UNIVERSITY of WASHINGTON

ISE Graduate Seminar Series

Analyzing Adversarial Decision-Making Using models of Instance Based Learning and Natural Language Processing

BIO

Prashanth Rajivan is an assistant professor of Industrial and Systems Engineering at the University of Washington. His research agenda is on the intersection of human factors, simulation modeling and computer security. Prior to this appointment, Prashanth Rajivan was a Postdoctoral Research Fellow at the Department of Social and Decision Sciences, Carnegie Mellon University, Pittsburgh. He holds a Ph.D. in Human Systems Engineering (2014) and M.S. in Computer Science (2011) from Arizona State University, USA. He received the National Science Foundation (NSF) CAREER award in 2022. His work on multi-agent models of teamwork in cyber defense was awarded the best student paper at HFES annual conference in 2014. His dissertation work was a finalist in the Human Factors Prize on Cyber Security in 2017.He is currently the chair of cyber security technical group at HFES, Co-chair for 2022 USEC (Symposium of Usable Security and Privacy) and is on the board of Modeling and Simulation Society.

Dr. Prashanth Rajivan

Date: November 21st, 2023

Time: 1:30 pm – 2:20 pm

Location: MEB 234

ABSTRACT

Adversarial decision-making could be characterized as decisions made in rare and novel situations, decisions on choices with risky and uncertain outcomes, and decisions made under the adversarial influence. Adversarial decision-making is ubiquitous in cyber security, including the detection of phishing attacks, the detection of misinformation on social networks, the detection of threats in security operations center, and decisions that adversaries make to choose human and computing nodes to attack. We are particularly interested in modeling and analyzing the cognitive processes associated with the operations of human memory in various security contexts to effectively explain adversarial decision making. In this talk, I will describe our work in the context of spear-phishing. First, I will describe a new simulation paradigm we have developed for studying human behavior in phishing attacks from both the attacker and end-user perspective. Next, I will present results of analyzing cognitive model developed to explain and predict human responses to phishing emails obtained from a laboratory experiment. I will describe the effectiveness of integrating natural language processing methods, such as, GloVe, and BERT with cognitive models to predict human response to phishing emails. Finally, I will introduce follow-on research directions I am currently pursuing in the context of misinformation and cyber defense operations.