GANNON UNIVERSITY

I-HACK

Institute for Health and Cyber Knowledge

New Cyber Engineering (CYENG) Courses

GU
GANNON UNIVERSITY
College of Engineering and Business

Instructor: Dr. Shayan (Sean) Taheri

1. Hardware Security – Semester: Fall 2023

Cybersecurity has emerged as a dark side of the digital age, and the scale of the world's cybersecurity problems has become daily news. With the convergence of computing and communications, coupled with exponential increase in data volume in Internet, it remains a rising and critical concern. Hardware plays an increasingly important and integral role in cybersecurity, with many emerging system and application vulnerabilities rooted in hardware. The complex supply chain introduces myriad security issues in hardware, including malicious changes, information leakage, side-channel attacks, counterfeiting, reverse engineering, and piracy activities. The topic of hardware security encompasses wide-ranging security and trust issues, which span the entire lifecycle of electronic hardware, and all its abstraction levels (chips, printed circuit boards - PCBs, systems, and system of systems). With increasing security vulnerabilities and trust issues, the role of hardware as a trust anchor of a computing system is being challenged. This course aims to provide holistic hardware security training and education to upper-level undergraduate engineering students. Also, it can serve as a useful reference for graduate students, security researchers, and practitioners, and also industry professionals, including design engineers, security engineers, system architects, and chief security officers. It contains material on the background of modern computing systems, followed by description of security issues and protection mechanism. The major parts of this course are: (a) Background on Electronic Hardware; (b) Hardware Attacks: Analysis, Examples, and Threat Models; (c) Countermeasures Against Hardware Attacks; and (d) Emerging Trends in Hardware Attacks and Protections.

2. Physical Assurance for Electronic Systems – Semester: Spring 2024

Increased complexity and globalization of the electronics supply chain has made hardware security a critical nationwide necessity. Over the past decade, physical inspection of electronics has grown significantly and is becoming a major focus for chip designers, original equipment manufacturers, and system developers. The long, complex lifespans of modern electronic devices, coupled with their diverse applications, render them increasingly vulnerable to various forms of malicious threats. Efforts of large, global industry and government to address such supply chain security problems involve offering solutions, training, and services. Although much focus is given to the digital domain, analog parameter-based physical assurance, inspection of electronics, and physical fingerprinting are rapidly providing opportunities for unique countermeasures. This course details the principles of invasive, non-invasive, and semi-invasive physical inspection techniques and their roles in hardware assurance from chip to system level.

3. CAD for Hardware Security – Semester: Fall 2024

Emerging hardware security vulnerabilities are menacing since it is almost impossible to amend the design after fabrication. Recent studies reported vulnerabilities, including side-channel leakage, information leakage, access control violations, malicious functionality, etc. Software-level security mechanisms can easily bypass these attacks and put the devices or systems at risk. However, there is a lack of automation in the existing techniques, and they rely on manual approaches that are neither efficient nor scalable for complex designs. The semiconductor industries are looking for automatic computer-aided design (CAD) tools for design verification and validation that efficiently increase the design accuracy with minimal testing time. The hardware engineers examine the security features by utilizing the CAD tools to aid analysis, identifying, root-causing, and mitigating system-on-chip (SoC) security problems to ensure the trustworthiness of the design. This course attempts to cover the utilization of CAD tools in hardware security. Its scope presents a comprehensive summary of hardware security defenses, describes the fundamentals of CAD tool usage, and highlights the significant research results.

4. Artificial Intelligence for Cybersecurity – Semester: Spring 2025

Organizations today are spending billions of dollars globally on cybersecurity. Artificial Intelligence (AI) has emerged as a great solution for building smarter and safer security systems that allow you to predict and detect suspicious network and hardware activities, such as phishing or unauthorized intrusions, in your network/hardware. This course presents and demonstrates the popular and successful AI approaches and models that you can adopt to detect potential attacks and protect your corporate systems. You will understand the roles of machine learning (ML) and neural networks (NNs) as well as deep learning (DL) in cybersecurity, and learn how you can infuse AI capabilities when building smart defensive mechanisms. As you advance, you will be able to apply these strategies across a variety of applications, including spam filters, network intrusion detection, hardware Trojan detection, side-channel analysis, botnet detection, and secure authentication. The course makes you ready to develop intelligent systems that can detect unusual and suspicious patterns and attacks, thereby developing strong network and hardware security defenses using artificial intelligence.

ONLINE | https://www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

CALL | +(1) (814) 871-5331

EMAIL | taheri001@gannon.edu

GANNON
UNIVERSITY

Believe in the possibilities.