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 paper, *Investing in Cyber Defense: A Value-Focused Analysis of Investment Decisions for Microgrids* by Bryan Hudgens, Cameron Hartner, Brian Adams, and Eva Regnier, from the Naval Postgraduate School in Monterey CA, examines the important values decision makers use to make decisions balancing cybersecurity needs and efficiency in microgrids. The next paper by Oksana Kulyk and Melanie Volkamer from the Karlsruhe Institute of Technology, Karlsruhe, Germany, *A Proxy Voting Scheme Ensuring Participation Privacy and Receipt-Freeness* examines the use of dummy ballots, proposed in another extension of Helios, to extend the proxy voting scheme towards participation privacy and receipt-freeness.

The final paper *The Need for Information Sharing and Analysis Organizations to Combat Attacks on State and Community Public and Private Networks* by Gregory White, Natalie Sjelin, and Keith Harrison discusses the need for an organized approach to developing community cybersecurity programs. Cities and states need to protect their systems but frequently plans to do so are lacking and the ability to respond to cybersecurity events is non-existent. This is especially true for smaller communities that do not have the budget to hire full-time security personnel or contract for security services. A critical step that states and communities can take is the establishment of a state or community Information Sharing and Analysis Organization (ISAO). This paper will describe how a state or community can use the creation of an ISAO to jumpstart various aspects of its cybersecurity program, incorporating a number of established programs in a single initiative.

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.