Introduction to the Cybersecurity and Privacy in Government Mini-track

Gregory B. White
UT - San Antonio
greg.white@utsa.edu

Wm. Arthur Conklin
College of Technology,
University of Houston
waconklin@uh.edu

Keith Harrison
UT-San Antonio
keith.harrison@utsa.edu

This mini-track explores the pressing issues surrounding the intersection of cybersecurity and government spheres of influence. Whether technical or policy, from information sharing to new analytical methods for detecting threats, this mini-track casts a wide net to cross disciplinary thinking to problems with far-reaching implications. The cybersecurity aspects of critical infrastructure systems have become a hot topic for countries across the globe. Information Technology has become pervasive in all aspects of our lives, and this includes elements referred to as the critical infrastructures.

The mini-track examines aspects associated with the security of information technology (IT) and operational technology (OT) and explores ways that IT can enhance the ability of governments to ensure the safety and security of its citizens. As governments have embraced IT to interface with citizens in a more efficient manner, security issues have risen to the forefront with the data disclosures and identity theft incidents that have occurred. Other critical issues include intellectual property theft and criminal acts involving computers. Additionally, information security is an area where policy has not kept up with technology, placing nations and their relations over this topic into uncharted territories.

This year's submissions cover a broad spectrum of security topics. Three papers were chosen this year. We express our sincere appreciation to those authors that submitted a paper for our consideration and offer our congratulations to those that were accepted.

The first paper, *"Reaching an Underserved Population in Communities: Project Xander- Cybersecurity for Non-Profits"* by Gregory White, examines a portion of every community that is increasingly becoming a target of cyberattacks. Non-profit organizations generally have little in terms of cybersecurity and limited funds to address cybersecurity, yet they are a target for cyberattacks. With limited funds to address cybersecurity, non-profits need to find innovative ways to address security. Project Xander, a program for high schools and colleges uses students to assist non-profits which provides students with real-world experience at the same time the non-profits receive valuable assistance to improve their cybersecurity posture.

The second paper "*Creating Synthetic Attacks with Evolutionary Algorithms for Proactive Defense of Industrial Control Systems Security Testing*" by Nathaniel Haynes, Thuy Nguyen, and Neil Rowe, describes research aimed at improving ICS honeypots by feeding them realistic artificially generated HTTP and IEC 60870-5-104 packets and examining their behavior to identify functional gaps in defenses. Experiments were conducted with Log4j and IEC 104 exploits against a web-based user interface to an ICS as a proof of concept. Results will be presented during the presentation.

The third paper by Natalie Sjelin, Jeremy West and Glenn Dietrich, "*High Value Assets (HVA) Lessons Learned for Small Government Agencies and Small to Mid-sized Organizations*" further describes the results of a study and assistance with evaluation of High Value Assets. This is a continuation of a study first described at HICSS-55. The paper describes the results and lessons learned utilizing the SLTT HVA process described in the previous paper with four pilot jurisdictions: a state agency, county, parish, and community. The five-phase approach developed will be discussed along with the results that were obtained in each of the pilot locations.

URI: https://hdl.handle.net/10125/102840
978-0-9981331-6-4