DISTINGUISHED WEBINAR SERIES IN ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

Artificial Intelligence Applications for Microarchitectural Side-Channel Attacks

Featuring Dr. Berk Gulmezoglu

Assistant Professor of Electrical and Computer Engineering

Iowa State University

Abstract:

Side-channel attacks are the art of exploiting unintended leaks—like timing, power, or sound—to uncover secrets your system never meant to share. Microarchitectural attacks are specialized side-channel attacks where attackers exploit the underlying hardware design features through fine-grained timing measurements. In the last decade, the diversity of microarchitectural attacks affecting x86 systems has tremendously increased, leading to hardware security issues. The increasing number of side-channel traces and the complexity of hardware/software components have pushed attackers to integrate Artificial Intelligence (AI) models into their attacks.

In this talk, Dr. Gulmezoglu will summarize various applications of AI in microarchitectural attacks and defense approaches. I will start by explaining the usage of the first instances of machine learning applications and continue with the latest AI models for microarchitectural attacks and defenses. Next, I will talk about our AutoEncoder and Transformer-based attack and defense techniques for Spectre and Website Fingerprinting attacks. I will conclude my talk with future research directions for both AI and microarchitectural attacks, including explainability of AI models and LLMs.

Biography:

Dr. Gulmezoglu is an Assistant Professor of Electrical and Computer Engineering at Iowa State University. He is currently associated with the Center for Cybersecurity Innovation & Outreach (CyIO). He founded the Microarchitecture and Artificial Intelligence (MAIS) Lab at ISU. His research focuses on (1) microarchitectural attacks, (2) applications of AI in cybersecurity, and (3) secure hardware design. He received B.S. and M.S. degrees Electrical and Electronics Engineering from Ihsan Dogramaci Bilkent University, Turkey, in 2012 and 2014, respectively. He received his PhD in Electrical and Computer Engineering from Worcester Polytechnic Institute in 2020.

DATE:
Thursday, Jan. 9th, 2025

TIME:
11:00-11:50 a.m. CST

LOCATION:
Virtual

Webinar LINK:
Join Directly

The **Distinguished Speaker Webinar Series** is aimed to advance the state-of-the-art concepts and methods in artificial intelligence and cyber security areas. The series is jointly hosted by the Center for Cyber Security Research (C2SR), the Artificial Intelligence Research (AIR) Initiative, and the School of Electrical Engineering and Computer Science (SEECS) at the University of North Dakota College of Engineering & Mines with support from University of Minnesota, North Dakota State University, University of Miami, Texas A&M Kingsville, University of Connecticut and West Virginia University.

For inquires please contact UND.C2SR@und.edu

Center for Cyber Security Research
College of Engineering & Mines
University of North Dakota

Artificial Intelligence Research Initiative
College of Engineering & Mines
University of North Dakota

University of Minnesota
University of Miami
University of Connecticut
NDSU North Dakota State University
Texas A&M University Kingsville
West Virginia University