UCF DEPARTMENT OF COMPUTER SCIENCE

Distinguished Speaker Series

SECURITY ANALYTICS FOR DEFEATING AUTOMATED INTERNET-SCALE THREATS

Friday February 24, 2017 ● 12:00PM-1:00PM ● Teaching Academy 117

Billions of devices are connected to the Internet today, significantly changing the threat landscape by lending adversaries unprecedented resources to launch automated attacks, and requiring new threat analysis and defenses. In this talk, I will argue that big data analytics can play an important role in securing the Internet, and exemplify my argument with applications to distributed denial of service (DDoS), malware analysis, and massively multiplayer online role-playing game (MMORPG) bot detection. First, I will present an analytical view of 50,000 unique and verified DDoS attacks on services on the Internet. I will show how adversaries' spatiotemporal traits follow predictable patterns, consecutive attacks follow certain patterns allowing prediction of future threat, and attackers are highly collaborative. Second, I will show how big data analytics are applied to malware analysis and software behavior profiling, and demonstrate optimizations to scale such analytics. Third, I will discuss an analytics framework for game bot detection in MMORPG using self-similarity of user behavior. By applying this framework to three large online games, I demonstrate how this analytics approach can be used to extract general features of behavior and effectively detect game bots in practice. I will conclude by highlighting my vision of how this analytics approach can be applied to realize effective and proactive defenses, and extended for other applications.

Aziz Mohaisen

Assistant Professor, University of Buffalo

Aziz Mohaisen is an Assistant Professor of Computer Science at the University at Buffalo. The current focus of his research is building security analytics for understanding and defending threat in software and networks, with applications to Malware, DDoS, DNS, MMORPG, IoT, Blockchain, etc. His work has been supported by various awards from NSF, NRF, AFRL and AFOSR. He was the recipient of the US Air Force Summer Faculty Fellowship (2016). Before joining UB in 2015, he was a senior research scientist at Verisign Labs in the Washington D.C. area (2012-2015) and a Research Engineer at ETRI in South Korea (2007-2009). He earned his M.Sc. and Ph.D. in Computer Science from the University of Minnesota in 2012, and was a recipient of the Doctoral Dissertation Fellowship (2011). Aziz is an avid (ultra)marathoner, and when not doing research or running, he likes to explore the world with his three growing kids.

Hosted by: Dr. Gary T. Leavens