Announcing the Final Examination of Hisham Alasmary for the degree of Doctor of Philosophy

Time & Location: February 24, 2020 at 10:00 AM in Research 1 (R1) 103
Title: Analyzing and Detecting Internet of Things Malware Using Residual Static Graph- and String-Based Artifacts

Recently, the Internet of Things (IoT) has become more wide and adopted many features from social networks and mainly uses sensing devices technologies. The wide-range of IoT-based applications causes a rapid increase in production and adoption. However, security and privacy are serious threats that users usually take precautions to protect their devices and information. With the massive growth of IoT devices, understanding the security shortcomings at first stage will educate IoT users to protect their connected things. Understanding IoT software through analysis, comparison (with other types of malware), and detection (from benign IoT) is an essential problem to mitigate security threats.

First, we look into a comparative study of Android and IoT malware through the lenses of graph-based measurements. We construct the abstract structures of the malware, using Control Flow Graph (CFG) to represent malware binaries, and use them to conduct an in-depth analysis of malicious graphs.

Machine Learning (ML) algorithms are actively used in the process of detecting and classifying malicious software from benign ones. Toward detection, we use different graph-based features extracted from the CFGs as mentioned above, and augment them with CFGs of the benign dataset and build a detection system. Furthermore, we classify the IoT malware to their corresponding families.

However, adversarial ML attacks on malware detectors are proposed in the literature. For instance, Adversarial Examples (AEs) on the CFG can be generated by applying small changes to the graph features that force the model to misclassification. Thus, we propose Soteria, a CFG-based AEs detector utilizing deep learning with random walks to construct in-depth features.

Moreover, we detect the malicious shell commands by extracting and analyzing the malicious shell commands in IoT malware. We utilize natural language processing techniques for feature generation, followed by a deep learning model to detect the malicious commands and malware samples.

Major: Computer Science

Educational Career:
Bachelor's of Computer Science, BS, 2009, King Khalid University, Abha, Saudi Arabia
Master's of Computer Science, MS, 2016, The George Washington University, Washington, D.C., USA

Committee in Charge:
Abedelaziz Mohaisen, Chair, Computer Science
Amro Awad, Electrical & Computer Engineering
Clay Posey, Management
Wei Zhang, Computer Science

Approved for distribution by Abedelaziz Mohaisen, Committee Chair, on January 31, 2020.

The public is welcome to attend.