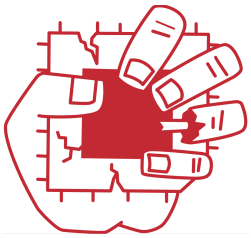
ECE 792-059
Performance and Security Analysis of Advanced Microarchitecture



Instructor: Samira Mirbagher Ajorpaz, smirbag@ncsu.edu

Description:

Microarchitecture has a security crisis. Features that are essential for performance, such as speculative execution, have been shown to cause devastating vulnerabilities. The community has recognized the need for preemptive security analysis of new performance features. This course first examines the use and design of advanced/ML-assisted prediction in microprocessors and then explores the security implications of state-of-the-art techniques that improve performance.

Processors use different kinds of predictors and resource sharing, providing improved performance and efficiency. Examples include multi-threading, conditional branch prediction, indirect branch prediction, predictive cache management policies (i.e., instruction or data replacement/prefetching), value prediction, speculative vectorization, MLP-aware fetch policy, storage-free memory dependency prediction, fat-loads, branch runahead, etc. We will learn about the development of such state-of-the-art microarchitecture designs as well as the use of machine learning for systems performance and security. We will also investigate the impact of recent side-channel exploits on several units of microarchitecture (BP, BTB, TLBs, i-cache, d-cache, data memory-dependent prefetcher, microarchitecture buffers, etc.) and the trade-off between security and performance, as well as adversarial machine learning attacks on ML-assisted microarchitecture and their defenses, including hardware design equipped with machine learning-based detection units for high performance and security.

Through this course, students acquire hands-on knowledge about performance and security opportunities of applying advanced techniques and ML for systems and are expected to be able to reason about the security of as-of-yet unimplemented performance enhancing features of microarchitectural designs and their potential defenses.

Prerequisites: ECE 563

Textbook: None. Journal and conference papers will be the source material for most discussions.

Topics: The course covers advanced design of microarchitectural units for performance and microarchitectural attacks targeting (1) caches, (2) branch prediction, (3) prefetching, (4) replacement policy, (5) multi-threading (TLBs), (6) coherency protocol, (7) microarchitectural buffers (MDS attacks), (8) adversarial attacks using ML in HW (9) injection-based attacks (LVI) and their (10) defenses in HW and SW.

Grading: TBD