UCF

COLLEGE OF ENGINEERING
AND COMPUTER SCIENCE

FINAL ORAL EXAMINATION

OF

Shayan Taheri
BS, Shahid Beheshti University, 2013
MS, Utah State University, 2015

for the degree of

DOCTOR OF PHILOSOPHY
IN ELECTRICAL ENGINEERING

April 28, 2020, 10:00 AM
HEC 450

Dissertation Committee:
Dr. Jiann-Shiun Yuan, Chairman Jiann-Shiun.Yuan@ucf.edu
Dr. Azadeh Vosoughi azadeh@ucf.edu
Dr. Rickard Ewetz Rickard.Ewetz@ucf.edu
Dr. Ulas Bagci bagci@crcv.ucf.edu
Dr. Wei Zhang wzhang.cs@ucf.edu

DISSERTATION RESEARCH IMPACT

This dissertation includes three different major areas that are mentioned along with their impacts according to the following: (1) the analog and mixed-signal integrated circuits are prevalent in electronic systems and products similar to their digital counterparts that improves processes in the sensing and communication mechanisms in the industry as well as the military. We target analog to digital converters that are included in this category of circuits. (2) the Internet of things (IoT) is a collection of many interconnected objects, services, humans, and devices from diverse areas, including industry, military, and commercial that can communicate, share data, and information to achieve a common goal in different areas and applications. We propose a biometric recognition system suitable for this type of connectivity. (3) Anomaly detection is an important tool for many applications, namely fraud detection, network intrusion detection, industrial damage detection, medical and public health, military surveillance, image processing, anomaly detection in text data, sensor networks, and so forth. We present detection of adversarial examples that are included in this category of anomalous data.

SELECTED PUBLICATIONS & PATENTS

Security interrogation and defense for SAR analog to digital converter, Taheri, Shayan and Lin, Jie and Yuan, Jiann-Shiun, in MDPI Electronics, 2017.

Mixed-Signal Hardware Security: Attacks and Countermeasures for Delta Sigma ADC, Taheri, Shayan and Yuan, Jiann-Shiun, in MDPI Electronics, 2017.

Leveraging Image Representation of Network Traffic Data and Transfer Learning in Botnet Detection, Taheri, Shayan and Salem, Milad and Yuan, Jiann-Shiun, in MDPI Big Data and Cognitive Computing, 2018.

Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system, Salem, Milad and Taheri, Shayan and Yuan, Jiann-Shiun, in MDPI Computers, 2019.

Razornet: Adversarial training and noise training on a deep neural network fooled by a shallow neural network, Taheri, Shayan and Salem, Milad and Yuan, Jiann-Shiun, in MDPI Big Data and Cognitive Computing, 2019.

DISSERTATION

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.

SHAYAN TAHERI