Computer Science & Engineering Spring Lecture Series 2023

UCONN UNIVERSITY OF CONNECTICUT

Speaker: Wujie Wen, Assistant Professor, ECE Department, Lehigh University

Date: Tuesday, March 21, 2023
Time: 12:00-1:00 EST
Location: UConn Library Conference Room 1102
Webex: https://uconn-cmr.webex.com/meet/cdc19010

Title: A New Paradigm of Efficiency, Security and Privacy by Design for Smart Data Processing

Abstract: Fueled by the proliferation of sensing data and the advancement of machine learning (ML), intelligence is becoming a household brand from cloud to edge, transforming today's Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) applications. While enticing, current smart data services, such as machine learning as a service (MLaaS) on cloud, face multifaceted challenges. This includes incapable of guaranteeing the low end-to-end latency, the trustworthiness of ML inference, and the confidentiality of clients' sensitive data. In this talk, I will address these issues by presenting a new paradigm of designing efficient, secure, and private ML-enabled smart data processing. The talk starts with the rethinking of data compression design ("DeepN-JPEG") to ease the communication latency bottlenecking the edge-cloud collaborative inference, followed by "CryptoGCN"-the very first effort to facilitate and accelerate Homomorphic Encryption (HE)-based private graph convolutional neural network (GCN) inference. I will share our key finding from this study, which is to significantly decrease the memory and computation footprint needed in costly HE operations by orchestrating ciphertext encoding, sparse matrix operations and model architecture design based on GCN's unique computing pattern. Then I will briefly introduce "Neuropots"- the very first cross-layer real-time proactive defense framework centered around the novel concept of "Multi-Purposed Neuron", for protecting ML inference execution on hardware against the emerging fault injection attacks at extremely low-cost. The prospects on the research along this direction will be also given at the end of this talk, offering the audiences an alternative thinking about efficiency, security and privacy by design tailored to smart systems.

Bio: Wujie Wen is an assistant professor in the Department of Electrical and Computer Engineering (ECE) at Lehigh University. He received his Ph.D. from the University of Pittsburgh in 2015. He earned his B.S. and M.S. degrees from Beijing Jiaotong University and Tsinghua University, Beijing, China, in 2006 and 2010, respectively. He was an assistant professor in the ECE department of Florida International University, Miami, FL, during 2015-2019. His research interests include efficient, reliable, and secure computing, design automation, as well as their applications to embedded, IoT, medical and Cyber-Physical Systems. His works have been published widely across venues in design automation, security, machine learning/AI etc., including DAC, ICCAD, DATE, HPCA, ICPP, USENIX Security, ACSAC, HOST, NeurIPS, CVPR, ECCV, AAAI etc. He received best paper nominations from all 4 major electronic design automation conferences-DAC, ICCAD, DATE and ASP-DAC. Dr Wen served as the General Chair and Technical Program Chair of ISVLSI 2018 and 2019, respectively, as well as program committee for many conferences such as DAC, ICCAD, DATE, HPCA etc. He is an associated editor of Neurocomputing and IEEE Circuit and Systems (CAS) Magazine. His research projects are sponsored by NSF, AFRL and Florida Center for Cybersecurity etc.