10th Annual Industrial Control System Security (ICSS) Workshop

In conjunction with the Annual Computer Security Applications Conference
Alohilani Resort in Waikiki, Honolulu, Hawaii
Tuesday, 10 December 2024
8:30 a.m. – 5:00 p.m.

Agenda

Time Slots		Workshop Program
Start	**End**	
8:30	8:40	**Welcome Slides (10 mins):** **General Co-chairs:** Harvey Rubinovitz, The MITRE Corporation, and Greg Shannon, Idaho National Laboratory **PC Co-Chairs:** Gabriela Ciocarlie, The Cybersecurity Manufacturing Innovation Institute (CyManII) Irfan Ahmed, Virginia Commonwealth University **Panel Chair:** Tomomi Aoyama, Nagoya Institute of Technology, Japan
8:40	9:40	**Keynote (1 hour):** *How to Attack and Defend Wind Farms* Sujeet Shenoi, F.P. Walter Professor of Computer Science and Professor of Chemical Engineering University of Tulsa, Oklahoma **Abstract.** As modern society grows more reliant on wind energy, wind farm deployments will become increasingly attractive targets for malicious entities. The geographic scale of wind farms, remoteness of assets, flat logical control networks and insecure control protocols expose wind farms to myriad threats. This presentation describes the anatomy of a generic wind farm and the attack vectors that can be leveraged to target its information technology, industrial control system and physical assets. It discusses attack scenarios involving unauthorized wind turbine control, wind turbine damage, wind farm disruption and damage, and substation disruption and damage. Additionally, it highlights mitigation techniques that provide robust security coverage and reduce negative cyber and physical impacts. The attack surface, targets, scenarios and mitigation techniques presented are common across wind farm deployments. However, it is still possible to add details about the unique aspects of wind farm assets, configurations and operations in order to develop a holistic risk management program geared for a specific wind farm deployment. **Bio.** Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma. An active researcher with specialties in cyber security, cyber operations, critical infrastructure protection and digital forensics, Dr. Shenoi works on exciting “problems” ranging from helping solve homicides to penetrating telecommunications systems, oil and gas pipelines, wind farms and voting machines. He spearheads the University of Tulsa's elite Cyber Corps Program that trains “MacGyvers” for U.S. government agencies. For his innovative strategies integrating academics, research and service, Dr. Shenoi was named the 1998-1999 U.S. Professor of the Year by the Carnegie Foundation.
9:40	10:00	**Research Paper (20 mins):** *Assurance of Application Security on IIoT Platforms with Knowledge Augmentation* Yannick Landeck and Dian Balta (fortiss GmbH) and Martin Wimmer and Christian Knierim (Siemens AG) **Abstract:** Industrial Internet of Things (IIoT) platforms are characterized by a heterogeneity of applications that increases the flexibility and efficiency of automated manufacturing. At the same time, manufacturers are concerned about whether untrusted third-party applications can be aligned with the domain’s requirements for security. Assurance activities, aiming to guarantee the secure development and operation of applications, are hampered by risk management challenges and the heterogeneity of required knowledge. Stakeholders such as Software Developers and System Integrators struggle to break down these challenges, e.g., how to mitigate threats to Industrial Control Systems (ICS) and derive actions for assurance. Additionally, they require knowledge to manage risks from heterogeneous facets such as application deployment, device configuration, or threat and risk assessment. In this paper, we propose an assurance engine that allows stakeholders to break down risk management challenges into dynamic assurance cases and to augment the latter with knowledge from corresponding facets. By leveraging knowledge representation, the assurance engine enables the comparison of risk management approaches for different stakeholders. Furthermore, we utilize formal semantics and logical deduction for reasoning to lay the grounds for the automated assessment of complex assurance cases on heterogeneous IIoT platforms.
10:00	**10:30**	**Break (25 minutes)**

10:30	11:15	**Invited Talk (45 mins):** *AI-assisted Cyber Targeting* Sarah Freeman, The MITRE Corporation
11:15	12:00	**Invited Talk (45 mins):** *Researching LLMs and Available Open-Source Tooling for Secure and Practical Use* Curtis Taylor, Monika Akbar, Gabriela Ciocarlie, Matt Luallen (CyManII) **Abstract:** Large language models (LLMs) have demonstrated significant potential in diverse domains, from natural language processing to artificial intelligence applications. As their use becomes more prevalent, addressing their secure and practical deployment is essential. This presentation explores the landscape of open-source tooling available for the development and deployment of LLMs, focusing on security, privacy, and operational efficiency and capabilities. Key tools and concepts are analyzed for their role in facilitating secure use cases, particularly within industries in support of critical manufacturing and its dependencies. The study highlights strategies to address risks associated with model biases, data leakage, and adversarial attacks, while also examining the balance between performance and safety. The insights offered in this presentation aim to guide businesses in adopting robust open-source and offline solutions for practical LLM deployment in various environments.
12:00	**13:30**	**Lunch (1 hour and 30 minutes)**
13:30	14:15	**Invited Talk (45 mins):** *Emulating Adversary Behaviors in Well-Known OT protocols: Caldera for OT* Nick Tsamis, The MITRE Corporation Abstract: MITRE's Caldera is an open-source adversary emulation platform that automates the execution of cyber threats to enhance detection and response capabilities. It leverages the MITRE ATT&CK framework to mimic real-world tactics, techniques, and procedures, offering a user-friendly platform for testing defenses, including in OT environments. Caldera for OT provides an extension to operate natively with OT system protocols, providing a unified and comprehensive approach to cybersecurity testing for combined IT and OT environments. The unified application enables cyber stakeholders to conduct realistic testing and inform network and endpoint cybersecurity detection coverage analysis. This talk will focus on how OT stakeholders can apply this open source capability to ensure cybersecurity detection and protection strategies are well-informed and relevant to threats of concern.
14:15	14:35	**Research Paper (20 mins):** *Towards Provable Security in Industrial Control Systems Via Dynamic Protocol Attestation* Arthur Amorim (University of Central Florida), Trevor Kann (Carnegie Mellon University), Max Taylor and Lance Joneckis (Idaho National Laboratory) **Abstract:** Industrial control systems (ICSs) increasingly rely on digital technologies vulnerable to cyber attacks. Cyber attackers can infiltrate ICSs and execute malicious actions. Individually, each action seems innocuous. But taken together, they cause the system to enter an unsafe state. These attacks have resulted in dramatic consequences such as physical damage, economic loss, and environmental catastrophes. This paper introduces a methodology that restricts actions using formalized protocols. These protocols only allow safe actions to execute. Protocols are written in a domain specific language we have embedded in an interactive theorem prover (ITP). The ITP enables formal, machine-checked proofs to ensure protocols maintain safety properties. We use dynamic attestation to ensure ICSs conform to their protocol even if an adversary compromises a component. Since protocol conformance prevents unsafe actions, the previously mentioned cyber attacks become impossible. We demonstrate the effectiveness of our methodology using an example from the Fischertechnik Industry 4.0 platform. We measure dynamic attestation's impact on latency and throughput. Our approach is a starting point for studying how to combine formal methods and protocol design to thwart attacks intended to cripple ICSs.

14:35	14:55	**Research Paper (20 mins):** *MFAA: Historical Hash Based Multi-Factor Authentication and Authorization in IIoT* Eyasu Getahun Chekole and Jianying Zhou (Singapore University of Technology and Design) **Abstract:** Industrial Internet of Things (IIoT) has been widely adopted in various critical infrastructures. However, machine-to-machine (M2M) communication in IIoT is particularly vulnerable to a wide range of authentication and authorization attacks. Although a variety of end-to-end security protocols can be used to secure communication channels, establishing such a secure channel is still challenging due to various reasons. The single-factor based Authenticated Key Exchange (AKE) schemes are no longer sufficient to provide adequate security in IIoT. Most password, smart card and biometric-based multi-factor AKE (MAKE) schemes are not also applicable in M2M communication as they require human involvement. Recently, historical data based multi-factor AKE (HMAKE) schemes have appeared to be promising to achieve AKE in IIoT. However, the state-of-the-art HMAKE schemes do not still sufficiently address the various security and performance requirements in IIoT. Advanced session hijacking attacks (which hijack already established sessions and get unauthorized access to resources) are also critical concerns. Therefore, we propose MFAA – a lightweight HMAKE scheme that effectively addresses most of the AKE-related authentication issues and the session hijacking-based unauthorized accesses in IIoT. In MFAA, we systematically refine and intertwine historical hashes to produce a highly leakage-resilient second authentication factor for AKE and an authorization token (against session hijacking attacks) with a negligible performance overhead. In general, the proposed scheme has the following key features: 1) provides mutually authenticated two-factor security; 2) highly leakage-resistant even under the assumption of a strong adversary; 3) properly achieves perfect forward secrecy; 4) effectively defends session hijacking-based unauthorized accesses; 5) very lightweight and effectively works for resource-constrained IIoT devices. The effectiveness of the proposed scheme is formally proved using the real-or-random (ROR) model. We also experimentally evaluate the runtime performance of the scheme. Overall, the proposed scheme is highly effective both in terms of security guarantee and efficiency.
15:00	**15:30**	**Break (30 minutes)**
15:30	15:50	**Research Paper (20 mins):** *Attacks on EtherNet/IP and Migrations through CIP Security File* Alexander Gebhard and Debbie Perouli (Marquette University) **Abstract:** With the Fourth Industrial Revolution (termed "Industry 4.0"), vendors and end users have been integrating Operational Technology (OT) more closely with conventional Information Technology (IT) networks. This allows end users to make real-time decisions, enhance productivity, and leverage up-and-coming technologies such as artificial intelligence in the manufacturing process. However, this does not come without risk. Most protocols that OT devices implement were conceived decades ago, often without any consideration to security. This leaves otherwise insecure devices exposed to IT networks. This paper investigates the security of the EtherNet/IP protocol from an attacker's perspective. We develop an attack-defense tree of possible man-in-the-middle (MitM) attacks against the EtherNet/IP protocol. We highlight nuances regarding the EtherNet/IP protocol, which make some traditional MitM attacks harder for attackers to execute. Then, we then demonstrate how the semantics of the EtherNet/IP OT protocol can be abused to execute various attacks. Finally, we give an analysis of EtherNet/IP's countermeasures and a discourse on the challenges of fortifying the EtherNet/IP protocol's security.
15:50	16:10	**Research Paper (20 mins):** *Conducting Attack Scenarios and Forensic Techniques in a Virtual ICS Testbed* Chris Churilla, University of Arizona **Abstract:** The global Industrial sector has seen a sudden rise in cybercriminal activity. The objectives of these threat actors vary, but the result is unequivocally the same; the compromise of the trusted systems that humanity relies on for food, medicine, fuel, transportation, and more. These core social institutions are increasingly subjected to cyber-attacks, underscoring the critical importance of developing robust defense and incident response methodologies in the face of escalating threats. This paper presents a virtual industrial control system (ICS) testbed model designed to address this challenge by providing a platform for rigorously testing the security posture of engineering workstations (EW) and advancing digital forensics within the ICS. Through simulations of real-world attack scenarios and forensic investigations within a virtual environment, the research demonstrates the potential for disrupting physical processes and identifying network and host vulnerabilities. While the virtual testbed offers significant financial and logistical advantages over physical or hybrid testbeds, challenges remain in creating fully faithful digital twin networks. Proposed initiatives aim to address these challenges and enhance the capabilities of virtual ICS testbeds, ultimately contributing to the resilience and security of critical infrastructure systems.

16:10	17:00	**Panel (50 mins):** *Beyond Automation: Empowering ICS Operators in Cyber Defense* **Moderator:** Tomomi Aoyama, Nagoya Institute of Technology, Japan **Panelists:** Sokratis Katsikas, Norwegian University of Science and Technology Nick Tsamis, The MITRE Corporation Max Taylor, Idaho National Laboratory **Abstract:** The growing complexity of Operational Technology (OT) security demands a delicate balance between human intervention and automation. This panel will examine the evolving role of human operators in cyber incident response within critical infrastructure, focusing on strategies to harmonize human oversight with automated threat detection and mitigation. Through insights on designing targeted incident response exercises, fostering situational awareness, and implementing adversary emulation, panelists will address current challenges and best practices for integrating human expertise with automated systems.
17:00		**Wrap-up**