In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Identifying Cache-Based Side Channels in Production Software

by

Mr. Shuai Wang

Pennsylvania State University

U.S.A.

Date : 28 Feb., 2018 (Wed.)
Time : 11:00am – 12:00noon
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Side-channel attacks recover secret information by analyzing the physical implementation of cryptosystems based on non-functional computational characteristics, e.g. time, power, and acoustic. Among all well-known side channels, cache-based side channels are notoriously severe, leading to practical attacks against certain implementations of theoretically secure crypto algorithms, such as RSA, ElGamal and AES. Such attacks target the hierarchical design of the modern computer memory system, where different memory access patterns of a program can bring observable cache status difference.

In this talk, Shuai Wang will present novel techniques to help software developers identify potential vulnerabilities that can lead to cache-based side channel attacks. The technique leverages constraint solving to detect potential cache access differences at each program point. He will also describe two approaches, which leverage symbolic execution and abstract interpretation to deliver scalable detection of side channels. The proposed techniques have been implemented into two practical tools, and both tools have discovered a large number of known and unknown side-channel vulnerabilities from real-world cryptosystems. He will conclude by discussing opportunities he is excited to explore in the future, including supporting the detection of new side channel threats, eliminating side channel vulnerabilities from existing software, and providing new infrastructures for side channel detection on embedded platforms.

Biography

Shuai Wang is a Ph.D. candidate in College of Information Sciences and Technology, Pennsylvania State University. He is advised by Dinghao Wu. Shuai Wang is broadly interested in computer security and specializes in software security. The overall goal of his research is to enable building more secure software systems. In addition to publications at top-tier venues for Computer Security and Software Engineering, his work has also achieved notable impacts. For example, his binary reverse engineering work has been adopted and enhanced by two teams among the seven finalists in the 2016 DARPA Cyber Grand Challenge (CGC) competition.

**** 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)