INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

June 2021

Upcoming Events

ICSJWG 2021 Fall Meeting

September 21-22, 2021

Incident Response Training Series

Asset Management (CDM142)
July 8
Course information and registration

Analyzing Cyber Risk (CDM111)
July 20-21
Course information and registration

Industrial Control Systems Evaluation (401v) Online Virtual Training

ICS Evaluation (401v) Online Virtual Training
July 12-25
Course information and registration

CISA Resources

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.

Call for Abstracts is Open!
The ICSJWG 2021 Fall Virtual Meeting

The Industrial Control Systems Joint Working Group (ICSJWG) 2021 Fall Virtual Meeting Call for Abstracts is now open! The Cybersecurity and Infrastructure Security Agency (CISA) will present the fourth virtual meeting scheduled to take place on September 21 and 22. As we develop the agenda for the meeting, we strive to have leading edge and timely information about current threats and mitigation techniques. Register here for the upcoming meeting.

The meeting will feature keynotes by CISA Leadership and a subject matter expert (SME) from the ICSJWG Community. Innovations included in this meeting are based on recommendations from attendees at previous meetings. Day 1 will consist of presentations from CISA leadership and ICS Partners. Day 2 will feature an overview of the CISA ICS Cyber-CHAMP© Training along with technical workshops from the CISA ICS Team. New to the lineup will be a table-top exercise based on a realistic scenario, illustrating how such exercises can complement an organization's preparedness and resilience posture. Additionally, the always popular "Capture the Flag" activity for all participants will be offered over both days of the meeting.

We welcome all ICS community members from around the globe, both those new to the concepts and as well as subject matter experts with years of experience. We look forward to virtually seeing you there and to continually building our partnership with the ICS Community.

The ICSJWG 2021 Spring Virtual Meeting - Recap

On April 20th and 21st, CISA presented the third virtual version of the Industrial Control Systems Joint Working Group (ICSJWG) bi-annual event, the ICSJWG Spring 2021 Virtual Meeting. We featured keynotes by Eric Goldstein, CISA Executive Assistant Director, Andre Ristaino from International Society of Automation, and Megan Samford from Schneider Electric.

On Day 1, ICS partners delivered presentations and participated in panel discussions while CYBER-CHAMP© CISA training sessions were held simultaneously, and participants were able to choose between main room presentations and training based on interest. Day 2 continued with simultaneous technical workshop style presentations. Additionally, a "Capture the Flag" activity for the participants was provided over both days of the meeting.

What We Urge You To Do To Protect Against The Threat of Ransomware

From: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

The number and size of ransomware incidents have increased significantly and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.
Continue to full memo…

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*

A Security Rating Model for the Internet of Things

By: Joe Fisher, President, Affinity IT Security Services

The Internet of Things (IoT) is upon us and continues to promise astonishing growth, as sensors and actuators of every sort become ubiquitous in both our professional and personal lives.

In this article we acknowledge the coming wave and all of its glorified benefits and disruptive potential, and also examine the history and future of the security of such devices. We elaborate the need for a simple and standard means by which to evaluate the relative security strength of IoT devices, and we propose a specific evaluation model to do so.

Our article concludes with a proposal and solicitation to conduct such evaluations for IoT products and discusses how this is mutually beneficial to vendors and consumers alike.
Continue to full article…

Building a Better Cyber Mouse Trap

By: Christine Hertzog, Principal Project Manager, Electric Power Research Institute

The electricity subsector is undergoing rapid changes with a proliferation of energy sources, intelligent systems and resiliency expectations. Two recent reports do an excellent job of documenting recommendations for the grid of the future (National Academies of Science, Engineering, and Medicine 2021: The Future of Electric Power in the United States and the future of cyber security for critical infrastructure (Cyberspace Solarium Commission report July 2020). Both reports are concerned with changing threat vectors for mission-critical infrastructure, particularly the volume, velocity, and variety of cyber-attacks.

EPRI has concerns about the current approach to cyber security, which is tactical and event-driven and too often changing its focus in reaction to external influences. This is not a sustainable situation for mission-critical infrastructure, especially given important metatrends that are also impacting the electricity subsector. These metatrends are decarbonization, digital transformation, valuation, and resiliency expectations. These metatrends are forcing a reconsideration of today's approach to OT cyber security. Fundamentally, the subsector must stop treating OT cyber security as an extrinsic afterthought and reformulate its perceptions of it as an intrinsic

principle persistently and consistently applied in organizations, their technologies, their practices and policies, and their workforce skills. In other words, it's time to build a better cyber mouse trap.
Continue to full article…

Crimes of Opportunity: Increasing Frequency of Low Sophistication Operational Technology Compromises

By: Keith Lunden, FireEye, Daniel Kapellmann Zafra, FireEye, and Nathan Brubaker, FireEye

Attacks on control processes supported by operational technology (OT) are often perceived as necessarily complex. This is because disrupting or modifying a control process to cause a predictable effect is often quite difficult and can require a lot of time and resources. However, Mandiant Threat Intelligence has observed simpler attacks, where actors with varying levels of skill and resources use common IT tools and techniques to gain access to and interact with exposed OT systems.

The activity is typically not sophisticated and is normally not targeted against specific organizations. Rather, the compromises appear to be driven by threat actors who are motivated to achieve ideological, egotistical, or financial objectives by taking advantage of an ample supply of internet-connected OT systems. As the actors are not interested in causing specific physical outcomes, they target whatever is available on the internet.

Mandiant has observed an increase in compromises of internet-accessible OT assets over the past several years. In this blog post we discuss previously undisclosed compromises and place them in context alongside publicly known incidents. Although none of these incidents have appeared to significantly impact the physical world, their increasing frequency and relative severity calls for analysis on their possible risks and implications.
Continue to full article…

CS2AI Ransom

By: Rick Kaun, VP Solutions, Verve, and Ron Brash, Director of Cyber Insights

Between May 6 and May 12, 2021 Colonial Pipeline, owner of 5,500 miles of pipeline carrying natural gas, gasoline, and diesel from Texas to New Jersey, shut down its operations in response to what it said was a ransomware attack targeting its IT network. In a media statement, Colonial officials indicated the damage was limited to their IT systems, but that the company "proactively took certain systems offline to contain the threat."

That response, which included disabling select OT/ICS systems, "temporarily halted all pipeline operations … which we are actively in the process of restoring." The company added that its operational technology (OT) systems were fine, and the shutdown was a measured response to enable quick recovery. Without such an abundance of caution, the IT malware might have proven much more disruptive thanks to the interconnectedness of pipeline infrastructure and participants upstream/downstream (e.g., custody transfers, shared remote metering, available storage/capacity, etc.).

Since the Colonial incident, several other major ransomware attacks on operating entities have been reported: Martha's Vineyard Ferry Service, FUJIFILM, and the JBS meat company who supplies 40% of all the US meat supply. This comes on the heels of several other large public ransomware events at the second largest paper company, Westrock, Molson Coors, and others just this year.

The reality is that industrial organizations are now in the crosshairs of the ransomware gangs as the impacts from lost availability is in the millions of dollars, so the ransom demands can be quite high. A recent report by Digital Shadows found that industrial goods and services was the number one most targeted industry in 2020 at 29% the number of attacks was more than those on the next 3 industries (retail, construction, and technology) combined.
Continue to full article…

Don't Just Mitigate Cyber Risk, Eliminate It

By: Andrew Ginter, VP Industrial Security Waterfall Security Solutions

Recent shutdowns of the Colonial Pipeline and JBS meat packing plants are only the latest evidence of a continuing trend. Ransomware is responsible for all OT production shut-downs due to cyber-attacks since at least the beginning of 2020. Today's most sophisticated ransomware groups use the tools and techniques that only a few years ago were the sole domain of nation state adversaries: command and control centers, manual remote operation, credential theft, lateral movement, data theft and eventually encryption and extortion.

There was a day when OT system owners and operators recognized the power of nation-state cyber-attacks but thought to themselves, "yes, but I'm not that important – why would a nation state ever target me?" The answer is now clear: profits. Multi-million-dollar ransoms are paid routinely by ransomware victims to criminals who use nation-state grade tools and techniques. Which businesses are today's targets? Anyone with money.

In this article we dig into the threat and explore OT cyber risk elimination rather than mitigation as a way to address the threat.
Continue to full article…

Affordable Operational Technology Protection: Cybersecurity as a Service

By: Daniel C. Gregory, CEO, AP Cyber, LLC

[Note: Complete article appears below.]

C-suites have traditionally struggled to justify investing in OT cybersecurity. Not only does implementing a true solution require a significant capital outlay; it requires continuous monitoring and real-time response, with no easily discernable or conventional return on investment. Further, implementing an internal comprehensive program requires recruiting and retaining highly skilled cybersecurity staff that are online 24/7/365. Implementing AI tools to automatically protect OT assets alone is ineffective. Basically, you are relying on AI to protect you from AI. Now add Quantum computers running AI and the fight is happening in real-time, all the time. Additionally, simply forwarding OT network data from a passive tap to an outside entity will delay timely and effective responses. No business can instantly institute let alone afford to implement and maintain such a program, but all businesses need protection against OT cyberattack and ransomware – now!

OT Cyber Security as a Service ("OT CaaS") wraps the CAPEX, design, implementation, continuous monitoring, response, and 24/7/365 skilled staff into one affordable monthly payment. Like buying insurance, OT CaaS is billed on a monthly basis- no upfront CAPEX is required. However, insurance compensates you after the attack and based on the hard cost of interruption to your business operations. Alternatively, OT CaaS protects your critical assets from cyberattack and ransomware, thus preventing business interruptions in the first place.

Clearly, OT CaaS must be designed, implemented, and delivered by trusted Tier-1 service providers. Not only must the solution be delivered reliably and seamlessly, but also the provider must regularly upgrade the solution to meet the everchanging threat environment. Such upgrades require participation in standards organizations, continuous testing and certification of conformance, and asset management. Additionally, the provider must provide reliable 24/7/365 support to secure the future. Applying tools and innovation without the support of a Tier-1 service provider leaves the burden on you to protect your OT assets, plus adds more complexity to your operations in the process. The days of relying on software vendor patches and after-the-fact response to attacks are over. Contracting OT CaaS from a Tier-1 team is the right solution to this vexing problem.

Air Gapped Edge Gateways: Best Practices for Cloud Connectivity

Attributed To: Brian Romansky, Chief Innovation Officer, OWL Cyber Defense

Cloud connectivity offers a wealth of benefits for energy providers and other critical infrastructure operators. Sending data from operational technology devices to the cloud allows asset owners to use remote diagnostic and analysis tools, improve supply chain management, and take advantage of enhanced services from machine vendors and other providers. New connections, however, can introduce new risks. Inadequately secured connections create opportunities for unauthorized parties to access critical systems, and some security

"solutions" have the potential to be hijacked and used to launch attacks by sophisticated threat actors. The complex dynamics of evolving threats and maturing cloud capabilities have led to a variety of security postures in the energy industry and the critical infrastructure sector in general. Most of today's scenarios fall into one of four categories, several of which might exist simultaneously within a single organization.
Continue to full article...

Protecting ICS System Details from Adversaries

By: Andrew Hildick-Smith, P.E. Principal, OT Sec LLC

Adversaries seeking to compromise control systems with a disruptive or destructive attack can maximize their success by performing detailed reconnaissance. Open-source intelligence (OSINT) searches can provide them with many valuable insights, but the jackpot is having a complete set of control system design or as-built documents, hardware and software inventories, configuration settings, a tag database, and copies of the HMI screens and control logic programs. These are the very things we intentionally collect and consolidate as an initial step in good cybersecurity and for incident response in case a control system is compromised and needs to be rebuilt. Here are some thoughts on basic steps an Industrial Control System (ICS) using organization can take to protect their system details and how the larger community can help.
Continue to full article...

Cybersecurity Resources for Control Systems Engineers

By: Steve Blaine, Automation Technologist, Jacobs

Lately, even the most sophisticated organizations and companies have seen their computer systems attacked and compromised. As control system engineers, we're all on high alert that our systems could be next. This article is written to inform you about some official guidance that is available to help you defend your industrial control system (ICS).

There are many defense and mitigation strategies that should be considered. Some of these actions are administrative and can be done very inexpensively. Others require sophisticated hardware and software, which can be very expensive. How should you decide which strategy is necessary and where it should apply? This can be a daunting task as there is a lot of information to consider. Further complicating things, each control system and the organizations that use them are all different. So, there is no ready answer for choosing how to defend your particular system.

A good place to start is with the knowledge and frameworks available from the organizations dedicated to answering this question. Hopefully, this article will provide an introduction to those resources so you can wrap your arms around the challenges with cybersecurity.
Continue to full article...

Understanding ICS Cyber-Attacks and Defense Measures

By: Daniel Ehrenreich, Secure Communications and Control Experts

The growing number of cyber-attacks on Industrial Control Systems (ICS) operating in a broad range of industrial, communications, utility and manufacturing applications is raising an important question: Do we correctly understand the cyber-attack surface and the actual risks to our organization? Who might initiate an attack, why a specific victim might be selected, what resources are required and how the motivation of an attacker is created?

Cyber security experts know well that it is impossible protecting all facilities and all zones in each facility with the strongest defense measure. Therefore, we must allocate resources to understand the attack environment.

The goal of this paper is to help the reader understand the risk level for each zone and select the most adequate, affordable and justifiable cyber defense.
Continue to full article...

Defending Critical Infrastructure Against Ransomware

By: Dr Oakley Cox, Principal ICS Analyst and Cambridge Team Lead, Darktrace

The Colonial Pipeline ransomware incident highlighted the significant threat that ransomware poses to organizations overseeing industrial control systems (ICS) and operational technology (OT). This white paper will closely examine a real-world ransomware attack on an energy supplier that was detected in real time by self-learning AI technology. Industrial ransomware can affect society at large, as seen in the gas shortages that resulted from the Colonial Pipeline incident. Even when critical infrastructure isn't directly compromised, global supply chains can be disrupted when major manufacturers, such as food processing facilities and suppliers for energy plants, are targeted. In addition to these broader social and economic consequences, ransomware targeting industrial environments has dire costs for the organization that is compromised, with operational downtime leading to considerable financial loss and disruption of heavy machinery threatening human safety.

With the rise of industrial ransomware, organizations should focus on self-learning and adaptive defense through early-stage threat detection, automated investigations, and Autonomous Response. These efforts will considerably increase resilience and complement more conventional measures such as patching, red teaming, and disaster recovery planning.
Continue to full article...

The Security of Dilemma of Smart Factories

By: Kazuhisa Tagaya, Global IoT Marketing Office, Trend Micro Incorporated

Industrial robots are the core of the automation of manufacturing processes in smart factories and are the most important components as they support the manufacture of all kinds of products such as automobiles, aircraft, processed foods, and pharmaceuticals. In addition, as equipment that realizes unmanned manufacturing in the post-COVID-19 world where minimal or no contact is a necessity, the importance of industrial robots that can repeatedly execute specified movements with high accuracy is regaining attention.

However, it is not commonly known that industrial robots are programmed using languages designed decades ago. Trend Micro has been conducting cybersecurity research on smart factories since 2017 and discovered vulnerabilities in "automation programs" that define the behavior of industrial robots and design flaws in "programming languages". These languages are legacy languages that were designed decades ago, but they continue to be used for purposes such as maintaining compatibility with successor models and reducing the burden of re-learning and are a technology that is still being used in modern smart factories.

In this paper, based on the results of our third joint research project with the Polytechnic University of Milan, from a short to long-term perspective, we analyze the design security risks involved in legacy languages and risk mitigation measures that all users of industrial robots should take.
Continue to full article...

Incident Response Preparedness Assessment Tool (IRPAT)

By: Bheshaj Krishnappa, Reliability First and David Sopata, Reliability First

The Bulk Electric System (BES) Critical Infrastructure is a complex amalgamation of people, processes and technology that is effectively managed to ensure the electric service reliability upon which our society depends. The BES Critical Infrastructure regulatory framework, is responsible for ensuring the reliability and security of the BES, which is comprised of substations, control centers, energy management systems, multiple communication technologies, supervisory control systems, etc. The critical operation of the BES is to provide monitoring, protection and control based on information gathered from field units and managed at multiple control centers. The BES components are constantly vulnerable to cyber and physical threats, and the vulnerable components include energy management systems, protection systems, communication links and networks. Cyber-attacks can start as spear phishing, denial of service, and/or man-in-the middle attacks, and they often manifest as loss of system view, loss of system control, loss of system availability or damage of a cyber asset. Physical attacks may initiate from malicious outside and inside threat actors, and they can manifest as unauthorized physical access causing harm to BES Facilities, such as property damage or theft of assets like copper.
Continue to full article...

Do IT Cryptographic Security Controls Work For Energy Systems?

By: Josh Carlson, Dragos, Inc., Dan Gunter, Former Dragos, Inc., Casey Roberts, Duke Energy Corp.
Colin Gordon, and George Masters, Schweitzer Engineering Laboratories, Inc.

The threats of unauthorized access to or manipulation of commands and data drive the incorporation of cryptographic security controls into critical energy system communication infrastructure. However, cryptographic security controls that are inappropriately or poorly applied can lead to a decline in reliability and availability and an inadvertent expansion of the attack surface available to attackers. Furthermore, most modern information technology (IT)-originating cryptographic security controls include encryption (a minimal-priority security control in energy systems), which brings the side effect of crippling the operators' ability to monitor their systems for intrusions.

This paper discusses reasons why many security techniques commonly applied in IT systems and based on cryptography may be unsuitable for application in critical portions of energy systems. We propose for system owners an approach to designing energy systems that separates system elements into those that are dynamic (designed to serve human users, reconfigurable, plug- and-play) and static (fixed-task, fixed-configuration, and machine-oriented, e.g., high-speed protection and telemetry). Lastly, we build on that approach with recommendations for operational technology (OT) cryptographic security controls in energy system networks.
Continue to full white paper...