UCF DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCEINCE

Spring 2015 Seminar Series

Presented by the CS Division

ATTACK-RESILIENT SYSTEMS AND NETWORKS

WEDNESDAY APRIL 15, 2015

10:00 AM – HEC 450

Traditionally, security research has focused primarily on preventing attacks from being successful; however, in many scenarios, thwarting all possible attacks is either practically impossible or financially unrealizable. In these scenarios, defenders have to mitigate the impact of successful attacks by designing the targeted systems and networks so that they sustain minimal losses in case of a successful attack, that is, by designing them to be attack-resilient. Even though attack-resilience resembles random-fault tolerant design in many respects, it is actually fundamentally different due to the strategic nature of the attackers, who may anticipate defensive countermeasures. This strategic nature of the conflict between defenders and attackers is captured most naturally using the game-theory nomenclature, which allows us to establish provable resilience properties. In this talk, I show how this approach can be applied to problems from various levels of system architecture, ranging from physical node placement to protecting users from social-engineering attacks. First, I discuss resilient sensor node placement for monitoring cyber-physical systems, and show how to find resilient placements in practice. Second, I consider the problem of providing integrity assurance for communication between resource-bounded devices, and introduce a stochastic message authentication scheme for solving this problem. Third, I discuss mitigation strategies against covert compromises of computer systems, and present results on the optimal schedule of mitigation moves. Fourth, I consider the problem of filtering malicious e-mail, such as spam and spear-phishing e-mail, and show how to find optimal filtering thresholds that take the heterogeneity of users into account. Finally, I give an overview of open research problems and outline directions for future work.

DR. ARON LASZKA

Vanderbilt University

Aron Laszka is a Postdoctoral Research Scholar at the Institute for Software Integrated Systems at Vanderbilt University. His primary research interests are cyber-security, economics of security, resilient design, and game theory for security. He has contributed to a variety of topics, including resilient network topologies, systematic risks in networked systems, mitigation of social-engineering attacks, and content-adaptive steganography. His current work is affiliated with the NSF-sponsored project Foundations of Resilient Cyber-Physical Systems (FORCES), and it is concerned with various security problems in cyber-physical systems. Previously, he was a Visiting Research Scholar at the Pennsylvania State University in 2013. He received the Ph.D. degree in computer science from Budapest University of Technology and Economics, Budapest, Hungary, in 2014.

Hosted by: Dr. Sheau-Dong Lang

UCF

4328 Scorpius Street Room 346 Orlando, FL 32816

WWW.EECS.UCF.EDU