SUNY Korea
The State University of New York

AMS SEMINAR II

Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques

SPEAKER

Jinsoo Hwang

Adjunct Professor

Dept. of Applied Math & Statistics

SUNY Korea

MONDAY
April 22, 2024

TIME
6:30 pm-7:30 pm

LOCATION
B105

Detecting ransomware is harder than general malware because of the ever-increasing number of ransomwares with different signatures, which makes traditional signature-based detection technique powerless against ransomware. Current ransomware detection techniques usually build a complex model that incorporates various behavioral traits. The traits include suspicious file activities, API call pattern or frequency, registry keys, file extensions, etc.

In this paper, we build a two-stage mixed ransomware detection model, Markov model and Random Forest model. First, we focus on Windows API call sequence pattern and build a Markov model to capture the characteristics of ransomware. Next, we build Random Forest machine learning model to the remaining data to control both false positive (FPR) and false negative (FNR) error rates. As a result of our two-stage mixed detection method we can achieve overall accuracy 97.3% with 4.8% FPR and 1.5% FNR.