Department of Computer Science

COMPUTER SCIENCE COLLOQUIUM

Small Mistakes in Code, Giant Vulnerabilities in Society: Gaps and Some Solutions for Secure Software Development

SPEAKER **Prof YAO Danfeng**

Associate Professor
Department of Computer Science
Virginia Polytechnic Institute and State University (Virginia Tech)
USA

DATE 18 December 2017 (Monday)
TIME 10:30 am - 11:30 am
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Software vulnerabilities are costly. NIST estimates that cost to be $60 billion each year, which includes the costs for developing and distributing software patches and reinstalling infected systems and the lost productivity due to malware and errors. The problem of software vulnerabilities is not new. What is new and promising is the increasing adoption of cryptography and security mechanisms in common software applications. However, it is difficult to write crypto code correctly. The practical task of securing cryptographic implementation is still in its infancy. This status is in sharp contrast with the multi-decade advancement of modern cryptography. This gap became particularly alarming, after multiple high-profile discoveries of cryptography-related vulnerable code in widely used network libraries and tools (e.g. the lack of authenticated encryption in iMessage, Diffie-Hellman key exchange downgrade vulnerability in TLS, and the exposure of random seeds in Juniper Network). In this talk, we will present our ongoing effort on cryptographic program analysis (CPA) where we design and develop rigorous static program analysis tools to detect crypto vulnerabilities in C and Java programs, as well as our empirical findings from the Stack Overflow forum that motivate the need for effective crypto coding assistance.

BIOGRAPHY

Yao Danfeng (Daphne) is an Associate Professor of Computer Science at Virginia Tech. In the past decade, she has been working on designing and developing data-driven anomaly detection techniques for securing networked systems against stealthy exploits and attacks. Her expertise also includes software security, mobile security, cloud security, and applied cryptography. Prof Yao received her Ph.D. in Computer Science from Brown University. Prof Yao is an Elizabeth and James E. Turner Jr. '56 Faculty Fellow and L-3 Faculty Fellow. She received the NSF CAREER Award in 2010 for her work on human-behavior driven malware detection, and the ARO Young Investigator Award for her semantic reasoning for mission-oriented security work in 2014. She received several Best Paper Awards, and was given the Award for Technological Innovation from Brown University. She holds multiple U.S. patents for her anomaly detection technologies. Prof Yao is an associate editor of IEEE Transactions on Dependable and Secure Computing (TDSC) and the lead program chair of the 2018 IEEE Security Development Conference (SecDev). She serves as the PC member in numerous computer security conferences, including ACM CCS, IEEE Security & Privacy Symposium. She has over 85 peer-reviewed publications in major security and privacy conferences and journals. Daphne is an active member of the security research community. She serves as the Secretary/Treasurer at ACM Special Interest Group on Security, Audit and Control (SIGSAC).

All are welcome!

In case of questions, please contact Dr WANG, Cong at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.