Introduction to the HICSS-55 Minitrack on Cyber Deception and Cyberpsychology for Defense

Kimberly Ferguson-Walter
Laboratory for Advanced Cybersecurity Research
Kimberly.j.ferguson-walter.civ@mail.mil

Matt Bishop
University of California Davis
Mabishop@ucdavis.edu

Cliff Wang
Army Research Office
Xiaogang.x.wang.civ@mail.mil

Sunny Fugate
Naval Information Warfare Center
Fugate@niwc.navy.mil

This minitrack provides a venue for innovative research that considers the human aspects and limitations of cyber attackers for improved defense within government and other computer networks. Cyber deception techniques are one of the maturing areas of research that focuses on taking advantage of the human limitations and innate performance deficiencies of cyber attackers. Cyberpsychology methods may be used to rigorously quantify the effectiveness of defense methods, provide useful metrics and measures, and understand the decision making and behavioral patterns of cyber attackers or defenders, including insider threats. This information can then be used to help improve defender effectiveness and impede attackers. This minitrack was created to help fill the gap in venues accepting multi-disciplinary work on these topics. The hope is to bring together the different research communities (e.g., computer science, behavioral science, etc.) and experts needed to make significant progress in this area.

This year the minitrack features six papers. These contributions address a range of cyber deception and cyberpsychology research questions that will encourage further exploration of key topics within this domain. One group of papers examines the use of Natural Language Processing (NLP) methods for very different purposes:

- *"TSM: Measuring the Enticement of Honeyfiles with Natural Language Processing"* (by Roelien Timmer, David Liebowitz, Surya Nepal, and Salil Kanhere) introduce Topic Semantic Matching (TSM) as a novel method for comparing file content, and provides a cyber deception use case of quantifying the enticement of honeyfile content.
- *"Modeling Phishing Decision using Instance Based Learning and Natural Language Processing"* (by Tianhao Xu, Kuldeep Singh, and Prashanth Rajivan) present work aimed at modeling user decisions made regarding phishing emails, aimed at deceiving users. They use NLP methods to represent email text within Instance-Based Learning models.
- *"Predicting the Threat: Investigating Insider Threat Psychological Indicators With Deep Learning"* (by Angela Horneman, Bob Ditmore, Craig Motell, and Matthew Levy) use NLP to investigate the relationship between the text in employee evaluations, psychological factors discussed in insider threat research, and established risk indicator categories.

The next set of papers uses rigorous human subjects research to dive deeper into different aspects of cyber attack and defense:

- *"The interaction of dark traits with the perceptions of apprehension"* (by Joana Gaia, David Murray, George Sanders, Sean Sanders, Shambhu Upadhyaya, Xunyi Wang, and Chul Yoo) examined similar psychological factors, with the aim of understanding how the Dark Triad and thrill-seeking tendencies relate to the economics of cyber crime. They used surveys to examine in what circumstances people would be willing to commit cyber crimes, as well as their tendencies toward white, grey, and black hat hacking.
- *"A Task Analysis of Static Binary Reverse Engineering for Security"* (by Megan Nyre-Yu, Karin Butler, and Cheryl Bolstad) conducted a task analysis on experts to explore the cognitive

URI: https://hdl.handle.net/10125/79607
978-0-9981331-5-7

processes reverse engineers use during static vulnerability discovery, providing insight into human aspects of a cyber expertise seldom studied.

Finally, the last paper discusses the need for multidisciplinary research teams and provides guidelines for the use of behavioral science in computer science research:

- *"Responsible Integration of Behavioral Science in Computer Science Research and Development"* (by Elizabeth Niedbala, Kimberly Ferguson-Walter, and Dana Lafon) provides examples of the negative consequences of misusing behavioral science and details common errors to avoid at each stage of the research process and introduces a simple checklist for research teams to use as a tool to help ensure rigorous, and high-quality research results.

We look forward to the interesting discussions these publications will generate, and hope they lead to further advances in the field.