Forced-Execution of Binaries and iOS Apps to Disclose Malicious Behavior

Xiangyu Zhang

Department of Computer Science
Purdue University

Date: September 18, 2015
Time: 11:15 a.m. – 12:30 p.m.
Location: Torgersen Hall 2150

Abstract

Malware is becoming increasingly advanced, making analysis very challenging. First, it is very difficult to acquire malware input specification, rendering the execution-based malware behavior analysis ineffective. Second, malware may contain multi-staged, condition-guarded, and environment-specific malicious payloads, making it difficult to reveal all payloads. Third, malware is often packed, obfuscated, or even self-modifying, and hence is extremely difficult for conventional static and symbolic analysis. In this talk, I will present a new and practical x86 binary analysis engine called X-Force. The core enabling technique behind X-Force is forced execution, which, as its name indicates, forces an arbitrary binary to execute without any input or environment setup. More specifically, X-Force monitors the execution of a binary through dynamic instrumentation, forcing the binary to ignore some conditional checks (or predicates) and supplying random values when inputs are needed. It tolerates invalid memory accesses by performing on-demand memory allocations and fixing the related pointers. Furthermore, by systematically force-setting a small set of branch outcomes, X-Force is able to explore different aspects or stages of the binary behavior. I will also present our recent experience in porting X-Force to iOS. Application of X-Force on iOS discloses that many of the top-100 apps on a regional Apple store have illegal hidden behavior such as stealing Apple IDs.

Speaker’s Biography

Xiangyu Zhang is an Associate Professor of Computer Science at Purdue University. He received his Ph.D. degree from the University of Arizona in 2006, and his M.S. and B.S. degrees from the University of Science and Technology of China. His research interest lies in dynamic and static program analysis and their applications in debugging, forensic analysis, and data processing. He is currently a Purdue University Scholar. He has received the 2006 ACM SIGPLAN Distinguished Doctoral Dissertation Award, NSF Career Award, and a few best paper awards in top conferences.