In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Augmenting Binary Code Analysis with Machine Learning

By

Prof. Kehuan ZHANG

The Chinese University of Hong Kong, Hong Kong

Date : 3 November 2023 (Friday)
Time : 3:30pm – 4:30pm
Venue : Rm 801, Ho Sin Hang Engineering Building, CUHK

Abstract

Binary code analysis is one of the most essential topics in system security and has many applications in attacks and defenses. Attackers may use binary code analysis techniques to find exploitable vulnerabilities, and defenders may rely on them to detect malicious software such as trojans, ransomware, and so on. In recent years, the rapid evolution of machine learning algorithms has enabled new technologies to augment existing binary code analysis tasks. This talk contains some of the recent works in this direction. It will begin with a new binary code disassembling method based on masked language modeling borrowed from natural language processing (NLP). The second part is about designing a fuzz testing framework to evaluate assembly code lifters (which convert assembly code into higher Intermediate Representations). The last part presents a tool called Bin2Sum that can automatically summarize a program's behaviors for a given piece of binary code. The talk will end with introductions to some planned future works using a hybrid approach that mixes traditional methods with machine learning algorithms, aiming to build solid tools with massive real-world applications.

Biography

Kehuan Zhang is an Associate Professor at the Department of Information Engineering, The Chinese University of Hong Kong (CUHK). He joined CUHK as an Assistant Professor in 2012 after obtaining his PhD degree from Indiana University Bloomington and was promoted to Associate Professor in 2018. He received his B.S. and M.E. degrees in computer science from Hunan University in 2001 and 2004, respectively. He worked in the industry between 2004 and 2007 as an FPGA logic developer for network equipment and a special display module used in the Shenzhou spacecraft and the Tiangong-1 space station. He has a broad research interest in the area of system security, including attacking and defense through side-channels, mobile systems security, IoT security, etc. He publishes high-quality research papers regularly on all of the four top conferences in the security area, including IEEE Security & Privacy, ACM CCS, USENIX Security, and NDSS. Some of his works have protected millions and billions of people around the world and have been widely reported.

**** ALL ARE WELCOME ****

Host: Prof. VONTOBEL Pascal (Tel: 3943-8390, Email: pascal.vontobel@ie.cuhk.edu.hk)
Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8385)