9th Annual Industrial Control System Security (ICSS) Workshop

In conjunction with the Annual Computer Security Applications Conference
AT&T Conference Center in Austin, Texas
Tuesday, 5 December 2023
8:30 a.m. – 5:00 p.m.

Agenda

Time Slots		**Workshop Program**
Start	**End**	
8:30	8:45	**Welcome Slides (15 mins):** **General Co-chairs:** Harvey Rubinovitz, The MITRE Corporation, and Greg Shannon, Idaho National Laboratory **PC Co-Chairs:** Irfan Ahmed, Virginia Commonwealth University, and Mina Guirguis, Texas State University **Panel Chair:** Gabriela Ciocarlie, The Cybersecurity Manufacturing Innovation Institute (CyManII)
8:45	10:00	**Keynote (1 hour and 15 mins):** *OT on the Edge*, Jonathan Homer, Chief Security Officer at CPS Energy **Abstract.** Today's industrial networks are no longer isolated data shares, with highly structured designs and defined processes for performance and security. As companies move their internal controls to external networks to embrace the technological advantages of cloud computing, artificial intelligence, and customer premise operations, the legacy designs and security of Industrial Control Systems is no longer sufficient. Faced with the realities of commoditization of components, extensive data integration with third parties, and other business driven decisions, ICS cybersecurity can no longer live in the shadows. **Bio.** Jonathan Homer is the Chief Security Officer at CPS Energy. He oversees cyber and physical security as well as business continuity. Prior to joining CPS Energy, his experience specialized in industrial control systems, incident response, digital telecommunications, and critical infrastructure. Jonathan owned an IT startup as well as providing consulting and management services for government laboratories and managed the cyber incident response teams within the federal government's Cybersecurity and Infrastructure Security Agency (CISA). He was named CISA's first 'Cyber Ninja' and was one of the primary architects of the Federal Government's Control Systems Interagency Working Group. Jonathan earned a Bachelor of Science in Industrial Technology from the University of Idaho and Master of Science in Technology Management from George Mason University.
10:00	**10:25**	**Break (25 minutes)**

10:25	11:15	**Invited Talk (50 mins):** *Measuring Defense: Prioritizing Security Solutions by Efficacy and Adversary Growth* Sarah Freeman, Chief Engineer at The MITRE Corporation **Abstract.** The year 2022 saw a record number of reported vulnerabilities, 26,448, emphasizing the need for updated approaches for addressing system and network weaknesses. This is even more true for cyber-physical systems (CPS) within critical infrastructure applications, as the hardware and software that comprise CPS are typically in service much longer than their IT-focused counterparts. Infrastructure Susceptibility Analysis (ISA) is a MITRE-developed methodology designed to improve the ability to predict future adversary capabilities and prioritize security modifications and enhancements by their ability to deter adversary success. This enables organizations to track their relative risk over time, including the potential benefits of various security solutions. This presentation will introduce the audience to MITRE's ISA and other MITRE research focused on improved security metrics. **Bio.** Sarah Freeman is Chief Engineer for Intelligence, Modeling and Simulation for MITRE's Cyber Infrastructure Protection Innovation Center (CIPIC), where she provides U.S. government partners and private sector entities with actionable cyber threat intelligence, developing innovative security solutions for the critical infrastructure within the U.S. Her current research focus includes predictive adversary analysis and evaluating the effectiveness of security solutions to deter adversaries.

11:15	12:05	**Invited Talk (50 mins):** *Security, Resilience and Artificial Intelligence in Cyber Physical Systems* Sukarno Mertoguno, Georgia Institute of Technology **Abstract.** Cyber physical systems (CPS) underlie many critical infrastructures and are prevalent across a wide range of areas including the electrical grid, factory production pipeline, machinery control, vehicular control, internet-of-things (IOT) devices, and commodity toy drones, just to name a few. By its nature, a CPS straddles the continuous-time physical domain and the discrete-time digital or cyber domain. Cyber components (e.g., communication and computing) couple with physical components (e.g., sensors and actuators) to carry out the intended functions of the CPS. Cyber physical systems are required to satisfy safety constraints in various application domains such as robotics, unmanned vehicles (e.g., aerial or ground), industrial manufacturing systems, and power systems. However, the once isolated system of computer-controlled machinery is now more exposed to the external world than ever, which renders ample opportunities of remote system disruption via cyber threats, in addition to the tradition threat of a physical component failing. Both may result in safety violations. Current emphasis on cyber security of CPS is on securing the operational technology (OT) network. For example, National Institute of Standards and Technology (NIST) devoted its guidance for securing CPS, SP 800-82 Rev.3, solely to network security with network segmentation as the primary recommended solution. However, network or communication is only one facet of CPS. While network is an important CPS and critical infrastructure component, sole emphasis on networking security will not be sufficient for defending the underlying CPS and its infrastructure against motivated and well-resourced adversaries. A recent article (Higgins KJ (2023) OT Network Security Myths Busted in a Pair of Hacks) indicates that the assumption of malicious events entering the system solely via the external network has been invalidated. The exploits discussed in the article did enter the system through the local (internal) network and propagated within the internal bus, avoiding the security protection provided by network segmentation. A holistic view and approach for defending CPS is needed. Machine learning (ML) plays many roles in defending CPS and critical infrastructure, from correlating cyber and physical events, to detecting anomaly, to automated fault recovery, etc. As with any other technologies, good understanding of the systems and problem space is prerequisite for effective application of ML. **Bio.** Dr. J. Sukarno Mertoguno is a faculty of the School of Cybersecurity and Privacy, Georgia Institute of Technology. His research covers broad area of computing systems and cybersecurity. He previously served as Chief Innovation Officer for the Information and Cyber Science Directorate (ICSD) of Georgia Tech Research Institute (GTRI) and as Deputy Director for Institute for Information Security & Privacy (IISP), Georgia Institute of Technology (GIT). He brought in innovative concepts and practical solutions. Before joining GTRI, he managed basic and applied science research in cyber security and complex software for The Office of Naval Research (ONR) where he developed several novel concepts, such as BFT++, Learn2Reason, CryptoFactory, NoiseFactory, and bottom-up formal methods, etc and initiated many innovative programs such as RHIMES and TPCP. Prior to ONR, he was a system & chip architect and an entrepreneur in San Francisco Bay Area, where he worked on various chips and systems, such as embedded processors, switching fabric, network processors, and various other hardware accelerators, including TCP/IP, NFS, mobile anti-malware, etc. He received his Ph.D. in electrical engineering from SUNY-Binghamton. He attended two different universities for two different degrees simultaneously, and graduated with a degree in electrical engineering from Trisakti University and a degree in theoretical physics from The University of Indonesia.
12:05	**13:30**	**Lunch**

13:30	14:20	**Invited Talk (50 mins):** *A Tale of Two Industroyers - An Analysis of the Russian Malware Used to Attack Ukraine's Power Grid* Alvaro Cardenas, UC Santa Cruz **Abstract.** In less than a decade, Ukraine has suffered from three cyber attacks attempting to cause electrical outages. On December 23, 2015, in the middle of freezing weather, Ukraine suffered the first blackout caused by cyber attacks. In this first incident, attackers gained remote access to the industrial networks of power companies, and a remote adversary operated the human-machine interface of operators, opening circuit breakers manually. A year later, on December 17, 2016, a fifth of Ukraine's capital Kyiv experienced another blackout. This time, the target was a transmission utility, and unlike the previous year when remote human attackers opened the circuit breakers, the attack in 2016 was launched automatically by the first known example of industrial malware targeting the power grid: Industroyer. Finally, on April 8, 2022, in the first months of the Russian invasion of Ukraine, operators discovered another malware tailored to attack circuit breakers automatically. This new piece of malware was called Industroyer 2, and it represented yet another attempt to target Ukraine's power grid. In this talk we will summarize our work in analyzing the malware to understand how it targeted industrial networks, as well as consider what future potential damages this type of malware may create in the future. **Bio.** 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, 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, including autonomous vehicles, drones, smart home devices, and SCADA systems controlling the power grid and other critical infrastructures. 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, the Eugene McDermott Fellow Endowed Chair at UTD, and the Distinguished Service Award from the IEEE Computer Society Technical Committee on Security and Privacy. He has also received best paper awards from various venues, including the ACM CPS & IoT Security Workshop, IEEE Smart Grid Communications Conference, and the U.S. Army Research Conference. One of his papers was also a finalist in the CSAW competition in Israel. Cardenas' research has been funded by NSF, ARO, AFOSR, NSA, NIST, MITRE, DHS, DoT, Phoenix Technologies, and Intel.
14:20	14:40	**Research Paper (20 mins):** *Security Hardening of Industrial Control Systems through Attribute Based Access Control*, Shwetha Gowdanakatte, Mahmoud Abdelgawad, and Indrakshi Ray, Colorado State University **Abstract.** Industrial Control Systems (ICS) form a part of nations' critical infrastructure. ICS comprises Programmable Logic Controllers (PLC) and other components. In an innovative and connected world, the vulnerabilities in ICS components can be exploited. Authentication and access control stand as the first level of defense for protecting ICS from cyberattacks. We demonstrate in our lab that PLC is prone to Denial of Service (DoS) attacks. Subsequently, an attribute-based access control mechanism is implemented to harden the security of PLC. The demonstration of the security hardened system showcases that PLC is no longer susceptible. Furthermore, the Coloured Petri Nets (CPN) is used to analyze the behavior of security hardened systems and provide formal assurance.

14:40	15:00	**Research Paper (20 mins):** *vPLC: A scalable PLC testbed for IIoT Security Research*, Syed Ali Qasim, Grand Valley State University; Muhammad Taqi Raza, University of Massachusetts Amherst; Irfan Ahmed, Virginia Commonwealth University **Abstract.** The rapid expansion of the Industrial Internet of Things (IIoT) has brought forward critical research challenges concerning scalability, robustness, and security. Traditional IIoT infrastructures, confined to lab environments with a limited number of Programmable Logic Controllers (PLCs), hamper large-scale research due to cost and scalability constraints. We propose a solution in the form of a highly scalable virtual PLC (vPLC) for IIoT applications. Our vPLC, as a software-as-a-service (SaaS), can generate hundreds of thousands of virtual PLC instances to simulate a large-scale IIoT network. The vPLC mimics the functionalities of an actual PLC by learning protocol semantics from network dumps of real PLCs and generating PLC templates. This ability allows users to initiate various PLC instances, thereby accurately replicating PLC functionalities like session initiation and control logic handling. In essence, our vPLC serves as an economical, scalable, and flexible research tool that enhances IIoT research and paves the way for advanced applications such as forensic analysis and threat intelligence within IIoT.
15:00	**15:30**	**Break (30 minutes)**
15:30	15:50	**Research Paper (20 mins):** *Improving the Resiliency of Embedded Networks in Heavy Vehicles - Towards Fault Tolerance*, Chandrima Ghatak, Saira Jabeen, and Indrakshi Ray, Colorado State University; Hossein Shirazi, San Diego State University **Abstract.** In both military and civilian sectors, Medium and Heavy Duty (MHD) vehicles form a critical part of infrastructure, logistics, and operations. Modern MHD vehicles are equipped with embedded computers that heavily rely on sensor data for maintaining operations. This data is often exchanged using standard protocols. The Society of Automotive Engineering's (SAE) J1939 Protocol on top of the Controller Area Network (CAN) is the common standard for data exchange in modern MHD vehicles. The resilience of this communication network is pivotal for the operational feasibility of MHD vehicles, especially in hostile environments where sensors may be compromised as a result of cyber attacks or kinetic malfunctions. This paper proposes the use of predictive machine learning algorithms to forecast accurate sensor readings when a sensor system becomes unavailable, whether due to physical or cyber-attacks. Utilizing real-world data from a Class 6 Kenworth T270 truck as a case study, we explore and evaluate the effectiveness of three different machine-learning methods in predicting missing sensor data. Our findings indicate that the machine learning models are capable of nearly accurate predictions, which can prevent the vehicle from entering into engine protection or limp mode. This not only maintains the vehicle's operational status for extended periods but also contributes to enhancing the resilience of networked cyber-physical systems.
15:50	17:00	**Panel (1 hour and 10 mins):** *Secure Manufacturing* **Moderator:** Gabriela Ciocarlie, The Cybersecurity Manufacturing Innovation Institute (CyManII) **Panelists:** Curtis Taylor, Oak Ridge National Laboratory Kyle Saleeby, Georgia Tech Dongyan Xu, Purdue University Wayne Austad, Idaho National Laboratory
17:00		Wrap-up