Dynamic Software Application Protection

Authors: Ravi Sahita, Ulhas Warrier and Prashant Dewan. Intel Corporation

Sophisticated malware attacks rising at an alarming rate can undermine the trust users have in the security of their PC software. Attacks are not limited to web based applications, but also include targeted attacks that attempt to steal user-data from applications. Anti-virus approaches are limited to known signatures and do not address stealth malware that can subvert the OS and services that software depends on. In our research on software protection, we have created a hardware-assisted service called Processor-Measured Application Protection Service (P-MAPS) that significantly reduces the Trusted Computing Base (TCB) and improves the runtime security of applications without interrupting the operation of the application or the Operating System. With P-MAPS, attacks on critical applications by day-0 and unknown malware can be mitigated.

Overview

In the P-MAPS model, there are two states of the platform (See Figure 1). The platform starts with a commodity OS as shown in state A with the OS in the TCB. P-MAPS is started by a user launching an application that requires P-MAPS services, which results in the state of the platform as shown in state B with only the P-MAPS Core, the CPU, the verified chipset and BIOS in the TCB. Note that with P-MAPS active, the OS executes in “guest” mode. The primary goal of this work is the on-demand creation of a reduced TCB which is used to protect application memory. Protected applications can continue executing within the OS without any interruption to the OS or other unprotected applications.

P-MAPS Architecture

The P-MAPS software consists of an OS-specific P-MAPS loader, and an OS-independent P-MAPS Core (See Figure 2). The P-MAPS loader uses Intel® Trusted Execution Technology (TXT) to authenticate and boot-strap the P-MAPS Core. In Intel® TXT terminology, the P-MAPS Core is the Measured Launched Environment. (MLE).

The P-MAPS Core uses Intel® Virtualization Technology to extend the protected environment that the P-MAPS Core executes to specific applications. The P-MAPS Core executes in the highest privilege mode
(VMX root mode) which ensures hardware-enforced separation between the protected applications and itself. The P-MAPS Core provides application authentication and application memory protection from software-based attacks that attempt to tamper with application while executing. The P-MAPS Core provides 3 runtime properties for the applications it protects. First, it isolates the application’s runtime memory from other software executing on the platform (including ring-0 services). Second, it encapsulates the application data memory such that only code in the measured application pages can access the data. Finally, it prevents circumvention of any function entry-points exposed in the application code. It is important to note that P-MAPS Core does not hinder the application’s use of OS services in any way.

![Figure 2: P-MAPS high-level architecture](image)

**Remote Attestation**
A protected application typically involves handling of secret data that is provisioned by a Provisioning Entity (Server) in the network. P-MAPS can be used to provide hardware-derived quotes to a trusted remote entity. The quotes are used by the remote entity to verify that the application is indeed executing with the required hardware-derived protection. A set of trusted 3rd parties participate to enable this attestation mechanism as in a standard Public Key Infrastructure mechanism.

**Summary**
In our research proof-of-concept, we demonstrate how Intel® TXT and Intel® VT hardware capabilities can be used to reduce the TCB of current PC systems on-demand (dynamically) from the full Operating System software to a substantially smaller (~2500X) P-MAPS TCB that provides runtime protection for standard applications. We have built this system to be used to provide protection without interfering with the typical scheduling and operation of the Operating System, including unprotected applications. P-MAPS can be used for application white-listing mechanisms to protect critical applications and thus mitigate day-0 software attacks on these protected applications. We continue to analyze different applications of the P-MAPS Core.