The University of Chicago Computer Science Department

PRESENTS:

"Human Augmentation for Internet Security"

Gang Wang
Virginia Tech

Abstract:
Human factors are playing a critical role in the security of today's Internet systems. On one hand, human factors are constantly exploited by attackers to launch serious attacks, leading to massive data breaches and ransomware infections. On the other hand, human (expert) intelligence is instrumental in detecting and combating new threats (e.g., zero-days) that automated methods such as machine learning often fail to capture.

In this talk, I will describe our efforts to improve security through human augmentation. Human augmentation includes (1) reducing the security risks introduced by human factors, and (2) integrating human intelligence to build more robust security defenses. First, I will describe our progress to reduce the risk of human factors by detecting and mitigating flawed system designs that severely weaken user-level defenses. Using spear phishing as an example, I will illustrate how data analytics and active measurements can make a key difference in this process. Second, I will share our recent results on improving the trust and robustness of security systems by generating "human-interpretable" outputs. By building an "explanation system" for deep learning based security applications, we allow security analysts to diagnose classification errors and patch model weaknesses. Finally, I conclude by highlighting my future plans of using data-driven approaches to augmenting security defenses for both humans and algorithms.

Bio:
Gang Wang is an Assistant Professor of Computer Science at Virginia Tech. He obtained his Ph.D. from UC Santa Barbara in 2016, and a B.E. from Tsinghua University in 2010. His research focuses on human (user) aspects of Internet security. His work takes a data-driven approach to addressing emerging security threats in massive communication systems (social networks, email services), crowdsourcing systems, mobile applications, and enterprise networks. He is a recipient of the NSF CAREER Award (2018), Google Faculty Research Award (2017), ACM CCS Outstanding Paper Award (2018), and SIGMETRICS Best Practical Paper Award (2013). His research has appeared in a diverse set of top-tier venues in Security, Measurement, Networking, and HCI. His projects have been covered by media outlets such as MIT Technology Review, The New York Times, Boston Globe, CNN, ACM TechNews, and New Scientist.

Wednesday, Febraury 20, 2019
3:30 pm
JCL 390
Host: Fred Chong