Title: Memory Defenses -- the Elevation from Obscurity to Headlines

Abstract: Recent attacks like Meltdown and Spectre have highlighted that modern processors are likely being shipped with latent vulnerabilities that are impossible to anticipate. Some of these vulnerabilities can be addressed with various hardware defenses. Meltdown and Spectre may have finally pushed these defenses from the shadows of academia into possible commercial reality.

This talk will describe three primary vulnerabilities in the memory system, and efficient hardware defenses to address each of these vulnerabilities. The first vulnerability is leakage of a program's memory intensity through memory controller timing channels. The second is leakage of a program's memory access pattern through exposed DDR buses. The third is a violation of memory integrity by a malicious cloud operator or malicious OS. In fact, modern Intel SGX systems already have support for guaranteed memory integrity and we show how the performance of that solution can be improved by nearly 4X.

Speaker Bio: Rajeev Balasubramonian is a Professor at the School of Computing, University of Utah. He received his B.Tech in Computer Science and Engineering from the Indian Institute of Technology, Bombay in 1998. He received his MS (2000) and Ph.D. (2003) degrees from the University of Rochester. His primary research interests include memory systems, security, and application-specific architectures, and his work appears regularly at the top architecture conferences. Prof. Balasubramonian is a recipient of a US National Science Foundation CAREER award, an IBM Faculty Partnership award, an HP Innovation Research Program award, an Intel Outstanding Research Award, various teaching awards at the University of Utah, and multiple best paper awards.