Spring 2014 Colloquium
Computer and Information Sciences

Data-Driven Analytics and Automation for Next-Generation Secure and Resilient Systems

Ehab Al-Shaer
University of North Carolina, Charlotte

Monday, April 21, 11:00 AM, Wachman 447

Abstract:
Despite the advances of cybersecurity over the past years, the gap between attack sophistication and defense capabilities is ever increasing. This can be attributed to many fundamental challenges. Firstly, the growing complexity of cyber and cyber-physical systems that usually involve hundreds of thousands of devices and millions of highly inter-dependent configurations (e.g., rules, policies, variables) increases the potential misconfiguration and security threat exponentially. Secondly, the asymmetry of cyber warfare, which allows adversaries to plan, launch and propagate attacks while defense strategies exhibit high uncertainty due to unknown attack strategies, increases the potential attack evasion and success. Thirdly, key system artifacts (e.g., logs and traces) that are important for estimating the state of the systems are often high-volume and semantically unstructured, which imposes real challenges in reasoning about failures or attacks.

In this talk, I will give an overview of our current and future research to address these challenges and enable next-generation secure and resilient systems. I will present our research work in data-driven analytics and automation using formal methods, statistical analysis and probabilistic reasoning and for improving the trustworthiness, resilience and assurability of large-scale complex systems. In particular, I will present three main thrusts of my research: (1) our formal analytics for modeling and verification of cyber and cyber-physical system behavior based on configuration and log data, (2) cyber agility using data- and model-driven techniques, and (3) evidential reasoning and formal analytics combined approach for network diagnosis and prognostication. My research application domains include security analytics of large-scale enterprises including financial institutions, data centers and health care systems, smart grid resilience, health diagnosis of critical infrastructure, sensor network mission assurability, and Software Defined Networking security.

Bio:
Ehab Al-Shaer is Professor of Computer Science, the director of Cyber Defense and Network Assurability (CyberDNA) Center, and the director of the NSF IUCRC Center on Security Configuration Analytics and Automation at UNC Charlotte. His area of research is security analytics, configuration verification and automation, firewalls and intrusion detection optimization, security metrics and moving target defense. Dr. Al-Shaer has edited/co-edited more than 12 books and book chapters, and published about 170 refereed journals and conferences papers in his area. He was designated as a Subject Matter Expert (SME) in the area of security configuration analytics and automation in Information Assurance Newsletter published by DoD in 2011. He was the General Chair of ACM Computer and Communication in 2009 and 2010 and NSF Workshop in Assurable and Usable Security Configuration in 2008. Dr. Al-Shaer was also the PC chair for many other conferences and workshops including ACM/IEEE SafeConfig 2009 and 2013, IEEE Integrated Management 2007, IEEE POLICY 2008, and others. In the past four years, Dr. Al-Shaer has received a total research funding of more than $6M during the past four years from various government and industry sources including NSF, AFRL, ARO, NSA, Duke, IBM, Telcordia, Bank of America, Wells Fargo, BB&T, DTCC and others. His research projects are mainly concerned with formal techniques for automated security configuration verification, synthesis and diagnosis, cyber agility, smart grid security, firewall metrics, diagnosis of cyber-physical systems, science of security, and predictive risk analysis.