In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Automated Semantics-Based Malware Detection through Program Analysis and Program Synthesis

by

Mr. Yu Feng

University of Texas at Austin

U.S.A.

Date : 19 Dec., 2017 (Tue.)
Time : 11:15am – 12:15pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Modern software development handles increasing layers of complexity by adding more and more layers of abstractions through public APIs, existing code bases, and off-the-shelf software from app stores. Although this saves programmers from reinventing the wheel, it also raises new challenges on building reliable and secure systems. Program synthesis promises to automate complex programming tasks and eliminate subtle vulnerabilities by generating programs from high-level specifications. In this talk, I will focus on techniques for performing semantics-based malware detection through program analysis and program synthesis.

In the first part of my talk, I will present Apposcopy, a new semantics-based approach for identifying a prevalent class of Android malware that steals private user information. Apposcopy incorporates (i) a high-level language for specifying signatures that describe semantic characteristics of malware families and (ii) a static analysis for deciding if a given application matches a malware signature. To reduce the manual effort of writing malware signatures in Apposcopy, in the second part of my talk, I will present a technique for automatically synthesizing malware signatures from very few samples of a malware family. The key idea underlying our technique is to look for a maximally suspicious common subgraph (MSCS) that is shared between all known instances of a malware family.

Biography

Yu Feng is a Ph.D. candidate in Computer Science at UT Austin. His research to date focuses on developing automated programming techniques that combine program synthesis and program analysis to improve software usability, reliability, and security. Yu has developed systems for tackling security vulnerabilities (FSE'14, NDSS'17, CCS'17), automating complex programming tasks (PLDI'17, POPL'17), and challenging the limits of existing program analysis (OOPSLA'15, APLAS'15). Yu was a visiting student at Stanford, where he worked on cutting-edge techniques for detecting Android malware.

**** ALL ARE WELCOME ****

Host: Professor Calvin C.K. Chan (Tel: 3943-8354, Email: ckchan@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)