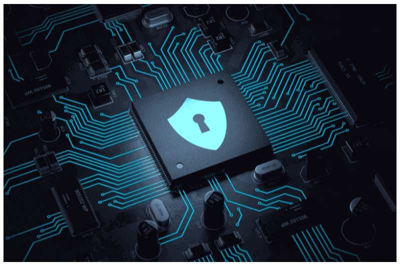
CSC2231: Topics in Computer Systems: Secure Computer Systems & Hardware

Instructor: Prof. Gururaj Saileshwar

Prerequisites:

- Undergraduate Computer Organization (e.g., CSC258, CSC385 or equivalent)
- OR Graduate Computer Architecture (e.g., CSC2224HF or equivalent)
- Introductory Operating Systems (CSC369 or equivalent)

Overview:



Trustworthy computer systems require protection from not just software vulnerabilities but also hardware vulnerabilities. In recent years, numerous hardware vulnerabilities have emerged leaving software systems open to exploitation: notable examples include processor speculation attacks, like Spectre and Meltdown, Cache Side-Channel attacks, and DRAM Rowhammer attacks. These attacks enable malicious software to extract sensitive data from systems or tamper critical data and even seize control of entire systems.

This course will discuss various aspects of hardware and micro-architectural security. Students will gain a thorough understanding of micro-architectural attacks, such as Spectre and Rowhammer, and learn to develop proof of concepts of such exploits on real systems. At the same time, we will also discuss micro-architectural defenses to thwart these exploits. We will also cover topics like side-channel attacks, trusted execution environments, and memory safety.

The lecture material for this course will be derived from the research papers published in security (USENIX Security, IEEE S&P) and computer architecture (ISCA, MICRO, HPCA, ASPLOS) conferences. The course will include hands-on programming assignments and students will also undertake a mini-research project to hone their expertise in secure computer architecture.

Tentative List of Topics:

- **Module-1: Micro-architectural Attacks and Defenses**
  - DRAM Rowhammer Attacks (fault model, attacks like PT-Hammer, RAMBleed, EccPloit, emerging counter-based defenses, randomization-based defenses)
  - Cache Side-Channel Attacks and Defenses (different types of attacks, cache template attacks, randomization-based defenses, partitioning based defenses)
  - Transient-Execution Attacks (Spectre, Meltdown, variants, and defense)
  - Other Side-Channels (power-based, memory contention, port-contention)

- **Module-2: Trusted-Execution Environments in Hardware**
  - **Commercial Proposals**
    - Isolation-Based Approaches (ARM TrustZone)
    - Enclave-Based Approaches (Intel SGX/Sanctum)
    - Virtual-Machine Based Approaches: (AMD SEV, Intel TDX)
    - GPU-Based Confidential Computing (NVIDIA Hopper CC)

- **Academic Proposals**
  - Techniques to reduce metadata overheads (Synergy, Morph).
  - Extensions to GPU (Graviton, HETEE)

- **Module-3: Memory Safety in Software**
  - Vulnerabilities & Exploits (Spatial/Temporal safety, Return-Oriented Programming)
  - Software solutions (Rust, Java, ASAN, Softbound, Control-Flow Integrity)
  - Hardware solutions (Capability computing, CHERI, REST, ARM MTE, AOS)
  - Memory Safety for GPUs

- **Module-4: Other topics (if time permits)**
  - Ransomware & Hardware-Based Defenses
  - Data-Oblivious Computation (constant-time, data-oblivious ML, Morpheus)
  - Obfuscated RAM (Basic design, principles, and techniques to reduce overhead)
  - Hardware-Trojans (problem, detecting and defeating backdoors)

Course Grading (Tentative):

- Two Mid-term exams (during class time): 15% each
- Three Programming Assignments: 30%
- Reviews of Research Papers: 10%
- Research Project (Report and Presentation): 30%

There will be a mix of traditional lectures plus a discussion of research papers. The midterm will test knowledge of the lecture material and the assigned papers. The assignments will be programming-based and use a mix of architectural simulators for modeling defenses and coding up micro-architectural attacks on real systems. The paper reviews will focus on papers on security and will be selected from the computer architecture (ISCA, MICRO, HPCA, ASPLOS) and security (IEEE S&P, USENIX Security) conferences.