Title: A Primitive for Revealing Stealthy Peripheral-Based Attacks on the Computing Platform’s Main Memory

Abstract:
Computer platform peripherals such as network and management controller can be used to attack the host computer via direct memory access (DMA). DMA-based attacks launched from peripherals are capable of compromising the host without exploiting vulnerabilities present in the operating system running on the host. Therefore they present a highly critical threat to system security and integrity. Unfortunately, to date no OS implements security mechanisms that can detect DMA-based attacks. Furthermore, attacks against memory management units have been demonstrated in the past and therefore cannot be considered trustworthy. We are the first to present a novel method for detecting and preventing DMA-based attacks. Our method is based on modeling the expected memory bus activity and comparing it with the actual activity. We implement BARM, a runtime monitor that permanently monitors bus activity to expose malicious memory access carried out by peripherals. Our evaluation reveals that BARM not only detects and prevents DMA-based attacks but also runs without significant overhead due to the use of commonly available CPU features of the x86 platform.