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)*

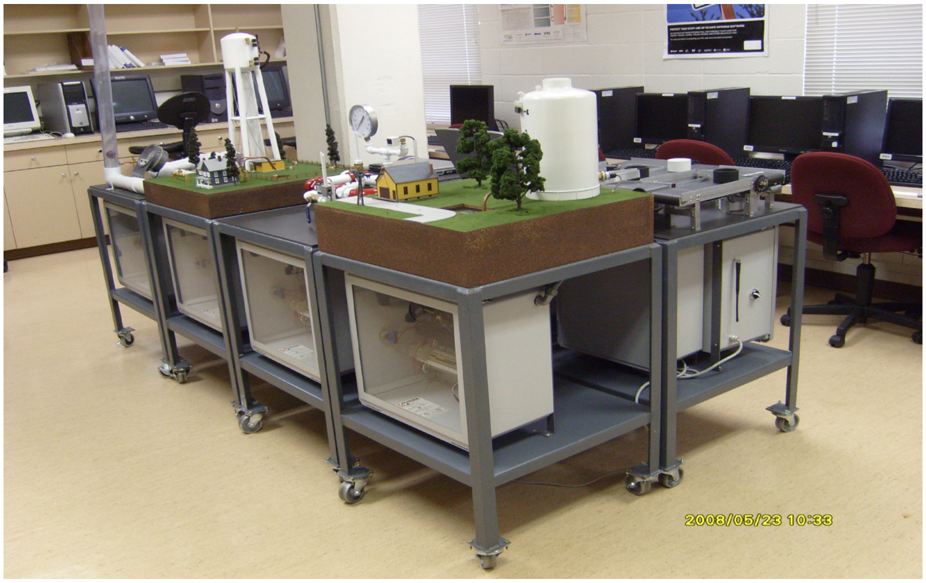


Figure 2. Critical Infrastructure Protection Center SCADA Lab

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.

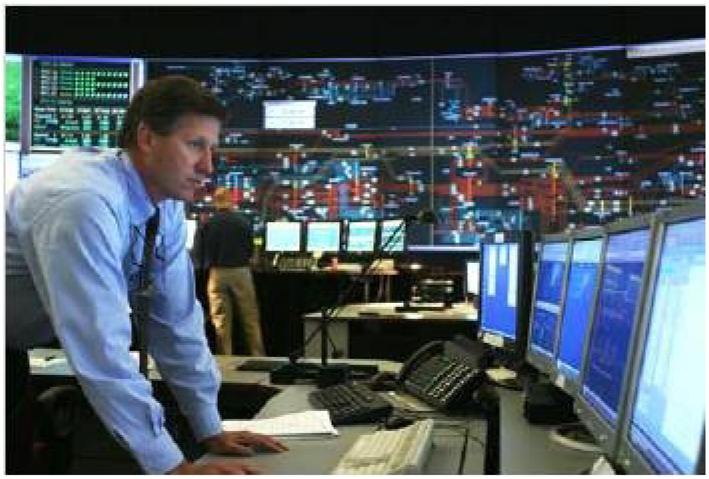
As with past conferences, there will be control system hacking demonstrations and discussions of actual control system cyber incidents. Additionally, there will be a tour of a working wastewater storage facility with emphasis on its control systems.

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