INTELLIGENT BEHAVIOR-BASED RANSOMWARE DETECTION SYSTEM FOR ANDROID PLATFORM

The Oakland University and School of Engineering and Computer Science communities are invited to attend Abdulrahman Alzahrani's defense of his Ph.D. dissertation. Seating is limited. RSVP with Katie Loodeen at loodeen@oakland.edu.

INTELLIGENT BEHAVIOR-BASED RANSOMWARE DETECTION SYSTEM FOR ANDROID PLATFORM

Committee: Huirong Fu, Ph.D. (Chair), Anyi Liu, Ph.D., Subramaniam Ganesan, Ph.D., Xiaodong Deng, Ph.D.

Time: **9:30 – 11:30 a.m.**
Date: **Thursday, July 11th, 2019**
Location: **347 EC**

The worldwide epidemic of ransomware monetary gains has grown astonishingly. This crimeware form is emerged to extort innocent users under the threat of locking their devices and/or encrypting their files. To mitigate the growth of ransomware attacks, cybersecurity researchers have proposed various solutions based on the functionality of those attacks. However, this polymorphic type is kept refined to increase the appearance of new families by utilizing new evasion techniques, such as sophisticated codes, dynamic payloads, and anti-emulation techniques, in order to survive against mitigation solutions.

This research introduces RanDetector, a new automated and lightweight solution for detecting and preventing ransomware variants in Android platform based on their behavior. In particular, RanDetector investigates the appearance of some information that is related to ransomware operations in an inspected application before integrating some supervised machine learning models to classify the application. In addition, during analyzing an application, RanDetector performs a linguistic analysis on the application's code and resources textural strings to enhance further revelation.