Transparent Computing in the AI Era

Shiqing Ma
Department of Computer Science
Rutgers University
March 9, 2022
11:30am EST
https://osu.zoom.us/j/93335718858?pwd=V1lPNm9tZnA5VHJtV0NKLIeyK3JBdz09

Abstract: Recent advances in artificial intelligence (AI) have shifted how modern computing systems work, raising new challenges and opportunities for transparent computing. On the one hand, many AI systems are black boxes and have dense connections among their computing units, which makes existing techniques like dependency analysis fail. Such a new computing system calls for new methods to improve its transparency to defend against attacks against AI-powered systems such as Trojan attacks. On the other hand, it provides a brand-new computation abstraction, which features data-driven computation-heavy applications. It potentially enables new applications in transparent computing, which typically involves large-scale data processing. In this talk, I will present my work in these two directions. Specifically, I will discuss the challenges in analyzing the deep neural network for security inspection and introduce our novel approach in examining Trojan behaviors. Later, I will talk about AI can help increase the information entropy of large security audit logs to enable efficient lossless compressed storage.

Biography: Shiqing Ma is an Assistant Professor in the Department of Computer Science at Rutgers University, the State University of New Jersey. He received his Ph.D. in Computer Science from Purdue University in 2019. His research focuses on program analysis, software and system security, adversarial machine learning, and software engineering. He is the recipient of Distinguished Paper Awards from NDSS 2016 and USENIX Security 2017.