SANS ICS SECURITY ORLANDO SUMMIT

Program Guide

@SANSICS #ICSSummit

Agenda

All Summit Sessions will be held in Horizons 5-7 (unless noted).

All approved presentations will be available online following the Summit at
https://ics.sans.org/ics-library/summit-archives
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Sunday, March 19

5:00-7:00pm	**Registration & Welcome Reception** *Hosted by RK Neal* 

Monday, March 20

8:00-8:45am	**Registration & Coffee** (LOCATION: HORIZONS 1-3)
8:45-9:15am	***Innovating a Brighter ICS Security Future*** The age of automation and digitization is upon us. We have been hard at work trying to shore up the many security issues that come with legacy ICS technologies. The benefits of doing more with the data and systems we are trying to protect are very real. As a community, we have been hard at work to lay the foundation to unlock more benefit than risk. I will review our most important work and where we need to go to best deal with the doubled-edged sword of innovation. We will also talk about how we might significantly close the gap between cyber attackers and defenders. Leadership in today's digital market favors those who can see beyond the immediate application of specific solutions to drive greater systemic value, all while addressing the inherent risks that come with a smaller, more connected world. Please join me as we set the stage for our incredible program and identify what we collectively must know and learn to chart an exciting – and secure – future. ***Mike Assante**, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*

Monday, March 20

9:15-9:45am

Musings of a SCADA Engineer Turned ICS Security Architect: Gas Pipeline SCADA

As control system engineers working for a smaller company or department with limited resources, we have to keep up with the times to continuously find ways to improve safety, reliability, and efficiency across countless disciplines. On top of our "normal" jobs, we're called on to be system admins, network engineers, desktop support and janitorial specialists. Now add cyber security to that list.

In this session I'll provide a background on natural gas pipelines and talk about the differences inherent to a Gas Pipeline SCADA system. I'll highlight some of the challenges I've faced individually as I've attempted to transition to a cyber security professional, and those that we've faced as a team while we adopted a cyber security culture. I'll talk about the challenges and triumphs establishing a comprehensive security program and implementing modernized situational awareness with an ICS security operations center.

***Sanford Rice**, SCADA System Developer, Atmos Energy Corporation*

9:45-10:30am

Secure SCADA Protocol for the 21st Century (SSP21)

Most SCADA protocols have no security, but will continue to be used in ICS for many years to come. Bolt-on security extensions introduce additional complexity, expand attack surface, and only function for a particular protocol. SSP21 is an open source development effort to create a secure encapsulation layer for SCADA protocols that can be used as a bump in the stack (master or outstation) or a bump in the wire (outstation only).

SSP21 is intended to fill a technology gap where existing technologies like TLS are not applicable, namely for serial communication channels and endpoints with limited bandwidth and/or processing capabilities. This presentation will focus on the following key points:

- **Main differences between SSP21 and past efforts to create secure SCADA protocols/wrappers**
- **Details of the SSP21 secure encapsulation layer**
- **PKI and key management in SSP21 systems**

SSP21 is sponsored by California Energy Systems for the 21st Century (CES21).

***J. Adam Crain**, Software Engineer & Security Researcher, Automatak*

10:30-11:00am **Networking Break and Vendor Expo** (LOCATION: HORIZONS 1-3)

11:00-11:30am

Is Everything Connected? Should It Be?

Over the past few decades, there has been a race to connect every device to every other device and to the boardroom. We have seen Internet of Things (IOT) devices play a role in hosting significant Distributed Denial of Service (DDOS) attacks – and ubiquitous remote connectivity has enabled events such as the Ukraine power outages. It is time to take a serious look at the engineering fundamentals of system design and ask the questions: "Is everything connected? Should it be?"

***Marty Edwards**, Director of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Dept. of Homeland Security*

Monday, March 20

11:30am-12:15pm

If We're Doing So Well, Why Are We Still Doing So Poorly?

Awareness campaigns, frameworks, community, public-private partnerships. We should be patting ourselves on the back for all the hard work we've been doing to advance the state of cybersecurity. Right? But wait! Why is ransomware flourishing? Why are IoT devices the scourge of security? How come the internet seems to be getting more dangerous?

MODERATOR: ***Mike Assante**, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*

PANELISTS: ***Dr. Art Conklin**, Director – Center for Information Security Research & Education, University of Houston*

***Marty Edwards**, Director of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Dept. of Homeland Security*

***Rob Putnam**, Cyber Commercial Leader, GE Power*

***Tyler Williams**, Global Technology Leader, Shell*

12:15-1:30pm

Lunch & Learn Sessions

Sponsor: Nozomi Networks

Real-time Mapping, Modeling and Anomaly Detection for ICS

In this presentation, attendees will learn about how the application of machine learning to the unique challenges of industrial control cybersecurity enables:

- Real time visibility with passive ICS network modeling
- Immediate detection with process anomaly detection
- Accelerated incident response with AI-enabled correlation
- Rapid remediation leveraging firewall integration

Presenter: ***Edgard Capdevielle**, CEO Nozomi Networks*

Location: Spring Lake

Sponsor: PAS, Inc.

ICS Cybersecurity and the Devil's Rope

Securing ICS is certainly a challenge, as the endpoints that matter most are highly complex and proprietary. Unfortunately, plants don't often have an accurate, comprehensive inventory of all their systems, and they do not typically monitor for changes to system configurations, such as control logic. How can you secure what you cannot see? And further, how can you know an unauthorized change has occurred?

In this discussion, we will examine how today's Devil's Rope has left our ICS vulnerable. We will examine best practices to adopting a more production-centric approach to securing both Level-2 controllers and Level-1 smart field instruments. Finally, we will look at case studies that support these best practices.

Presenter: ***David Zahn**, CMO & GM, Cybersecurity Business Unit, PAS, Inc.*

Location: Sandy Lake

Sponsor: Waterfall Security

A Comparison of value in Cybersecurity Strategies – Prevention versus Detection

The threats to our critical infrastructure continue to evolve. As new cyberattacks are created and discovered, it is incumbent upon us to evaluate the capabilities of our defensive strategies and technologies against these new offensives.

This session will investigate and report on how the modern, targeted online and removable media threats to industrial cybersecurity fare against the most popular defenses deployed to protect critical infrastructure and industrial control systems, with special focus on the effectiveness of the three classes of defense – protective, detective, and directive.

Presenter: ***Michael Firstenberg**, Director of Industrial Security, Waterfall Security*

Location: Bay/Park Lake

Monday, March 20

1:30-2:15pm	***Demo: The Ukraine Event In a Box*** Idaho National Lab will provide a hardware-based demonstration illustrating several elements from the Ukraine cyber attacks resulting in power outages in Western Ukraine in December 2015. The demonstration will leverage hands-on activities for participants, including various scenarios/capabilities used by the attackers to include: operator HMI exploitation, leveraging trusted paths to mis-operate field devices, etc. The goal of the demonstration is to provide electricity sector experts with meaningful and tangible lessons-learned from the Ukraine attacks, with the goal of informing/arming the defender. ***Tim Conway**, Technical Director – ICS & SCADA Programs, SANS Institute* ***Andy Bochman**, Senior Cyber and Energy Security Strategist, INL* ***Joseph Price**, Deputy Director, Critical Infrastructure Protection Division at Idaho National Laboratory*
2:15-3:00pm	***The 1990s Called – They Want Their Technology Back: How ICS Is Still Using Paging Technologies*** Pagers are prevalent even to this day in the many sectors around the world. With the prevalence of software define radios, and price points that will give even the most novice attacker the ability to sniff and decode messages sent to pagers. This talk will focus on the basics of pagers, the protocols that are used, the systems that are currently using them, and the analysis of some of the pages that have been observed from researchers at Trend Micro during the project. This talk will focus only on the pager messages used within ICS fields and messages that have been observed that are relevant to the audience at SANS ICS. ***Stephen Hilt**, Sr. Threat Researcher, Trend Micro*
3:00-3:30pm	**Networking Break and Vendor Expo** (LOCATION: HORIZONS 1-3)
3:30-4:15pm	***I'll Let Myself In: How Threats Are Slipping In the Actual Back Door While You're Looking at Logs*** Many organizations are accustomed to being scared at the results of their network scans and digital penetration tests, but seldom do these tests yield outright "surprise" across an entire enterprise. Some servers are unpatched, some software is vulnerable, and networks are often not properly segmented. No huge shocks there. As head of a Physical Penetration team, however, my deliverable day tends to be quite different. With faces agog, executives routinely watch me describe (or show video) of their doors and cabinets popping open in seconds. This presentation will highlight some of the most exciting and shocking methods by which my team and I routinely let ourselves in on physical jobs. ***Deviant Ollam**, Security Auditor & Pen Test Consultant, The CORE Group*

Monday, March 20	
4:15-5:00pm	***Disassembly and Hacking of Firmware Where You Least Expect It: In Your Tools*** This live hacking demonstration will investigate vulnerability and capability assessment of firmware attacks; physical ramifications of tool attacks; instances where "less security" is better; and security tips for firmware. You'll leave with a better understanding of the location and use of firmware in unexpected places and gain insight into the attack methodologies for and security of devices with firmware, so you can better protect yourself. ***Monta Elkins**, Hacker-in-Chief, FoxGuard Solutions*
5:00-5:15pm	***Introduction to ICS NetWars: Be the First to Play!*** NetWars is a popular hands-on challenge that lets SANS students push their limits and build new skills. ICS NetWars takes it to the next level to challenge control systems professionals. Find out what's new and why you should go for the glory. ***Tom Van Norman**, Senior Technical Staff, CounterHack Challenges*
5:15-6:15 pm	**Networking Reception** (LOCATION: HORIZONS 1-3)
6:30-9:30pm	**ICS Game Night** ***ICS NetWars makes its world debut here tonight! Be one of the first to play it for skill-building and bragging rights!*** Whether you want to test your technical skills with ICS NetWars, hone your strategic thinking with a challenging simulation game, or just cheer on other attendees, you're sure to learn something new and expand your professional network during this exciting evening of work-meets-play.

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

Tuesday, March 21	
8:00-8:45am	**Registration & Coffee**
8:45-9:00am	***Ernie Rakaczky ICS Security Lifetime Achievement Award*** Ernie Rakaczky, Jr. was best known by his peers as an advocate with a passion for progress, innovation, and investment in the ICS field. He became a strong supporter of U.S. and Canadian efforts to enhance the security of ICS on an international scale, and an activist to bridge the gap of IT and OT through education and awareness of proper automation systems to security professionals. Ernie served on the GICSP steering committee, where his expertise and insight directed the formulation of the certification. Those who worked alongside Ernie will remember him for his dedication and contributions to shaping the ICS security field and his optimistic outlook on the potential to make a difference. Join us to honor the legacy of this leader as we present the inaugural Ernie Rakaczky ICS Security Lifetime Achievement Award. ***Mike Assante**, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*
9:00-9:45am	***Exploring the Unknown ICS Threat Landscape*** ICS (in)security is hiding in plain sight. This presentation will be our first public discussion on unique research on industrial control system software, malware, and the consequences of poor operations security. Our premise for this project is the belief that there is a wealth of information surrounding Industrial Control Systems that is unrecognized by the traditional IT cybersecurity industry. We will walk through our methodology, show real-world findings and conclusions of what this means in our space. ***Robert M. Lee**, CEO, Dragos Inc.* ***Ben Miller**, Director of Threat Operations, Dragos Inc.*
9:45-10:30am	***From Research to Reality: Real-World Applications of Threat and Vulnerability Data Analysis*** In October 2016, Kaspersky Lab launched the first non-government run ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) – a non-commercial project focused on collecting and sharing the latest ICS threat vectors, incident investigation, vulnerability research, analysis etc., from Kaspersky researchers as well as external sources. This talk will highlight major research, case studies, findings, and analysis, covering the following topics: • ICS Threat intelligence: attacks and threats; • Vulnerability research: Statistics and main vulnerability vectors; • Threat analysis: what are the major threats in ICS field, how the threats changed; • Modern attack vectors on ICS. ***Clint Bodungen**, Senior Researcher, Critical Infrastructure Threat Analysis, Kaspersky Lab, North America* ***Vladimir Dashchenko**, Senior Research Developer, Critical Infrastructure Threat Analysis, Kaspersky Lab*
10:30-11:00 am	**Networking Break and Vendor Expo** (LOCATION: HORIZONS 1-3)

Tuesday, March 21

11:00-11:45am

Operation BugDrop: Stage 1 Cyber Reconnaissance in the Real World

In February 2017, CyberX's threat intelligence research team discovered a massive cyber-reconnaissance operation targeting critical infrastructure, scientific research and media in the Ukraine and other countries. The operation requires a massive back-end infrastructure to store, decrypt and analyze several Gigabytes per day of unstructured data that's captured from its targets (including audio recordings, screen shots, documents and passwords). In this session, CyberX's VP of Research will describe how their team discovered the malicious operation, reverse-engineered the malware, and dissected its C&C mechanisms; as well as provide recommendations on how to protect your ICS infrastructure from these types of cyber-intrusions.

***David Atch**, VP of Research, CyberX*

11:45am-12:30pm

USACE Control System Cybersecurity Program: Processes and Lessons from the Corps

The global climate of cyber threats continually increases in intensity. The U.S. Army Corps of Engineers has responded by launching an aggressive cybersecurity program for control systems spanning the entire system lifecycle. Starting with enterprise-wide inventory implementation and moving through system hardening to Authority To Operate (ATO) issuance and continuous monitoring, USACE has developed a comprehensive control system cybersecurity methodology based on real cyber risk that is being incorporated in other cybersecurity programs across all of the Department of Defense (DoD) and other branches of the military.

***Phillip Copeland**, Director, Critical Infrastructure Cyber Security, U.S. Army Corps of Engineers*

***Gregory Garcia**, Chief Information Officer/G-6, U.S. Army Corps of Engineers*

12:15-1:30pm

Lunch & Learn Sessions

Sponsor: Claroty

Leveraging DPI for Visibility and Anomaly Detection into ICS Networks: Power Generation Example

Leveraging an attack scenarios from electric generation environment, the team will demonstrate how advanced DPI can detect adversaries across kill chain stages, provide actionable alerts and deliver the context required for IT Security/SOC Teams to efficiently and collaboratively investigate resolve issues.

Presenter: Colin Blou

Location: Spring Lake

Sponsor: RK Neal

ICS Security. Simplified.

The current cybersecurity market is bursting with new technologies that promise better security through advanced algorithms, software defined networks and bleeding edge techniques. A major power company recently decided to take a back-to-the-basics approach to cybersecurity. They started by extending, augmenting and orchestrating a select group of best in class IT tools into their control systems. Then they tied these tools together in a single platform, allowing them to leverage information from multiple sources in one portal. The resulting gains in cybersecurity maturity have been measurable and significant. Join us for an open discussion on how this simplified approach makes robust ICS cybersecurity accessible, affordable and sustainable.

Presenter: Rick Kaun, Application Engineering, Verve Industrial Protection & Eric Byres, ISA Fellow

Location: Sandy Lake

Sponsor: Recorded Future

Threat Intelligence Stories: Ransomware, Grizzly Steppe, and More

Malware has been historically used to damage or disable a computer's normal functioning. There has been a significant shift from code used to prevent the user's ability to operate the machine, to code used to hold data and information at ransom. In this discussion, we'll examine KillDisk; a malware that has morphed from destructive to larcenous. We'll explore the earliest stages of ICS malware as it is passed around on the dark web and illicit sites and finally end with a close observation of a recent cyber attack tied to Grizzly Steppe.

Presenter: Wendy DeLuca, Solution Engineer, Recorded Future

Location: Bay/Park Lake

Tuesday, March 21

1:30-2:15pm	***Top-Down, Purpose-Based Cybersecurity*** Cyber attacks that cause physical damage or affect physical processes are no longer limited to theory or speculation. Innovations within the Departments of Defense and Energy reveal a commonality in a top-down, purpose-based approach to preventing unacceptable losses and significant consequences resulting from malicious cyber activity. Such an approach allows an organization to apply limited resources to critical, key elements of their operation without necessitating a need to cover the entire waterfront. ***David E. Stone***, Colonel, United States Air Force, Air Force Cyber College
2:15-3:00pm	***Controls, Captains, and Careers*** The gloves are coming off, as we put tough questions to this panel of ICS pros. How are we really doing? How can we build teams with the right skills to make an impact on security? What controls are successful IS practitioners embracing, and what's a waste of time? MODERATOR: ***Mike Assante***, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute PANELISTS: ***Eric Byres***, P.Eng, ISA Fellow ***Steve Mustard*** (@steve_mustard), Chair, Cybersecurity Committee, Automation Federation ***Justin Opatrny,*** Cyber Security Consultant – OT, General Mills
3:00-3:20pm	**Networking Break and Vendor Expo** (LOCATION: HORIZONS 1-3)
3:20-4:00pm	***IT and OT Convergence – It's a Thing for Attackers, Too!*** This live demo will welcome the audience into the minds of a simulated adversary group tasked with the goal of creating a destructive critical infrastructure attack. Successful attacks targeting complex environments require diverse adversary teams capable of developing a sound concept of operations and executing that plan across diverse IT and OT supported environments. This talk will feature an on-stage demo of open-source facility recon and targeting, leveraging ICS field device attack vectors, process control manipulation, zero-day fun time, and firmware manipulation. ***Jason Dely****, Technical Director – Industrial Control Systems, Cylance* ***Christopher Robinson****, Principal Consultant, Cylance*

Tuesday, March 21

4:00-4:45pm	***Incentivizing ICS Security: The Case for Cyber Insurance*** Over the past couple of decades, cybersecurity—as a field—has had difficulty speaking to executives and boards about risk. Our community often qualifies cyber risk as "high, medium, and low" or "red, yellow, and green." When compared to more mature areas of traditional risk management, which feature quantifiable metrics and graphs as complex as the Dow Jones Industrial Average, our security professionals may look like they're carrying crayons to a math test. Fortunately, in the past few years, we've seen a jump in maturity when discussing cyber risk management. By applying leading and lagging metrics, quantifying the impacts due to cyber risk beyond "criticality," and branching into data analytics, many information security professionals have found new ways to communicate cyber risk in meaningful ways for executives and boards. This presentation will highlight the new metrics and methodologies used for quantifying cyber risk and cyber program improvements in critical infrastructure. Recognizing the many different drivers for maturing a cyber risk management program, the presenter will also discuss the internal and external partners for these sort of program improvements, and, why security professionals should become very good friends with the insurance industry. ***Jason Christopher**, CTO, Axio*
4:45-5:30pm	***How the Midcontinent Independent System Operator (MISO) moved to Active Defense and Advanced in the Hunting Maturity Model (HMM)*** Industry is shifting away from traditional cyber security approaches. We commonly hear that preventative security solutions are lagging and that we should assume we are already breached. MISO considered the available information and agreed that a different approach to security was needed. Steps were taken in late 2014 to prepare for new Cyber Security capabilities. Those activities have enabled MISO to move towards Active Defense, including the ability to hunt for anomalies and indicators of compromise across its infrastructure. This presentation will cover how MISO was able to implement and use these new proactive capabilities. Examples will be shown of hunting activities that MISO is performing. The activities will also be mapped to where they fit within the Hunting Maturity Model (HMM). The presentation will also demonstrate what Cyber Hunting means at a practical level. Much of what has been written about Cyber Hunting leaves an abstract and cloudy perception about the topic. Three specific examples will be used to show activities at HMM levels 0, 1, and 2. Outcomes of the examples will include the lessons learned and the value that the activities brought to MISO. ***Jamie Buening**, Information Security Analyst, Midcontinent Independent System Operator (MISO)*
5:30-5:45pm	***Closing Remarks*** ***Mike Assante,** Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

@SANSICS  **#ICSSummit**