NJIT

Department of Computer Science

Security Vulnerabilities in Modern Computing Hardware: Causes and Consequences

Yanan Guo
University of Pittsburgh

Hosted by Cong Shi

Date: Wednesday, February 14, 2024
Coffee: 10:45 AM – 11:00 AM
Time: 11:00 AM – 12:00 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=m232c0193928796f16a9d0e9961a762b5

Abstract:

Computing hardware typically prioritizes performance and efficiency, treating security as a secondary concern. Unfortunately, this leaves the door open for extremely potent security threats. Adversaries have been exploiting hardware features to extract sensitive data from software systems for the past two decades. Recently, this issue has further escalated with new hardware developments that aggressively push the performance optimization boundaries, resulting in even the most securely designed software systems being compromised.

In this talk, I will present two significant security vulnerabilities introduced by recent developments in modern CPUs. In the first part, I will demonstrate that the special-purpose prefetch instructions in CPUs can lead to new cache side channels that are highly efficient and accurate. In the second part, I will show that the design of CPU frequency scaling can compromise existing defense strategies against hardware attacks. Finally, I will provide an overview of my future research plans towards developing more secure computing systems.

Bio:

Yanan Guo is a PhD candidate in Electrical and Computer Engineering at the University of Pittsburgh, advised by Prof. Jun Yang. Yanan's research interests lie in computer architecture and systems security. She has studied a variety of topics, including microarchitectural side channels, memory encryption and authentication, and memory safety vulnerabilities. Her research has made significant contributions to enhancing the understanding of security in commodity processors, particularly from companies such as Intel, AMD, and Nvidia. Her work has appeared at top-tier computing venues including S&P, MICRO, and HPCA, and has recently been shortlisted for the Top Picks in Hardware and Embedded Security 2023.