UNIVERSITY OF SOUTH FLORIDA

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 re-training to build a robust ML model.

Examining Committee
Lingling Fan, Ph.D., Chair
Yu Sun, Ph.D., Co-Major Professor
Kaiqi Xiong, Ph.D., Co-Major Professor
Yicheng Tu, Ph.D.
Lawrence Hall, Ph.D.
Xiaopeng Li, Ph.D.

Monday, November 9th, 2020
3:00 PM
Online (Collaborate Ultra)
Please email for more information
yli13@usf.edu
THE PUBLIC IS INVITED

Publications

1) **Yi Li**, Jing Lin, Kaiqi Xiong. “An Adversarial Attack Defending System for Securing In-Vehicle Networks” IEEE Consumer Communications & Networking Conference (CCNC), January 9-12, 2021.
2) **Yi Li**, Kaiqi Xiong, and Xiangyang Li. “Applying Machine Learning Techniques to Understand User Behaviors When Phishing Attacks Occur.” EAI Endorsed Transactions on Security and Safety 6, no. 21, 2019.
3) **Yi Li**, Kaiqi Xiong, and Xiangyang Li. “A Machine Learning Framework for Studying User Behaviors in Phishing Email Processing”, 34rd IFIP TC-11 SEC 2019 International Conference on Information Security and Privacy Protection, Lisbon, Portugal, June 25-27, 2019.
4) **Yi Li**, Kaiqi Xiong, and Xiangyang Li. “An Analysis of User Behaviors in Phishing Email Using Machine Learning Techniques”, The 16th International Conference on Security and Cryptography (SECRYPT 2019), Prague, Czech Republic, July 26-28, 2019.
5) **Yi Li**, Marcos Serrano, Tommy Chin, Kaiqi. Xiong and Jing Lin. “A Software Defined Networking-Based Detection and Mitigation Approach Against KRACK.” The 16th International Conference on Security and Cryptography (SECRYPT 2019), Prague, Czech Republic, July 26-28, 2019
6) **Yi Li**, Kaiqi Xiong and Xiangyang Li. “Understanding User Behaviors When Phishing Attacks Occur” IEEE International Conference on Intelligence and Security Informatics (ISI), 2019.
7) **Yi Li**, Kaiqi Xiong, Tommy Chin, and Chengbin Hu. "A Machine Learning Framework for Domain Generation Algorithm (DGA)-Based Malware Detection." IEEE Access, vol. 7, pp. 32765-32782, 2019.
8) Tommy Chin, Kaiqi Xiong, and Chengbin Hu, and **Yi Li**. "A machine learning framework for studying domain generation algorithm (DGA)-based malware." SecureComm, pp. 433-448. Springer, Cham, 2018.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

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.