In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Computer Science and Engineering
and Department of Information Engineering

Seminar

Checksum-Aware Fuzzing Combined with Dynamic Taint Analysis and Symbolic Execution

by

Dr. Tielei Wang
Georgia Institute of Technology

Date : 1 March, 2012 (Thur.)
Time : 11:00am-12:00noon
Venue : Room 833 Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Software security has become a central and critical aspect of the computer security problem. Software vulnerability detection techniques attract significant interest from both attackers and software developers. Fuzz testing is a typical vulnerability detection technique, and has proven successful in finding security vulnerabilities in large programs. However, traditional fuzz testing tools have a well-known common drawback: they are ineffective when target programs employ checksum mechanisms to verify the integrity of inputs.

This talk introduces TaintScope, a checksum-aware fuzzing system based on dynamic taint analysis and symbolic execution. TaintScope can locate checksum-based integrity checks in programs, then enforce execution flow alterations at located checksum check points to make malformed input to pass the checksum checks. Furthermore, TaintScope can automatically fix the checksum fields in malformed test cases using combined concrete and symbolic execution. In addition, TaintScope implements taint-based fuzzing and white-box fuzzing to generate malformed inputs. By combining these techniques, TaintScope has detected dozens of previously unknown vulnerabilities in several popular applications.This work received the Best Student Paper award at the IEEE Symposium on Security & Privacy (Oakland) 2010.

Biography

Tielei Wang is currently a postdoc research fellow at Georgia Institute of Technology. He earned his Ph.D. degree in Computer Science in July 2011, and his B.S. degrees in Physics and Economics in July 2006 all from Peking University. His research focuses on system security, especially software vulnerability detection, exploit and patch generation. He won the China Computing Federation (CCF) Distinguished PhD Dissertation Award in 2011, the Peking University Distinguished PhD Dissertation Award in 2011, and the IEEE Symposium on Security & Privacy (Oakland) Best Student Paper Award in 2010. He was also selected as the Most Valued Contributor by Secunia in Jan 2012 for his research in software security.

**** ALL ARE WELCOME ****

Host: Professor Dah-Ming Chiu (Tel: 3943-8357, Email: dmchiu@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)