Control Systems Security Program/ ICS-CERT

March 2012 Issue

ICSJWG Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

ICSJWG 2012 Spring Conference Update

Thank you to everyone who submitted an abstract for the Spring Conference! Many great abstracts were received and conference organizers had a difficult time choosing potential presentations. Nonetheless, abstracts were selected and an agenda consisting of subject matter that will reach a wider audience of government professionals (federal, state, local, tribal, and international); control systems vendors and systems integrators; research, development, and academic professionals; and owners and operators (management, engineering, production, and information technology) has been produced.

Also, the success of the panels from the Fall Conference in Long Beach led to an expansion of panel events in the plenary sessions of the Spring Conference. The three panels planned for this conference are "Information Sharing and Analysis Centers (ISAC): Mission, Trends, & Products," "Key Take-Aways from Digital Bond's SCADA Security Scientific Symposium (S4) and Project Basecamp,", and "Security Responsibilities of the Control Systems Vendor."

For more information on the panels and the conference itself, and to view the draft agenda, please visit the conference website at: http://www.us-cert.gov/control_systems/icsjwg/conference.html

We look forward to seeing you in Savannah!

CSET™ Version 4.1 Released!

CSSP has released Version 4.1 of the Cyber Security Evaluation Tool (CSET™). This version provides users with the option of creating or modifying their network diagram in Microsoft Visio. This new functionality supplies a Visio stencil with network shapes recognized by CSET™. CSET™ imports the Visio diagram, assigns questions to the included components, and looks for general network vulnerabilities as if the diagram had been created within CSET™ itself. In addition, a diagram export function from CSET™ to Visio is also provided.

About the ICSJWG

The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC). The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR.

For more information, visit http://www.us-cert.gov/control_systems/icsjwg/

Table of Contents

To download the latest version of CSET™ please visit our website at: http://www.us-cert.gov/control_systems/satool.html

ICS-CERT to Provide Attribution to Researchers in Products

ICS-CERT has changed its Vulnerability Disclosure Attribution Policy due to the feedback that was received during the Industrial Control System Vulnerability Disclosure Panel on the last day of the ICSJWG 2011 Fall Conference. Attribution will now be made in ICS-CERT Alerts and Advisories regardless of whether there was previous coordination. This will enable stakeholders to easily identify additional sources of information related to vulnerabilities.

For more information on this change, please reference page 2 of the November issue of the ICS-CERT Monthly Monitor:
http://www.uscert.gov/control_systems/pdf/November_MonthlyMonitor.pdf

NIST Releases Final Smart Grid 'Framework 2.0' Document

An updated roadmap for the Smart Grid is now available from the National Institute of Standards and Technology (NIST), which recently finished reviewing and incorporating public comments into the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*. The document reflects the roughly 240 comments on the draft version, which was released for public comment in October 2011.

For full details, please visit: http://www.nist.gov/smartgrid/framework-022812.cfm

Advanced Training Events Scheduled for Fiscal Year (FY) 2012

CSSP is currently offering advanced cybersecurity training sessions at the Control Systems Analysis Center located in Idaho Falls, Idaho. These sessions provide intensive hands-on training in protecting and securing control systems from cyber attacks, including a realistic Red Team/Blue Team exercise that is conducted within an actual control systems environment. It also provides an opportunity for attendees to network and collaborate with other colleagues involved in operating and protecting control systems networks.

- **Day 1:** Welcome, overview of DHS CSSP, a brief review of cybersecurity for industrial control systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.

- **Day 2:** Hands-on classroom training on Network Discovery, instruction for using Metasploit, and separation into Red and Blue Teams.

- **Day 3:** Hands-on classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.

- **Day 4:** A 12-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment and with maintaining operations to a batch-mixing plant and an electrical distribution Supervisory Control and Data Acquisition (SCADA) system.

- **Day 5:** Red Team/Blue Team lessons learned and roundtable discussion.

The following advanced training events have already been scheduled for FY 2012:

- **April 9-13**: Industry Partners (Reserved)
- **April 23-27**: International (Reserved)
- **May 14-18**: International & Industry Partners
- **June 18-22**: Industry Partners
- **July 16-20**: Industry Partners
- **September 10-14**: Industry Partners
- **October 8-12**: Industry Partners

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant.

As scheduled advanced training gets closer, an invitation along with a link to register for the course will be sent out and posted to the following website - http://www.us-cert.gov/control_systems/cscalendar.html. Please monitor the site periodically, as this schedule is updated as new courses are confirmed.

Register by clicking on the link provided on our webpage - http://www.us-cert.gov/control_systems/cscalendar.html. Registration is open approximately 2 months before the start of a class. Due to high demand, class size is limited to approximately 40 people with a maximum of 2 individuals per company per event. Classes fill quickly, so early registration is encouraged. Notification of cancellation is appreciated, with as much advance notice as possible so that others who wish to take the course can do so.

ICSJWG Subgroup Status

Below is an update on the progress of the ICSJWG subgroups. If you would like to become a member of any of the subgroups, send an email with your contact information to icsjwg@dhs.gov or contact the co-chairs directly.

Homeland Security — Industrial Control Systems Joint Work Group (ICSJWG)

- **Roadmap to Secure Industrial Control Systems Subgroup**

  GCC Co-Chair: Perry Pederson (Perry.Pederson@nrc.gov)
  SCC Co-Chair: Tim Roxey (Tim.Roxey@nerc.net)

  The Roadmap subgroup has taken the first version of the *Cross-Sector Roadmap for Cybersecurity of Control Systems* to private, public, and government contacts within all Critical Infrastructure and Key Resources (CI/KR) sectors where it has been well received. Currently, activity is focused on developing a metrics plan to include in the next version of the document in order to make the Roadmap more robust.

- **Vendor Subgroup**
  GCC Co-Chair: Marty Edwards (Marty.Edwards@dhs.gov)
  SCC Co-Chair: Eric Cosman (ECCosman@dow.com)

  The Vendor subgroup is busy with three subcommittees that are working to develop reports for release during the Spring Conference in Savannah. First, the Cross-Vendor Subcommittee is developing a position paper that outlines the direction that the ICS community should take to improve security and the importance of owners/operators, vendors, and system integrators collaborating to design, implement, and maintain ICS security. Second, the Vulnerability Disclosure Subcommittee is finalizing a paper intended to provide a consensus-based foundation for ICS vendors and integrators working to develop a vulnerability disclosure policy. Third, the Improve Communications Subcommittee is working to assess ICSJWG communications and information sharing capabilities and is currently assessing its tier 1- and tier 2-level improvements.

- **Workforce Development Subgroup**
  GCC Co-Chair: Keri Nusbaum (Keri.Nusbaum@dhs.gov)
  SCC Co-Chair: Michael Glover (M.Glover@prime-controls.com)

  The Workforce Development subgroup is currently working to map standards' requirements and Knowledge, Skills, & Abilities (KSAs) and consolidating these with the National Initiative for Cybersecurity Education (NICE) Framework. This will allow a comprehensive look at the state of the workforce and help develop alternatives which impact education and the application of expertise in all sectors involved with our nation's CI/KR.

- **Research & Development Subgroup**
  GCC Co-Chair: Doug Maughan (Douglas.maughan@dhs.gov)
  Acting SCC Co-Chair: Zach Tudor (Zachary.tudor@sri.com)

  The R&D subgroup has scheduled its first meeting since the Fall Conference. The meeting will take place on Tuesday, April 10, from 3:00-4:00pm EDT and will consist of a Menlo Report presentation on Ethical Principles Guiding Information and Communication Technology Research and a discussion on the latest news involving the R&D community.

Homeland Security Information Network (HSIN) Portal

HSIN is the information sharing tool used by ICSJWG subgroup members. All subgroup members can stay abreast of upcoming meetings through the calendars and subgroup reference materials in HSIN (e.g., charters, meeting minutes, agendas, etc.).

In addition, the "Alert Me" feature notifies users of changes to the portal, which eliminates the need for users to constantly log in to find out if updates have been made. Alerts can be sent immediately, daily, or weekly. To sign up for alerts, click on the "Alert Me" link on the left-hand side of the ICSJWG homepage and choose your delivery option. ICSJWG subgroup members who still need access to HSIN can send an email to icsjwg@dhs.gov to request an account.

- **If you do not currently have a HSIN account**, please provide your name, company, contact information, critical infrastructure sector, and ICSJWG subgroup affiliations to icsjwg@dhs.gov.

At this time, DHS is not able to grant non-U.S. citizens or those residing outside of the U.S. and its territories access to the HSIN portal. The owners of the HSIN portal are reviewing sharing agreements concerning information posted to the site. Until that process is complete, international user accounts will be on hold. ICSJWG Communications will contact all international members immediately if there are new developments.

Participation is Key!

Your participation and input is **critical** to the success of these subgroups and to the overall mission of the ICSJWG in coordinating cybersecurity efforts to secure industrial control systems across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

Industrial Control Systems Contributed Content

ICSJWG is now accepting contributions from the community pertaining to control systems security for the June Quarterly Newsletter. If you want to submit an article for the June Newsletter, please email icsjwg@dhs.gov, and we will take your submission into consideration for publication. The deadline for submissions for the June Newsletter is **Friday, June 1, 2012.**

Past ICSJWG newsletters are located on the CSSP website http://www.us-cert.gov/control_systems/icsjwg/index.html and in HSIN https://cs.hsin.gov/C10/C1/ICSJWG/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Newsletters%2fICSJWG%20Quarterly%20Newsletter&View=%7b6F252F6A%2d18EB%2d447A%2d96D4%2d106024729AB9%7d.

Also, thank you to all members who contributed content for the March Quarterly Newsletter! The following content was submitted by members of the ICSJWG for publication and distribution to the ICSJWG community. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations. The advice and instructions provided in the contributed content should be confirmed and tested prior to implementation.

#1 ICS and SCADA Security Myth: Protection by Air Gap

By: Eric Byres, Byres Security Inc.

The existence of an "air gap" between control system networks and the rest of the world has been one of the most enduring fairy tales in the field of SCADA/ICS security. The idea is that in a properly designed system, there is a physical gap between the control network and the business network. Since digital information cannot cross such a gap, bad things like hackers and worms can never get into critical control systems. From this, a corollary flows:

"*Companies that get worms in their systems obviously have not created the proper air gap and deserved to be infected.*"

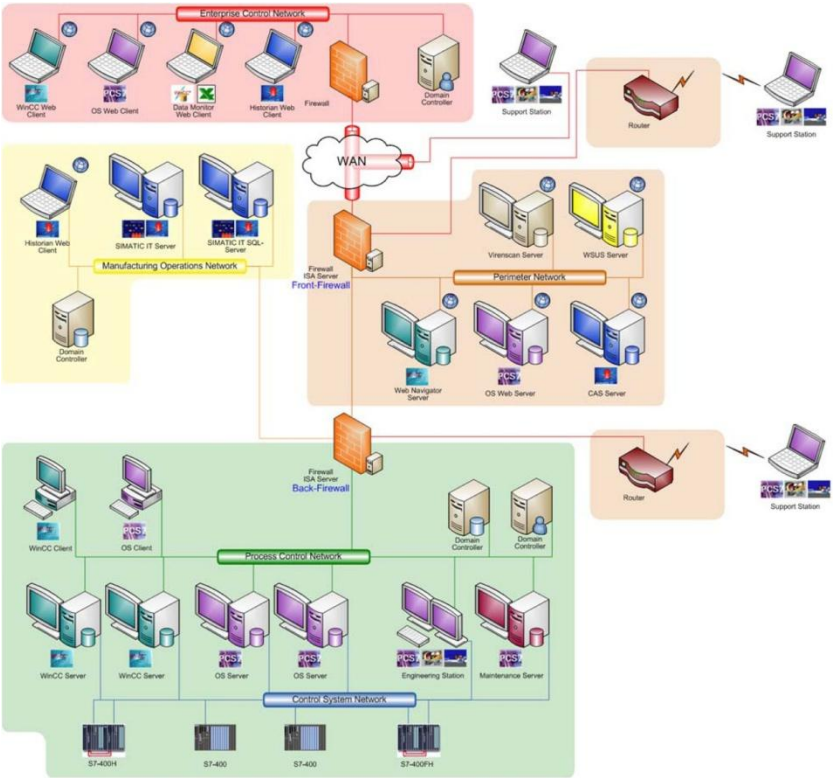
Now there are many materials supporting the idea of the air gap. Every week a new SCADA and ICS vulnerability notice comes out and every week end users get to read statements like this:

"*In addition, it is important to ensure your automation network is protected from unauthorized access using the strategies suggested in this document or isolate the automation network from all other networks using an air gap.*"

(Source: SIEMENS-SSA-625789: Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU)

Now while PR departments love to hide behind "air gap" when discussing their product vulnerabilities, no vendor engineer or manager really believes the air gap fantasy. For example, at the 2011 Siemens Summit, Stefan Woronka, Siemens Director of Industrial Security Services, stated: "*Forget the myth of the air gap – the control system that is completely isolated is history.*"

Next, check out the diagram of a high-level security architecture taken directly from Siemens' Security Concept manual (pg 42). (Note: you can click on the image to enlarge it.)



Can you spot the air gap in the drawing? Funny, neither can I.

Let's try another vendor - download the security manual from Rockwell, search for the term "Air Gap". You won't find it. Search the diagrams for an air gap. You won't find it.

Air Gaps Don't Work in the Real World

There is a good reason why you won't find the air gap mentioned in vendor engineering manuals. As a theory, it is wonderful. In real life, it doesn't work.

Sure you can simply unplug the connection between the control system and the business network and presto, you have an "air gap". Then one day you get new logic from your engineering consultant—perhaps it addresses a design flaw that has been causing your company considerable downtime. A little while later Adobe sends you a software update—perhaps it is for a critical vulnerability in the PDF Reader your staff uses to view operational manuals. Next your lab group sends a process recipe that will improve product quality. The list keeps growing—patches for your computer operating systems, anti-virus signatures, remote support and system software—you can't ignore them all.

So what do you do? Maybe you load some files onto a USB drive and carry that onto the plant floor. But isn't that how Stuxnet spread? Or maybe putting everything onto a laptop is the solution, but what if the laptop is infected? A serial line and a modem—sorry, the Slammer worm got into a number of control systems that way. Even the trusty CD can be turned into the carrier of evil bits.

As much as we want to pretend otherwise, modern control systems need a steady diet of electronic information from the outside world. Severing the network connection with an air gap simply spawns new pathways—pathways like the mobile laptop and the USB key, which are more difficult to manage and just as easy to infect.

Anyone Who Has Ever Seen an Air Gap, Please Raise Your Hand

So are there air gaps in any control systems? Sure—in trivial systems. For example, the digital thermostat controlling the furnace in my home probably has a true air gap. And maybe they exist in very, very high risk systems—for example, I am led to believe that reactor control systems in nuclear plants are truly air gapped.

But do air gaps exist for all the control systems that manage our power grid, our transportation systems, our water, and our factories? I will let Mr. Sean McGurk, the former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security answer that:

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system, or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network." Source: The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing. 58:30 -- 59:00

A control system protected by a real air gap

Time to Grow Up and End the Fairy Tale

Government, vendors, and industry need to accept that the dream of an air gap is dead. As I have noted in the past, vendors must stop hiding behind the air gap fantasy in their security notices, especially when even their own engineers don't believe it. But the vendors aren't the only ones that need to stop the air gap myth. Too many end users still tell management security risks are under control because their systems are isolated.

For effective ICS and SCADA security, the entire industry needs to move past the myth of air gaps and learn to deal with the reality: Control systems are connected to the outside world. Cyber security countermeasures must face up to this fact.

Chemical Cybersecurity Roadmap Web Site Launched

By: Chemical Sector-Specific Agency

The American Chemistry Council (ACC) has launched its new Chemical Cybersecurity Roadmap Web site, www.chemicalcybersecurity.com, as a clearinghouse for information related to securing control systems in the Chemical Sector. The site was developed in collaboration with the ACC Industrial Automation and Control Systems Working Group, the Chemical Sector Coordinating Council, and the Chemical Roadmap Working Group.

The site addresses the importance of control systems security in the Chemical Sector and demonstrates what ACC and industry are doing to manage risk. Metrics, milestones, and free tools that help advance cybersecurity posture are provided. The site also includes a list of conferences, seminars, and workshops relevant to cybersecurity and 2011 events in which Chemical Roadmap Working Group members participated.

The Chemical Roadmap Working Group is comprised of the Chemical Sector-Specific Agency, National Cyber Security Division (NCSD), and industry partners. The working group met throughout 2011 to fulfill the milestones in the 2009 Roadmap to Secure Control Systems in the Chemical Sector. The Roadmap was developed jointly to present a plan for voluntarily improving cybersecurity in the sector. In addition to the Web site, the sector has created a Case for Action document that frames the necessity of implementing security measures. A DVD is also available providing several resources: Cybersecurity standards; sample procurement language; training options; a cybersecurity tabletop exercise; and NCSD's CSET™.

The Chemical Roadmap Working Group's efforts have been presented at several industry conferences and the Chemical Sector Security Summit. The working group plans to continue its outreach campaign, and its work toward achieving Roadmap milestones in 2012.

For more information, please contact Robert Kirk at ChemicalSector@dhs.gov.

CSSP Contact Information

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at https://forms.us-cert.gov/report/.

In addition, the ICS-CERT Monthly Monitors are published on HSIN as appendices to the ICSJWG newsletter and can be found here http://www.us-cert.gov/control_systems/ics-cert/.

ICS-CERT MONTHLY MONITOR

Other important contact information:
Website Address: http://www.us-cert.gov/control_systems/
ICS-CERT Email: ics-cert@dhs.gov
Phone: 1-877-776-7585
CSSP Email: cssp@dhs.gov