidents can be extremely inconvenient and have significant financial impacts. The effect of disruptions, however, can be more than inconveniences or lost revenue. For example, each year 8,500 tank cars of chlorine move by rail through the middle of Washington, D.C. passing within two blocks of the U.S. capital. In a worst-case scenario, the complete release of the contents of just one 90-ton car of chlorine in the center of Washington, D.C. has the potential to kill or injure 100,000 people. Death occurs by slow suffocation as the chlorine gas reacts

(Continued on Page 3)

Rail *(Cont. from 2)*

with moisture in the lungs, forming hydrochloric acid. Exposure, even if not fatal, can result in lung congestion, pulmonary edema, pneumonia, pleurisy, or bronchitis.

Various algorithmic approaches for position, scheduling, and routing optimization have been developed since the mid 1970's. These and other alternatives for solving this integrated problem have been incorporated into virtually all modern computer dispatch systems from the major railroad vendors. Current system designs do not include trust management systems to provide support for both safety and security, rendering PTC communications vulnerable to mal-actors. The addition of trust management systems, while supporting system security, introduces additional overhead that can potentially adversely affect cross-domain railroad dispatch operations. Existing work on safe cross-domain dispatch operations considers the impact of physical train attributes, but has yet to consider the impact of the trust management systems on allowable traffic delays and system velocity.

GMU has adopted a two-prong approach to addressing security vulnerabilities, accidents, and establishment of appropriate trust management systems. The first approach GMU is exploring is the application of Use and Misuse Cases to determine requirements prior to exploitation of the wireless communications vulnerabilities. Use Cases are a de-facto industrial standard, and are used as a common base to discuss system requirements among all stakeholders. Widely used for capturing functional requirements, Use Cases specify the desired set of interactions between a system under design and its users. Due to the recent trend in misusing and/or abusing systems defects and vulnerabilities by various mal-actors, Use Cases have been augmented with Misuse Cases to specify and hopefully eliminate known undesirable interactions between mal-actors and a system under design. A Misuse Case specifies interactions that should not occur between a mal-actor and a system under design.

The second approach being explored by GMU is the use of forensic analysis in the analysis of accidents that have or could have been the result of exploitation of vulnerabilities. Unfortunately, existing railway networks do not have mechanisms for the comprehensive, secure, centralized collection of forensic data. This GMU project involves investigating the root cause of undesirable incidents or railroad accidents as well as recreating potential scenarios that permit forensic analysis of wireless based commands in addition to the usual examination of physical equipment, human factors, environmental conditions, and others. The outcome of the accident analysis is usually a description of one or more chains of interactions resulting in multiple accident scenarios. Such scenarios can occur for a variety of reasons which may include human error, unexpected environmental conditions, failure of equipment, communication related issues such as delays and dropping of packets with PTC information, and deliberate attacks against networked systems. Proper collection and analysis of accident data can be used to compute accident frequency and patterns. These can pinpoint locations requiring special operational attention and possibly safety and security improvements.

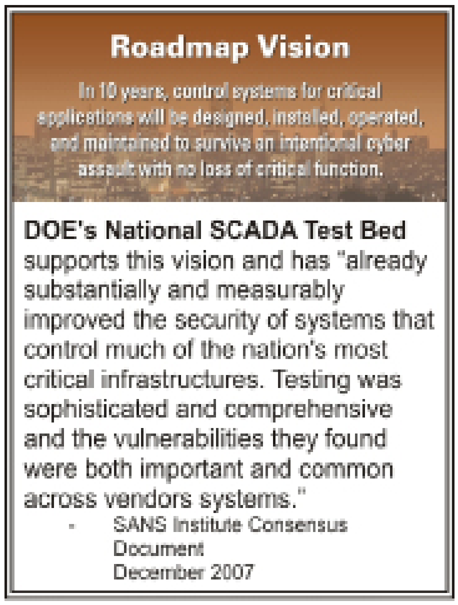
The GMU effort has created numerous different algorithms for the safe and secure scheduling of trains through the interchange point between two different railroads. The algorithm supports positive train separation under a worst-case traffic density scenario, allowing for the safe and secure scheduling of trains through an interchange point while minimizing traffic delays and maximizing system velocity. The algorithm is independent of the specific security trust management system, the PTC system, and the scheduling and dispatch system. ❖

This article has summarized some of the research that GMU is conducting to help secure the nation's vital rail infrastructure. For a list of more projects in this area, including academic peer- and professionally-reviewed papers, please visit the following website and search under Resume: http://ise.gmu.edu/~duminda/index.html. dispatch system.

Faced with Cyber Threat, the Energy Sector Responds

by Hank Kenchington, Deputy Assistant Secretary (acting),
Department of Energy, Office of Electricity Delivery and Energy Reliability
and Katie Jereza, Energetics Incorporated

When the DoD confirmed last November that a widespread electronic attack had breached networks within U.S. Central Command and at least one highly classified network, it brought home for many the idea that in the digital age, even our most protected — and most vital — networks are penetrable. The last decade has seen cyber threats edge toward the forefront of national security concerns; during the recent presidential campaign, President Barack Obama equated them to the threat of nuclear or biological weapons. In his February 12 *Annual Threat Assessment*, Director of National Intelligence Dennis C. Blair acknowledged that a number of nations have been the target of cyber attacks and U.S. critical infrastructures are just as vulnerable. He claimed that this is evident in the growing number of state and non-state adversaries as well as terrorist groups that are increasingly targeting our information infrastructure for exploitation or disruption. "Cyber attacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours to weeks," Blair said. In January, the departing Director of National Intelligence, J. Michael McConnell, concurred with this statement when he concluded that the potential for a coordinated attack that could cause lasting damage and cascade through our dependent critical infrastructures makes cyber security, "the soft underbelly of this country."



The Growing Physical/Cyber Convergence Threat

The supervisory control and data acquisition (SCADA) and other process control systems used in the nation's critical infrastructures are among those networks that face increasing threats from cyber attack. SCADA systems monitor and control a variety of physical processes, from electricity generation to food processing, in numerous critical infrastructure sectors, including nuclear, chemical, energy, and water. In the past, when these systems were operated primarily in closed networks on proprietary operating systems, their protection involved building physical access controls for highly unlikely attacks. Today however, to improve reliability and monitoring, control system networks are increasingly connected to business IT networks which are in turn connected to the internet.

In 2005, the National Infrastructure Advisory Council (NIAC), a council that directly advises the U.S. President on infrastructure issues, convened a Physical/Cyber Convergence Working Group to explore the security concerns brought on by these connections. The group found that the "cyber threat to critical infrastructure control systems is real — it is present today and the frequency and sophistication of these attacks is growing."

A Collaborative Response

Faced with these mounting threats, the energy sector has made great and longstanding efforts as an industry to respond. The U.S. Department of Energy (DOE) has been working with the private sector since the 1990s to address the cyber threat to energy control systems. In 2003, the DOE Office of Electricity Delivery and Energy

(Continued on Page 5)

Energy *(Cont. from 4)*

Reliability (OE) developed the National SCADA Test Bed (NSTB) Program to assess common control systems for vulnerabilities and perform research and development in control systems security. At the time, the industry benefited from diverse public and private activities, but most efforts were operating autonomously without a common vision for security or strategic framework for coordination.

In 2005, DOE teamed up with the U.S. Department of Homeland Security and Natural Resources Canada to convene industry leaders in the energy sector and help them define a common vision and end states along with priority activities that would take the sector there. About 55 participants, many of them electricity, oil, and natural gas asset owners and operators, worked together to develop the 2006 *Roadmap to Secure Control Systems in the Energy Sector*, which envisions that by 2015, control systems in the energy sector will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

The Roadmap provided a strong framework to guide the industry in aligning its efforts. With clear goals and priority activities to rally around, it helped research programs in the public and private sector put each dollar on a direct line to addressing a well-defined industry need. A year after its release, the NIAC recognized the Roadmap's groundbreaking success and called upon other critical sectors to develop their own sector-specific roadmaps, using the energy sector roadmap as a model.

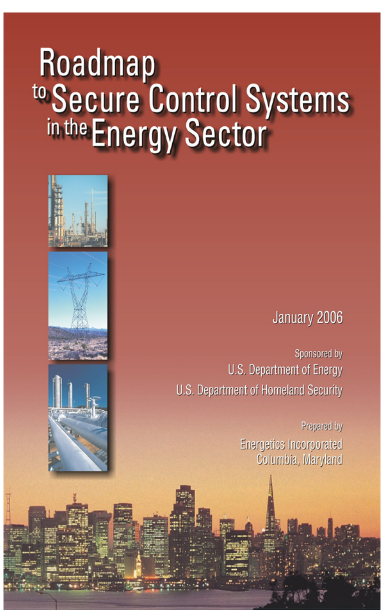
The Roadmap also encouraged OE to restructure its NSTB Program to align with the industry-defined goals and priorities. The NSTB Program also began looking at industry projects as a better way to quickly move new technologies into the marketplace. To help track progress on all energy sector efforts, OE developed the interactive energy Roadmap, or ieRoadmap (found at www.controlsystems roadmap.net), an interactive online tool that allows both public and private sector project leads to self-populate a project database, map their projects to specific Roadmap challenges, and identify collaborative opportunities to leverage work among projects. So far, more than 100 projects from 21 public and private organizations have been added to the ieRoadmap.

(Continued on Page 13)

The Escalating Threat

By connecting control systems to the internet, operators have opened them to a world where attacks are happening every day, and on a scale that has never before been possible. The Slammer worm of January 2003 had infected 90% of vulnerable hosts across the world within 10 minutes of the first attack. The attack showed a scale and speed unrivaled by physical attacks, yet it was a relatively benign virus that exploited a vulnerability for which a patch had been released six months earlier.

An attack targeted at a critical infrastructure facility that attempts to disrupt service, insert false information, or create lasting physical damage is where the nation is really at risk. Intelligence officials have warned attackers are becoming more targeted, more sophisticated, and potentially better financed as attacks are coupled with extortion demands. Outside the United States, cyber attacks into utilities followed by extortion demands have been used to disrupt power, in at least one case causing a power outage that affected multiple cities. The potential is not only there—the attacks have already begun and are rapidly escalating.



Vulnerability Analysis of SCADA HMI Systems

by Robert Wesley McGrew and Rayford B. Vaughn
Department of Computer Science and Engineering
Critical Infrastructure Protection Center, Mississippi State University

Introduction

In 2007, the Critical Infrastructure Protection Center at Mississippi State University[1] began to investigate control system vulnerabilities and architectures using software and commercial devices commonly found in critical infrastructure environments. An element of this investigation has focused upon the Human Machine Interface software generally deployed as part of SCADA systems.

The software used by operators in the "control center" of a SCADA system is referred to as Human Machine Interface (HMI) software. The HMI software serves a dual purpose of presenting the data acquired from various elements of the SCADA system and allowing the operator to manipulate parameters of the system that are under the operator's supervisory control. HMI software is often configured to mimic the look and feel of a tangible control panel, with elements like switches, dials, sliders, and readouts. Figure 1 provides an example of these elements.

Vulnerabilities have been discovered in these software packages that reflect a lack of robust security architecture and violate commonly-accepted principles of software security engineering. The first example of these vulnerabilities (in the popular GE Fanuc product iFIX) was publicly revealed after being properly reported to U.S. CERT[2] and to the vendor for appropriate mitigation.[3]

Vulnerabilities

The iFIX software serves as a HMI for end-user operators, and as an integrated development enviroment used by engineers to create the interfaces and scripts that make up the HMI. Software-enabled security features are also provided that allow for varying levels of access for different users. For example, an operator's account can be denied access to modify the interface, exit the full-screen interface, or shut down the system.[4] A number of vulnerabilities in this product have been found that serve as useful examples of how design decisions and legacy code can affect the security of a modern control system. The vulnerabilities discovered are

Figure 1. Screenshot from HMI system in the MSU CIPC SCADA Lab

(Continued on Page 7)

[1] Critical Infrastructure Protection Center, http://www.security.cse.msstate.edu/cipc/ (current February 2009).
[2] United States Computer Emergency Readiness Team, VU\#310355, http://www.kb.cert.org/vuls/id/310355 2008.
[3] See http://support.gefanuc.com/support/index?page=kbchannel&id=S:KB13253&actp=search.
[4] GE Fanuc, 2008. Proficy HMI/SCADA - iFIX - iFIX Technical Benefits, 2005, http://www.gefanuc.com/Downloads/en/proficyifix_cutheet_gfa562.pdf (current Februrary 2009).

HMI Systems *(Cont. from 6)*

briefly described below. The authors believe that similar vulnerabilities exist in other vendor's HMI products and are currently investigating this hypothesis within their SCADA security laboratory.

Password Disclosure

Passwords in the iFIX product are not hashed securely for storage. The passwords for each user are obfuscated by an exclusive-or (XOR) operation against a static key before being stored in a file. The operation is easily reversible by an attacker, resulting in the disclosure of all user passwords on an iFIX system. This is especially dangerous when the system is configured to authenticate users over a network, since the obfuscated passwords were not properly encrypted. An attacker with the ability to "sniff" network traffic can intercept and decrypt the users' passwords.

Authentication Bypass

The security architecture of iFIX does not prevent the modification and replacement of key security modules by the user. As a result, it is possible for an attacker to produce a copy of the iFIX login program and security manager library. The attacker can then modify to the way key security modules operate. The modified modules can then be used on a target system to log in with no password, bypassing iFIX's attempts at authentication and access control. We have demonstrated this attack.

Bypassing Run-Time Restrictions

Restrictions can be placed on iFIX users in terms of what they are allowed to do in an iFIX system. This includes the ability to halt the system, run external programs, "alt-tab" to other programs, and exit the full-screen interface. This prevents iFIX users from using the computer the iFIX system is running on for unauthorized tasks. This protection can be bypassed by an attacker through the use of a USB drive or CD configured to use Microsoft Windows' "Auto-Run" functionality. Using this method, an attacker can run malicious code designed to exit the iFIX interface, or leverage other vulnerabilities in the product. We have also demonstrated this attack and have automated it on a USB drive.

Secure Software Engineering Principles and HMI

For almost 30 years, the software engineering community has had at its disposal a number of well known and important security engineering principles. They were first documented in 1970[5] in a then U.S. government classified report which established the need for security measures within the software engineering community as well as the untrusted nature of computing systems. As described in early fundamental papers, security engineering principles that directly relate to the vulnerabilities described in this paper include the principles of:

- "complete mediation," in which every access to a system's resources must be checked for authorization;
- "security through obscurity," where it is inadvisable to depend on obscurity for system security; and
- "least privilege," in which each element of the system should operate at the lowest level of access possible to perform its task.[6]

While such principles and practices made their way into operating system developments and application software to a certain extent, the major software intensive application domain of industrial control system software seemed to not adopt or place priority on these principles. There are many plausible reasons for this lack of security attention to include the lack of overlap between the IT community and the industrial process control community; the relatively isolated nature of control systems in their early implementations, and the fact that such systems were almost never

(Continued on Page 12)

[5] Ware, W., 1970, Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security; Rand Report R609-1, The RAND Corporation, Santa Monica, CA.
[6] Saltzer, J., \& Schroeder, M., 1974. The Protection of Information in Computer Systems, \emph{Communications of the ACM} 17, 7 (July 1974), web: http://www.cs.virginia.edu/~evans/cs551/saltzer/ (current February 2009).

Cyber Security for Industrial Control Systems

by Joe Weiss, PE, CISM

Joe Weiss is the Managing Partner of Applied Control Solutions, LLC, which provides strategic guidance and consulting to optimize and secure control systems. Joe maintains a blog on control system cyber security at http://community.controlglobal.com/unfettered. This article combines some new comments with recent topics of interest on his blog and past white papers.

Control systems operate the industrial critical infrastructures of electric power, water, chemicals, pipelines, and manufacturing. Cyber vulnerabilities of control systems are increasing for many reasons. According to the intelligence community, there are increasing threats from both terrorists and nation-states. The faltering economy is creating a base of knowledgeable, potentially disgruntled ex-employees. However, the majority of control systems' cyber vulnerabilities result from the "human factor."

In recent years, control systems have incorporated new, technical and operational changes to meet new environmental requirements and initiatives as well as various productivity demands. As systems become more complex such as the Smart Grid, the chances for human error and accidents increase. Most control system cyber incidents are not caused by traditional IT security vulnerabilities such as buffer overflows but by inadequate training, policies, procedures, and testing — "people" issues. If personnel are not adequately trained and an appropriate security culture established, even the best mitigation technologies can be defeated.

The Center for Strategic and International Studies (CSIS) was tasked with creating the Commission on Cybersecurity for the 44th Presidency to develop recommendations to improve cyber security in federal systems and in critical infrastructure. CSIS requested that Joe Weiss prepare a white paper on cyber security for industrial control systems. The paper is available at http://www.controlglobal.com/whitepapers/2008/132.html.

Control systems' vulnerabilities already have been intentionally and unintentionally exploited, resulting in more than 100 critical infrastructure control system cyber incidents worldwide. The results of these incidents have ranged from trivial irritations, to significant equipment and environmental damage, to deaths.

There are many ways to improve cyber security of control systems. This article covers only a few, including improved awareness and understanding, communication, information sharing, warning and response, and regulation.

Understanding Control System Cyber Security

At the outset, it is important to recognize that Information Technology (IT) security is not the same as cyber security for industrial control systems. Traditionally, the corporate IT organization has been responsible for the cyber security of computing systems. The computing systems IT staff are knowledgeable about, and accountable for, the business systems, desktops, laptops, mobile devices, and corporate web sites. The question as to whether the traditional corporate IT organization or the Operations group is responsible for control system cyber security is frequently asked, but there is no consensus answer. Many professionals take strong positions on either side of the issue.

The control systems used to produce, transmit and distribute electricity (as well as in other industrial applications) were

(Continued on Page 9)

Cyber Security *(Cont. from 8)*

originally designed to be isolated from the corporate networks managed by IT. They have been traditionally operated and maintained by Operations. These systems include power plant distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, remote terminal units (RTU) and intelligent electronic devices (IED).

However, these critical systems are often linked to corporate and other external networks, including the Internet. Additionally, SCADA, DCS and PLC operator consoles are becoming more Microsoft Windows -based---thus being implemented on industry standard workstations such as HPUX or Sun Solaris, which makes the question of responsibility even more complex.

In a 2004 survey, 16 utilities responded as to whether SCADA was "owned" by operations or IT and which provided computer and network support. The results were mixed, but a majority stated that they were not part of corporate IT, nor did they get support from IT on any Energy Management System (EMS) tasks. Ironically, several of these organizations "bounced" between Operations and IT because of their Microsoft Windows workstations. These mixed results are consistent with the informal responses received from many different utilities and other industrial organizations.

Making matters more complicated is the frequent sharing of IT infrastructure such as LANs, firewalls and routers by Operations. Many of the SCADA and power plant operator / engineer workstations and the substation and power plant laptop computers appear to be the same as traditional IT business systems despite the fact they have very different applications and remote connections. Therefore, IT often lacks knowledge of the different operational and administrative control system needs. Even the System Administrator function is different for Operations than it is for the Corporate IT applications.

Thus it is important for executive leadership and government policymakers to understand that IT security improvements (a) may not improve control system cyber security because the two portfolios do not overlap, and (b) have the potential of greatly impacting both the security and performance of control systems, especially if traditional IT security policies and technologies are applied without understanding implications to control systems, or without adapting them appropriately to the control system environment.

Specific examples include:

- Using block encryption, which can slow control systems to the point of creating a denial of service.
- Automatically implementing security patches on control system workstations, which can (and have) shut down control systems.
- Implementing anti-virus on control system workstations that are not configured to accommodate these tools, which has slowed down or shut down control system workstations.
- Performing system-wide diagnostics, maintenance, and/or scans that can (and have) shutdown control systems.
- Implementing firewalls with rules that restrict or delay control system communications, which can result in shutdown of control systems.
- Performing penetration testing of control systems, which can (and have) shut down control systems. In fact, in at least one instance the testing actually damaged firmware that had to be replaced before the control system could be used, resulting in very expensive facility downtime.

Another area that falls between IT and Operations is the issue of Sarbanes-Oxley (SOX) compliance. SOX was originally intended to prevent financial problems and requires all computer systems critical to the financial well-being of the company to be addressed. Traditionally, this has focused on critical IT business systems. However, SCADA and power plant control systems are obviously critical to the bottom-line of all industrial organizations as they "make the things that are sold." Arguably, the EMS handles more financial transactions than any other electric utility system. Therefore, these critical operational systems should also be included in SOX

(Continued on Page 14)

Legal Insights

Will New Cyber Security Efforts at the Federal Level Spur Legal Reform?

by Timothy P. Clancy, J.D., Principal Research Associate for Law

Critical infrastructure control systems are a legacy of hardware and software designed with two primary goals: performance and reliability. Security was a secondary consideration. Now with new security threats on the rise, IT managers must be able to retrofit current systems to provide the necessary level of security — but without compromising performance and reliability.

At the same time, engineers must design for the future. Infrastructure owners and operators need control hardware and software that have system protection and security built in from the beginning. All the while, new technologies are emerging — technologies making ever increasing use of the Internet and commercial operating systems. These pose an even greater security risk for critical infrastructure asset owners and operators.

For many in the field of critical infrastructure policy, these issues can seem like a broken record. Many of these points were raised in the report by the President's Commission on Critical Infrastructure Protection (PCCIP) in 1997.

There have been notable achievements by federal agencies and groups like the Multi-State ISAC through better standards development, more research, and improved procurement policies by federal, state, and local governments. The Department of Homeland Security (DHS) and the DOE have established control system testbeds at national laboratories and universities to validate new approaches to security, but more needs to be done. Government procurement policies for SCADA systems have been strengthened.

There remains a critical need for design guidelines and standards to address the need for interoperability, redundancy, and security of control systems. The National Institute of Standards and Technology (NIST) has been leading the way in developing voluntary technical standards and spurred by Congress and DHS, several CI/KR sectors have taken steps to implement stronger standards for control systems security.

There has been a flurry of activity by industry trade association groups, technical advisory boards, and engineering and standards working groups. Prominent are the NERC cyber security reliability standards for control systems in the electric system. The Oil and Gas and Water Sectors have also made strides to incorporate cyber security standards. However, with so many different sets of standards being promulgated, it is difficult to determine whether an enterprise is truly secure.

The recently announced Consensus Audit Guidelines (CAG) by the SANS Institute, while aimed at federal IT systems not SCADA, could be a major step forward. The guidelines are in draft form but have already been developed in consultation with federal CIOs. They seek to establish a baseline and metrics for agency information security and control that is mapped to known threats.

Such an effort if widely adopted by the federal government and most important, federal contractors and the defense industrial base, could have an enormous impact on private sector cyber security practices. It is likely that the next Federal Information Security Act (FISMA), being considered by Congress, will impose tougher mandates including compliance to such a consensus standard. If such metrics and benchmarks were adopted by the federal government, would they be mandated for companies in the Defense Industrial

(Continued on Page 12)

Cyber Conflict Perspectives

An Exciting New CIP Project

by Eneken Tikk, M.Jur.

Introduction by Editor: This year started with a big step in the growth of a nascent project at the Center for Infrastructure Protection. A new staff member has joined the center: Ms. Eneken Tikk, legal advisor to NATO's Cooperative Cyber Defence Centre of Excellence, and a former member of the staff of Estonia's Ministry of Defense and advisor to Estonia's departments of Justice and State. Working at our Arlington office as a Visiting Research Fellow, Ms. Tikk is an integral member of the Center's team on international cyber conflict.

After a fruitful roundtable organized by the Center in June 2008, several institutions and experts have joined together to develop a "consolidated view" on cyber conflicts — exploring and combining different perspectives on international cyber conflict resolution.

The goal of the International Cyber Conflict project is to develop wider international understanding and coordination of the many variables of cyber conflict law and policy. The project will provide advice on coordinated international policies and procedures regarding cyber incidents; assemble and share best practices within government and industry; create academic programs and professional training; and develop a clearinghouse of cyber conflict information relevant to both business and government decision-makers.

The project will provide interdisciplinary insights into a domain that for too long has been regarded as primarily a technological issue. The project will assess a variety of solutions addressing different aspects (appropriation, forensics), areas (legal, military, policy, economic) and levels (organization, nation, international community) of cyber conflict.

As cyber security has risen into the agenda of most countries and international organizations, the need for bridging the views and approaches is evident. The fast-moving nature of cyber conflict leaves a single government with few or no effective responses if there is no coordination of efforts on and between national (public-private) and international levels.

To create a secure system that supports the information society, national security concerns, and civil liberties at the same time, any approach has to take into account all potential levels of involvement. Millions of entities and organizations in the public and private sectors have plans to optimize and support their everyday information processes. Considering that today's economy and societies in general are increasingly dependent on networking, national cyber security has to be considered as part of such planning to allow for concerted defense in case of a cyber conflict.urrently, national threat assessments and approaches to critical infrastructure serve as bases for international coordination and response. Therefore, a robust and continuous dialogue needs to be established between international organizations capable of providing responses and remedies to different aspects of cyber conflict (such as NATO, EU, COE, ICANN and others).

Upcoming Event by CIP Partner

The Cooperative Cyber Defence Centre of Excellence is hosting a Conference on Cyber Warfare in June 17-19, 2009 in Tallinn, Estonia. CCD CoE is soliciting research papers within the emerging field of cyber warfare. For more information, please visit http://www.ccdcoe.org/99.html

(Continued on Page 15)

Legal Insights *(Cont. from 10)*

Base Sector? Would this lead to the CAG becoming a de facto standard for private sector cyber security? How would this influence civil legal liability for security failures or breaches?

These questions are not far-fetched. Already federal laws such as Sarbanes-Oxley Act (PL 107-204) and the Gramm-Leach-Bliley Act (PL 106-102) — originally written to improve the integrity of private sector financial reporting — have been used to force greater compliance with cyber security best practices. This is also evident in the Healthcare and Public Health Sector the Health Insurance Portability and Accountability Act (HIPPA, PL 104-191). Development of consensus guidelines at the federal level as part of a revised FISMA could pose a major shift in the legal landscape for cyber security practices across all infrastructure sectors, especially for owners and operators of critical SCADA systems. ❖

HMI Systems *(Cont. from 7)*

Figure 2. Critical Infrastructure Protection Center SCADA Lab

managed or maintained by IT staff in industrial settings. Such systems are pervasive in what is today referred to as our national critical infrastructure as defined by the U.S. government under Homeland Security Presidential Directive-7[8]. While much of this software is based on old architectures, it is today being made "net" accessible for ease of maintenance and for efficiency purposes. As a result, critical infrastructure software now exists within highly sensitive environments which can be attacked or exploited by adversaries.

Conclusions

Compared to vendors of software that witness mainstream use, SCADA software and hardware vendors seem to have only recently begun to pay attention to the development of secure software. It is important that vendors carefully scrutinize legacy code for vulnerabilities that would arise from that code being put into modern operating systems and networking environments. Software engineering principles for designing secure software may be utilized incorrectly or not at all in older versions of code. Thus far in our investigation, we are finding this problem to be generally true and have begun to research mitigation strategies that are not reliant on the vendor's code itself. ❖

---

[7] Weiss, J., and Delson, M., 2007. Cyber Security of Substation Control and Diagnostic Systems. In: Grigsby, L.L., Electric Power Engineering Handbook, CRC Press.

[8] Homeland Security Presidential Directive 7, 2003. "Critical Infrastructure Identification, Prioritization, and Protection" White House, December 17, 2003, http://www.fas.org/irp/offdocs/nspd/hspd-7.html (current February 2009).

Energy *(Cont. from 6)*

Increased Public-Private Collaboration

The widespread industry response spawned the development of the Energy Sector Control Systems Working Group (ESCSWG), made up of mostly industry representatives, to guide the energy sector in implementing the Roadmap. The working group assessed 23 private sector projects for alignment with Roadmap goals and priorities at its first ieRoadmap Workshop in May 2008. The workshop helped the ESCSWG track Roadmap progress and provided each project with individual recommendations for increasing the impact of their work. Project leads acted on working group recommendations to refocus their projects, explore additional end uses for their research, and engage additional asset owner partners.

Energy Sector Control Systems Working Group

The working group also served as an invaluable resource for prioritizing funding and guiding research activities in the NSTB Program, which has grown to be a national resource comprising facilities from five national laboratories. To support the Roadmap, NSTB conducts cyber security assessments of control systems and related technologies, develops advanced control system technologies, conducts modeling and simulation to better evaluate risk, and engages in industry partnership and outreach.

Measurable Results

To date, NSTB has assessed 90% of the current market offering of control systems in the U.S. electric sector and 80% of the current market offering in the oil and gas sector. Twenty test bed and on-site field assessments have led vendors to develop 11 hardened control system designs — 31 of these systems are now employed in the marketplace. Participating vendors have issued five software patches, now being used by 82 system applications.

NSTB's concerted outreach works to provide the knowledge and capabilities it develops to those who can use it. NSTB has trained more than 1,800 energy sector stakeholders on best practices for control systems security, and NSTB's Common Vulnerabilities Report alerts asset owners and operators of the most common vulnerabilities found across vendor systems and offers security recommendations.

Since its inception, NSTB has supported more than 50 research projects that have helped provide vendors and asset owners with critical information and products, while DOE is providing nearly $8 million over three years to fund five industry-led projects managed through NSTB. These industry efforts have already produced measurable results that can be widely used in the energy sector to increase security.

Digital Bond's Bandolier project, for example, has released audit files that can be downloaded into existing vulnerability scanners and used to audit control systems against an optimal security configuration. Using these files, the scanner can flag vulnerable configurations while also aggregating and correlating security events to help utilities identify attack attempts. Files designed specifically for four common control systems are already available as subscriber content (for $100) on Digital Bond's site, and more are being developed. Schweitzer Engineering Laboratories' Hallmark project is commercializing the Secure SCADA Communications Protocol — originally developed by Pacific Northwest National Laboratory — which provides message integrity by marking original SCADA messages with a unique identifier and authenticator before sending. The receiving device must first validate the message before enacting the command, reducing the potential for attackers to send faulty commands. The technology will be available in a hardware device by April 2009.

A Sector Transformed

Three years after the Roadmap's release, the ESCSWG and the NSTB Program have begun analyzing the impact of the Roadmap in preparation for a Roadmap update this year. What

(Continued on Page 18)

Cyber Security *(Cont. from 9)*

compliance. Because these systems are not well understood by IT and these systems cannot be fully secured, it is important that Operations be involved in validating SOX compliance of control systems.

Communications and Awareness of Control System Cyber Security

Better understanding of control system cyber security will also improve understanding of cyber incidents that traditionally have been considered only in light of IT security. Therefore it is important to include control system experts in cyber security discussions regarding utilities and related infrastructures. Unfortunately, this has not always occurred. For example, last year, the National Journal ran an article, featured on the cover page, in which the author claimed that the 2003 northeast blackout and the 2008 south Florida blackout were caused by hackers. [Note: these hacking claims were immediately labeled bogus by the electricity and control system communities, the private sector professionals who managed the respective utilities during blackouts, and the government investigators of the blackouts.]

While the National Journal author interviewed various IT security experts for his article, no control system cyber security professionals were quoted or referenced. At a conference in Washington, D.C., former CIA Director James Woolsey asked a panel of energy experts about the claims in the article. This panel did not include anyone from the control system cyber security community, and thus the panelists' responses lacked the clarity and understanding of the true problems with control system cyber security. While both the article and the panel received media and Washington attention, unfortunately that attention was not informed by the experts who should have been consulted on the issues.

Unfortunately, the converse is also true. The CIA's Tom Donahue gave a presentation at the SANS Conference in 2008 concerning the extortion attempts at several non-U.S. utilities involving control systems. Because Tom did not provide more details, many in the industrial control system community discounted it as hype. This does not help promote awareness and understanding either.

In addition to improving awareness of the control system aspects of cyber security, it is equally important to change our communications regarding cyber incidents. As those in the control system professions know (and as mentioned above), most control system cyber vulnerabilities are not caused by cyber attacks or hacking, but by human error and failures in training, policies, and procedure. Cyber threats from terrorists, unfriendly nation-states, and criminals grab the headlines and make good press. Unfortunately, they also may create a "the sky is falling" atmosphere, in which the claims are discounted as unsupported cries of fear, uncertainty, and doubt (FUD). In such an atmosphere, it is more difficult to bring attention to any claims of cyber vulnerabilities, especially the non-headline-grabbing "human factor" vulnerabilities.

While it is important to remain cognizant of potential cyber threats from terrorists, unfriendly nation-states, and criminals, our awareness of and communication about control system cyber incidents and vulnerabilities should be (a) focused on the overwhelmingly more-likely "human factor" causes, and (b) informed by professionals with experience in control system cyber security, not just IT security.

Information Sharing, Warning, and Response for Control System Cyber Incidents

Although there have been some very significant economic impacts from control system cyber incidents, they often are not even recognized as cyber incidents. In December 2008, two electric utilities completed power plant DCS upgrades with the most modern, secure systems available from two different control system suppliers. Shortly afterward, both electric utilities experienced cyber incidents that could have shut down the plants. However, like more than 100 other incidents in my control system cyber incident database, these incidents have not been made public or even confidentially shared in a systematic manner within the industry.

(Continued on Page 15)

Cyber Conflict *(Cont. from 11)*

The Center's International Cyber Conflict project was launched to address these aspects of cyber conflict and to promote cross-border and cross-disciplinary dialogue in the field. In 2009 the project will be run in cooperation with subject-matter experts from the NATO-accredited Cooperative Cyber Defence Centre of Excellence, US Army Command and General Staff College, National Defense University, Naval Postgraduate School, as well as experts in the private sector and government.

In the upcoming months, the Center will release several papers and presentations developed by the project participants. While we will have several private workshops for the participating subject matter experts, the first major public event will be a conference in autumn of 2009, in Estonia. Reports and event information will be published in *The CIP Report* and distributed via our listserv. For more information, please contact Eneken Tikk, etikk@gmu.edu, or Maeve Dion, mdion@gmu.edu. ❖

Cyber Security *(Cont. from 14)*

We need a Computer Emergency Response Team (CERT) for control systems, through which information on these incidents may be shared and aggregated, and through which best practices for response and mitigation can be developed and shared.

Regulation

People continue to speculate that if good data were available on the cost of incidents resulting from poor cyber security practices, that data may be persuasive enough for businesses to make the right changes in security systems, policies, and procedures. There has been work by the Electric Power Research Institute (EPRI) and the U.S. Cyber Consequences Unit to quantify the potential economic impacts of cyber attacks. At the 2008 Control System Cyber Security Conference, Bryan Singer (Chairman of ISA SP-99 Manufacturing and Control Systems Security standards body) gave a presentation on his economic impact experience. The attendees thought the presentation was informative and valuable, but it had almost no impact on additional security funding when they got back to their offices. There have been other anecdotal data on financial impacts of control system cyber incidents. However, these types of numbers fall on deaf ears as most senior management simply do not believe it is real.

The bottom line is there is simply no perceived economic driver to address industrial control system security without strong government regulations. And the regulations truly need to be <u>strong</u>. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security standards are treated as simply a compliance game. On the other hand, the Nuclear Regulatory Commission (NRC) is taking strong steps to require a viable control system cyber security program, so perhaps the nuclear power industry will be the leader on this issue.

Summary

Control systems are different from traditional IT systems. Securing and maintaining control systems will require Operations and IT experience. Attempting to secure these systems without appropriate knowledge and care is a dangerous undertaking. Understanding this is important not only to securing the control systems, but also to effectively communicating the vulnerabilities and discussing the incidents. One step that could help would be developing a CERT for control systems. If the costs of control system cyber incidents are not motivating proper security practices, then strong regulation may be the only solution. ❖

2009 National Infrastructure Protection Plan (NIPP) Announcement

In February the Department of Homeland Security (DHS) released a 508-compliant version of the 2009 National Infrastructure Protection Plan (NIPP). Currently, the 2009 NIPP is available only in electronic format; hard copies will not be available for several weeks, but may be requested from NIPP@dhs.gov. An electronic version is available on the DHS website at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. An electronic version is also available on the CIP website: http://cip.gmu.edu/archive/NIPP_2009.pdf.

From the Executive Summary:

The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:

> *Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.*

The NIPP provides the unifying structure for the integration of existing and future CIKR protection efforts and resiliency strategies into a single national program to achieve this goal. The NIPP framework supports the prioritization of protection and resiliency initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters.

Save the Date -- 2009 Control System Cyber Security Conference

The 9th Control System Cyber Security Conference will be held October 19-22, 2009 in the Washington DC area. Congressman James Langevin, former Chair of the U.S. House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology is expected to repeat his plea, made at last year's conference, for concerted public-private efforts to secure the industrial critical infrastructures.

Conference Topics

- Telecommunications impacts on control system security.
- Smart Grid and renewables, with concentration on identifying and remediating security vulnerabilities in
the control systems necessary to make a smarter grid a reality.
- Nuclear power issues including the cyber security Regulatory Guide.
- Security in the chemical industry, including CFATS regulations which may expand beyond chemical plants
to water and other types of industrial facilities including power plants.
- Security in the oil, gas, and refining industries, including the convergence of safety and security.
- Security in the water and wastewater industries, including strategies to deal with security for older
infrastructure and systems that are not expected to be replaced in the near future.
- Industry and academia research and development.

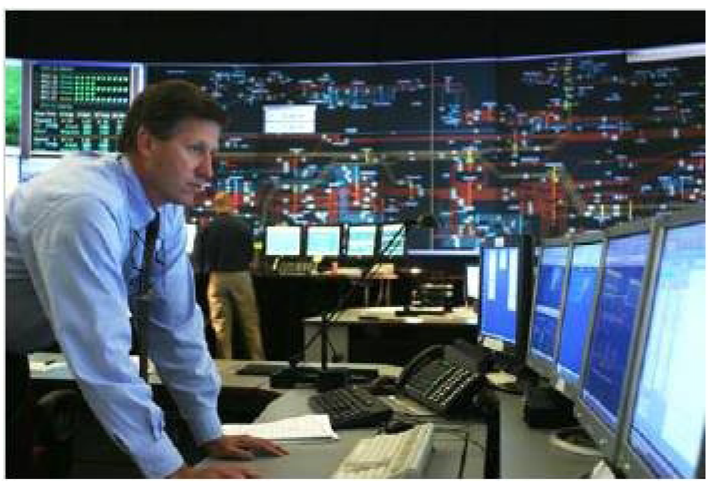
As with past conferences, there will be control system hacking demonstrations and discussions of actual control system cyber incidents. Additionally, there will be a tour of a working wastewater storage facility with emphasis on its control systems.

If you have any questions, or for more information including sponsorship opportunities, please contact Joe Weiss at (408) 253-7934 or joe.weiss@realtimeacs.com.

Energy *(Cont. from 13)*

we're finding is a sector that is markedly changed — it is more secure, more aware, and more demanding of enhanced security as it moves forward. When the Roadmap was released, many utilities were either unaware of the cyber threats they faced, or lacked a compelling business case for security.

Today, the industry no longer needs to be convinced. Asset owners now demand security that is "baked in," not added on. The shift has focused to action, and we're pushing to train more asset owners in implementing secure configurations. NSTB has expanded its training to include a day-long red team/blue team training event that invites asset owners and operators to participate in a simulated attack scenario on an actual control systems environment.



The Roadmap has strengthened public-private partnerships and has stakeholders across the sector calling for increased collaboration. The ESCSWG made it clear to researchers that projects must engage end-users to produce useful, applicable end results. Now, they're introducing the Matchmaker Initiative, in which the working group helps match asset owners who want to help with projects who need their guidance. And the Roadmap has changed the way asset owners and vendors work to solve security issues. Aside from encouraging vendors to have their systems tested for vulnerabilities, user groups are now pooling resources to fund additional assessments themselves.

As new technologies emerge and end-user needs evolve, gaps in the Roadmap's goals and priorities are becoming clear. NSTB has begun supporting the ESCSWG in performing a gap analysis that will help refocus priorities and update end states for the 2019 time frame of 2009's Roadmap update. It is vital that efforts across the industry remain geared toward that common vision — the energy sector has shown how real progress can be made within that framework.

As our nation turns its focus toward mitigating the cyber threat, increased resources and minds will be called upon to solve this complex and widespread problem. This opens the potential for great strides to be made in securing all critical infrastructure sectors, but it will present challenges to researchers, program managers, and policy makers as they decide how to move forward. The energy sector has shown how a strategic framework such as the Roadmap can focus multiple resources to make the greatest impact on those who own and operate our critical infrastructures. A common vision, driven by industry, will build coalitions among diverse stakeholders and make real progress with lasting impact. ❖

The Center for Infrastructure Protection works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1