Machine Learning for Advanced Computer Security Threats and Defenses

Dr. Sai Manoj P D
George Mason University

Monday, March 4, 2019
11:00 am – 12:00 pm
Showcase Room, Research Hall

Abstract:

The increasing complexity of modern computing systems has promised enhanced processing capabilities, but has also resulted in the growth of security vulnerabilities, making such systems an appealing target for evolving sophisticated cyber attacks such as malware and side channels. While the malware can infect the system to leak or perform unauthorized activities, the side-channel attacks rely on the side-channel information such as timing to decrypt the secret information. On the other hand, advancements in the field of machine learning (ML) led to its adoption into numerous applications ranging from computer vision to security. To address the latency and inefficiencies of software-based malware detection techniques, hardware-assisted malware detection (HMD) technique has emerged as a panacea. HMD techniques utilize the microarchitectural event information obtained through hardware performance counters (HPCs) fed to ML classifiers to detect and classify a given application as benign or malware. HMDs are resource efficient and performs detection at a faster rate than software-based detection. In this talk, the issue of limited number of available HPCs to make the HMD feasible for runtime malware detection is addressed. Further, the techniques on how the ML can be utilized to craft attacks that can bypass even the sophisticated HMD techniques is introduced. Similarly, a shield against side-channel attacks is introduced. In order to craft sophisticated malware, an adversarial attack is introduced by exploiting the HMD systems to tamper the security by introducing the perturbations in the HPC traces with the aid of the proposed adversarial sample generator application. In addition, this talk also introduces how ML can be utilized for securing the computing systems against side-channel attacks through the proposed Entropy-Shield, a defense for timing-based side-channel attacks such as Flush+Reload. In contrast to the existing defenses that focuses on architectural changes or perturbing cache lines, the proposed Entropy-Shield primarily focuses on minimizing the entropy of the side-channel information obtained by the attacker without interfering with the original functionality of the victim application.

Short Bio:

Dr. Sai Manoj P D is currently a research assistant professor at Department of Electrical and Computer Engineering at George Mason University. He has nearly 3 years of experience as a post-doctoral researcher (2years in TU Wien Austria and ~1 year in GMU). He obtained his PhD from Nanyang Technological University (NTU) Singapore, and Masters from International Institute of Information Technology Bangalore (IIITB), India. His current research interests include computer architecture security, IoT security, adversarial machine learning, neuromorphic computing and secure SoC design. His work has been well received in top tier conferences and journals such as ACM/IEEE DAC, ICCAD, CICC, ESWEEK, Trans. CAS-I, Trans. CAD, and Trans. Computers. One of his papers got nominated for best paper award in DATE 2018, his team has won Xilinx open hardware competition (held across Europe) in 2017, master thesis offered by him (in collaboration with

Austrian Institute of Technology (AIT)) got selected for best thesis award in TU Wien 2017, IMS student paper finalist in 2015, and A. Richard Newton Young Research Fellow award.