Introduction: 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 privacy in 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 includes critical infrastructures that need to be secure.

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 while maintaining privacy. 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 the 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 and privacy are still important topics that need 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. Six papers were chosen from the submissions. 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.

There are two sessions in this mini-track with three papers in each. The first paper in the first session is *Topological Data Analysis for Enhancing Embedded Analytics for Enterprise Cyber Log Analysis and Forensics*: by Bihl, Gutierrez, Bauer, Boehmke, and Saie. This paper describes embedded analytics for log analysis, which incorporates five mechanisms: numerical, similarity, graph-based, graphical analysis, and interactive feedback. Topological Data Analysis (TDA) is introduced to provide novel graph-based similarity understanding of threats enabling a feedback mechanism to further analyze files.

The second paper is *Towards an Evaluation Framework for Threat Intelligence Sharing Platforms* by Bauer, Fischer, Sauerwein, Latzel, Stelzer, and Breu. The authors present a framework for analyzing and comparing relevant Threat Intelligence Sharing Platforms. The framework provides a set of 25 functional and non-functional criteria supporting potential users in selecting suitable platforms. They demonstrate the applicability of the framework by assessing three platforms: MISP, OTX and ThreatQ.

URI: https://hdl.handle.net/10125/63976
978-0-9981331-3-3

The final paper in the first session is *Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor* by Chris Bronk and Paula deWitte. This paper addresses the issue of cybersecurity in the global maritime system. Covered are the problem of protecting maritime traffic from attack as well as how cyberattacks change the equation for securing commercial shipping from attack on the high seas.

The first paper in the second session is *Understanding the Stakeholder Roles in Business Continuity Management Practices – A Study in Public Sector* by Jonna Jarvelainen. This study focuses on Business Continuity Management (BCM) stakeholders in continuity practices in the public sector and reports on the results of a qualitative case study with 16 interviews based on the premise that BCM requires commitment from all levels of an organization.

The second paper in the second session is *An Accurate and Scalable Role Mining Algorithm based on Graph Embedding and Unsupervised Feature Learning* by Abolfathi, Raghebi, Jafarian, and Banaei-Kashani. The authors propose an accurate and scalable approach to the role mining process of extracting meaningful roles from existing access control lists. They propose a deep learning algorithm based on random walk and present experimental results.

The final paper in the second session, and in this mini-track, is *The Role of Consequences in Securing Cyber-Physical Systems* by Wm. Arthur Conklin. This paper examines how security measures need to take a wider approach than just application of IT controls to a new environment if one is interested in truly managing the risk of cyber-physical systems. Although these systems use computers to manage the communication and control of the processes, the systems are distinctly different from IT systems in business.

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