9 TH ANNUAL

ICS Security

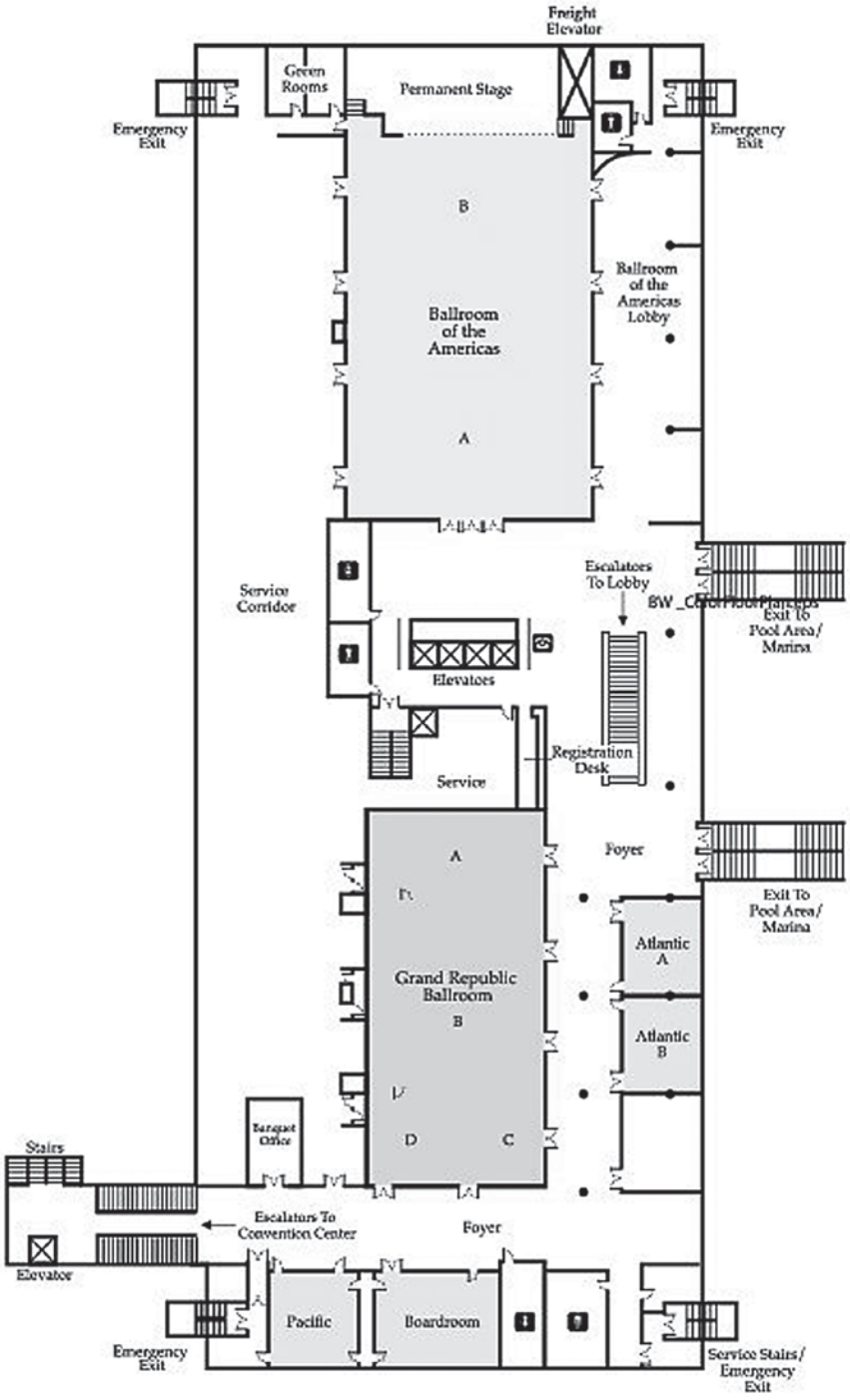
SUMMIT

Program Guide

Chairman: Michael J. Assante

SANS ICS Industrial Control Systems

Disney's Contemporary Convention Center Level Two



Agenda

All Summit Sessions will be held in the Ballroom of the Americas B (unless noted).

All approved presentations will be available online following the Summit at ***https://files.sans.org/icsorlando2014****.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Sunday, March 16

5:00-8:00 pm

Registration

Location: The Contemporary Resort Convention Center - Level 2 Registration Desk

---

6:00-8:00 pm

Paul's Security Weekly

Location: Ballroom of the Americas B

Sponsored by

The Security Weekly (formerly "PaulDotCom") mission is to provide free content within the subject matter of IT security news, vulnerabilities, hacking, and research. We strive to use new technologies to reach a wider audience across the globe to teach people how to grow, learn, and be security ninjas. The mixture of technical content and entertainment will continue to set a new standard for podcasting and Internet TV. We operate in a relaxed environment, we have fun, and we've been known to "Hack Naked." Get in on the action with a live broadcast from Orlando, where we'll be interviewing our great line-up of guests on the latest and most pressing topics in SCADA/ICS security.

Host: ***Paul Asadoorian***

Guest Interviews: ***Michael J. Assante****, Director - ICS & SCADA, SANS Institute*
Matt Luallen*, President & Co-Founder, CYBATI*
Jonathan Pollet*, Founder and Principal Consultant for Red Tiger Security*
Justin Searle*, Managing Partner, UtiliSec*

8:00-11:00 pm

From Exposure to Closure Act IV

Location: Ballroom of the Americas B

Presented by

Back by popular demand, Exposure to Closure will run for an exclusive one-night only engagement. The Heist starts with an intrusion at Acme Power & Light but not all is as it appears. Watch through four acts with twists and turns through incident response, forensic deconstruction, and eventually recovery.

Audience members will be on the edges of their seats as our cast of security geeks take an entertaining turn as actors, but will also walk away with practical, applicable knowledge including:

- Real-life lessons of incident response from seasoned professionals
- How cyber attacks can penetrate into the most secure ICS networks
- Emerging cyber threat intelligence methodology being applied by leading security firms
- Overview of how governments interact and can (and can't) assist companies security programs

All Summit Sessions will be held in the Ballroom of the Americas B (unless noted).

Monday, March 17

7:00-8:15 am

Registration

Location: The Contemporary Resort Convention Center - Level 2 Registration Desk

---

8:15-8:30 am

Welcome & Opening Remarks

***Michael J. Assante**, Director – ICS & SCADA, SANS Institute*

8:30-9:30 am

What's All the Fuzz About?

We will begin the session by summarizing the current status of Project Robus, an ongoing search for vulnerabilities in ICS protocols.

We will provide some high-level background theory on the science and art of fuzzing, including:

- Type of fuzzers: pure random, template/mutational, and generational
- Selecting intelligent test cases using DNP3 as a case study
- Important properties of fuzzers including health checking & repeatability
- Metrics for evaluating fuzzing effectiveness
- Where fuzzing works, and where it falls short

We will introduce the Aegis fuzzing framework w/ DNP3 support to be released at the event and do a few pre-recorded demonstrations of fuzzing some systems from our research that now have patches available.

Finally, we will compare the tool we are releasing to existing commercial offerings using quantitative metrics like code coverage analysis. We will make a strong case why the industry needs to take responsibility for its own testing practices and adopt a white-box approach to security testing.

Speakers: ***Adam Crain**, Security Researcher, Automatak*
***Chris Sistrunk**, Senior Consultant, Mandiant*

9:30-9:50 am

Vendor Expo & Networking Break

Location: Ballroom of the Americas A

9:50-10:45 am

ICS Analyst Panel

As awareness of the specialized security needs of industrial control systems grows, the security product and services markets have grown as well. Specialized security devices and service offerings are emerging, while every incumbent security vendor also has market material highlighting how their product can secure critical infrastructure systems. How these market forces play out and what products and vendors thrive (and which fail) are key factors for security managers to understand when selecting security technology and service providers for ICS environments. This panel of industry analysts will provide insight into their ongoing research and projections and answer questions from the Summit audience.

Moderator: ***John Pescatore**, Director of Emerging Technologies, SANS Institute*

Panelists: ***Andy Bochman**, Founder & Principal, Bochman Advisors LLC*
***Bob Lockhart**, Research Director, Navigant Research*
***Sid Snitkin**, Vice-President & GM Enterprise Services, ARC Advisory Group*

10:45-11:45 am

Survival Solutions for the ICS Vulnerability Avalanche

It is no secret there is an avalanche of new vulnerabilities waiting to be found in ICS equipment, thanks in part to new fuzzing tools like Robus and Codenomicon. It is also well known that the ICS vendors are not able to keep up with these disclosures – according to one analyst, less than half of the of vulnerabilities listed by ICS-CERT have patches. Even patched, most control protocols are completely unauthenticated, so in the words of Dale Peterson, "controllers are insecure by design."

While replacing all the PLCs, RTUs and DCS in the world with new products might be the answer for some, most utility and manufacturing engineers will have to make do with the equipment they already have, regardless of the flaws. For these unfortunate but real-world professionals, the only answer is some sort of compensating security control while they wait for the day of the perfectly secure ICS equipment to arrive.

One security control used similar high vulnerability, no-solution situations in the IT world are firewalls with Deep Packet Inspection (DPI) capabilities. This is mainstream technology for IT protocols like HTTP and SMTP, but until recently has been unavailable for industrial control protocols. This talk looks at the lessons learned in creating and deploying a DPI firewall for complex ICS protocol, namely EtherNet/IP. We discuss why DPI is needed for ICS and SCADA security, how DPI technology has evolved in the past decade, what is available today and the challenges going forward. We look at the technical issues in creating a SCADA DPI firewall that is useable and the solutions we see emerging. We will also talk about the synergy between application layer fuzzing technology and DPI technology. The talk closes with a case history of the use of an EtherNet/IP firewall to ensure the safety of turbine systems in the oil and gas industry.

Speaker: ***Eric Byres****, CTO, Belden*

11:45 am-1:00 pm

Lunch & Learn

Location: Grand Republic Ballroom B

Presented by

WATERFALL® Stronger Than Firewalls

Stronger Than Firewalls: A Spectrum of Solutions

Unidirectional Security Gateways have been securely integrating control system applications with corporate networks for nearly a decade now, without incurring the safety and reliability risks which always accompany firewall deployments. Waterfall's stronger-than-firewalls solution suite now includes a spectrum of technologies both based on and complementing Unidirectional Gateways. Waterfall's mission is to replace all uses of firewalls in industrial control system networks with safer and more secure alternatives. Join us to explore the spectrum of solutions and the connectivity needs each element of the spectrum addresses.

Speaker: ***Andrew Ginter****, VP Industrial Security, Waterfall*

Lunch & Learn

Location: Ballroom of the Americas B

Presented by

QUALYS® Continuous Security

ICS Vulnerability Management: Beyond the PLC

A lot of research has been released that includes vulnerabilities in ICS Software and PLCs, leaving many companies searching for solutions. Join Qualys for a Lunch & Learn where we will discuss successful methodologies for identifying vulnerabilities that have been found inside and outside of many ICS environments. We will discuss how these methodologies can be used to identify the threats that currently exist and to be prepare for emerging threats in the future.

Speaker: ***Terry McCorkle****, Director of Product Marketing – Vulnerability Management, Qualys*

1:00-2:00 pm

Out of Control: Demonstrating SCADA Exploitation

America's next great oil and gas boom is here: the United States is on track to become the world's top oil producer by 2020. Companies in all segments of the oil and gas industry rely heavily on technology to control and monitor their operations. But what happens when those systems go out of control? Cimation's cyber security expert, Marc Ayala, examines vulnerabilities common to Remote Terminal Units and other SCADA devices, identifies attack vectors that could be used to seize control and discusses remediation techniques to protect critical infrastructure. Using a live simulation of industrial processes found in field environments, Cimation experts mimic hacker activity to exploit protocols in a live control system. Word of warning: stay out of the splash zone!

Speakers: ***Marc Ayala****, Senior Technical Advisor; Sr. Instrumentation, Process Automation and Control Consultant, Cimation*
Eric Forner*, ICS/SCADA Security Consultant, Cimation*

2:00-2:45 pm

Information and Communication Technology (ICT) Supply Chain Security-Emerging Solutions

Software and hardware supply chain is a serious concern in the industrial control systems (ICS) space. Asset owners/operators and suppliers are in a symbiotic relationship – acquirers cannot conduct business without information and communication (ICT) products and services. Where do the subcomponents come from and what do we know about their contents? Which code libraries were used by the sub-supplier? Why do we need to know? Several solution sets have emerged over the last 6 years, developed in IT/communications, defense, and the ICS space. These include ISO and IEC standards, NIST documents, certification framework, Common Criteria extensions, and efforts by software industry consortium. The presentation will survey ICT supply chain security problem space, provide an overview of available solutions developed to date, and recommend how to use these solutions in the ICS context.

Speaker: ***Nadya Bartol****, Senior Cybersecurity Strategist, CISSP, CGEIT, Utilities Telecom Council*

2:45-3:15 pm

Vendor Expo & Networking Break

Location: Ballroom of the Americas A

3:15-4:15 pm

Solution Session

Location: Ballroom of the Americas B

Presented by

AlertEnterprise!

Defend Like a Hacker

Hackers know your people/systems/perimeter better than most security organizations. Why is that? When attacking your network, attackers don't face the cultural, organizational and political challenges in today's corporate environment. Hardened silos between IT, physical security and operations don't hamper the hacker's ability to maneuver through your systems, but enhance the ability to go silent and undetected for months.

In this presentation we will dive into each of the silos, defender challenges and how the attacker approaches your security defenses. By understanding what "Hackers Do, You Don't" we can start to formulate real-world operational security defenses, often times by converging the data from systems you already have implemented. Concepts of 'open source intelligence' and 'continuous monitoring' have a different context in real-world attacks. By understanding how attackers approach a target we realize how to better defend again new threats.

Speaker: ***Ron Fabela****, Sr. Product Manager, AlertEnterprise*

Solution Session

Location: Grand Republic Ballroom B

Presented by

DISPERSIVE TECHNOLOGIES PIKE

Virtual Dispersive Networking (VDN)

Smart Grid, Smart Meters, Smart Appliances, Smart Cars, mobile apps, disruptive generation, and an expectation of unprecedented consumer information is forcing many utilities to rethink how they provide service and interact with consumers. SCADA system designers and manufacturers have moved to standard IT based platforms to provide enhanced capability, but at the cost of introducing well known vulnerabilities to the GRID. NERC compliance rules are ever changing and becoming more restrictive as the government becomes more concerned about Cyber-Attacks. How do you secure the future network? How do you stay compliant? How do you meet consumer demand?

By disrupting computer network operations, hackers have the capability to shut down key parts of your critical infrastructure. Cyber warfare and the evolving threat landscape present significantly increased risks, both physical and economic, to electric utilities, co-operatives, and municipalities. VDN's quantum leap in network security, our patented Spread Spectrum IP® (SSP), divides and disperses individual data transmissions simultaneously across multiple, independent routes where source, destination, encryption and routing are continuously shifting to protect these assets. These features create unprecedented security and control for data where it is most vulnerable; while it is in motion. Learn how VDN can help protect your SCADA systems, communication between network zones, and allow for secure access for remote workers.

Speaker: ***Michael Seymour****, VP -IT, Pike*

4:15-5:00 pm

Going Global: Global ICS Professional Certification

Cyber security threats continue to increase in both frequency and sophistication. Industries getting more automated, integrated, and interconnected, are facing a real challenge. People are crucial. A standardized foundational set of skills, knowledge, and abilities for ICS across industries was lacking, until now. In this talk you will learn all about the new Global ICS Professional security certification.

- The GICSP is a new certification that focuses on the knowledge that professionals securing critical infrastructure assets should know.
- Holders of the GICSP will demonstrate a globally recognized level of competence that defines the architecture, design, management, risk and controls that assure the security of critical infrastructure.
- The GICSP is the "bridge" to bring together IT, engineering and cybersecurity professionals to achieve security for ICS from design through retirement.
- The GICSP is expected to be adopted on a global basis as a gateway certification for critical infrastructure-industrial control system professionals.

The approach to create this certification program was an industry driven effort, including end-users, ICS suppliers, and subject matter experts.

Moderator: ***Michael J. Assante****, Director – ICS & SCADA, SANS Institute*

Panelists: ***Marc Ayala****, Senior Technical Advisor; Sr. Instrumentation, Process Automation and Control Consultant, Cimation*
Paul W. Forney*, CSSLP, System Architect – Common Architecture & Technology, Schneider Electric/ Invensys*
Graham Speake*, Security Architect, Evangelist, Yokogawa*
Tyler Williams*, Global Oil & Gas Company*
Doug R. Wylie*, CISSP, Director, Product Security Risk Management, Rockwell Automation*

5:00-5:30 pm

New CPNI ICS Security Awareness Courses

The UK Centre for the Protection of National Infrastructure (CPNI), working with UK CPNI SCADA and Control Systems Information Exchange (SCSIE), knows that there is a need to provide security awareness communications to key personnel in a way that is understandable to a wide audience.

CPNI and its key partners have developed two ICS Security Awareness Courses for the UK CNI. One of the courses is aimed at raising security awareness of ICS to Senior Managers in the Industry and within UK Government. The second course is focussed on Engineers/Practitioners, again to raise the awareness of the security issues and offer mitigations. Both these courses are being piloted in March 2014 and will be rolled out to the UK CNI in April 2014.

Both these courses have been developed to raise awareness. They have been designed to provide the first steps of an ICS Security pathway and they are designed to point attendees to future ICS Security courses provided by other training providers, including SANS. CPNI will present key information about these courses and explain why it believes there is a need to provide less technical ICS Security awareness training.

Speakers: ***Sandra C****, Cyber Security Advisor, CPNI*
David H*, Advisor, CPNI*

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.

6:30-8:30 pm

Networking Reception

Location: Grand Republic Ballroom B

Open to All Attendees

Sponsored by

Rockwell Automation & Iguana

Please join your peers, friends and speakers from a wide cross section of industries, company sizes and experiences at the networking reception. Refreshments provided by: Iguana and Rockwell Automation.

8:00-10:00 pm

Game Night

Location: Grand Republic Ballroom A

Are you interested in testing or expanding your ICS cybersecurity skills for free? Have you spent your career defending ICS environments and always wanted to spend some time attacking an ICS environment in a safe way? This year the ICS Summit will provide a unique opportunity for you to test your abilities in a number of different live environments with a variety of skill-level options. The exercise will feature hands-on local kits from the CYBATI ICS mastery stations allowing players to interact with the devices directly and see the impacts of their actions.

The CYBATI stations will challenge attendees through a series of cyber-physical red team exercises ranging in skill set from beginner/observer, to intermediate and advanced. The objectives and exercises during this free event will allow participants to transition through the typical ethical penetration testing lifecycle of information gathering and analysis, vulnerability identification, penetration attempts and mitigating control recommendations.

All of the environments will allow for individual participation or team participation.

Please sign up to play at the registration desk prior to Game Night.

All Summit Sessions will be held in the Ballroom of the Americas B (unless noted).

Tuesday, March 18

7:00-9:00 am

Registration

Location: The Contemporary Resort Convention Center – Level 2 Registration Desk

---

8:00-8:45 am

EARLY MORNING BONUS SESSION

Location: Grand Republic A

Live Demonstration of the Aegis Fuzzing Framework

Speakers: ***Adam Crain****, Security Researcher, Automatak &* ***Chris Sistrunk****, Senior Consultant, Mandiant*

Following their presentation on day one at the ICS Security Summit, ICS control system security researchers Adam Crain, founder of Automatak and Chris Sistrunk, independent researcher, will provide a live demonstration of the Aegis Fuzzing Framework. The Aegis Console has been provided to all ICS Security Summit Attendees on the Attendee Resource DVD. The Aegis console has been pre-installed on the SamuraiSTFU Virtual Machine located on the Resource DVD.

If you want to see some of the commands and functionality of the Aegis Fuzzing Framework, please plan on attending this event prior to the start of the second day of the summit.

SUMMIT

9:00-10:00 am

Cybersecuring DoD Industrial Control Systems

DoD is planning to adopt the NIST Risk Management Framework and will sunset the DoD Information Assurance Certification and Accreditation Process (DIACAP). Recognizing that new malware like Stuxnet is targeting Operational Technologies; the new DoDI 8500 requires the same level of cybersecurity control for Industrial Control Systems (such as utility SCADA, Building Controls, etc.,) as traditional Information Technology systems.

Speaker: ***Michael Chipley****, PhD PMP LEED AP BD +C, President, The PMC Group LLC*

10:00-10:20 am

Vendor Expo & Networking Break

Location: Ballroom of the Americas A

10:20-11:20 am

Real-World NIST Cybersecurity Framework Implementation for ICS Industries in Critical Infrastructure Sectors

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity" on February 12, 2013 was issued. This Executive Order calls for the development of a voluntary Cybersecurity Framework ("Framework") that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk.

Critical infrastructure is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Due to the increasing pressures from external threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk.

This panel will discuss the goals, intent and practical implementation of the new NIST Cybersecurity Framework in relation to the Electric Sector Cybersecurity Capabilities Maturity Model, the Electric Sector Risk Management Process and other related standards and models.

Moderator: ***Ed Goff****, CISSP, Enterprise Architect – IT Security, Duke Energy*

Panelists: ***Samara Moore****, Director for Cybersecurity Critical Infrastructure Protection, White House National Security Staff*
Jason Christopher*, Technical Lead – Cyber Security Capabilities & Risk Management, US Dept. of Energy*

11:20 am-Noon

So Easy a Child Could Do It: Teaching Your Management About SCADA

When dealing with information security and technical topics it is often true that the technical means exist to achieve security. Security is usually not achieved though, due to issues of policy, bureaucracy, and a lack of user understanding that leads to poor choices. When dealing with niche technical topics such as SCADA it can seem absolutely impossible to inform people outside of the technical community on what these systems are, why they are so important, and how to defend them.

In September 2013, Robert M. Lee, authored the book *SCADA and Me: A Book for Children and Management.* The children's picture book quickly became influential due to its ability to make the often abstract topic of SCADA relatable to anyone, no matter their level of technical skill. This presentation will explore the lessons learned from SCADA and Me and how the audience members can use similar lessons to help educate those around them. Your ability to explain SCADA systems and the security challenges is key to your ability to garner support – and funding – from upper management for your initiative.

Speaker: ***Robert M. Lee****, Co-Founder, Dragos Security LLC*

Noon-1:15 pm

Lunch & Learn

Location: Grand Republic Ballroom B

Presented by

SECURICON
Information Security Solutions

Segmentation as a Means of Achieving System Reliability

System Reliability is a paramount condition for any critical infrastructure environment. From power generation to manufacturing to network systems, the mantra that is preached for these systems today is "running all the time, every time." The increased integration of ICS systems and Information Technology systems adds a layer of complexity for both ICS and IT operators.

ICS and IT operators face major challenges, not only due to their interconnected systems but, more importantly, due to the responsibility of maintaining 24-hour reliability of those systems. Operational and business requirements often dictate the actions that operators can carry out. A component to helping achieve system reliability that is often overlooked and typically out of operator hands is Segmentation – sometimes referred to as "zoning."

In this Lunch and Learn, Securicon engineers will talk through examples and explore real-world scenarios of segmentation that represent both strong approaches and those that create weaknesses to be exploited. Attendees will come away with an understanding of ICS and IT network segmentation and its role in not only protecting your systems, but also how segmentation can help with keeping your systems up and running.

Speaker: ***Daniel Chew****, Managing Consultant, Securicon*

Lunch & Learn

Location: Ballroom of the Americas B

Presented by

tenable network security

Tiptoe Through The Network: Practical Vulnerability Assessments in Control Systems Environments

I will never forget my assignment for a vulnerability assessment against a control systems network. "Hey, can you go somewhere, run "scans" against this system, and oh by the way don't crash it or a large portion of the USA could lose power". Needless to say, I turned down that assignment, as they required that a traditional network-based "scan" be run. There has to be a better way to preform assessments in such environments! Fast forward 10 years later and I've worked with much safer techniques for assessing the security of SCADA/Control systems infrastructure. Working for Tenable Network Security has also provided me great insights into several techniques, including:

- Using credentials to login to systems and audit for missing patches and configuration changes
- Tuning vulnerability scans to be less intrusive yet still accurate and providing useful information
- Implementing passive vulnerability scanning to discover hosts on the network and enumerate vulnerabilities, without sending a single packet to the end-user system.

Speaker: ***Paul Asadoorian****, Product Evangelist*

1:15-2:00 pm

The SCADA that Didn't Cry Wolf: Who is Really Attacking your ICS Devices?

These attackers had a plan, they acted upon their plan, and they were successfully targeting SCADA devices that were Internet facing. This talk will profile, provide intelligence, and list actors that attacked my ICS devices in the wild. This talk will also feature a demo of the attackers in progress, exfiltrating perceived sensitive data. In addition, I will discuss in greater detail how I geo-located these individuals, and tracked their movements, operations, and attacks. Some of the findings are truly surprising and substantial, and may not be what you think they are. This talk will release brand new statistics and attack details seen nowhere else in the ICS community.

Speakers: ***Kyle Wilhoit****, Threat Researcher, Trend Micro*

2:00-3:00 pm

Building Security Into ICS and SCADA Products

George Wrenn and Paul Forney will speak about Schneider Electric's process to secure its offerings and enable compliance to both national and internationally recognized cyber security standards. Learn their ISO/IEC-based approach to building security into ICS and SCADA products.

Speakers: ***Paul W. Forney****, CSSLP, Schneider Electric, System Architect*
George Wrenn*, CISSP, ISSEP, CEH, Schneider Electric, Cyber Security Officer (CSO)*

3:00-3:30 pm

Vendor Expo & Networking Break

Location: Ballroom of the Americas A

3:30-4:15 pm

Just Trust Me! How To Arm Internet-Enabled Devices with Integrity

By 2015, Cisco estimates there will be 50 billion "things" connected to the Internet. These range from sensors to track dairy cows to industrial control and automation systems to the wired home. All are potentially vulnerable to attacks, hacks and malware due to basic design and software issues traditionally inherent in embedded systems.

Already, the Internet of Things (IoT), including ICS and SCADA systems, has been the target of many hacks, including the student in Texas who took control of an $80 million yacht, a Polish teen who derailed a train after taking control of the network and the medical devices that have been hacked by researchers and hobbyists. Perhaps more importantly, the systems that provide power, water and other critical infrastructure remain highly vulnerable.

The good news is that OEMs CAN control security and the unique aspects of these many embedded systems offer some benefits for security. This talk will highlight key security tenets: do I know you, and can I trust you?

Speaker: ***Stacy Cannady****, Technical Marketing – Trustworthy Computing TRIAD (Threat Response, Intelligence, and Development), Cisco and Member Representative, Trusted Computing Group*

4:15-5:00 pm

Bridging the Security Governance Divide in Utilities

Andy will describe how CISOs can improve communications with senior business leadership, and how executives can create a culture that fosters better cybersecurity behaviors throughout the company.

This presentation will examine the current state and then walk attendees through the steps it takes to build organizations better equipped to support the cybersecurity challenges and opportunities of today and tomorrow.

Speakers: ***Andy Bochman****, Founder & Principal, Bochman Advisors LLC*

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.

SANS Industrial Control Systems

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

MEDIA PARTNERS

CONTROL ENGINEERING

NAVIGANT RESEARCH

EXHIBITORS

AlertEnterprise Delivers IT-OT Convergence to protect Critical Infrastructure from Cyber and Operational security threats. Correlating threats across IT systems, Physical Security and SCADA/DCS Systems enables true prevention of theft, sabotage, insider threat and acts of terrorism. AlertEnterprise solutions deliver Identity and Access Management, Situational Intelligence and Incident Management and Response.

The Anfield Group specializes in utility security and reliability services. This includes a variety of solution-based consultation programs covering the gamut of critical infrastructure security disciplines. Through decades of hands-on security and reliability experience in this field we are able to bring a unique perspective on security problem solving unlike any other consulting firm.

Codenomicon's fully automated Defensics testing solutions enable you to find zero-day vulnerabilities in over 200 protocols and file formats, including ICS, SCADA and standard Internet protocols. Codenomicon Defensics complies with the Embedded Device Security Assurance (EDSA) Communications Robustness Testing (CRT) requirements of the ISA Security Compliance Institute (ISCI).

FoxGuard Solutions develops innovative programs and services to improve the cybersecurity and compliance posture of industrial control systems in critical infrastructure markets. FoxGuard provides assistance with patch validation and distribution, software updating, and system hardening for control system devices, research and development services, engineering services, and field implementation services.

IGUANA is a range of solutions designed for the protection of critical networks and data assets, defending against modern cyber-attacks. IGUANABlue ensures the Availability of your infrastructure and assets, guarding critical data from attacks. IGUANAGreen assures the Integrity and Confidentiality of data, encrypting at the highest level, enabling secure communications.

IOActive is the leader in hardware, software and wetware security consulting. Serving as trusted advisors to the global 500, our team of internationally recognized experts partner with you to solve your toughest security challenges. Our core competencies include penetration testing, reverse engineering, code review and hardware security assessments.

NexDefense empowers industry professionals with cyber security technology products and services specifically designed for securing ICS/SCADA technology. NexDefense is the exclusive licensee of the SOPHIA Fingerprinting and Monitoring Tool, developed at Idaho National Laboratory. This easy-to-use and passive tool enables ICS users to maintain high levels of control system integrity.

OPSWAT provides solutions to secure and manage IT infrastructure for critical infrastructures, SCADA control systems and other highly secure environments. Metascan and Metadefender help organizations protect against advanced threats by using multiple antivirus engine scanning, data sanitization and file filtering. Learn more at www.opswat.com/metascan and www.opswat.com/metadefender.

For more than 30 years, Parsons has quietly worked behind the scenes delivering cyber security services that protect our nation's most sensitive information and critical infrastructure. Our commercial and federal cyber security services span specialty research and product development, consultation, cyber risk and vulnerability assessments, cyber architecture roadmaps, and technology program management. For more information, please visit www.parsons.com.

EXHIBITORS

Pike Enterprises and Dispersive Technologies have partnered to commercially deliver Virtual Dispersive Networking(tm) (VDN) to the utility community to enhance GRID security and replace traditional VPN .VDN divides and disperses data randomly across multiple, independent routes where source, destination, encryption, and routing continuously shift. VDN is the next generation network which provides substantial improvements in security, speed, and resiliency.

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 6,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The QualysGuard Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and Web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations, including Accuvant, BT, Dell SecureWorks, Fujitsu, NTT, Symantec, Verizon, and Wipro. The company is also a founding member of the CloudSecurityAlliance (CSA). For more information, please visit www.qualys.com.

Raytheon Cyber Products, a leading provider of commercial-off-the-shelf cyber security solutions for government and industry, is a wholly owned subsidiary of Raytheon Company. Founded on deep knowledge of cyber security, the company's portfolio of products address cyber challenges including insider threat, secure information sharing, data loss prevention, and data analysis.

Throughout the world, our Allen-Bradley® and Rockwell Software® product brands are recognized for innovation and excellence. Every day we help solve industrial automation challenges and help support the safe, secure and reliable operation of industrial control systems that are owned and operated by both private companies and local, state and national governments. Through innovation and investments, open collaboration and cooperation, we continually strive to help enhance and improve the physical and cybersecurity protections being applied in these systems, especially those that serve critical infrastructures and manufacturing.

Securicon, headquartered in Alexandria, VA., has been providing professional expertise in information and technology security consulting for applications, ICS, and network security, to critical infrastructure owners for over a decade. We specialize in Industrial Control System Assessments and Compliance for Utilities, Process Control and the Federal government sectors.

Tenable Network Security is relied upon by more than 17,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard for identifying vulnerabilities, preventing attacks and complying with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

Waterfall® Security Solutions Ltd. is the leading provider of Unidirectional Security Gateways™, securely integrating industrial control systems with business networks, without incurring the safety and reliability risks which accompany firewalls. Unidirectional Gateways simplify regulatory and standards compliance, and reduce security program operating costs. For true security, demand Unidirectional Security Gateways.