CS7292: Reliability and Security in Computer Architecture

3:30 pm - 4:45 pm, MW

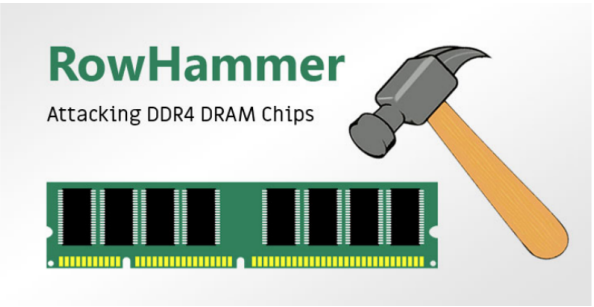
Meeting link for office hours (or remote lectures, if any):
https://bluejeans.com/8070165133

Instructor Information

Instructor	Email	Office Hours & Meeting Link
Moin Qureshi	moin@gatech.edu	2pm-3pm, Tuesday https://bluejeans.com/8070165133
Co-Instructor		
Gururaj Saileshwar	gururaj.s@gatech.edu	2pm-3pm, Thursday https://bluejeans.com/6546523909

Prerequisite: CS6290 or ECE6100 (can be taken together with instructor permission)

Overview :



Building trusted computer systems require that the system is protected from both adversarial attacks and naturally occurring errors. In this course, we will discuss different aspects of hardware security, hardware reliability, and (sometimes) the interplay between the two. As systems become more complex, there are new modes of security vulnerability emerging, such as *Row-Hammer* and *Transient-Execution* attacks, and the defense for these continues to be broken by newer attacks. Furthermore, Ransomware attacks are causing havoc in critical infrastructure, and there are new privacy concerns emerging as users integrate new ML-based models in their daily lives. In this course, we will discuss classical topics (such as side-channel, trusted execution environment, and memory safety) along with the new and emerging threats. The lecture material for this course will be derived from the research papers published in architecture and security conferences. As part of this course, the students will also do an independent research project.

TOPICAL OUTLINE:

HARDWARE-SECURITY

Row-Hammer (fault model, attacks PT-Hammer, RAMBleed, EccPloit, defense & pitfalls)

Cache Side-Channel (different types of attacks, cache Template attacks, defense)

Other Side/Covert Channels (power-based, memory contention DRAMA, port contention)

Transient-Execution Attacks (Spectre, Meltdown, variants, and defense)

Trusted-Execution Environment (SGX and ARM TrustZone, techniques to reduce overheads)

Memory Safety (capability-based computing, CHERI, REST, Califorms, AOS)

Obfuscated RAM (Basic design, principles, and techniques to reduce overhead)

Data-Oblivious Computation and Randomization (constant-time, Ghost-Rider, Morpheus)

Ransomware Attacks (attack phases, detection schemes, ransomware-tolerant SSDs)

Hardware-Trojans and Counterfeits (problem, detecting and defeating backdoors)

ML Model-Security and User-Privacy (model stealing, cache telepathy, Slalom, DarKnight)

HARDWARE-RELIABILITY

Error Detection and Correction (parity, checksum, CRC, ECC, TMR, RAID)

Tolerating Limited Endurance (wear leveling, adversarial patterns, lifetime reduction attacks)

Retention Failures (DRAM refresh, AVATAR, new memory technologies, tradeoffs)

Processor Reliability (AVF analysis, DIVA, redundant multi-threading)

Course Grading:

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 will use architectural simulators. The paper reviews will focus on papers on security and reliability and will be selected from the architecture and security conferences.

Grading Scale

The default plan is to assign your final letter grade according to the standard scale below. However, the cutoffs for certain letter grades may be lowered based on the instructor's discretion. For example, if your total course grade is 90% or higher, you are guaranteed to receive an A. And if the cutoff is lowered to 88%, all students who received course grades of 88% or higher will receive an A. However, no cutoff will be raised relative to the standard scale below:

A 90-100%,
B 80-89%,
C 70-79%,
D 60-69%

Office of Disability Statement: https://disabilityservices.gatech.edu/

Academic Honor Code:
http://www.policylibrary.gatech.edu/student-affairs/academic-honor-code

Institute Absence Policy: http://www.catalog.gatech.edu/rules/4/