Defense of a Doctoral Dissertation
Countermeasure Against Various Network Attacks Using Machine Learning Methods
by
Yi Li
For the Ph.D. degree in Computer Science and Engineering

With the rapid development of the computer network, our life is already inseparable from it. Wi-Fi has been used everywhere, more and more devices have been connected to the internet, and many companies and individual tend to store their data and information online. Furthermore, it is now very convenient to communicate with each other through email and text messages. However, widespread networks also provide more attack surfaces for attackers. There are a variety of network attacks that are aimed at information theft. To better defend against those network attacks, one needs to have a broad knowledge of the existing attacks. In this dissertation, we focus on attacking different attack surfaces and propose the corresponding defending schemes.

We first focus on the domain name security and defend against Domain Generation Algorithm (DGA) based malware and propose a machine learning approach to accurately identifying DGA domains and clustering these domains to find out their DGAs. We then focus on the Wi-Fi security and countermeasure against Key Reinstallation Attack (KRACK), which utilizes the serious weakness in the 4-way handshake and aimed at stealing personal information. We propose a Software-Defined Networking (SDN)-based detection and mitigation framework to defend against KRACK. Next, we propose two study designs to understand how a user will behave when encountered phishing attacks. In addition, we study the adversarial attack that will compromise the machine learning (ML) model we used in securing an in-vehicle network and propose the adversarial retraining to build a robust ML model.

Publications
5) Yi Li, Kaiqi Xiong and Xiangyang Li. "Understanding User Behaviors When Phishing Attacks Occur" IEEE International Conference on Intelligence and Security Informatics (ISI), 2019.

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.