SOFTWARE-DEFINED NETWORKING: IMPROVING SECURITY FOR ENTERPRISE AND HOME NETWORKS

Curtis R. Taylor
PhD Candidate
WPI - Computer Science

Friday, April 14, 2017
Time: 1:00 p.m. - 2:00 p.m.
Location: Morgan Room, Campus Center

Committee Members:

Prof. Craig A. Shue, WPI - Computer Science
Prof. Mark Claypool, WPI - Computer Science
Prof. Thomas Eisenbarth, WPI - Electrical and Computer Engineering
Dr. Nathanael Paul, Moated Security, UTK (External Committee Member)

Abstract:

Software-defined networking (SDN) is a networking paradigm that allows logically centralized control of network switches and routers. SDN can help address a network operator’s limited visibility in network traffic while providing the benefits of a centralized network control platform. SDN also has the potential to drastically increase security and network control in residential networks where, in contrast to the enterprise, resources are scarce.

However, there are concerns with traditional switch-based SDN related to switch scalability. Furthermore, switch-based SDN is ultimately limited in that it can only gather network packet information. Moreover, network security research, in particular with respect to SDN, is lacking in the residential environment.

This presentation discusses our dissertation research efforts of introducing SDN into the enterprise by pushing the SDN functionality to the end-hosts. In doing so, we address scalability concerns and provide network operators with better situational awareness by incorporating host-context into network information. In the residential network, we use SDN, along with cloud-based resources, to introduce enterprise-grade network security solutions which were previously infeasible. As part of our residential efforts, we build and evaluate device-agnostic security solutions that are able to better protect the increasing number of Internet of Things (IoT) devices.