Transparent Computing Systems Enabled by Program Analysis

Shiqing Ma
Purdue University

3/26/2019 at 10:30 am
CoRE A 301

Abstract

Modern computing systems are complex and opaque, which is the root cause of many security and software engineering problems. In enterprise level system operations, this leads to inaccurate and hard-to-understand attack forensics results. In deep learning systems, such opaqueness prevents us from understanding the misclassifications and improving the model accuracy. Hence, there is a pressing need for improving the transparency of these systems to help us solve the corresponding security and software engineering problems.

In this talk, I will focus on my research efforts of developing novel program analysis techniques to improve the transparency of such systems and their applications in attack forensics and deep learning systems. For attack forensics, I will first describe a compiler-based execution partitioning technique MPI which helps accomplish accurate, semantics-rich and multi-perspective attack forensics. For deep learning systems, I will introduce novel state differential analysis and input selection techniques to analyze deep learning model internals for addressing the misclassification problem. Finally, I will briefly present my ongoing and future work on intelligent systems (i.e., systems that combine traditional computing components and artificial intelligent components).

Bio

Shiqing Ma is a Ph.D. candidate in the Department of Computer Science at Purdue University, co-advised by Professors Xiangyu Zhang and Dongyan Xu. His research interests lie in solving security and software engineering problems via program analysis techniques with a focus on improving the transparency of modern computing systems. He is the recipient of two Distinguished Paper Awards at ISOC NDSS 2016 and USENIX Security 2017.

Faculty Host: Desheng Zhang