Trusted Execution Technology

Intel Trusted Execution Technology (Intel TXT) is the name of a computer hardware technology whose primary goals are (a) Attestation – attest to the authenticity of a platform and its operating system (OS); (b) assure that an authentic OS starts in a trusted environment and thus can be considered a trusted OS; (c) provide the trusted OS with additional security capabilities not available to an unproven OS.

Intel TXT uses a Trusted Platform Module (TPM) and cryptographic techniques to provide measurements of software and platform components so that system software as well as local and remote management applications may use those measurements to make trust decisions. This technology is based on an industry initiative by the Trusted Computing Group (TCG) to promote safer computing. It defends against software-based attacks aimed at stealing sensitive information by corrupting system and/or BIOS code, or modifying the platform's configuration.

Details

The Trusted Platform Module (TPM) as specified by the TCG provides many security functions including special registers (called Platform Configuration Registers - PCRs) which hold various measurements in a shielded location in a manner that prevents spoofing. Measurements consist of a cryptographic hash using a Secure Hashing Algorithm (SHA). The current TPM specification uses the SHA-1 hashing algorithm. SHA-1 is a cryptographic hash function designed by the United States National Security Agency (NSA) and published by the United States National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). A characteristic of the cryptographic hash algorithm is that (for all practical purposes) the hash result (referred to as a hash digest or a hash) of any two modules will only produce same hash value if the modules are identical.

Measurements

Measurements can be of code, data structures, configuration, information, or anything that can be loaded into memory. TCG requires that code not be executed until after it has been measured. To further protect the integrity of the measurements, hash measurements are not written to PCRs, but rather a PCR is "extended" with a measurement. This means that the TPM takes the current value of the PCR and the measurement to be extended, hashes them together, and replaces the content of the PCR with that hash result. The effect is that the only way to arrive at a particular measurement in a PCR is to extend exactly the same measurements in exactly the same order. Therefore, if any module being measured has been modified, the resulting PCR measurement will be different and thus it is easy to detect if any code, configuration, data, etc. that has been measured had been altered or corrupted.

Chain of trust

The technology supports both a static chain of trust and a dynamic chain of trust. The static chain of trust starts when the platform powers on (or the platform is reset), which resets all PCRs to their default value. For server platforms, the first measurement is made by hardware (i.e., the processor) to measure a digitally signed module (called an Authenticated Code Module or ACM) provided by the chipset manufacturer. The processor validates the signature and integrity of the signed module before executing it. The ACM then measures the first BIOS code module, which can make additional measurements. The measurements of the ACM and BIOS code modules are extended to PCR0 – said to hold the static core root of trust measurement (CRTM) as well as the measurement of the BIOS Trusted Computing Base (TCB). The BIOS measures additional components into PCRs as follows:

PCR0 – CRTM, BIOS code, and Host Platform Extensions

(Note: CRTM is measured by the processor and initial BIOS code is measured by the ACM – all other measurements made by BIOS or other firmware code – but only after that code had been measured)

PCR1 - Host Platform Configuration

PCR2 - Option ROM Code

PCR3 - Option ROM Configuration and Data

PCR4 - IPL (Initial Program Loader) Code (usually the Master Boot Record - MBR)

PCR5 - IPL Code Configuration and Data (for use by the IPL Code)

PCR6 - State Transition and Wake Events

PCR7 - Host Platform Manufacturer Control

The dynamic chain of trust starts when the operating system invokes a special security instruction, which resets dynamic PCRs (PCR17-22) to their default value and starts the measured launch. The first dynamic measurement is made by hardware (i.e., the processor) to measure another digitally signed module (referred to as the SINIT ACM) which is also provided by the chipset manufacturer and whose signature and integrity are verified by the processor. This is known as the Dynamic Root of Trust Measurement (DRTM). The SINIT ACM then measures the first operating system code module (referred to as the measured launch environment – MLE). Before the MLE is allowed to execute, the SINIT ACM verifies that the platform meets the requirements of the Launch Control Policy (LCP) set by the platform owner. LCP consists of 3 parts: (1) verifying that the SINIT version is equal or newer than the value specified; (2) verifying that the platform configuration (PCONF) is valid by comparing PCR0-7 to known-good values (the platform owner decides which PCRs to include); (3) verifying that the MLE is valid, by comparing its measurement to a list of known-good measurements. The integrity of the LCP and its lists of known-good measurements are protected by storing a hash measurement of the policy in the TPM in a protected non-volatile location that can only be modified by the platform owner.

Execute as a Trusted OS

Once the LCP is satisfied, the SINIT ACM allows the MLE to execute as a Trusted OS by enabling access to special security registers and enabling TPM Locality 2 level access. The MLE is now able to make additional measurements to the dynamic PCRs. The dynamic PCRs contain measurement of:

PCR17 – DRTM and launch control policy

PCR18 – Trusted OS start-up code (MLE)

PCR19 – Trusted OS (for example OS configuration)

PCR20 – Trusted OS (for example OS Kernel and other code)

PCR21 – as defined by the Trusted OS

PCR22 – as defined by the Trusted OS

The technology also provides a more secure way for the operating system to initialize the platform. In contrast to the normal processor initialization [which involved the boot-strap-processor (BSP) sending a Start-up Inter-Processor Interrupt (SIPI) to each Application Processor, thus starting each processor in “real mode” and then transitioning to “virtual mode” and finally to “protected mode”], the operating system avoids that vulnerability by performing a secure launch (a.k.a. measured launch) which puts the Application Processors in a special sleep state from which they are directly started in “protected mode”.

Application

PCR values are available both locally and remotely. Furthermore, the TPM has the capability to digitally sign the PCR values (i.e., a PCR Quote) so that any entity can verify that the measurements come from, and are protected by, a TPM, thus enabling Remote Attestation to detect tampering, corruption, and malicious software. Additionally, those values can be used to identify the execution environment (the particular BIOS version, OS level, configuration, etc.) and compare them to their own lists of known-good values to further categorize the platform. This ability to evaluate and assign trust levels to platforms is known as Trusted Compute Pools.

Some examples of how Trusted Compute Pools are being used:

- Isolation – the ability to control if a platform connects to the production network or is quarantined based on its trust level or failure to pass its launch control policy.
- Trust Based Policy – such as restricting critical apps to only execute on platforms that meet a specified trust level
- Compliance and Auditing – Demonstrating that critical, personal, or sensitive data has only been processed on platforms that meet trust requirements

References

External links

- Intel Trusted Execution Technology (http://www.intel.com/technology/security/)
- Trusted Execution Technology Overview (http://www.intel.com/technology/security/downloads/TrustedExec_Overview.pdf)
- Trusted Execution Technology Architectural Overview (http://www.intel.com/technology/security/downloads/arch-overview.pdf)
- Intel Trusted Execution Technology Software Development Guide (http://download.intel.com/technology/security/downloads/315168.pdf)
- Intel Virtualization Technology (http://www.intel.com/technology/virtualization/)
- GlobalPlatform white paper on standardized TEE (https://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf)

Article Sources and Contributors

Trusted Execution Technology *Source*: http://en.wikipedia.org/w/index.php?oldid=536414671 *Contributors*: Andrewpmk, André Pessoa, CecilWard, Chowbok, CitizenB, Cybercobra, DHR, Dbiagioli, Denniss, Digitaleragroup, Djechelon, Dmforcier, Dougher, DrSeehas, Frap, Gabriel Torres, GeeJo, Imroy, Jarble, Jibun, Katanzag, Kinema, Leotohill, MaxSem, Mogism, Nealmcb, None Error, Northox, Orange & Viridian, Orenburg1, Ramu50, Rchandra, Robertmh, RoyBoy, Ruud Koot, Samuelvd, Seidenstud, Soumyasch, Teddks, Terrel Shumway, Titustimuli, Wdfarmer, Zuwiki, 61 anonymous edits

License