VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Shih-Lien (Linus) Lu
WSU Everett
Hardware Security
Nov. 27, 2023, 3:10 – 4PM Pacific
Team Link: Click here to join the meeting
Meeting ID: 240 564 196 072| Passcode: tHaY5j
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 162 752 447#

Abstract:

Hardware forms the foundation of information technology. Without secure hardware, there is no guarantee of any secure and trusted information system. Hardware security encompasses a wide range of topics and areas of study, making it a complex and expansive field. In this presentation we will first give an overview of the hardware stack, its design process and why it is so challenging to ensure hardware security. Then we will discuss a type of vulnerability called microarchitectural side channels, which are a class of security vulnerabilities that exploit the implementation of microarchitectural components in modern processors. These attacks are particularly insidious because they allow attackers to extract or communicate information from a system without exploiting software bugs, malware, or compromised login credentials. This presentation will provide an overview of the cause of microarchitectural side-channel vulnerability and will examine a few examples and how to take advantage of them. We will conclude by exploring potential strategies to mitigate such vulnerabilities and generally ensure hardware security.

Bio:

Shih-Lien is a Professor at the School of Electrical Engineering and Computer Science at WSU Everett campus. He taught at Warner Pacific University from 2021 to 2023 as the sole faculty in Cybersecurity while on leave without pay from PieceMakers Technology Taiwan, where he was the Chief Solutions Officer. He was a Director at Taiwan Semiconductor Manufacturing Company (TSMC) from 2016 to 2021. From 1999 to 2016, he was with Intel Corp., first as a research scientist, a research group manager, and then the Director of Memory Architecture Lab in Intel Labs. He served on the faculty of the ECE Department at Oregon State University as an Assistant Professor from 1991 to 1995 and as a tenured Associate Professor until 2001. From 1984 to 1991, he worked on the MOSIS project at USC/ISI, which provides US research and education community VLSI fabrication services. His research interests include computer architecture, memory circuits & technology, and hardware security. An IEEE Fellow, Shih-Lien received his B.S. in Electrical Engineering and Computer Science from UC Berkeley and M.S. and Ph.D. both in Computer Science and Engineering from UCLA.

WASHINGTON STATE UNIVERSITY
MONTANA STATE UNIVERSITY
University of Idaho
CWU