INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

December 2021

Upcoming Events

Save the date! ICSJWG Spring Virtual Meeting, **April 26-27, 2022**. Call for Abstracts now open!

Trainings:

Industrial Control Systems Evaluation (401v + 301v) Trainings:

Jan 10-14, **In-person** 301L PILOT - 4 days,

Idaho Falls, Idaho

Course information and registration

Jan 10-28, Online (401v)

Course information and registration

Jan 17-28, Online (301v)

Course information and registration

Feb 7-10, **In-person** 301L - 4 days, Idaho Falls, Idaho

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.

The ICSJWG Spring 2022 Virtual Event- Save the Date

Please save April 26- 27, 2022 in your calendars for the Spring 2022 Virtual Event. Call for Abstracts is now open if you're interested in presenting or know someone who would make a great presenter. We will have two full days of presentations, panels, demonstrations, technical workshops from subject matter experts, and we are excited to share that the Capture the Flag event will start the week prior.

The meeting welcomes all Industrial Control Systems (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 continue to build our partnership with the ICS Community. For more information, please contacts us at:ICSJWG.Communications@Cisa.dhs.gov

CISA Announces Cybersecurity Advisory Committee

Established in June 2021, the CISA Cybersecurity Advisory Committee operates as a board of industry and state, local, and tribal government leaders who advise the CISA Director on policies and programs related to CISA's cybersecurity mission.

Committee members—with subject matter expertise in various critical infrastructure sectors—participate in the development, refinement, and implementation of recommendations, policies, programs, planning, and training pertaining to CISA's cybersecurity mission.

The Committee directs its subcommittees—established by the CISA Director as necessary—to work on specific study topics to address cybersecurity issues, including information exchange, critical infrastructure, risk management, and public and private partnerships. Click Here to explore more information.

CISA Releases Services Catalog Version 2.0

On November 29, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released its interactive Services Catalog Version 2.0. The CISA Services Catalog is a single resource that provides users with access to information on services across all of CISA's mission areas that are available to federal government; State, Local, Tribal and Territorial Government; private industry; academia; NGO and non-profit; and general public stakeholders.

Version 2.0 allows users to filter and quickly home in on applicable services with just a few clicks. To learn more about CISA Services Catalog, visit the CISA Services Catalog on CISA.gov or access the full catalog here.

The U.S. Government does not endorse any specific commercial products, processes, or services. Any opinions or comments by commercial entities are provided for informational use only and do not imply an endorsement of any kind by the U.S. Government.

A Collaboration between CISA and Singapore CSA

Recognizing the need for a framework to map out the cybersecurity skillsets that Operational Technology (OT) cybersecurity professionals should be equipped in different job roles and to chart their career pathway, Cyber Security Agency of Singapore (CSA) launched the OT Cybersecurity Competency Framework (OTCCF) on October 8th, 2021 at the Singapore International Cyber Week.

The framework is developed jointly by CSA and Mercer (Singapore) with the support of other Singapore government agencies and in consultation with more than 70 industry and academic stakeholders. Compared with other existing skills frameworks, the OTCCF provides more granularity in terms of coverage and applicability in OT cybersecurity. By providing greater clarity to key stakeholders, the OTCCF will guide organizations in talent attraction and development. OTCCF also outlines the pathways that could apply to job roles, inclusive of vertical and lateral advancement opportunities.

Click here to read the full Collaboration article.

Binary Analysis with Architecture and Code Section Detection Using Supervised Machine Learning (WiiBin)

Authors: Bryan Beckman and Jed Haile, Idaho National Laboratory National and Homeland Security, Critical Infrastructure Protection/CyberCore - Idaho Falls, ID USA; Bryan.Beckman@inl.gov ; Jed.Haile@inl.gov

When presented with an unknown binary, which may or may not be complete, having the ability to determine information about it is critical to future reverse engineering, particularly in discovering the binary's intended use and potentially malicious nature. This article details techniques to both identify the machine architecture of the binary, as well as to locate the important code segments within the file. This identification of unknown binaries makes use of a technique called byte histogram in addition to various machine learning (ML) techniques, which we call "What is it Binary" or WiiBin. Benefits of byte histograms reflect the simplicity of calculation and do not rely on file headers or metadata, allowing for acceptable results when only a small portion of the original file is available. Utilizing WiiBin, we were able to accurately (>80%) determine the architecture of test binaries with as little as a 20% contiguous portion of the file present. We were also able to determine the location of code sections within a binary by utilizing the WiiBin framework. Ultimately, the more information that can be gleaned from a binary file, the easier it is to successfully reverse engineer.

Various techniques and tools currently exist which allow for the determination of a binary file's architecture. These include programs such as IDA Pro, Binwalk, and Ghidra. The basic byte histogram concept that will be presented here was previously described in an article titled Automatic classification of object code using machine learning. In this article, the previously described technique will be reiterated and expanded upon to further increase the overall accuracy of architecture detection. In addition to architecture prediction, the same histogram technique can be used for the first time to determine where, within a binary file, the code/instruction sections exist. This detection and location ability makes the reverse engineering of a binary significantly easier once this information is obtained.

Click here to read the full Binary Analysis article.

The U.S. Government does not endorse any specific commercial products, processes, or services. Any opinions or comments by commercial entities are provided for informational use only and do not imply an endorsement of any kind by the U.S. Government.

Clarifying the Cyber Security Aspects of IT-OT Convergence

Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Modernization of utility operations, manufacturing processes and traditional control architectures lead to deployment of enormous number of Industrial Internet of Things devices (IIoT) devices and ecosystems. Deployment of modernized architectures requires massive retrofitting of traditionally used serial protocols to ethernet based communication and TCP-based protocols. As a result of this trend, industry experts realized that ICS-OT architectures can no longer work in a silo, and they shall be integrated with the IT zone for purpose of achieving enhanced productivity, improved production quality, fewer outages, and reduced cost of maintenance. The integration among the IT and the ICS-OT zone started after the Stuxnet attack in 2010, when the management in industrial organizations realized that the air-gap segregation among ICS-OT and the IT systems does not protect the industrial zone from an internally generated cyber-attack.

Furthermore, organizations realized that coordinated analysis of data collected from the ICS-OT zone and the IT zone enhance the capability of the SOC team to detect cyber-attacks. Consequently, the IT experts realized the outstanding benefits of that approach and created a new term “IT-OT Convergence”. However, the ICS-OT experts in industrial organizations never evaluated the actual meaning of that term.

Clarifying the “IT-OT Convergence” term.

Before diving into that term, I see it important clarifying the actual meaning of ICS, OT and IIoT as people often interchangeable use these terms. Important mentioning, that even in these days the ISA-99 workgroups are debating on the correct definitions applicable for modernized systems.

A) Operational technology (OT) is referring to the hardware, the operating system, application programs, HMI and networking devices, deployed for communicating data and controlling physical processes within the Purdue level 0,1 and 2 zones.

B) Industrial Control System (ICS) or IACS (A-Automation) is referring to the process running within the Purdue level 0,1 and 2 zones by using OT products. The ICS-OT process shall assure compliance with the operation safety, reliability, and enhanced productivity goals.

C)Industrial IoT (IIoT) is referring to all types of field installed components and ecosystems aimed to improve the industrial productivity, detect fault, and collect real time data. These devices are communicating with the ICS-OT network and support specific functions for managing improved processes.

Click here to read the full Cyber Security Aspects article.

Internet of Things Security Guidance: Call for Industry Experts

Author: Benjamin Carter, CIS CTO Intern, Research Associate

The Internet of Things (IoT) comprises a boundless range of devices, services, and applications, providing new and unprecedented levels of interconnectivity. As a result, there is the need and opportunity for the security community to chart new instructions and recommendations for vendors in order to provide built-in security for IoT.

The Center for Internet Security (CIS) is forming an IoT Embedded Security Working Group to mature and enhance guidance for vendors on security recommendations. The recommendations found in the guidance are based on the type and constraints of control systems, IoT protocol support, and other considerations to ensure their devices run in the most efficient and secure manner. This guidance categorizes the types of devices based on how constrained TLP:WHITE those devices might be by resources, as well as the cost to provide recommendations for the appropriate security applications. While currently in the internal review process, we are preparing a panel of external reviews to assess detailed guidance for vendor implementations of each protocol in the sets of protocol stacks. Comparative guidance will be agreed upon by the expert reviewers to aid in vendor selections of protocols and protocol stacks for implementation. This will provide industry-specific recommendations as well as granular recommendations for vendors based on their business and security needs. Developers are still left to sort through numerous message formats and supporting sets of protocols in order to first determine what should be implemented, and then to define how to secure it.

Click here to read the full Internet of Things article.

A Risk Assessment for Ransomware Prevention in Operational Technology (OT)Environments

Author: Tom Winston, Ph.D., Director of Intelligence Content, Dragos, Inc., info@dragos.com

Ransomware has become the primary attack vector for many industrial organizations during 2021. Incidents like Colonial Pipeline, Honeywell, and JB Foods showed the world that even when industrial control systems are not specifically the target, ransomware attacks on enterprise IT systems which are integrated with operational technology (OT) cause major disruptions. This paper considers a novel approach to conducting a risk assessment in such environments to produce a quantifiable value an organization’s risk exposure.

Ransomware not only creates unusable file systems, but it can also halt processes, stop production, disrupt distribution, and can cost millions of dollars and cause weeks long headaches for victims. By dumping data to dedicated leak sites ransomware gangs can release intellectual property and personally identifiable information (PII). The techniques are varied, but they have common themes, accessing the infrastructure through known vulnerabilities. Once adversaries achieve initial access, they execute other programs to gain a foothold in critical enterprise IT systems and can move laterally to OT systems. Victims must pay the ransom to regain access to their file systems and regain control of their processes that use the file systems. Victims must decide the best course of action for their organization.

Best practices, and better “cyber hygiene” have proven ineffective against the blended approaches ransomware adversaries employ. The research in this paper explores a solution to securing environments that is rooted in complex systems analysis and advanced mathematics, presented in a way that stakeholders can use immediately. In this approach we avoid much of the differential calculus that underpins it, to make this paper easier to read and digest across a wide variety of industries.

Click here to read the full Risk Assessment article.

OT Security—Pushing the Curve

Author: Andrew Ginter, VP Industrial Security Waterfall Security Solutions

2021 has not been a good year for Operational Technology (OT) security. The Colonial Pipeline outage was the big news, followed quickly by the JBS meat-packing outage that shut down production at all the firm's North American plants, followed by a host of lesser incidents. The latest news is a near miss at CS Energy in Australia - ransomware crippled the IT network but the firm was able to physically isolate their power plants' networks before the ransomware propagated there and triggered a shutdown.

Can the Government Protect Us?

What is the trend here? Well, ransomware groups are getting much better at what they do – more specifically, these groups seem to be trailing nation-state actors by only about five years in terms of attack techniques and technology. For example, there was a day when nation-states were by far the most prolific users of targeted attacks - but today's ransomware groups are using targeted techniques routinely. Another example - there was a day when supply chain attacks were the stock and trade of only nation states - think NotPetya and SolarWinds, both attributed to Russian intelligence agencies. But this year a ransomware group pushed their malware to 1500 victims simultaneously through a compromised Kaseya cloud service for software updates.

What does this mean for us? Well, thinking back only a year on two, a lot of us were saying "Yes, but why would a nation state target us? After all, we're just not important enough to be a nation-state target." Today, we cannot say that anymore. Ransomware groups are using the tools and techniques of yesterday's nation states and are breaching IT and OT defenses routinely. And ransomware groups target everyone with money. Do we have money? Yes? Then we're a target. Look closely at what today's nation states are doing and take fair warning - what nation states do to each other today, ransomware groups will do to all of us in just another few years.

Click here to read the full OT Security article.

Developing a Cyber Mission Assurance (CMA) Process for Control Systems using Table-Top Exercises (TTX)

Authors: Mr. Daryl Haegley – Director, Mission Assurance & Cyber Deterrence, Office of Principal Cyber Advisor to SECDEF, daryl.r.haegley.civ@mail.mil

Dr. Michael Chipley – President, The PMC Group LLC, mchipley@pmcgroup.biz
Dr Leigh Armistead – President, Peregrine Technical Solutions, leigh.armistead@goldbelt.com

This paper discusses the development of a process and training mechanism for ICS cybersecurity systems. All Five Eye (FVEY) nations (United States, United Kingdom, Canada, New Zealand, and Australia) have demonstrated progress in development of Control Systems (CS) federated risk assessment methodologies and Cyber Mission Assurance (CMA) that account for holistic asset risks, beyond the scope of traditional Information Security. Greater collaboration between the FVEY CMA working group (WG) nations would facilitate the norming of best practices/processes and risk frameworks for cyber vulnerabilities on common Operational Technology (OT) platforms/components as well as provide opportunities for the sharing of threat intelligence and vulnerability information. The FVEY CMA WG continues to capture national inputs with respect to all considerations in prioritization modeling for incorporation into a future FVEY Prioritization of Defense Critical Assets approach. The CS CMA Assessment Table-Top Exercise (TTX) is critical to progression of this work.

The purpose of the CS CMA Assessment TTX was to establish a joint cyber mission assurance process for acceptance and adoption by all nation members of the FVEY, which is comprised of: United States, Canada, New Zealand, United Kingdom, and Australia. Cyber Mission Assurance is meant to determine the risks to military mission's operational readiness, with an emphasis placed on cyber threats and impacts. The CS CMA Assessment TTX is UNCLASSIFIED and designed to be executed on a fictional base and mission set with representative systems and platforms of the current relevant terrain. It can be held in-person or virtually and goes through the processes and procedures of all aspects of a real-world CS CMA Assessment. The desired outcome of the CS CMA Assessment TTX is for a standardized CS CMA Assessment process to be developed and agreed upon for use by all FVEY member nations.

Click here to read the full Cyber Mission Assurance article.

Collaboration in Coordinated Vulnerability Disclosure (CVD)

Author: Lindsey Cerkovnik

CISA's Industrial Control Systems (ICS) Vulnerability Disclosure Team is responsible for the public disclosure of vulnerabilities and associated mitigations, and patches affecting ICS, Internet of Things (IoT), and medical devices. Throughout the years, the ICS Vulnerability Disclosure Team has continued to identify and leverage innovative approaches to reduce risk to critical infrastructure owners and operators through the Coordinated Vulnerability Disclosure (CVD) process. As the need for more collaboration in CVD grows, the CISA ICS Disclosure Team has evolved to meet it.

In 2021, the ICS Disclosure Team coordinated a suite of vulnerabilities affecting the Object Management Group's Data Distribution Service (DDS) middleware protocol and API standard for data-centric connectivity. DDS provides low-latency data connectivity with extreme reliability while retaining a scalable architecture needed by business and mission-critical Internet of Things (IoT) applications.

Multiple vendors implement open source and proprietary versions of the OMG DDS standard, including Real-Time Innovations (RTI), eProsima, GurumNetworks, Object Computing (OCI), Twin Oaks Computing, and Eclipes Foundation – ADLINK. These products support a range of applications in a number of critical infrastructure sectors—Dams, Defense Industrial Base, Energy, Healthcare and Public Health, and more.

Click here to read the full Vulnerability Disclosure article.