Announcing the Final Examination of Shayan Taheri for the degree of Doctor of Philosophy

Time & Location: April 28, 2020 at 10:00 AM in N/A -virtual Zoom
Title: Secure and Trustworthy Hardware and Machine Learning Systems for Internet of Things

The rapid growth and employment of Internet of Thing (IoT) devices and systems including mobile phones, portable devices, and remote sensor network systems have imposed new challenges for security and energy efficiency. These challenges target software and hardware parts of IoT devices with focusing on lightweight computation and improved security. This means developing new methods to make the devices and the systems secure and energy efficient for the software or the hardware layers. In this dissertation work, we studied the design and development of various attacks and defenses for hardware and software, specifically the artificial intelligence (AI)-based elements in the systems. We described the intersections of cybersecurity with hardware and AI. These intersections need to be explored for the sake of making information and data secure and privacy protected with less energy consumption. The security of hardware originates from the outsourcing of integrated circuits (ICs) fabrication process that introduces a wide range of attacks. We developed various methods to ensure hardware security on ICs, especially for mixed-signal analog-to-digital converters. In addition, the security of AI comes from leveraging the applicable methods in detection and classification of the abnormal data. An AI system is able to learn from the data and perform their defensive actions. The AI systems can also be the target of attacks including adversarial examples and neural network Trojan. Regarding on defending the AI system, a new architecture using cycle generative adversarial network (GAN) is proposed in this dissertation to make the victim neural network robust against adversarial examples. Computer simulation results are provided to demonstrate the effectiveness of our proposed architecture and defense.

Major: Electrical Engineering

Educational Career:
Bachelor of Science, B.Sc., 2013, Shahid Beheshti University
Master of Science, M.Sc., 2015, Utah State University

Committee in Charge:
Jiann-Shiun Yuan, Chair, Department of Electrical and Computer Engineering
Azadeh Vosoughi, Department of Electrical and Computer Engineering
Rickard Ewetz, Department of Electrical and Computer Engineering
Ulas Bagci, Department of Electrical and Computer Engineering
Wei Zhang, Department of Computer Science

Approved for distribution by Jiann-Shiun Yuan, Committee Chair, on April 13, 2020.

The public is welcome to attend.