Introduction to the Cybersecurity and 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 of detection of 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 has become a hot topic for countries all across the globe. Information Technology has become pervasive in all aspects of our lives and this includes elements referred to as critical infrastructures.

The mini-track examines aspects associated with the security of information technology (IT) and operational technology (OT) used by governments and critical infrastructures and explores ways that IT can enhance the ability of governments to ensure the safety and security of its citizens. Governments have embraced IT to interface with citizens in a more efficient manner. Security issues have risen to the forefront as a result of data disclosures and identity theft incidents discussed in mainstream media. Other critical issues include intellectual property theft and criminal acts involving computers. Many foreign governments have more control over their infrastructure, but in the end, security is still an important topic that needs to be addressed. 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, illustrating just how wide the area is. Three papers were chosen from the submissions of which the majority were international papers. We express our sincere appreciation to those authors that took the time to submit a paper for our consideration and our congratulations to those that were accepted.

The first two papers address different aspects of IoT security which is becoming ever more increasingly prevalent in our critical infrastructure. The first paper, *A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges* by Maaike Harbers, Mortaza Bargh, Ronald Pool, Jasper Van Berkel, Susan Van den Braak, and Sunil Choenni, presents a conceptual framework of challenges in addressing Security, Privacy, and Safety threats, along with solution directions to overcome them. The next paper by Trevor Bihl, Daniel Steeneck, *Multivariate Stochastic Approximation to Tune Neural Network Hyperparameters for Critical Infrastructure Communication Device Identification* discusses improving Z-Wave RF fingerprinting classification and performance via stochastic approximation methods.

The final paper *Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices* by Margit C. Scholl, Frauke Fuhrmann, and L. Robin Scholl identifies four research questions aimed at identifying and transferring information security awareness insights into a practical implementation. The authors present a comprehensive review of scientific literature focusing on the human factors involved in information security, then use this extensive compiled information to answer their identified research questions.

We sincerely hope that the attendees enjoy this session and will contribute to the discussion we are certain that will occur following the paper presentations.

URI: http://hdl.handle.net/10125/50165
ISBN: 978-0-9981331-1-9