Introduction to the HICSS-49 Minitrack on Innovative Behavioral IS Security and Privacy Research

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Anthony Vance
Brigham Young University
anthony@vance.name

Allen C. Johnston
University of Alabama at Birmingham
ajohnston@uab.edu

This minitrack provides a venue for innovative research that rigorously addresses the risks to information system security and privacy, with a specific focus on individual behaviors within this nomological net. Domains include work related to detecting, mitigating, and preventing both internal and external human threats to organizational security. Papers may include theory development, empirical studies (both quantitative and qualitative), case studies, and other high-quality research manuscripts.

This year the minitrack features nine papers covering a range of behavioral privacy and security topics and methods. One group of papers addresses phenomena related to human-centered security, including an examination of the factors that lead people to engage in security and privacy threat mitigation actions, as well as the provision of a framework for malicious insider profiling based on a text mining analysis of public data sources. A third paper in this group presents a system for password creation that leverages visual cues to reduce the high level of entropy typically associated with strong password selection and recall. The three papers presented within this group are as follows:

- “Measuring the Human Factor in Information Security and Privacy” by Dupuis, Cressler, and Endicott-Popovsky.
- “Validating Common Characteristics of Malicious Insiders: Proof of Concept Study” by Liang and Biros.
- “CPasswords: Leveraging Episodic Memory and Human-Centered Design for Better Authentication” by Camp, Abbott, and Chen.

A second group of papers featured within this minitrack is focused on phenomena related to privacy and data disclosure, including the development of a holistic picture of customer expectations of fair data collection and usage, an examination of personal identity relative to privacy and identify theft recovery planning, and the impact of fine-grained data requests on smartphone user’s information disclosure. The three papers presented within this group are as follows:

- “Consumers’ Expectations of Fair Data Collection and Usage – A Mixed Method Analysis” by Niemann and Schwaiger.
- “Privacy and Identity Theft Recovery Planning: An Onion Skin Model” by Alashoor, Baskerville, and Zhu.
- “Investigating Users’ Reaction to Fine-Grained Data Requests: A Market Experiment” by Eling, Rasthofer, Kolhagen, Bodden, and Buxmann.

Finally, a third group of papers within this minitrack is focused on deception and surveillance. These papers include a study of an automated approach to the detection of intentionally deceptive linguistic cues in spontaneous online communication, a study that validates the existence of four dimensions of source credibility in the context of social engineering attacks, and an examination of individuals’ behavioral and emotional coping approaches to online government surveillance. The three papers presented within this group are as follows:

- “Real or Spiel? A Decision Three Approach for Automated Detection of Deceptive Language-Action Cues” by Ho, Hancock, Booth, Liu, Liu, Timmarajus, and Burmester.
- “Measuring Source Credibility of Social Engineering Attackers on Facebook” by Algami, Xu, and Chan.