June 2018

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— I C S J W G E X P A N D I N G T H E C O M M U N I T Y —

Upcoming Events

- August 28–30: ICSJWG 2018 Fall Meeting
  Hilton Cincinnati Netherland Plaza
  Cincinnati, OH
- June 4–8; June 25–29; July 23–27; August 20–24: Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, Idaho
  Registration for these respective trainings is *closed*
- *Tentative*
  October 1–5: Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, Idaho
  Registration will be available ~90 days prior to the start date

NCCIC Resources

Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Information Products

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on members like you for our Newsletter, Meetings, and Webinars. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, linguistic styles, or recommendations.

2018 Spring Meeting Recap

The 2018 Spring Industrial Control Systems Joint Working Group (ICSJWG) Meeting, which occurred April 10–12, 2018, in Albuquerque, New Mexico, was a recognized success, bringing together 275 critical infrastructure stakeholders for three full days of collaborative discussions of current and pressing ICS security issues. The Meeting included a keynote speech addressing cyberattacks within the Dark Web, the Internet of Things, phishing, and Wi-Fi. There were a series of engaging and topically current breakout sessions led by either the private sector or DHS National Cybersecurity and Communications Integration Center (NCCIC) representatives, and there was a hands-on technical workshop to educate participants on the latest malware threats and File Validation Techniques.

A key highlight of the Meeting was its concluding "Ask Me Anything" session, which included NCCIC cyber threat, assessment, incident response, and training representatives fielding questions from stakeholders. This discussion illuminated important perspectives between the NCCIC and the private sector, concepts such as IT vs. OT within the ICS context, how vendors and the NCCIC can better work together on critical vulnerability information, and the near-term future of what the NCCIC mission will focus on with respect to the threat landscape.

The ICSJWG program office has incorporated feedback from the Spring Meeting into its planning of future Meetings. Many thanks to those who provided evaluations!

2018 Fall Meeting—Announcement; Keynote Speaker Updates

The ICSJWG team is excited to announce the ICSJWG 2018 Fall Meeting! It will occur August 28–30, 2018, in Cincinnati, Ohio, at the Hilton Cincinnati Netherland Plaza hotel. Detailed information for the Meeting is available on the ICSJWG web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

At this time, the team is pleased to announce the confirmation of two keynote speakers for this Meeting: Rick Driggers, Deputy Assistant Secretary of the DHS Office of Cybersecurity and Communications, and Robert M. Lee, CEO and Founder of Dragos, Inc.

If you have any questions about the upcoming 2018 Fall Meeting, or generally about anything ICSJWG-related, please feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

ICSJWG Steering Team (IST)—Brief Leadership Update

After a year of strong leadership from Todd Therrien, the ICSJWG Steering Team (IST) has undergone a change in leadership. The new Chair and Vice-Chair of the Team are, respectively, Art Conklin, Director of the Center for Information Security Research and Education at the University of Houston, and Donovan Tindill, Senior Security Consultant for Industrial Cyber Security at Honeywell. The ICSWJG would like to sincerely thank Todd for his dedication to the ICSJWG and his work as IST Chair.

The ICSJWG program and mission looks forward to the contributions that this new leadership will bring.

Contributed Content Disclaimer: *The advice and instructions provided in the contributed content are specified as is with no warranties and should be confirmed and tested prior to implementation.*

Defining Control Security

By: Andrew Ginter, VP, Industrial Security, Waterfall Security Solutions

Definitions are important - good ones shape our understanding of concepts while poor ones impair that understanding. Consider the definition:

pen: a tube of ink with a tiny ball bearing at the tip

How useful is that definition? If we give the definition to a non-English-speaker, would it seem like a word worth remembering? Consider a different definition:

pen: a tool for writing or drawing with ink

Someone new to the language would likely hear this second definition and say “ahh - so that's what those things are called,” because she sees people using pens every day.

Now consider the definitions of “cybersecurity” and “information security”.

For article, click here.

Emerging Consensus For an ICS Security Approach

By: Courtney Schneider, Cyber Policy Research Manager, Waterfall Security Solutions

An increasing body of experience with industrial control system (ICS) security, as well as the emerging Industrial Internet of Things (IIoT) are driving a new consensus as to the difference between information technology (IT) and operations technology (OT) / ICS security programs. NIST, ANSSI, the ARC, the Gartner Group and others all recognize that preventing mis-operation of industrial systems in order to preserve safe and reliable operations is a fundamental priority for industrial sites, while the top priority on IT networks is one variation or another of “data protection.”

Full article, click here.

Coordinated Approach towards ICS Cyber Security

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Cyber security threats and severe attacks appear in variety forms and became a hot topic during the past decade. IT related threats may be generated by internally or externally generated actions. OT (ICS, SCADA) attacks might risk life of people and cause outage and damage. Most organizations already experienced some form of cyber-attack caused by viruses, ransomware, phishing, activation of trojans, Distributed Denial of Service (DDoS), etc.

In the IT field, identity theft is the attempt to act as someone else, in order to illegally retrieve personal information or access to confidential, private or commercial data. In the OT field, sabotage may lead to manipulation of production processes (food, pharma, chemicals, water, sewage, energy, etc.) aimed to cause loss of confidence and consequently financial and reputation damages.

There are many ways to protect your organization through cyber defense, which involve deployment of technologies, security processes, trainings, drills collaboration with cyber defense authorities, etc.
In this paper, I will elaborate on there (3) broadly used defense triads.

For full article, click here.

ICS Security Manager as a Service

By: Isiah Jones, MPS, CISSP, GICSP, C|CISO, Director, ICS Cyber Security Engineering, LEO Cyber Security

As ICS assets and operations increasingly become the targets of opportunity it is important that new strategies and ideas for focused and tailored security approaches are introduced to the community. ICS security manager as a service can enable the community to contract skilled resources for a new role dedicated solely to securing ICS within resource constrained operations staff for ICS asset owners and operations of some of the world's most critical infrastructures operated, monitored and controlled by automation and control systems.

The ICS Security Manager as a Service is like CISO as a Service on the IT side of the house with respect to building a security program. However, unlike the CISO as a Service, the ICS Security Manager as a Service is intended to be a more technical, hands-on role as well. Examples of duties and tasks the ICS Security Manager would perform as a service are: leading, coordinating and implementing day to day security tasks such as building ICS system security plans, inventory lists and testing products and services for ICS operators' operations and assets.

Such a service would most benefit ICS owners and operators who cannot afford a full-time resource within their staff. Some example asset owners and operators would be electric cooperatives, municipalities, and small businesses that own and operate pipelines, water and wastewater plants and hydro dams.

For the full article, click here.

The Case for Penetration Testing in ICS Environments

By: Krish Sridhar, P.E, GSEC, MBA, Sr. Business Manager, Industrial Cybersecurity, aeSolutions

Rising awareness of securing industrial control systems (ICS) and focus of organizations to roll out ICS cybersecurity programs have prompted a fresh look at the applicability and benefits of penetration (pen)

testing. A well designed pen testing project in a controlled environment provides insights and in-depth findings that cannot be otherwise obtained from traditional risk assessments alone. It complements risk based assessment by taking a deeper look at critical zones and conduits that were identified during the assessment. The results and recommendations help generate cybersecurity requirements specifications and drive standardization of security measures across multiple plants within an organization. This paper highlights the benefits of pen testing in an ICS environment and offers guidelines to design and conduct a pen testing project

To keep reading, click here.

A Call to Action for "Improving Software Component Transparency"

By: Bryan S. Owen, P.E, Principal Cyber Security Manager, OSIsoft

Critical Infrastructure Protection standards have just started to address supply chain management for industrial control system (ICS) software. As these programs mature the industry will need to improve software component transparency.

To continue reading, click here