ECE 592-096 Secure Processor Architecture

Instructor(s): Dr. Amro Awad (ajawad@ncsu.edu)

Objective or Description: help students understand the recent advances in both hardware attacks and architectural defenses and support in modern processor architectures. The course will cover advanced topics such as trusted execution environments, side-channel attacks, memory safety hardware support, memory security (integrity and confidentiality, access control and other emerging topics.

Prerequisites: basic understanding of computer architecture (ECE563)

Textbook:

Topics:

- Threat Models in Different Confidential Computing and Secure Environments
  - Threat Model in ARM's TrustZone and ARM's CCA
  - Threat Model in Intel's SGX and Intel's TME
  - Threat Model in RISC-V's Keystone
  - Threat Model in AMD's SEV, AMD's SEV-SNP, and AMD's SME
- Basics in Security Primitives and Constructs Implementations
  - Memory Encryption
    - Direct Encryption
    - Counter-Mode Memory Encryption
  - Memory Integrity Verification
    - Merkle Tree
    - Tree-of-Counters
    - Caching and Update Schemes of Integrity Trees
- Access Control Implementations and Challenges
- Hardware-Support for Memory Safety
- State-of-the-art side-channel attacks

Grading: the course will have 30% midterm, 40% final exam, and 30% project
+/- grading will be used