In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Exploiting Memory Errors on the Data Plane

by

Professor Zhenkai Liang

School of Computing

National University of Singapore

Date	**:**	**18 Oct., 2017 (Wed.)**
Time	**:**	**2:00 – 3:00pm**
Venue	**:**	**Room 833, Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

Abstract

As defense solutions against control-flow hijacking attacks gain wide deployment, control-oriented exploits from memory errors become difficult. As an alternative, attacks targeting non-control data do not require diverting the application's control flow during an attack. Although it is known that such data-oriented attacks can mount significant damage, no systematic methods to automatically construct them from memory errors have been developed. In this work, we study exploits of memory errors from the data angle. We have developed a new technique, called data-flow stitching, which systematically finds ways to join data flows in the program to generate data-oriented exploits. We have constructed new attacks on the data plane from known vulnerabilities. The constructed exploits can cause significant damage, such as disclosure of sensitive information (e.g., passwords and encryption keys) and escalation of privilege. We further study the expressiveness of such data-oriented exploits. By identifying data-oriented gadgets and gadget dispatchers, we demonstrate that data-oriented exploits can be used to construct Turing complete computations.

Biography

Zhenkai Liang is an Associate Professor of the School of Computing, National University of Singapore. His main research interests are in system and software security, web security, mobile security, and program analysis. He has served as the technical program committee members of many system security conferences, including the ACM Conference on Computer and Communications Security (CCS), USENIX Security Symposium and the Network and Distributed System Security Symposium (NDSS). He is also an associate editor of the IEEE Transaction on Dependable and Secure Computing. As a co-author, he received the Best Paper Award in ICECCS 2014, the Best Paper Award in W2SP 2014, the ACM SIGSOFT Distinguished Paper Award at ESEC/FSE 2009, the Best Paper Award at USENIX Security Symposium 2007, and the Outstanding Paper Award at ACSAC 2003. He also won the Annual Teaching Excellence Award of NUS in 2014 and 2015. He received his Ph.D. degree in Computer Science from Stony Brook University in 2006, and B.S. degrees in Computer Science and Economics from Peking University in 1999.

**** ALL ARE WELCOME ****

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