In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Opportunities and Challenges of Side-Channel Security in the Era of Confidential Computing

By

Dr. Yinqian Zhang

Department of Computer Science and Engineering, The Ohio State University

Date : 6th March, 2019 (Wed)
Time : 10:00am – 11:00am
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Side-channel security studies information leakage (and its countermeasures) due to some "side effects" of a program's execution, such as its execution time, computer (micro-)architecture access patterns, power consumption, etc. Many previous works on side-channel security have studied attacks from unprivileged applications, most notably in the context of public clouds hosting customers' virtual machines and containers, mobile phones running untrusted apps, and browsers loading third-party scripts. The recent emergence of confidential computing has dramatically shifted the landscape of side-channel security, both in terms of attacks and defenses. Enabled by new CPU extensions, such as Intel SGX and AMD SEV, confidential computing allows applications to be securely executed on untrusted software stacks. A variety of privacy-sensitive applications, such as confidential cloud computing and privacy-preserving blockchains, are made possible by confidential computing. While the demand for a high degree of confidentiality has offered new opportunities for side-channel security, however, side-channel threats from privileged software also bring unprecedented challenges. This talk will highlight these opportunities and challenges; it will also present some existing solutions that might shape future research directions.

Biography

Dr. Yinqian Zhang is an assistant professor of the Department of Computer Science and Engineering at The Ohio State University. His research interest lies in computer security in general. His most prominent research is on the topic of side-channel security, particularly in the context of cloud computing, mobile computing, and confidential computing. Over the past ten years, he has published numerous high-quality peer-reviewed research papers in well-regarded conference proceedings and journals, including over 20 papers published at the "big four" security conferences (i.e., IEEE S&P, ACM CCS, Usenix Security, and NDSS). As an expert in system security and side channels, he has been frequently invited to serve on the technical program committees of these top security venues. Dr. Zhang was a recipient of Google Ph.D. Fellowship in Security in 2013, CAREER Award from the National Science Foundation in 2018, and Lumley Research Award from the Ohio State University in 2019.

**** ALL ARE WELCOME ****

Host: Professor Kehuan Zhang (Tel: 3943-8391, Email: kehuan@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)