Department of Computer Science, The University of Hong Kong

CS Seminar

Towards Transparent Malware Debugging on x86 and ARM

Dr Fengwei Zhang
Director of COMPASS Lab
Department of Computer Science
Wayne State University

Date:
June 7, 2018
Thursday
2:00 pm

Venue:
Room 328
Chow Yei Ching Building
The University of Hong Kong

Abstract:

With the rapid proliferation of malware attacks on the Internet, understanding these malicious behaviors plays a critical role in crafting effective defense. Existing malware analysis platforms leave detectable fingerprints like uncommon string properties in QEMU, signatures in Linux kernel profiles，and artifacts on basic instruction execution semantics. Since these fingerprints provide the malware a chance to split its behavior depending on whether the analysis system is present or not, existing analysis systems are not sufficient to analyze the sophisticated malware. In this talk, I will present the framework for transparent malware analysis, which leverages the hardware features in existing PC and mobile devices to increase the transparency of malware analysis. In particular, I will introduce MalT on the x86 architecture and Ninja on the ARM architecture. MalT uses the system management mode as the execution environment and performance monitor unit as hardware assistant to facilitate the analysis, whereas Ninja involves the TrustZone technology and embedded trace macrocell to improve the transparency. Moreover, both MalT and Ninja are OS-agnostic, and do not require modification to the operation system or the target application.

About the Speaker:

Dr. Fengwei Zhang is an Assistant Professor and Director of the Computer And Systems Security (COMPASS) lab at Wayne State University. He received his Ph.D. degree in computer science from George Mason University in 2015. His research interests are in the areas of systems security, with a focus on trustworthy execution, transparent malware debugging, transportation security, and plausible deniability encryption. He has been published at top security venues including IEEE S&P, USENIX Security, NDSS, IEEE TIFS, and IEEE TDSC. He is a recipient of the Distinguished Paper Award in ACSAC 2017. For more information about him, please visit his homepage at: http://www.cs.wayne.edu/fengwei

All are welcome!
For enquiries, please call 2859 2180 or email enquiry@cs.hku.hk
Department of Computer Science
The University of Hong Kong