Faculty Candidate Seminar

Program Anomaly Detection in Cyber-Physical Systems

Long Cheng
Virginia Tech

Abstract: Recent studies have revealed that control programs in cyber-physical systems (CPS) suffer from both control-oriented attacks (e.g., code-injection or code-reuse attacks) and data-oriented attacks (e.g., non-control data attacks). Securing CPS against malicious attacks is of paramount importance because these attacks may cause irreparable damages to physical systems. Unfortunately, existing detection mechanisms are insufficient to detect runtime data-oriented exploits, due to the lack of execution semantics checking. This talk focuses on providing new security capabilities by enforcing cyber-physical execution semantics in defending against cyber attacks in CPS. I will present an event-aware anomaly detection framework that leverages the event-driven nature in characterizing CPS control program behaviors. As an instantiation of the proposed framework, I describe a new program behavior model, named event-aware finite-state automaton (eFSA) in defending against data-oriented attacks. I will also describe the Event Triggering and Control Actuation Integrity security enforcement, which is able to identify advanced CPS attacks and anomalies in a preventative manner. This talk concludes with a discussion of my future research directions.

Bio: Long Cheng is currently pursuing his second Ph.D. in the Department of Computer Science at Virginia Tech. His research interests include system and network security, cyber forensics, cyber-physical systems (CPS), Internet-of-Things (IoT), mobile computing, and wireless networks. He received his first Ph.D. degree from Beijing University of Posts and Telecommunications China in 2012. Dr. Cheng received the Best Paper Award from IEEE Wireless Communications and Networking Conference (WCNC) in 2013, the Erasmus Mundus Scholar Award from the European Union in 2014, and the Pratt Fellowship at Virginia Tech in 2017. His research activities span across the fields of cyber security and networking. Dr. Cheng has published over 60 papers in peer-reviewed journals and conferences, including IEEE Transactions on Information Forensics and Security (TIFS), IEEE/ACM Transactions on Networking (ToN), Transactions on Parallel and Distributed Systems (TPDS), IEEE Transactions on Mobile Computing (TMC), Annual Computer Security Applications Conference (ACSAC), Privacy Enhancing Technologies Symposium (PETS), IEEE Conference on Computer Communications (INFOCOM), ACM Conference on Embedded Networked Sensor Systems (SenSys), and IEEE International Conference on Network Protocols (ICNP).

Date: February 28, 2018

Time: 11:00 am

203 Computer Science Building

MISSOURI S&T