**Title**: Looking Beyond Microarchitectural-Only Side Channels

**Speaker**: Joseph Ravichandran, PhD Student, MIT

**Abstract**:

Modern systems are becoming increasingly complex, exposing a large attack surface with vulnerabilities in both software and hardware. Today, it is common for security researchers to explore software and hardware vulnerabilities separately, considering these vulnerabilities in disjoint threat models. In this talk, I will discuss the importance of considering a broader threat model when studying microarchitectural side channels and looking beyond microarchitecture-only side channels. A broader threat model considers the combined effects of exploiting vulnerabilities residing in different system layers. I will use a few examples to demonstrate how a broader threat model can help advance our hardware security research in multiple ways.

**Bio**:

Joseph Ravichandran is a PhD student at MIT studying microarchitectural security in Dr. Mengjia Yan's lab. He has extensive experience in binary exploitation and reverse engineering, developing the PACMAN attack against pointer authentication on the Apple M1 chip and discovering and patching a novel Linux kernel vulnerability. He has given talks at ISCA, an ICML workshop, and DEF CON.