Homeland Security

December 2011

ICSJWG Quarterly Newsletter

ICS Roadmap Document

The ICSJWG Roadmap to Secure Industrial Control Systems subgroup has completed the “Cross Sector Roadmap for Cybersecurity of Control Systems”. This important document may be used by the ICSJWG community and all sectors as a model to develop or enhance other roadmaps and plans to secure control systems. The Roadmap subgroup is reaching out to all ICSJWG members to spread the word about the model in an effort to enhance the collaborative efforts of stakeholders, operators, and vendors to secure our nation’s critical infrastructure.

This will be a living document, revised over the next two years to maintain currency and relevance. The Co-Chairs welcome comments and insights into the current contents with an eye to improving both the document and its application to legacy systems and to those in development and planning. Key issues and common obstacles which are sector specific or cross-sector need to be addressed more comprehensively in the next version.

The document may be found on the ICSJWG site in the ICSJWG subgroups section at Roadmap to Secure Industrial Control Systems: http://www.us-cert.gov/control_systems/icsjwg/index.html.

Springfield, Illinois Water Pump Update

On November 16, 2011, ICS-CERT learned that an Illinois Statewide Terrorism & Intelligence Center (STIC) daily intelligence report containing raw, unconfirmed, single-source information was improperly released to the public media. This report erroneously stated that the supervisory control and data acquisition (SCADA) system at a water district in Springfield, Illinois, had been attacked by a cyber intruder based in Russia and that this attack destroyed a water pump at the facility. Multiple media outlets acquired the report and ran stories claiming that a nation-state cyber attack on U.S. critical infrastructure had occurred.

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

Upon further review and analysis, however, no evidence was found to support a malicious intrusion of the water district's SCADA system or the intent by a foreign entity to destroy the water pump. The foreign IP addresses located in the system's records were revealed to be legitimate addresses used by a third-party vendor to access the SCADA system while vacationing abroad. This was corroborated by network logs and other evidence collected by DHS fly-away teams and FBI investigators.

Additionally, further investigation into the water pump itself revealed failure due to normal wear-and-tear and deterioration due to the high iron content of the water. This particular pump also had a history of performance issues and was recommended by investigators to be replaced by the water district. For the full ICS-CERT Information Bulletin, see below:

http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf

ICSJWG Improve Communications Subcommittee

The ICSJWG would like to introduce a new subcommittee being formed under the Vendor subgroup called the ICSJWG Improve Communications Subcommittee. The Improve Communications Subcommittee was formed in order to assess and enhance the communication channels within the ICSJWG and present its findings at the ICSJWG 2012 Spring Conference in Savannah, Georgia. The subcommittee's kick-off meeting took place on Wednesday, December 14th, 2011.

CSET™ Version 4.0.1 Available for Download

The Department of Homeland Security (DHS) Control Systems Security Program (CSSP) has released an interim Version 4.0.1 of the Cyber Security Evaluation Tool (CSET™). This new version of the tool can be downloaded from the CSSP website: http://us-cert.gov/control_systems/satool.html.

This interim Version 4.0.1 release addresses some minor issues identified in report formatting and corrects a problem with Zone Security Assurance Level (SAL) calculations. Additionally, this release incorporates a new sub-report to isolate and show user comments in a single location, includes modifications to clarify how firewall analysis is performed, and improves upon the gap analysis for pass/fail standards.

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 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:

- **January 16-20**: Industry Partners
- **February 13-17**: Industry Partners
- **March 12-16**: Industry Partners
- **April 9-13**: Industry Partners (Reserved)
- **April 23-27**: International (Reserved)
- **May 21-25**: Industry Partners (Reserved)
- **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.

Additional offerings are being planned and will be announced once dates are finalized. 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.

One can register on the webpage by clicking the registration link associated with the class of interest. Registration is open approximately two months before the start of a class. Class size is limited to approximately 35 people with a maximum of two individuals per company per event. Due to high demand, 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.

Upcoming ICSJWG 2012 Spring Conference

Come to Savannah, Georgia this May! The ICSJWG 2012 Spring Conference dates have been finalized as May 7 - 10, 2012. This conference will be held at the Hyatt Regency Savannah in Savannah, Georgia. The ICSJWG 2012 Spring Conference is open to all members interested in learning about cybersecurity issues facing the nation's critical infrastructure control systems. The conference will operate with three track themes, including: vulnerability/mitigation, solution trends, and community selection. This is an excellent resource for government professionals (federal, state, local, tribal, and international); control system vendors and systems integrators; research, development, and academic professionals; and owners and operators (management, engineering, production, and IT). Conference attendees will be able to discuss the latest initiatives impacting security of industrial control systems and will have the opportunity to interact with colleagues and peers who may be addressing the risks of threats and vulnerabilities to their systems.

There is no cost to attend the conference sessions or any associated meetings and training. Travel, accommodations, meals, beverages, and other incidental expenses are the responsibility of the conference participants and will NOT be covered by ICSJWG or CSSP. Check out the ICSJWG site for past conference information and stay tuned for upcoming ICSJWG 2012 Spring Conference announcements and “Call for Abstracts” information! http://www.us-cert.gov/control_systems/icsjwg/

ICSJWG 2011 Fall Conference Information

The ICSJWG 2011 Fall Conference was a great success, thanks to the engaged participants and knowledgeable presenters. We appreciate the participation, comments, and insight provided during the subgroup meetings, presentations, and training. The contributions of industry and government professionals ensure that our mutual efforts to secure control systems will continue to be successful. The presentations illustrate and enhance the collaborative partnership fostered between federal agencies/departments and private asset owners/operators of industrial control systems.

Presentations with speaker release forms and the final agenda are posted to the ICSJWG site at http://www.us-cert.gov/control_systems/icsjwg/presentations/fall2011/presentations.html and on the Homeland Security Information Network (HSIN) - https://cs.hsin.gov/C10/C1/ICSJWG/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%202011%20Fall%20Conference%20Presentations&View=%7b6F252F6A%2d18EB%2d447A%2d96D4%2d106024729AB9%7d.

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@hq.dhs.gov or contact the co-chairs directly.

Homeland Security

Industrial Control Systems Joint Work Group (ICSJWG)

- **GCC/SCC Subgroup**

  GCC Co-Chair: Marty Edwards (Marty.Edwards@dhs.gov)
  SCC Co-Chair: Tim Roxey (Tim.Roxey@nerc.net)

  In Long Beach, the Government Coordinating Council (GCC)/ Sector Coordinating Council (SCC) working group approved the Vendor and Workforce Development Charters and discussed several membership and outreach initiatives to promote the ICSJWG and its mission. The group also formally approved the Roadmap document and determined to update it on an annual basis in the future.

- **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 completed the initial Cross-Sector Roadmap document and the revised Charter. Both documents have been reviewed and approved by the ICSJWG GCC/ SCC and distributed to the ICSJWG community through the ICSJWG website and HSIN.

- **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 committed to developing white papers and improving communications:

  - First, the Cross-Vendor Position Paper outlines the direction that the industrial controls system (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. (*Lead: Eric Cornelius, Eric.Cornelius@dhs.gov*)
  - Second, the ICS Common Vulnerability Disclosure Framework paper is intended to provide a consensus-based foundation for ICS vendors and integrators working to develop a vulnerability disclosure policy. The paper provides recommended ranges and formats for different aspects of the disclosure process. (*Lead: Rob McComber, Robert.Mccomber@telvent.abengoa.com*)
  - Third, the Improve Communications Subcommittee seeks to assess and enhance the communication channels within the ICSJWG and present its findings at the ICSJWG 2012 Spring Conference in Savannah, Georgia. *(GCC Lead: Neil Hershfield, Neil.Hershfield@dhs.gov; SCC Lead: Ralph Mackiewicz, ralph@sisconet.com*)

- **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 has completed the subgroup charter and is currently allocating tasks to complete the updated milestones. The document has been reviewed and approved by the ICSJWG GCC/ SCC and distributed to the ICSJWG community through the ICSJWG website and HSIN.

- **Research & Development Subgroup**

  GCC Co-Chair: Dr. Douglas Maughan (Douglas.Maughan@dhs.gov)
  SCC Co-Chair, Acting: Zach Tudor (zachary.tudor@sri.com)

  The R&D subgroup had an impressive turnout at their last meeting held during the ICSJWG 2011 Fall Conference. During the meeting, Dr. Maughan reviewed the charter, highlighting specific goals and objectives and the subgroup's interaction with other ICS-focused working groups. He reminded members that the subgroup is still seeking applicants for the SCC co-chair, though Mr. Tudor agreed to act in this position in the interim. If anyone is interested in applying for the position, please send an email to icsjwg@hq.dhs.gov. In addition, the subgroup discussed R&D requirements and plans, including a method for identifying existing and planned R&D needs and priorities, and several members presented R&D efforts they were managing across and within specific sectors.

Homeland Security Information Network

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@hq.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@hq.dhs.gov.

At this time, DHS is not able to grant non-U.S. citizens or those residing outside of the U.S. or 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@hq.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 March Quarterly Newsletter. If you want to submit an article for the March Newsletter, please email icsjwg@hq.dhs.gov, and we will take your submission into consideration for publication. The deadline for submissions for the March Newsletter is **February 29, 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 December 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.

ISA-62443.03.03 (99.03.03): Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels

From Eric Cosman, Vendor Subgroup Co-chair

The ISA99 committee has recently completed a ballot on the proposed draft standard ISA-63443.03.03 (ISA-99.03.03). The ballot passed with 18 approval votes and five disapproval votes. Reflecting the widespread interest in the draft, more than 500 comments were received during the ballot process. These comments will be reviewed and responded to in the coming months by ISA99 Working Group 4, Task Group 2. As a result of this exercise there may be further improvements to the draft, which would require a re-ballot.

As yet another clear indication of the global interest in the work of ISA99, the draft is currently also being circulated for voting to IEC TC65 as IEC 62443-3-3. The deadline for that process is mid-March 2012.

The committee is confident that this process will culminate in the release of this document as an approved international standard, providing an important component of the ISA-62443 / IEC 62443 body of standards.

Moving Forward through Collaboration

"We all have defined roles, the key will be to take ownership and responsibility for those we have control of..."

From Ernest A. Rakaczky, Program Director, Control System Cyber Security, Invensys Operations Management

Collaboration within the process control cyber security community is imperative and for the most part, our biggest challenge today is how quick we can get there.

Over the past years, we have read and listened to many communicate the value and need to collaborate as we move forward in defining cyber security measures within the process control community. These measures range from standards, guidelines, best practices, specific technologies, among others. This article is not adding to that list but is based more around what is needed for collaboration and why so many times we get so close but fall short.

True collaboration

I strongly believe there are three major ingredients needed for true collaboration to take place:

- Parties working toward a common goal;
- Parties that have established a trusted relationship; and
- Parties that understand their own boundaries and are willing to respect the boundaries of those in collaboration.

> ***"Without all three, collaboration will never happen, because all three are so interdependent on each other in any successful collaborative effort."***

Before we review each of the above in more detail, the intent for this paper is not to address who or what each contributor needs to do but to address more of the thought process and sensitivity each contributor in a collaborative effort needs to establish. In general, this collaborative community can bring members together from many and very different areas of interest, and possibly not limited to the following:

1. The End-User
2. Government Agencies
3. Control System Vendors
4. Researchers
5. Academia
6. Standards Groups
7. Security Technology Suppliers
8. System Integrators
9. Media
10. Sector Specific Industry Groups

Parties working toward a common goal

Within this objective, it is pretty clear and by far the one area everyone is continuously working towards, and that is, a safer and more robust critical infrastructure. But it is also the one objective that seems to be the cause of many collaborative efforts to quickly breakdown. Many times, it seems everyone is working on different timelines, form a 10-15 year strategic Industry Roadmap to a vulnerability being discovered so we need to alert the world yesterday. I know this may be looking at it from two separate ends of the spectrum, but for all those activities, even in between, we need to make sure we establish that timeline from the onset and that it is well understood and agreed upon by all parties involved.

Likewise, it is imperative that the collaborative groups establish and take ownership of the areas they are going to take responsibility for resolution. This is a clear way to ensure understanding of timelines and also set the foundation of establishing a trusted environment.

Parties that have established a trusted relationship

I believe within the control system cyber security community, there are many pockets where this trusted relationship is well established and where the biggest contributing factor was time. A majority of this community has been working together the better part of the past 10 years; we are now at a point where time is no longer on our side so we need to quickly build from this base a much broader trusted community, a task much easier to say than to establish.

Unlike 10 years ago, we do have a great program in-place that does facilitate and nurture our ability to grow this trusted base and that is through the current ICSJWG program. It clearly has the foundation in place to bring all interested parties together and actively participate. There is no better way to gain trust and at the same time ensure your concerns, ideas, solutions, guidance, etc. are being heard and contributing to a possible resolution effort.

From bi-annually face-to-face meetings to monthly sub-working group calls, you can clearly see the growth of this trust and a much broader/mixed participation from the various community groups.

But as this group grows it becomes even more evident and critical that we all establish a respect and an understanding of each member's boundaries, for without this respect, trust will never be possible.

Parties that understand their own boundaries and are willing to respect the boundaries of those in collaboration.

One element we do not talk about much is the overall life-cycle of a control product; I bring this to attention because it is also in this life-cycle many of the boundaries exist. It is within the various life-cycle phases we see clear crossover from various community members, areas of responsibilities, areas of ownership, and areas of resolution control.

Granted many members cross over many boundaries but many members have a more direct focus on a given life-cycle timeline.

Fundamentally there are three major life-cycle phases:

- **Control Product being Developed**
- **Control Product being Implemented**
- **Control Product supporting an Industry's Operational requirement**

From this understanding we clearly see that within these life-cycle phases the majority of time for the control product is supporting an operational requirement. This was the primary focus and effort spent in establishing standards, compliance, best practices, etc., a very tactical but very necessary effort. However, efforts also focused on control products that were already obsolete and/or at the end of their supported life-cycles.

Now let's look at company WIDGET Controls and they just released their new control product, if company WIDGET Controls has not addressed cyber security in the first two life-cycle phases, we are faced with the same issues for the next 10-15 years. It is this scenario that has so many researchers focused and at times frustrated with control system applications today. It is also one area, where the control system vendor has full control and ability to make a long-term difference.

Although there are definite life-cycle boundaries within the control product, the community of interest has pretty much a vested interest and requirements in all life-cycle phases.

So how can we establish some sort of balance and help to facilitate as these boundaries get crossed? Once crossed, the level of urgency, communication, mediation, and others get escalated and many times we lose focus. It is at this junction where we need to learn to respect the areas we have no physical control and trust those that do, and trust they will take ownership through resolution. At the same time we must build on the established US-CERT/CSSP programs it has put in place and leverage tools, information, training and most important their ability to be that foundational point of true collaboration.

Software Assurance Events

From the DHS Software Assurance Program

SwA Forum - Spring 2012 *March 26-30, 2012 at MITRE-1, 7525 Colshire Drive, McLean, VA 22102-7539*
The Software Assurance (SwA) Program of the Department of Homeland Security's National Cyber Security Division co-sponsors SwA Forums semi-annually with organizations in the Department of Defense and the National Institute for Standards and Technology. The purpose of the forums is to bring together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software.
https://buildsecurityin.us-cert.gov/bsi/1293-BSI.html?branch=1&language=1

SwA Working Group Sessions – Summer 2011 *June 25-28, 2012 at MITRE-1, 7525 Colshire Drive, McLean, VA 22102-7539*
The SwA Program of the Department of Homeland Security's National Cyber Security Division co-sponsors the Software Assurance Working Group's sessions to provide venues for public-private collaboration in advancing software assurance initiatives. Status updates from the SwA Working Groups are presented during SwA Forums and to other relevant stakeholder groups.
https://buildsecurityin.us-cert.gov/bsi/1294-BSI.html?branch=1&language=1

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@hq.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 can be found here - http://www.us-cert.gov/control_systems/ics-cert/.

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