BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK | Computer Science

THE DEPARTMENT OF COMPUTER SCIENCE & THE COMPUTER SCIENCE GRADUATE STUDENT ORGANIZATION (GSOCS) PRESENT

INVITED SPEAKER SERIES

Dr. Heng Yin
Syracuse University

Monday, May 2, 2016 at 12:00 PM
Engineering Building Room R15 (3rd Floor)

A Semantics-Centric Approach to Fight Android Malware

Abstract: The number of new Android malware instances has grown exponentially in recent years. McAfee reports that 2.47 million new mobile malware samples were collected in 2013, which represents a 197% increase over 2012. Greater and greater amounts of manual effort are required to analyze the increasing number of new malware instances. This has led to a strong interest in developing methods to automate the malware analysis process. In this talk, I will present a series of semantics-centric techniques to fight Android malware. First of all, we need a powerful analysis framework to quickly understand the inner-working of a given malware sample. To this end, we developed a virtualization-based analysis framework called DroidScope, which can seamlessly reconstruct both OS and Java level semantic views to provide a holistic view of a malware attack. Moreover, we need to automatically classify malware samples by their functionalities and behaviors and discover zero-day malware. We proposed a new semantics-based technique for malware classification, by capturing the semantics-level behavior of an app in form of ``Weighted Contextual API Dependency Graphs". Then by computing the similarity between these graphs, we can accurately and reliably detect malware variants and zero-day malware. Furthermore, we believe that malware detection can be more effective by getting end users into the loop. In particular, we developed a new technique that can automatically generate human-readable descriptions of a given app, such that any unexpected descriptions will cause suspicions and flagged by end users. To encourage wide adoption and follow-up research, these research products are available in form of source code release and/or web services.

Bio: Heng Yin is an Associate Professor in the department of Electrical Engineering and Computer Science at Syracuse University. His research interests mainly lie in computer security. In particular, he is interested in applying program analysis techniques and virtualization techniques to improve software and system security and defeat malware attacks. He earned his PhD degree in Computer Science from the College of William and Mary in July 2009. He was a member in BitBlaze Binary Analysis Research Group at UC Berkeley before joining Syracuse University. In 2011, he received NSF Career award. His publications frequently appear in top-notch conferences and journals such as ACM Conference on Computer and Communication Security (CCS), USENIX Security Symposium, ISOC Network and Distributed System Security Symposium (NDSS), etc. His research is supported by National Science Foundation, DARPA, Air Force Research Lab, and Department of Energy.