Learning to Reason: Accelerating System Security through joint Statistical and Formal Learning

Speaker: Dr. Tian Lan and Dr. Guru Venkataramani
Electrical and Computer Engineering Department
George Washington University
Friday, April 5, 2019
2-3PM, T3

Abstract

Identifying vulnerabilities in software systems is crucial to minimizing the damages that result from malicious exploits and software failures. This often requires proper identification of vulnerable execution paths that contain program vulnerabilities or bugs. However, with rapid rise in software complexity, it has become notoriously difficult to identify such vulnerable paths through exhaustively searching the entire program execution space. In this talk, we present a joint (statistical-formal) learning based inference methodology, that is used in an automated Statistics-Guided Symbolic Execution framework to integrate the swiftness of statistical inference and the rigorousness of symbolic execution techniques. This novel method helps to achieve precision, agility and scalability in vulnerable program path discovery. We evaluate our approach on four real-world applications including polymorph, CTree, Grep and thttpd that come from diverse domains. Results show that our methodology is able to assist the symbolic executor, KLEE, in identifying the vulnerable paths for all of the four cases, whereas pure symbolic execution fails in three out of four applications due to memory space overrun.

Biography

Dr. Tian Lan is is an associate professor of ECE at George Washington university in Washington, DC. He received the B.A.Sc. degree from the Tsinghua University, and the Ph.D. degree from the Princeton University. His research interests include cloud/edge computing, network optimization, and cyber security. Dr. Lan received the 2008 IEEE Signal Processing Society Best Paper Award, the 2009 IEEE GLOBECOM Best Paper Award, and the 2012 INFOCOM Best Paper Award, and GWU Hegarty Award for faculty in innovation.
Dr. Guru Prasadh Venkataramani is an associate professor of electrical and computer engineering at George Washington University in Washington, DC. He obtained his PhD from Georgia Tech, and his current research interests are in computer architecture and security. He is a recipient of NSF Career Award, ORAU Ralph E. Powe junior faculty enhancement award, best poster award in PACT’11, GWU Hegarty Award for faculty in innovation. His research has been funded by NSF, ONR and SRC. He served as one of the two General Chairs for IEEE HPCA 2019, and is a senior member of both IEEE and ACM.