OpenDTeX Research Project

Providing trusted building blocks to add security properties on x86 platforms

TPM 1.2 – SRTM – DRTM – Intel TXT – IOMMU – Secure Boot – Secure Enclave

Project description

This research project aims at providing trusted building blocks to ensure strong **security properties during the boot chain** and to allow **secure execution of isolated enclaves on x86** architectures.

This project leverages TCG technologies, such as **TPM** and **DRTM**, to provide trusted execution of a minimal TCB (Trusted Computing Base). Besides, each building block can display proof of integrity up to the platform user, by implementing the concept of trusted banner, thus creating a **trusted path between the user and the TCB**.

The results of this project have been integrated in a **Linux-based** prototype, as well as in the **PolyXene** multi-level security operating system.

Project context

French research project "RAPID": civil and defense use cases.

Consortium: AMOSSYS, Bertin Technologies and Telecom ParisTech.

Security model

The project implements a security model based on a **whitelist approach**, in constrast to common security products (AVs, IDS, ...) that depend on a black list approach, which have proven to expose serious weaknesses.

The security mechanisms rely upon **a minimal and verified TCB** (Trusted Computing Base), which excludes the BIOS in the context of a DRTM.

A strong hypothesis is also considered in the secure enclave use case: the administrator/user and operating system can be malicious.

Secure boot

Provides integrity measurement of boot chain and local integrity attestation, either implicitly (through unsealing operations) or explicitly (through a secret banner).

Integrity measurement at launch time

OpenDTeX supports the static chain of trust (SRTM) and measures all launch time components: BIOS, MBR, boot loader (Grub 2.0), initrd, kernel, etc.

OpenDTeX also supports the dynamic chain of trust (DRTM) and measures a minimal environment: Intel SINIT, Secure Loader (MLE), initrd, kernel, etc.

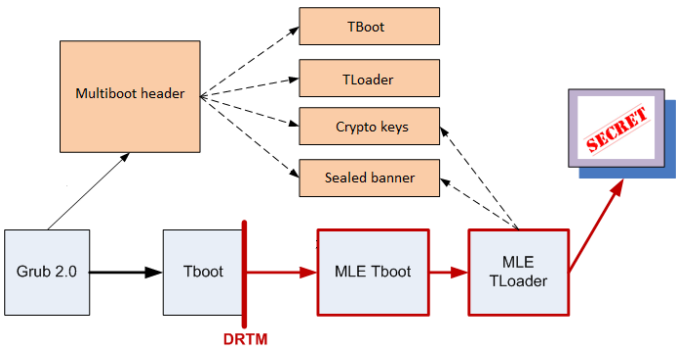
Sealing of critical components

Critical components of boot chain, such as the Linux kernel, may be unsealed when platform integrity is verified. This permits **local implicit attestation of integrity**.

Secret banner

A shared secret (either text or image), can be unsealed and shown to the user when platform integrity is verified. This permits **local explicit attestation of integrity**.

Design



Headquarters: 4 bis allée du Bâtiment • 35000 RENNES Cedex • France • www.amossys.fr

Phone: +33 2 99 23 15 79 • **Email**: etudes@amossys.fr

OpenDTeX Research Project

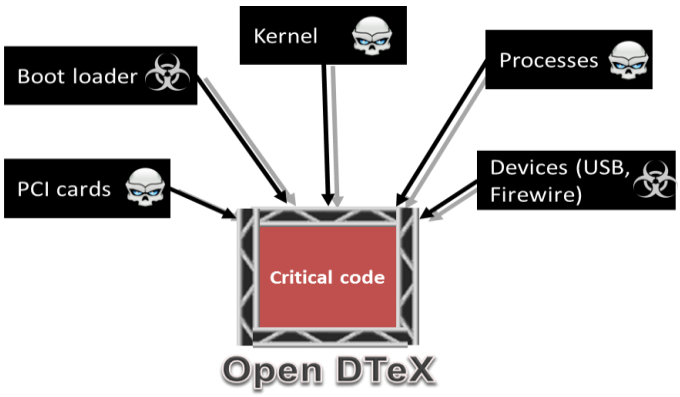
Providing trusted building blocks to add security properties on x86 platforms

TPM 1.2 – SRTM – DRTM – Intel TXT – IOMMU – Secure Boot – Secure Enclave

Secure enclave

OpenDTeX allows execution of sensitive code in a trusted environment, isolated from the operating system. This permits execution of critical operations **even if the operating system (or the administrator) is untrusted or compromised**.

Secure enclave mechanism relies on the DRTM technology, launched during OS runtime. DRTM launch sequence puts the OS in pause during execution of critical operations. Besides, critical operations are protected, in terms of integrity and confidentiality, from external DMA tampering thanks to the IOMMU chipset access control.



Use cases

Different use cases could leverage this secure enclave mechanism:

- Protection of email writing and signature in a trusted user interface
- Transmission of smart card PIN through a trusted path
- Virtual smart card/wallet
- Execution of critical code isolated from the OS or the user/administrator

Design

Integrity proofs

Both secure boot and secure enclave mechanisms are able to provide a proof of integrity up to the local platform user.

Secure banner

This is a shared secret (either a text or image only known from the user) sealed by the TPM. This shared secret is shown to the platform user if platform integrity matches the reference one (explicit local attestation).

When the shared secret is shown to the platform user, a **trusted path between the TCB and the user is thus established**. Besides, this secure banner mechanism allows to protect against the well-known "Evil maid attack": the user enters his password only after he has seen the shared secret.

Sealing of critical components

Unsealing of sensitive components provides implicit local attestation of platform integrity.

Integrity attestation with a smartphone

Platform integrity can be **attested towards an Android smartphone**, which plays the "remote" verifier role.

OpenDTeX developments

OpenDTeX work notably include:

- Development of a TPM 1.2 API library independent from the BIOS or OS
- Development of a minimal TSS API library independent from the OS
- Extension of Grub 2 (implementation of SRTM)
- Extension of TBoot (implementation of a dedicated DRTM MLE)
- **Implementation of DRTM at OS runtime**

Contact and availability

Please contact us for further information regarding any technical aspects or availability of project components.

Headquarters: 4 bis allée du Bâtiment • 35000 RENNES Cedex • France • www.amossys.fr

Phone: +33 2 99 23 15 79 • **Email**: etudes@amossys.fr