Analyzing Semantic Correctness of Protocol Implementations with Symbolic Execution

Mr. Sze Yiu Chau  
PhD Candidate  
Department of Computer Science  
Purdue University  
USA

Date : 4 January 2019 (Friday)  
Time : 11:00 a.m. – 12:00 noon  
Venue : Room PQ703, 7/Floor, PQ Core, Mong Man Wai Building,  
The Hong Kong Polytechnic University

Abstract

In order to achieve security, protocol implementations not only need to avoid low-level memory access errors, but also faithfully follow and fulfill the requirements prescribed by the protocol specifications at the semantic level. Failure to do so could lead to compatibility issues and damage the security guarantees intended by the original design. In this talk, I will discuss how to use symbolic execution to analyze semantic correctness of protocol implementations. The main intuition is that, while symbolic execution faces scalability challenges, it provides a systematic means of exploring possible execution paths and a formula-based abstraction, both of which are useful in finding semantic level implementation flaws. In many cases, scalability challenges can be avoided with concolic inputs carefully crafted by exploiting features of the input formats used by target protocols. I will first present our recent work on analyzing implementations of X.509 certificate validation. Our analysis of 9 small footprint TLS libraries has uncovered 48 instances of noncompliance, as well as some inaccurate claims in a previous work based on fuzzing. I will then present our most recent work on analyzing implementations of PKCS#1 v1.5 RSA signature verification, and explain how some of the implementation flaws we found can lead to new variants of the Bleichenbacher-style low-exponent RSA signature forgery.

About the Speaker

Sze Yiu Chau is a PhD Candidate at Purdue University, Department of Computer Science, working with Prof. Ninghui Li and Prof. Aniket Kate. His research interest is mainly on the (in)secure design and implementation of widely deployed systems and network protocols. In particular, he and his colleagues have investigated exploitable weaknesses in many popular content delivery apps on Android, as well as the robustness of X.509 certificate validation and RSA signature verification implemented in various open source software, which led to the discovery of many vulnerabilities with varying degrees of severity. Prior to joining Purdue, Sze Yiu received his BSc in Information Technology from The Hong Kong Polytechnic University, Department of Computing, with First-class honours.

All are welcome!