NJIT

Department of Computer Science

Proactive and Adaptable Architecture for Security and Performance

Samira Mirbagher Ajorpaz,
Postdoctoral Scholar, UC San Diego

Hosted by Przemyslaw Musialski

Date: Wednesday, March 9, 2022
Time: 11:00 AM to 12:00 PM
WebEx: https://njit.webex.com/njit/j.php?MTID=m5e4aa816695b66ee0a057e8394d55c77

http://cs.njit.edu/seminars

Abstract:
Cost of global cybercrime grows by 15% per year. The average cost of a data breach was 3.86 million USD in 2020. The average time to identify a data breach is 280 days. There are 100 Zettabytes of data in the clouds, but the vulnerability does not end there. In 2018, with the disclosure of transient microarchitectural attacks, we learned that every processor currently in use is insecure. These new microarchitectural attacks are inherently different from previous security threats, as they exploit the foundations of processor performance. Patching these hardware vulnerabilities from software reduces computing speed by half. Securing the system for each variant of these attacks individually is untenable due to the cumulative performance overhead. Hardware patches are expensive and must wait for a new generation of processors to be built. Hardware response, lagging behind such security threats, offers attackers years of opportunities that have not been possible before. In this talk, we will explain a proactive and adaptable architecture as a solution to the current state of security and performance. We will describe machine learning techniques to enable robust proactive and adaptive defenses, as well as solutions to several important challenges of application of machine learning in processors for security and performance.

Bio:
Dr. Junqiao Qiu is an assistant professor in the Department of Computer Science at Michigan Technological University. He received his Ph.D. in the Computer Science and Engineering Department at University of California Riverside in 2020 under the supervision of Prof. Zhijia Zhao. His research interests are broadly in the area of parallel computing, compiler techniques, and systems. He is a recipient of UC DYP Award, UC Riverside Dean's Distinguished Fellowship, and Best Paper Award at ASPLOS'20. Samira Mirbagher Ajorpaz is a postdoctoral scholar and UC Fellow in the Computer Science and Engineering Department at the University of California San Diego. Before this, she was a postdoctoral researcher at Texas A&M University, where she also received her PhD in Computer Science in 2019. She is interested in making computation faster and more secure. Her focus is on microarchitecture and designing prediction units with small-scale and tight-time margins. She is also drawn to teaching leadership and service roles in her university

and research communities. She has served on the Program Committee of
top-tier conferences in computer architecture. She taught Graduate Machine Learning at Texas A&M University and Advanced Microarchitecture at UC San Diego. Her recent publication on improving Virtual Address Translation was selected for the IEEE-Lance-Stafford-Larson Award 2021.
Her publications have appeared in ISCA and MICRO. She is known in industry for inventing the PerSpectron; microarchitectural level attack detection.