Deniz Aytemiz

April 18th Paper Summaries

1. Applying the Principle of Least Privilege to System Management Interrupt Handlers with the Intel SMI Transfer Monitor

   SMM is a privileged CPU mode on Intel which is responsible for low level hardware control. SMM code can access memory and registers of operating systems. Its privileged broad access creates vulnerabilities for attackers. Intel created SMI Transfer Monitor(SMT) tool in order to monitor potential vulnerabilities of SMM.
   In this paper, the description of STM design and its performance is quantized and discussed. Possible SMM-based attacks and their countermeasure policies are exemplified. It is found that STM has fine-grained protections with within limits latency costs.It also provides isolated execution of workload that advantages partitioning malicious code from the workload.

2. PANOPLY: Low-TCB Linux Applications with SGX Enclaves

   Intel SGX is a security measure in CPUs which allows user level applications to run in hardware isolated environments called enclaves. Enclave memory is isolated from the rest of the software, even OS and hypervisor. In this paper authors present the PANOPLY system which supports applications in enclaves, preserving high-level guarantees. PANOPLY provides an abstraction called micron which consists of code and data in an isolated enclave unit. They expose standard POSIX abstraction to application logic. PANOPLY impose integrity in inter enclave interactions ensuring legitimate data and control flow is processed. In this paper its usage in-real world applications and evaluation of its performance in contrast with previous systems are given. It is stated that with respect to previous systems it archives 2 orders of magnitude lower TCB.