CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar



"Confidential Computing and Trusted Execution Environment: Challenges, Opportunities, and the Future"

Professor Mengyuan Li

Assistant Professor, USC

Monday, June 9th
11:00-12:00 p.m.
Location: EH 2430

Abstract:

Confidential Computing, or Trusted Execution Environment (TEE), represents a cutting-edge design in server-grade CPUs. This technology acts as a protective shield for cloud tasks, safeguarding the confidentiality and integrity of cloud workloads against a range of threats, including attacks from privileged software, physical attackers, and untrustworthy hypervisors. As the demand for secure private data handling continues to rise, the adoption of Confidential Computing has become widespread across various industries. Evidence of this includes the adoption of TEE in server-grade CPUs from major vendors like Intel, AMD, and ARM. Furthermore, leading cloud service providers, such as AWS, Google Cloud, Microsoft Azure, and IBM Cloud, now offer commercial Confidential Computing services. In this talk, I will outline my contributions to the study of complex, heterogeneous Confidential Computing systems. I will share my insights into two real-world vulnerabilities we uncovered within commercial Confidential Computing systems, along with our joint efforts with CPU manufacturers to address these issues in the latest server-grade CPUs. At the hardware design level, I will discuss a novel ciphertext side-channel attack targeting hardware-accelerated memory encryption, which is a crucial hardware feature to protect the memory of cloud workloads. Moving to the software system design level, I will illustrate how inadequately designed TEE operating systems can pose a threat to the security of Confidential VMs. Finally, I will outline my ongoing efforts and future directions in enhancing the security and effectiveness of Confidential Computing and my research vision towards building secure and performant hardware systems.

Biography:

Dr. Mengyuan Li is an Assistant Professor of Computer Science at the University of Southern California (with a courtesy appointment in the ECE department) . Before joining USC, he was a postdoctoral researcher at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL). He holds a Ph.D. from Ohio State University and a bachelor's degree from Shanghai Jiao Tong University. His research vision is to contribute to the creation of a secure and trustworthy computing environment where private data and programs are well protected. In pursuit of this vision, his research interests include system security and privacy, cloud security, Trusted Execution Environments, confidential computing, CPU security, micro-architectural security, GPU security, and AI security. He has published over 20 papers at leading security and privacy conferences, including IEEE S&P, Usenix Security, and CCS, and holds multiple technology patents.

Hosted By: Prof. Zhou Li