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 mintrack 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 minitrack 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 minitrack 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. Five papers were chosen from the submissions which included several 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, presented in a half-session, is *An Optimization Framework for Generalized Relevance Learning Vector Quantization with Application to Z-Wave Device Fingerprinting* by Trevor Bihl, Michael Temple, and Kenneth Bauer which discusses improving Z-Wave device discrimination using RF-DNA Fingerprints. The second paper in the same session is *Securing Birth Certificate Documents with DNA Profiles* by Mark Tannian, Christina Schweikert, and Ying Liu. The paper discusses the benefits and potential for using DNA profiling as a means of birth certificate authentication.

The second session starts off with *State and Community Information Sharing and Analysis Organizations* by Gregory White, Keith Harrison and discusses information sharing, the development of the Information Sharing and Analysis Organization program, and the need for state and community information sharing and analysis. The next paper *Proper incentives for proper IT security management - A system dynamics approach* by Jose J. Gonzalez and Denis Trcek argues that system dynamics models of security systems can improve the security management situation by increasing the awareness that misaligned incentives can backfire. The final paper in the mini-track is *An Evolution Roadmap for Community Cyber Security Information Sharing Maturity Model* by Wanying Zhao and Gregory White. This paper again visits the issue of cybersecurity information sharing and presents a model for collaborative info sharing.

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/10125/41442
ISBN: 978-0-9981331-0-2