Temple University
College of Engineering

Fall Seminar Series
Department of Electrical and Computer Engineering

Wednesday, October 12, 2022
Noon – 1:00 PM EST

https://temple.zoom.us/j/94146176080

Machine Learning for Detection and Evaluation of Hardware-oriented Attacks

Professor Han Wang

Electrical and Computer Engineering

Abstract: The emerging, more sophisticated hardware-oriented attacks impact a diverse range of computing platforms, from edge to cloud continuum, threatening computer systems owned by individuals, organizations, or governments. Compared with software-oriented malware, hardware-oriented attacks demand more dedicated detection and defense approaches beyond upgrading since they exploit hardware vulnerabilities. The emerging Internet of Things, heterogeneous hardware accelerators, and the shift to cloud services for computation-intensive workloads worsen the situation further. Among all hardware-oriented attacks discovered in the past several years, side-channel attacks (SCAs) present the most threats due to their stealthy execution, lack of physical attacking evidence, and passive nature. In this talk, I will first present our solution that investigates the security challenges at its foundation: the hardware level, as the dynamic behavior of the system, including the program itself, is visible at this level. This hardware-based approach includes developing effective machine learning-based detection with hardware features. Then I will talk about machine learning vulnerabilities in the face of sophisticated side-channel attacks, including the leakage of label information. Finally, I will outline future work around hardware-oriented attacks, emerging applications, and diverse computation platforms.

Biography: Han Wang is an assistant professor in the Department of Electrical and Computer Engineering, Temple University. She received her Ph.D. from the University of California Davis, under the supervision of Prof. Houman Homayoun. Her research interests lie in side-channel attacks, machine learning, embedded system, and Internet-of-Things. In particular, she has been working on developing machine learning algorithms for effectively detecting microarchitectural attacks, proposing lightweight defense mechanisms to protect the computer system from attacks exploiting hardware vulnerability, and security assessment of emerging applications like deep learning in the face of hardware-oriented attacks. She is also one member of the Intel-sponsored Noyce research project for the security and privacy of AI-enabled IoT Eco-Systems. She has been published in top conferences and journals, including DATE, ICCAD, NDSS, ICCD, and JETCAS. She is a recipient of the DAC Young Student Fellowship in 2018 and Intel-sponsored Noyce fellow since 2021.