INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

CISA CYBER+INFRASTRUCTURE

September 2020

Upcoming Events

ICSJWG Webinar Series

"Robust Cyber Risk Management- Simplified"

Wednesday, October 14, 2020
1:00PM-2:15PM (EDT)

Industrial Control Systems Cybersecurity Training provided by INL or in Idaho Falls, Idaho

CYBER-CHAMP® Training:
Foundational Training:
September 28, 2020
October 5, 2020
Advanced Training:
October 12, 2020
October 19, 2020
Additional Trainings at INL:
October 12 – 16 (401v)*
October 19 – 30 (301V)
December 7 – 11 (401v)*

**401 Training – must have completed 301 to attend this session.*

CISA Resources

COVID-19
CISA Service Catalog
CISA ICS Security Offerings
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.

The ICSJWG 2020 Fall Virtual Meeting

On September 21st and 22nd, Cybersecurity Infrastructure Security Agency (CISA) presented the second virtual version of the Industrial Control Systems Joint Working Group (ICSJWG) bi-annual event.

We featured keynotes by CISA Director Chris Krebs, and Keith Lunden, Mandiant Threat Intelligence. Innovations included during this meeting were based on recommendations from attendees at previous meetings. On day one, presentations from Industrial Control System (ICS) partners were delivered. Day two provided an overview of the updated CISA ICS CYBER-CHAMP Training, which is being introduced during the month of September. Day two continued with technical presentations from the ICS Community and the CISA ICS Team. Additionally, a "Capture the Flag" activity for the participants was provided over both days of the meeting.

The meeting was attended by ICS community members from around the globe, both new to the concepts and subject matter experts with years of experience. All presenter-approved presentations are available on the ICSJWG Engagement Hub until the Spring 2021 Meeting. The link to available presentations is here. We look forward to continually building our partnership with the ICS Community.

The ICSJWG 2020 Spring Virtual Meeting – Save the Date!

The ICSJWG is currently planning the next of our bi-annual meetings, again in a virtual format. We expect to launch the event in April 2021. We will provide updates as they occur, but for now, SAVE THE DATE for the ICSJWG Spring 2021 Virtual Meeting!

The ICSJWG Webinar

This webinar will start with common OT cyber risk fallacies: compliance is not due diligence, insurance does not keep the lights on, cyber catastrophes are not like hurricanes, we are all targets, and governments have limited ability to protect us from sophisticated attacks. Andrew Ginter will explore powerful new approaches to physical and "analog" mitigations for cyber risk, including: Security PHA Review (SPR), Consequence-Driven Cyber-Informed Engineering (CCE), Secure Operations Technology (SEC-OT), and manual operations fallbacks. Mr. Ginter will then return to CCE to review the intrinsic limits and costs of conventional software-based mitigations, and to explore how all these mitigations fit into a robust, defensible, security program. He will conclude by exploring common organizational resistance to robust programs, including confusing detection with prevention, confusing encryption with protection, confusing statistics with prediction, "air-gapped" fallacies, and "reverse lottery" ROI calculations.

The next ICSJWG webinar will be provided Wednesday, October 14, 2020; 1:00 PM – 2:15 PM (EDT). To participate in this webinar, please RSVP to ICSJWG.Communications@cisa.dhs.gov with a work-related email including

your name, company's name, role (vendor, owner-operator, etc.), State or Country from which you will be calling, and sector affiliation no later than Tuesday, October 13, 2020.

CYBER-CHAMP© Training

CISA hosts the ICSJWG to ensure a variety of ICS stakeholders have opportunities to improve their cybersecurity posture and education. ICSJWG is pleased to announce a continuation of the CISA hosted ICS training program facilitated by Idaho National Laboratory (INL). This training program has been integrated with the ICS CYBER-CHAMP© educational maturity model to produce additional modules within the ICSJWG training tracks—both foundational and advanced.

Foundational:
Session 3—Cybersecurity Differences within IT and ICS Domains: Introduces the differences between IT and ICS Domains. Topics include generations of ICS; communication, operations, and support differences; and why ICS domains should be separate from IT domains. This session will be on September 28.
Please register for this session here.
Session 4—Cyber Risks to ICS: Introduces Cyber Risks to ICS systems. Topics include Risk Curve; threat trends; adversarial risk, OSINT, OPSEC, and supply chain risks; and basics to determine ICS critical cyber risk. The risks outline the importance of understanding your network and why ICS networks are different than IT networks. This session will be on October 5.
Please register for this session here.
Advanced:
Session 9—Analyze Previously Captured ICS Traffic to Discover Vulnerabilities: Introduces tools to analyze previously captured ICS traffic. Topics include determining data flow; the kind of remote access used; and knowing what is coming in and out of your network. Open source tools will be available for everyone to use. This session will be on October 12.
Please register for this session here.
Session 10—Assessing Wireless Vulnerabilities in an ICS Environment: Discussion on high-level wireless communications. Topics include: IEEE 802.11 Protocols (Wi-Fi), IEEE 802.15 Protocols, and a quick intro to 5G Protocols. In the session we will also look at a few wireless packet capture tools. This session will be on October 19.
Please register for this session here.

If you missed Sessions 1, 2, 7, or 8, they are available via the ICS Learning Portal.

Please see our webpage for additional information.

CISA ICS Offerings and Capabilities Fact Sheet

Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions.

To support the ICS community's cyber risk management efforts, CISA offers ICS owners and operators a wide range of products, services, and capabilities. Please visit the CISA ICS Security Offerings page to learn more.

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*

Bow Tie Model of Destructive Malware- ICS Historian Case Study

By: Bryan Owen & Lubos MIcoch – OSIsoft; Dan Michaud-Soucy & Josh Carlson – Dragos

Industrial Control System (ICS) environments are inherently hazardous based on high energy and reactive chemicals often used within them. ICS owner/operator staff have long understood the essential need to recognize the various hazards within the environment and then prioritize them with an associated mitigation strategy. Bow Tie models put hazards directly into focus and provide a risk assessment framework to analyze causal relationships within various environments. The model helps identify relevant threats, defenses against those threats, impacts, and methods to reduce those associated impacts from creating an adverse event related to the hazard. Selecting effective barriers can reduce both the likelihood of the event and lessen the impact of the event should it take place. *Continue to full article…*

"Russians in the Grid" Enrichment Process

By: Bryan Beckman – Idaho National Laboratory

Threat intelligence sources are numerous, and the quality of their intelligence is equally variable. The need for quality, actionable, and sharable intelligence is becoming increasingly important as cyber-threats continue to increase. In this paper, we describe the process we used to enrich U.S. CERT's Technical Alert entitled "Russian Government Cyber-Activity Targeting Energy and Other Critical Infrastructure Sectors," affectionately referred to as "Russians In the Grid," from a series of separate but related reports to a final, actionable, unified Structured Threat Information Expression (STIX) v2 representation of the report. In the process, we detail the tools and procedures we used, some of which are automated and others highly manual. We identify some of the limitations of current STIX enrichment tools and techniques and propose enhancements to allow for more effective enrichment and better overall threat intelligence to be used for more effective threat data-sharing, as well as machine learning-based predictive threat work being conducted at Idaho National Laboratory.

A few key items need to exist for threat intelligence to be useful and effective. The threat indicators and courses of action must be stored in a format allowing it to be easily sharable and actionable. If threat intelligence is generated and stored in a proprietary format, that intel automatically has reduced value due to its limited audience, whereas intel generated and stored in standardized format, such as Structured Threat Information Expression version 2 (STIX2) [1], affords the ability for anyone with the desire or need to be able to read, understand, and utilize the data contained inside. Properly utilizing and supporting a standardized format such as STIX2 allows for threat intelligence to be distributed and shared amongst agencies, corporations, and asset owners. The effective sharing of intel makes it increasingly difficult for a threat actor to utilize the same attack on multiple targets. *Continue to full article…*

Embedded Vulnerabilities

By: Ron Brash – Verve Industrial

Awhile back I wrote about the fact that URG11 and network stack flaws are not anything new, and are miscreants left over from the 1990's and early 2000's – a period where these types of software flaws were rampant.

For the most part, these flaws represent an era that devices lacked proper robustness testing, and had customers obligated to trust the vendor's security practices. Whilst most of these were stranded in a land of security by obscurity or islanded ("air-gapped"), eventually were retired or rotated out of deployment and into the hands of researchers with ubiquitous network-stack protocol "fuzzers" (a strategy/application where you test all permutations of a protocol to see if there unintended effects or erroneous logic).

Yet, despite some of these vendors possibly having visibility or reports on these exact issues (or ones like them), stack-based vulnerabilities are commonly forgotten by vendor quality assurance and systems integration processes.

Well even if these systems are deployed in critical infrastructure, energy, oil & gas, manufacturing, building automation, or are consumer Internet of Things (IoT) products – the same issues are fundamentally present in all of those types of systems, and represent a variable level of opportunity & susceptibility to exploitation by a malicious entity. *Continue to full article…*