Title: Anti-virus hardware: Exploring the new domain in system security.

Abstract: Anti-virus software (AVS) tools are used to detect Malware in a system. However, software-based AVS are vulnerable to attacks. A malicious entity can exploit these vulnerabilities to subvert the AVS. Recently, hardware components such as Hardware Performance Counters (HPC) have been used for Malware detection. In this talk, we will discuss HPC-based techniques for improving system security and privacy. Subsequently, we will discuss their pitfalls. Finally, we will present PREEMPT, a zero overhead, high-accuracy and low-latency technique to detect Malware by re-purposing the embedded trace buffer (ETB), a debug hardware component available in most modern processors. The ETB is used for post-silicon validation and debug and allows us to control and monitor the internal activities of a chip, beyond what is provided by the Input/Output pins. PREEMPT combines these hardware-level observations with machine learning-based classifiers to pre-empt Malware before it can cause damage. We will conclude the talk with future research directions and challenges.