ABSTRACT: In computer systems, manufacturing variances and hardware effects are typically abstracted away by the software layer. This dissertation explores how these effects, specifically memory remanence, can be used both as an attack vector and a tool to defend emerging computing systems.

To achieve this, we show how time-keeping, anonymity, and authenticity can be affected by memory remanence. In terms of attacks, we explore the deanonymizing effect of Approximate Computing in the context of approximate memory in Probable Cause. We show how any data passing through an approximate memory will be watermarked with a device specific tag that can point the attacker back to the device. In terms of defenses, we first present TARDIS; an approach to provide a notion of time for transiently powered embedded devices without requiring any hardware modification using remanence effect of SRAM. TARDIS allows for these devices to keep a coarse-grained notion of time without the need for a running clock. Second, we propose data retention voltage of memory cells as a new type of physical unclonable function that allows for low-cost authentication and counterfeit resistance in computer systems.

Advisor: Prof. Atul Prakash