UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

A Machine Learning Framework for Domain Generation Algorithm (DGA)-Based Malware Detection

by

Yi Li

For the Ph.D. degree in Computer Science & Engineering

Attackers usually use a command and control (C2) server to manipulate the communication. To perform an attack, threat actors often employ a domain generation algorithm (DGA), which can allow malware to communicate with C2 by generating a variety of network locations. Traditional malware control methods, such as blacklisting, are insufficient to handle DGA threats. In this research, we propose a machine learning framework for identifying and detecting DGA domains to alleviate the threat. We collect real-time threat data from the real-life traffic over a one-year period. The proposed machine learning framework consists of a two-level model. In the two-level model, we first classify the DGA domains apart from normal domains and then use the clustering method to identify the algorithms that generate those DGA domains. Furthermore, we build a deep neural network (DNN) model to enhance the proposed machine learning framework by handling the huge dataset we gradually collected.

Wednesday, April 24, 2019
2:00 PM
ENB 337

THE PUBLIC IS INVITED

Examining Committee

Kaiqi Xiong, Ph.D., Co-Major Professor
Yu Sun, Ph.D., Co-Major Professor
Yicheng Tu, Ph.D.
Lawrence Hall, Ph.D.
Xiaopeng Li, Ph.D.

Yu Sun, Ph.D.
Graduate Program Director
Computer Science and Engineering
College of Engineering

Sudeep Sarkar, Ph.D.
Department Chair
Computer Science and Engineering
College of Engineering

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.