INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

March 2021

Upcoming Events

ICSJWG Webinar Series

"Supply Chain Risk Management in Operational Environments"

Wednesday, June 2, 2021
1:00PM-2:15PM (EDT)

Industrial Control Systems Evaluation (401v + 301v) Online Virtual Training

April 5-18 (401v)
Course information and registration
April 12-23 (301v)
Course information and registration
April 19-May 2 (401v)
Course information and registration
April 26-May 7 (301v)
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.

Registration is Open!

THE ICSJWG 2021 Spring Virtual Meeting

The Industrial Control Systems Joint Working Group (ICSJWG) 2021 Spring Virtual Meeting Registration is now open! The Cybersecurity Infrastructure Security Agency (CISA) will present the third virtual meeting scheduled to take place on April 20th and 21st. Please register for the meeting here.

The meeting will feature keynotes by Eric Goldstein, CISA Executive Assistant Director of the Cybersecurity Division and Andre Ristaino, International Society of Automation & Megan Samford, Schneider Electric. Innovations included during this meeting were based on recommendations from attendees at previous meetings. Day 1 will consist of presentations from CISA leadership, ICS Partners, and an overview of the updated CISA ICS CYBER-CHAMP training which is a continuation of the training that was introduced in September 2020. Day 2 will provide technical workshops from the CISA ICS Team, and more presentations from ICS partners. Additionally, a "Capture the Flag" activity for the participants will be provided over both days of the meeting.

The meeting welcomes all ICS community members from around the globe, both new to the concepts and subject matter experts with years of experience. We look forward to virtually seeing you there and continually build our partnership with the ICS Community.

THE ICSJWG Webinar

Supply Chain Risk Management in Operational Environments will be presented by Dr. Jessica Smith, Senior Cyber Security Research Scientist

The next ICSJWG webinar will be provided on Wednesday, June 2, 2021; 1:00 PM – 2:15 PM (EDT). Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating the multitude of risks that threaten a component or device, to ensure that the device is operating correctly, and that the overall system is resilient. While much of this is placed on the shoulders of the manufacturer, there is still a responsibility placed on the end user to perform their own double-checks. Is the device a counterfeit? Are the components in a device from reliable sources? Are the companies providing the devices reliable? There are direct steps that an end user can take to ensure basic integrity and reliability in their devices, and this presentation will walk through an example to illustrate.

This presentation will discuss what SCRM entails; how ICS manufacturers and owner/operators can improve their SCRM; how this relates to both traditional hardware and software verification and validation, and to cybersecurity; current threats to supply chains; mitigations an end user can perform, and how current research projects like DOE sponsored VARS and CyTRICS can help. Registration information will be available soon.

The Cyber Security Evaluation Tool (CSET)

The Cyber Security Evaluation Tool (CSET®) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.

The CSET Download is available on GitHub: Releases · cisagov/cset · GitHub. You can also find older legacy versions of the software on GitHub.

Stakeholder Notification

Critical Infrastructure Colleagues and Partners, the Cybersecurity and Infrastructure Security Agency (CISA) has recently released a Personal Security Considerations fact sheet. This document encourages critical infrastructure owners and their personnel to remain vigilant and report suspicious behavior that individuals may exhibit in order to thwart an attack. It also contains several easily implementable security measures that can mitigate threats to personal safety. CISA also added a Homeland Security icon to cisa.gov cover page for easy navigating to this fact sheet as well as other tools and resources available to stakeholders. For more information and to access the fact sheet, visit here. For questions regarding the fact sheet and to contact your local Protective Security Advisor, please email central@cisa.gov.

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*

SolarWinds Response

By: Katherine Hutton, Stealth Path Inc.

Synopsis: Effective implementation of a Zero Trust security strategy would likely have prevented what is plausibly the most damaging cyberattack in US history, the full impact of which is far from realized. This whitepaper explores how SolarWinds, or any one of the 18,000 companies compromised by the SolarWinds breach, could have leveraged Zero Trust principles to establish tripwires alerting to the attack in its earliest stages. Coupling these strategies with an effective/progressive prevention posture, the plausible result would have been early identification and eradication.

What is the Core Issue? The SolarWinds breach generated a lot of commentary. How did it happen? How should the 18,000 impacted customers respond? What does it mean for national security? Most of the focus is on the impact of the attack rather than the root of the problem: the lack of detection and mitigation of anomalous behavior. What if SolarWinds could have detected abnormal behavior in its system as soon as it occurred? What if all of SolarWinds' customers had the capability to do the same?

The intent of this whitepaper is to advocate that organizations adopt a Zero Trust strategy to implement these protections.

Continue to full article…

Accidental Convergence In OT Environments

By: Michael Rothschild, Senior Director of Marketing, Tenable

Modern-day industrial and critical infrastructure organizations rely heavily on the operational technology (OT) environment to produce their goods and services. Beyond traditional IT operations that utilize servers, routers, PCs and switches, these organizations also rely on OT, such as programmable logic controllers (PLCs), distributed control systems (DCSs) and human machine interfaces (HMIs) to run their physical plants and factories. While OT devices have been in commercial use since the late 1960s, a complete transformation has occurred, changing the way we operate, interact with and secure the OT environment. Many organizations have opted to converge their IT and OT environments, which can yield many benefits; at the same time, these decisions are not without risk. Convergence can produce new attack vectors and attack surfaces; it can result in breaches that start on one side of the converged infrastructure and laterally creep to the other, from IT to OT and vice versa. Threats that impact OT operations are not the same as those that impact IT environments, thus the required security tools and operating policies are different. Deploying the right ones can harness all of the benefits of a converged operation without increasing the security exposure profile of the organization. It is important for organizations to establish a carefully planned strategy prior to any convergence initiative, rather than bolting on security as an afterthought.

Continue to full article…

Taxonomy of The Attack on SolarWinds and Its Supply Chain

By: Satya Gupta, Founder and CTO, Virsec

We are witnessing a significant uptick in a new class of attacks that exploit vulnerabilities in code used in high-value workloads, in Fortune 500 companies and government organizations. Conventional host-based security controls cannot effectively protect against these Remote Code Execution (RCE) vulnerabilities. This enables attackers to dwell in a victim's infrastructure for long periods of time, increasing the risk of extensive damage. What began on December 7th, 2020, as a notable but seemingly isolated attack on FireEye has quickly snowballed into one of the most serious waves of breaches to date. Although the FBI is still investigating, it appears that a concerted campaign by sophisticated Russian bad actors throughout 2020 has impacted FireEye (leaking sensitive security research tools), the US Treasury and Commerce Departments, nuclear testing labs, and a wide range of Fortune 500 companies. As a blunt New York Times headlines summarized: "Billions Spent on U.S. Defenses Failed to Detect Giant Russian Hack. "While most of the security news this year has focused on ransomware and the elections, these RCE attacks have been more subtle and insidious, sneaking into networks, burrowing into monitoring tools like SolarWinds, and dwelling for months aiming at stealing sensitive information. Following is a technical analysis based on currently available information, of the complex kill chains used in these attacks. As new information becomes available, we will continue to update our analysis and recommendations.

Continue to full article…

Industrial Control Systems: Understanding Vulnerabilities, Risk and Mitigation

By: Antonio Mauro, Founder and CEO of DeepInspect and Caroline Akawi, Junior OT Cybersecurity Specialist at DeepInspect

perspective. It is designed to understand what exactly ICS is, where we find them, the different types of systems that can be found within the ICS framework. The paper is divided into three sections, the first being an introduction to the Internet of Things (IoT) and ICS systems. In this section the reader can expect a thorough analysis of what Operational Technology (OT) is, how it differs from Information Technology (IT) and how it plays a role in our lifeline industries. Section two will explore the technical side of ICS with an analysis of ICS standards and protocols and how these differ depending on the industry. The final section will break down the vulnerabilities in ICS systems, the risks and the mitigation process. This section includes both theoretical and practical knowledge such as understanding what risk is and how to calculate it using the risk formula. It also touches on the securities levels of vulnerabilities and ways to implement mitigation tactics into your own ICS. This section also explores legacy control systems and the differences in risks and mitigation compared to that of a modern system. It is important to note that this paper was majorly influenced by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST).

Continue to full article…

Exploring the OPC Attack Surface

By: Uri Katz and Sharon Brizinov, The Claroty Research Team

Claroty researchers in 2020 conducted an extensive analysis of the OPC network protocol prevalent in OT networks worldwide. During that research, Claroty found and privately disclosed critical vulnerabilities in OPC implementations from a number of leading vendors that have built their respective products on top of the protocol stack. The affected vendors sell these products to companies operating in many industries within the ICS domain.

OPC (Open Platform Communications) is a common network protocol used in products to monitor and control systems from different vendors whose proprietary communication protocols are incompatible. Due to its massive popularity, the OPC protocol has attracted a lot of attention from researchers and attackers. Many researchers are fuzzing the OPC protocol and producing beneficial results. For example, Kaspersky Lab published a detailed report in 2018 claiming to have identified 17 security issues in some well-known OPC UA implementations.

The vulnerabilities discovered by Claroty could be exploited to cause a denial-of-service condition on devices operating on industrial networks, as well as information leaks, and remote code execution. Our research identified weak spots in different OPC specification implementations within different components of the OPC architecture. These components include the OPC server, OPC gateway, and a third-party library implementation of the OPC protocol stack.

Specifically, in our research we focused on three products:

- Industrial Automation OPC library by Softing Inc.
- ThingWorx Kepware Edge and KEPServerEX OPC Servers by Kepware PTC
- MatrikonOPC Tunneller by Matrikon Honeywell

These three products are integrated into many other vendors' offerings as a third-party component. For example, Softing's OPC library is being used as a third-party OPC protocol stack by some vendors, and the KEPServerEX OPC Server is being used as an OEM shelf solution by other well-known vendors, including Rockwell Automation and GE, both of which have published advisories informing their users of these security issues. We believe these vulnerabilities affect multiple other products sold by vendors across all ICS vertical markets.

In this report, we will explain the OPC protocol in depth, its architecture, and common usage in order to gain a deeper understanding of the impact of these vulnerabilities. We will also describe the vulnerabilities we uncovered, and explain the potential threat posed by attackers who exploit these vulnerabilities to take over OPC servers and gateways, and potentially harm manufacturing facilities and production lines.

Continue to full article…

Education is Essential for ICS Cyber Security Preparedness

By: Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Cyber security awareness for Industrial Control Systems (ICS), also known as Operating Technology (OT), is highly important for managing water and electricity supply, transportation, communications and manufacturing facilities. Effectively educating the control engineers and users on ICS-OT cyber security risk can be done through well-defined preparedness. The education program shall involve a) ICS operators and experts, b) IT experts who want to learn ICS basics and cyber defense solutions and c) managers who must make correct decisions related to allocation of resources. This paper highlights few important processes and allow you effectively achieving these goals.

Continue to full article…

Lessons from 2020: Defeating Targeted Ransomware Attacks at Industrial Sites

By: Michael Firstenberg, Director of Industrial Security Waterfall Security Solutions

2020 was not a good year for cyber-attacks on industrial control systems (ICS) and operational technology (OT) networks. Nine attacks shut down physical operations at industrial sites, and all were targeted ransomware. In addition, the single biggest cyber-attack in history–the SolarWinds Orion supply chain breach –impacted as many as 18,000 organizations, many of which were industrial enterprises with physical operations. Ransomware, targeted ransomware, supply chain breaches and the continued complexities of cloud connectivity are all top-of-mind concerns for security teams at industrial enterprises. Security teams responsible for industrial operations are re-evaluating their security programs in light of this new, pervasive threat environment.

Continue to full article…

OT Data in the Cloud: An Evolving Paradigm

By: Devin McCrate, Owl Cyber Defense

Many industries have seen significant improvements in operational efficiency and reduced downtime by adopting advanced analytics and optimization algorithms that run on cloud services. Critical infrastructure operators have been slow to adopt this new technology, due to well-justified concerns over the security and regulatory compliance of external connections. However, the potential benefits of OT-to-cloud connectivity grow more apparent each year, creating additional incentives for critical infrastructure operators and device manufacturers to support secure external network connections. The adoption of hardware-enforced security technology to deliver data to the cloud can help the industry accelerate adoption of cloud services, without the need for complex network analysis, and while fully meeting all regional and federal regulatory requirements. Equipment vendors are starting to explore the integration of this technology directly into their new designs, to enable advanced support and maintenance services that are driven by real-time machine data.

Continue to full article…