Automatic Generation of Data-Oriented Exploits

Zhenkai Liang
School of Computing
National University of Singapore

Date: April 1, 2016
Time: 11:15 a.m. – 12:30 p.m.
Location: Torgersen Hall 2150

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 develop a new technique called data-flow stitching, which systematically finds ways to join data flows in the program to generate data-oriented exploits. We build a prototype embodying our technique in a tool called FLOWSTITCH that works directly on Windows and Linux binaries. In our experiments, we find that FLOWSTITCH automatically constructs 16 previously unknown and three known data-oriented attacks from eight real-world vulnerable programs. All the automatically-crafted exploits respect fine-grained CFI and DEP constraints, and 10 out of the 19 exploits work with standard ASLR defenses enabled. The constructed exploits can cause significant damage, such as disclosure of sensitive information (e.g., passwords and encryption keys) and escalation of privilege.

Speaker's 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 member 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 Transactions 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.