Industrial Control System Security (ICSS) Workshop

In conjunction with the Annual Computer Security Applications Conference

Tuesday, 8 December 2020
8:30 a.m. – 5:00 p.m. (All times in EST)

Tentative Agenda. Subject to change

8:30 *Welcome and Introduction*, Harvey Rubinovitz, Adam Hahn, The MITRE Corp; Irfan Ahmed, Virginia Commonwealth University

8:50 *Looking at security risk management from many Perspectives*, Andrew Kling, Schneider Electric

ABSTRACT: One of the hardest decisions an asset owner must make when faced with known vulnerabilities or exploits is whether to take down their plant in order to apply patches and upgrade end of life process control components. There are risks if you do (productions loss, opportunity costs, failed upgrades) and (cyber)risks if you do not. In this presentation we will discuss several options that could be considered when presented with known cyber-risks. Note: On the surface this may feel like a standard defense in depth strategy, and in some respects it is. But these strategies are meant to address specific attack techniques, known vulnerabilities and exploits, so it is better to think of these techniques as reactive rather than the defense in depth, proactive approach.

Runtime Application Self Protection (RASP) is an emerging collection of approaches to address the fundamental issue with cyber-exploits, that is the ability for malicious processes to access memory where they should not be able. If you control memory access, you control an entire class of exploits (memory-based attacks)
Patching – Our most traditional approach to defend against exploits in the wild
Signatures – Antivirus is the most common signature-based solution. YARA rules are a way of identifying malware (or other files) by creating rules that look for certain characteristics. There are several signature-based solutions that can be shared to slow or stop the exploitation of certain vulnerability types.
Mitigations – frequently OEMs advise their customers to take specific actions in order to close off known attack vectors. Closing ports on a firewall, disabling unused services, implementing access controls, network segmentation, implementing secure protocols, etc. are all common recommendations to react to specific vulnerabilities.
Security Tools – OEMS such as Schneider Electric take time to partner with security tool vendors who often bring their own unique approach to addressing active exploits
Network Anomaly detection – similar to signature checking, the ability to identify an exploit on the wire before it reaches the device. Good examples are, “magic” packets that can cause crashes, buffer overflows, RCE, etc.
AI/ML – an emerging technology, maligned somewhat today, but do not underestimate how this can and will be used in the future
Upgrades – whether this is a component by component upgrade or a rip and replace, one way to eliminate legacy cybersecurity issues is to upgrade to the current generation

Biography: Andrew Kling is an Industry Automation Product Security Officer at Schneider Electric. Andy has over three decades of software development experience, having worked in multiple industries. He has worked in the R&D organization of Schneider Electric since 2001. Currently, Andy leads the Industry Automation business unit in cybersecurity. At Schneider Electric, Andy has managed many process control engineering teams. As a result of this experience, Andy has ushered the Schneider Electric Development organization to comply with ISA 62443 standards at the process, product, and system levels, achieving several world firsts along the way.

Andy has a Master's Degree in Software Engineering – Artificial Intelligence from Northeastern University and a Bachelor's of Science in Information Sciences from the University of Massachusetts, Lowell. In addition, Andy is a participating Senior member of ISA, primarily contributing to the ISA 62443 cybersecurity standards and the ISA Global Cybersecurity Alliance.

9:15 *K7: A Protected Protocol for Industrial Control Systems that Fits Large Organizations*, Eli Biham, Sara Bitan, and Alon Dankner, Israel Technion

ABSTRACT: One of the main obstacles of securing industrial control systems is the lack of an appropriate security model that is both implementable by vendors and addresses the inherent security and usability issues needed by organizations. Current solutions such as device passwords and IPSec lack scalable key management infrastructure and [inc granularity access control mechanisms. In this paper we propose a novel security model for industrial control systems that supports organizational level authorizations and authentication requirements, while hiding the low—level details (e.g., keys and pass- words) from the users. It also allows to easily add and remove l'I.Cs, engineering stations,
HMI devices and users, and assign permissions to them. A major advantage is its support for hybrid ICS systems, and the simple ability to upgrade the security of legacy devices to functionality of new secure protocol. Without loss of generality, we base our protocol, K7, on the Siemens S7 protocol, and enhance it with new cryptographic features to support the extra functionality. We use a ticket-based system (e.g., Kerberos with LDAP server) to support the exchange of permissions and keys, and incorporate it into our protocol. To prove our solution, we implemented K7 as a protocol converter add-on to standard Siemens clients and PLCs that transform them into augmented devices that use K7. We hope that Siemens and other vendors will add direct support for K7 on their ICS systems.

9:40 *What and Where to Monitor for Intrusion Detection in Industrial Control Networks*, Alvaro Cardenas, University California Santa Cruz

ABSTRACT: In this presentation we will look at two related problems for intrusion detection in control systems: where to monitor the system to detect anomalies, and what to monitor, in order to obtain an accurate picture of the real world. We first discuss what we can and cannot detect depending on the location of our network monitor, and identify locations that maximize our visibility to attacks. We also propose the addition of hidden sensor measurements to a system to improve its security. Hidden sensor measurements are by our definition measurements that were not considered in the original design of the system, and are not used for any operational reason. We only add them to improve the security of the system and using them in anomaly detection and mitigation.

Biography: Alvaro A. Cardenas is an Associate Professor of Computer Science and Engineering at the University of California, Santa Cruz. Before joining UCSC, he was the Eugene McDermott Associate Professor of Computer Science at the University of Texas at Dallas. Earlier in his career, he was a postdoctoral scholar at the University of California, Berkeley, and a research staff member at Fujitsu Laboratories. He holds M.S. and Ph.D. degrees from the University of Maryland, College Park, and a B.S. from Universidad de Los Andes in Colombia. His research interests focus on cyber-physical systems and IoT security and privacy. He is the recipient of the NSF CAREER award, the 2018 faculty excellence in research award from the Erik Johnson School of Engineering and Computer Science, and the Eugene McDermott Fellow Endowed Chair at the University of Texas at Dallas. He has also received best paper awards from the IEEE Smart Grid Communications Conference and the U.S. Army Research Conference. One of his papers was also a finalist to the CSAW competition in Israel.

10:05 **Break (30 minutes)**

10:35 *Securing Critical Infrastructure: Challenges and Opportunities*, Jianying Zhou, Singapore University of Technology and Design

ABSTRACT: Critical infrastructure becomes a strategic target in the midst of a cyber-war. Governments are investing significantly in response to the risks and challenges while researchers and vendors are aggressively developing and marketing new technologies aimed at protecting critical infrastructure. In this talk, I will briefly describe the framework and features of a cyber-physical system (CPS) which serves as the core to provide critical services in different industrial domains. Then I will discuss the challenges we face and the approaches we can take to defend against cyber attacks. After that I will present a few novel technologies developed in iTrust for preventing and detecting attacks to CPS. I will further introduce the fully operational CPS testbeds in iTrust, and show how the testbeds are used to validate the security technologies so that the owners and operators of critical infrastructure can be confident that the technologies to be deployed will actually protect their systems in the event of a cyber-war.

Biography: Jianying Zhou is a professor and co-center director for iTrust at Singapore University of Technology and Design (SUTD). He received PhD in Information Security from Royal Holloway, University of London. His research interests are in applied cryptography and network security, cyber-physical system security, mobile and wireless security. He has published 200+ referred papers at international conferences and journals with 10,000+ citations, and received ESORICS'15 best paper award. He is a co-founder & steering committee co-chair of ACNS. He is also steering committee chair of ACM AsiaCCS and ACM CPSS. He received the ESORICS Outstanding Contribution Award in 2020, in recognition of contributions to the community.

11:00 *Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments*, Andres Murillo Singapore Univ of Technology and Design, Riccardo Taormina Netherlands Delft University of Technology; Nils Tippenhauer Saarland, Germany CISPA Helmholtz Center for Information Security; Stefano Galelli Singapore University of Technology and Design

ABSTRACT: Recently, Digital Twin—based solutions have been proposed as experimentation platforms to study the behaviour of Cyber~Physical Systems (CPS) under attack, and design appropriate detection and mitigation measures. Existing solutions focus on physical process, control logic, or network communication simulation. Unfortunately, none of the Digital Twin solutions currently available provide a realistic and holistic solution to represent all three aspects. In this work, we propose the Digital HydrAuLic SIMulator (DHAL SIM), a Digital Twin for water distribution systems that simulates physical, control, and network processes. DHALSIM builds on the integration of the WNTR hydraulic simulator and MiniCPS—an industrial network emulator—which are run in a co-simulation environment. Thanks to this integration, DHALSIM is able to simulate the hydraulic processes characterizing a water distribution system as well as full stack emulation of we]l—known industrial control protocols. The Digital Twin is demonstrated on the standard benchmark case study of C-Town, where we carry out a number of cyber-attack experiments. To our knowledge, DHALSIM is the first Digital Twin that implements a well known physics simulator with a virtual industrial logic and network emulation environment. DHALSIM is open source and available to the research community.

11:25 *Scalable VPN-forwarded Honeypots: Dataset and Threat Intelligence Insights*, Yan Lin Aung, Hui Hui Tiang, Herman Wijaya, Martín Ochoa, and Jianying Zhou, Singapore University of Technology and Design

ABSTRACT: Since the Mirai malware performing distributed denial—of—service at- tacks in 2016, subsequent large-scale attacks exploiting IoT devices raise significant security concerns for the stakeholders involved. The efficacy of setting up honeypots to survey the threat landscape and for early detection of threats to IoT devices is evident. However, the availability of dataset collected by these IoT honeypots to advance research on IoT security has been scarce and limited. With this paper, we contribute network traffic dataset collected by a high-interaction IoT honeypots deployed in the wild for 1.5 years during 201'?-2018. The honeypots are manifested on 40 public [P addresses in the Wild while forwarding

the traffic to 11 real IoT devices. Using Zeek tool, the dataset is generated in JSON format from 258,871 PCAP files resulting more than 81.5 million logs. To foster further research, the attacks, exploitation and intrusion attempts present in the dataset as well as threat intelligence insights are provided with an aid of an open-source threat-hunting and security monitoring platform.

12:00 **Lunch (One hour 30 minutes)**

1:30 *Presidential Executive Order 13920 and the OT Maginot Line*, Joe Weiss, Applied Control Solutions, LLC\

ABSTRACT: Cyber security was initially an IT function. To IT, the only thing to protect was the Internet Protocol (IP) network. Consequently, all monitoring and protection occurred at the IP networks which inherently contain cyber security and cyber logging. Control systems also use IP networks, but additionally use control system hardware devices such as process sensors, actuators, drives, etc. Unlike IT devices such as firewalls, routers, and switches, control system devices have no cyber security, authentication, or cyber logging capabilities. Additionally, control system devices utilize lower level, non-IP networks that have no cyber security or cyber logging. For control system applications, the OT approach has been to emulate what has been done for IT. That is, provide all monitoring and protection around the OT network excluding protecting the actual equipment. Effectively, IT/OT has set up a Maginot Line similar to what was done during World War II. However, just like the Germans in World War II, the Chinese evaded the "OT Maginot Line" by installing hardware backdoors in this case in large electric transformers that would allow the attackers backdoor access to the transformer equipment behind all OT monitoring and protection. The Chinese also provided counterfeit pressure and differential transmitters which operate behind all firewalls and are 100% trusted. This is a major safety concern. These attack vectors which would allow the Chinese to damage critical equipment at a time of their choosing resulted in Presidential Executive Order (EO) 13920. The EO included all hardware and control systems yet excluded all network equipment. There are millions of pressure and differential pressure transmitters and more than 200 large electric transformers in the US bulk electric grid without a capability to detect if backdoors are present. Process sensor monitoring to detect potential counterfeit devices and hardware backdoor communications is needed to meet the intent of the EO.

Biography: Joe Weiss is an expert on instrumentation, controls, and control system cyber security. He has published over 80 papers, chapters on cyber security for Electric Power Substations Engineering and Securing Water and Wastewater Systems, coauthored Cyber Security Policy Guidebook and authored Protecting Industrial Control Systems from Electronic Threats. He has amassed a database of more than 1,250 actual control system cyber incidents. He is an ISA Fellow, Managing Director of ISA99, a Ponemon Institute Fellow, and an IEEE Senior Member. He was featured in Richard Clarke and RP Eddy's book-Warning – Finding Cassandras to Stop Catastrophes. He has patents on instrumentation, control systems, and OT networks. He is a registered professional engineer in the State of California, and has CISM and CRISC certifications. In 2006, Marshall Abrams and Joe gave the first control system cyber security talk at ACSAC.

1:55 *Automated Detection of Configured SDN Security Policies for ICS Networks*, Sandeep Gogineni Ravindrababu, and Jim Alves-Foss. University of Idaho

ABSTRACT: There is a. distinction between security policies and technologies that implement those policies. There is also a distinction between intended policy and deployed or configured policy. Therefore there is a need to confirm compliance between policy and reality. This work discusses the first steps of a project to a.uto1na.tica.lly detect the security policy implemented in the control rules of an SDN switch, deployed in an industrial control system network.

2:20 *Leveraging Digital Twins of SCADA Automation Controllers for Resiliency, Incident Response, and Deception,* Jared Smith, and Jordan Johnson, Oak Ridge National Laboratory

ABSTRACT: US critical infrastructure consists of a complex array of cyber-physical and digital systems. When we think of power grid devices, we most often think of devices that physically open and close breakers, measure sensor outputs, or manipulate physical processes. However, with the rise of "smart" grids and an Internet-connected US power system, the devices that automate the actions of physical devices and utilities are now widely deployed. These devices, known as automation controllers, have unparalleled access to controlling the systems that keep our lights on and factories running, yet they are in a precarious position that can be leveraged by adversaries to wreak havoc. These devices are deployed as physical units with little flexibility for hot-swapping when faults occur or performing forensics on compromised controllers. To that end, at Oak Ridge National Lab, we have developed the first digital twin of a SCADA automation controller, completely configurable, IEC 61131-3/Modbus/DNP3 compatible, Vendor-agnostic, and seamlessly deployable as containers on any host operating system. Our platform, called DEFCON-SCADA, has led us to explore their deployment into utilities, factories, solar deployments and more. We have also explored additional uses, including for deceiving adversaries using built-in SDN compatibility as well as enabling cyber first responders to train on SCADA networks provisioned and interconnected entirely with a combination of these digital twins and an SDN layer enabled by OpenFlow-compatible SDN infrastructure. In this talk, we lay out what these kinds of systems can do, and what the future of "smart" grids may look like when large parts of a utility's infrastructure is made up of virtual SCADA devices, able to replace failed, misconfigured, or compromised physical devices in seconds without operator input.

Biography:
Jared Smith is a Principal Cyber Threat Researcher at SecurityScorecard (SSC) and formerly the Lead Scientist for AI in Cybersecurity at Oak Ridge National Laboratory (ORNL). At SSC, Jared helps drive the R&D team responsible for collecting disparate signals on the security posture of over 1.5 million companies, governments, and critical infrastructure facilities. At ORNL, he led an array of DHS, DOE, and IC-funded projects covering digital forensics, malware analysis, critical infrastructure security, and security analytics. Jared received his PhD in Computer Science from the University of Tennessee in summer 2020, where he leveraged the de facto Internet Routing protocol, BGP, along with the complex dynamics of the Internet to build, measure, and evaluate a novel DDoS defense system that can defeat DDoS no matter the bandwidth and raw size of the attack(s). Jared has 4 pending patents, multiple commercial licenses of his technologies, 10+ peer-reviewed publications at venues including NDSS, USENIX, and IEEE S&P, and nearly 30 invited conference talks.

Jordan Johnson is an NSF CyberCorps® scholar who received his M.S. in Computer Science from Tennessee Tech University in 2019. Since then, he has been working at Oak Ridge National Laboratory (ORNL) to research and develop new cyber security solutions for cyber-physical systems with a particular focus on energy management systems. Jordan's work has led to several pending patents and peer-reviewed academic papers. Jordan is currently the Principal Investigator of an ORNL program focused on building digital twins for SCADA automation controllers.

.

2:45 **Break (30 minutes)**

3:15 *Trustworthy Critical Infrastructures via Physics-Aware and AI-Powered Software Security,* Saman Zonouz, Rutgers University

ABSTRACT: Critical cyber-physical infrastructures, such as the power grid, integrate networks of computational and physical processes to provide the people across the globe with essential functionalities and services. Protecting these critical infrastructures' security against adversarial parties is a vital necessity because the failure of these systems would have a debilitating impact on economic security and public health and safety. Our research and development projects aim at provision of real-world solutions to

facilitate the secure and reliable operation of next-generation critical infrastructures and require interdisciplinary research efforts across adaptive systems and network security, cyber-physical systems, and trustworthy real-time detection and response mechanisms. In this talk, I will focus on real past and potential future threats against critical infrastructures and embedded devices, and discuss the challenges in design, implementation, and analysis of security solutions to protect cyber-physical platforms. I will introduce novel classes of working systems that we have developed to overcome these challenges in practice, and finally conclude with several concrete directions for future research. Additionally, I will briefly go over our other projects on x86 malware/memory analysis and embedded systems security solutions to support access control applications in cyber-physical settings.

Biography: Saman Zonouz is an Associate Professor in the Electrical and Computer Engineering Department at Rutgers University. His research has been awarded by Presidential Early Career Awards for Scientists and Engineers (PECASE) by the United States President in 2019, NSF CAREER Award in 2015, National Security Agency (NSA) Significant Research in Cyber Security in 2015, Google Security Award and Hall of Fame Recognition in 2015, Top-3 Demo at IEEE SmartGridComm 2015, the Faculty Fellowship Award by AFOSR in 2013, the Best Student Paper Award at IEEE SmartGridComm 2013, the University EARLY CAREER Research award in 2012 as well as the Provost Research Award in 2011. The 4N6 research supporters include National Science Foundation (NSF), Department of Homeland Security (DHS), Office of Naval Research (ONR), Department of Energy (DOE), Advanced Research Projects Agency Energy (ARPA-E), Department of Education (DOE), Siemens Research Labs, WinRiver, GrammaTech, Google, ETAP, and Fortinet. Saman has served as the chair, program committee member, guest editor and a reviewer for top international journals and conferences (e.g., IEEE Security and Privacy – Oakland, CCS, NDSS and DSN). Saman served on Editorial Board for IEEE Transactions on Smart Grid, and was invited to Co-Chair the organization of the National Science Foundation's CPS PI Meeting in 2017. He obtained his Ph.D. in Computer Science, specifically, intrusion resilience architectures for the cyber-physical infrastructures, from the University of Illinois at Urbana-Champaign in 2011.

3:40 *Physics-driven, Artificially Intelligent Virtualization and Camouflage for Survivable Cyber-Physical Systems*, Julian Rrushi, Oakland University

ABSTRACT: We present research on physics-driven operating system and algorithmic mechanisms capable of (i) virtualizing the operating system of industrial control systems with an artificially intelligent hypervisor, which restructures and adapts its own inner workings to match the physics of physical equipment and their physical processes, with the objective of safely collecting high-accuracy security monitoring data at high speed, as well as executing fast agile responses against malware with surgical accuracy; (ii) leveraging the physics-driven architecture of the hypervisor to create physics-compliant cyber decoys along with decoy physical equipment; and (iii) a nonlinear dynamics formalism, rooted in cyber-physical (CPS) decoys and the hypervisor's awareness of physics, which strengthens computational game theory with the objective of modeling and controlling adversarial cyber interactions on CPS environments.

Biography: Dr. Julian Rrushi is an assistant professor of engineering at Oakland University, Michigan. Julian completed a B.S. in Computer Science, an M.S. in Information Technology, and a Ph.D. in Computer Science at the University of Milan. He researches operating systems, hardware architectures, and artificial intelligence to break new ground in computer security. Julian is a recipient of a Young Faculty Award from DARPA, class of 2020.

4:05 *Open Source Models for Simulating Industrial Control Systems for Cybersecurity Research*, Tommy Morris, University of Alabama

Abstract: Researchers need access to data from industrial control systems during normal operation and periods of cyber-attack. This talk will introduce a set of high fidelity models available for researchers to simulate the behavior of a storage tank, gas pipeline, heat exchanger, 2D robotic manipulator, and Heating

Ventilation and Air Conditioning (HVAC). Each system was designed with physical processes, sensors, and actuators implemented in Matlab Simulink, with OpenPLC Programmable Logic Controller with custom ladder logic, SCADABR custom Human Machine Interfaces, and VirtualBox virtual machines to encapsulate individual computing components and provide a Ethernet TCP/IP network layers. The systems are available for download on Github and include scripts to stimulate the systems with normal and cyber-attack scenarios as well as data logs captured from the systems.

Biography: Dr. Tommy Morris currently serves as the founding Director the Center for Cybersecurity Research and Education (CCRE), the Eminent Scholar of Computer Engineering, and Professor of Electrical and Computer Engineering at the University of Alabama in Huntsville. His primary research interests include cyber security for industrial control systems and cyber physical systems. Dr. Morris is also a leader in the field of cybersecurity education. He has served as PI of multiple Gencyber camps, national high school curriculum design projects for the U.S. Army jROTC, the National Security Agency, for deaf and hard of hearing students, and serves as PI of UAH Scholarship for Service and DoD Cybersecurity Scholarship programs. Prior to joining UAH, Dr. Morris was an Associate Professor at Mississippi State University from 2008-2015 and a circuit design and verification engineer at Texas Instruments from 1991-2008.

4:30 *Discussion Period and Wrap-up, Summary and Topics for Next Year*, Harvey Rubinovitz, The MITRE Corporation; Adam Hahn, The MITRE Corp; and Irfan Ahmed, Virginia Commonwealth University