Adversarial Decision Making in Phishing Attacks

Prashanth Rajivan, PhD
Assistant Professor
Department of Industrial & Systems Engineering
University of Washington

Abstract: Humans, just as much as technology, are at the crux of many of our cyber security challenges, as both the problem and the solutions. Humans are the adversaries who instigate attacks; the weakest-links who fall victims to exploitation; and the defenders who can execute effective responses to emerging threats. Yet, we know very little about human behavior in cyber security. In this talk, I will discuss my research on dynamic decision making in the context of social engineering attacks (e.g., Phishing). This talk will describe a new simulation paradigm developed for studying and modeling human behavior in phishing attacks from both the attacker and end-user perspectives in which the objective of the attacker is to increase error rate of end-user decision making through persuasion and deception. I will present results from both qualitative and quantitative analysis of the artificial phishing dataset generated using this methodology. Finally, I will discuss follow-on research directions I plan to pursue through my new lab for behavioral research in information and computer security (BRICS) that will use interdisciplinary approaches to advance the behavioral science of cyber security.

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 and computer security. His areas of interests include security and privacy decision making, simulation and modeling, computer supported cooperative work, and applied cognitive science. Prashanth examines how human behavior affects information security and privacy to develop models of effective interventions that reduce the risk from attacks and promote safe behaviors online. 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 is the author of several peer-reviewed publications and book chapters. 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.