Intel Trusted Execution Technology (Intel TXT)

Thomas Gaska
CS-680 Virtualization

Agenda

- Threats
- Trusted Computing Challenge
- Trusted Execution Technology Overview
- Protection Requirements
- Protected Execution
- Root of Trust and the TPM
- Late Launch
- The Realization in Chipsets
- What's the Future
- References

Threats

"Information Protection"

Typical Software Vulnerabilities:
- Virus, Worms, etc.
- Spyware, secret stealing
- Spam, Adware

Typical Software Exposures:
- Using unprotected regions for system code
- Buffer Overflow
- Failing to set locks

Internal misuse:
- Activity out of policy, or other unwanted

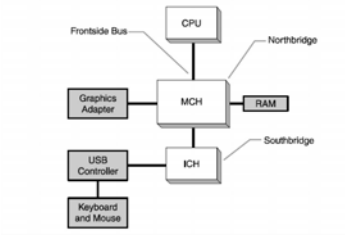
Platform-based vulnerabilities:
- Hyperjacking, rootkits
  - Blue Pill – VMM injection and system control
- BIOS and SMM-based attacks

Data or security techniques can not be compromised under any conditions

Trusted Computing

- A Trusted (Computing) Platform is a platform that is trusted by local and remote users.
- A relationship of trust must be established between the user and the computing platform so that the user believes that an expected boot process, a selected operating system, and a set of selected security functions in the computing platform have been properly installed and operate correctly.

Standard PC Computer Architecture



MCH = Memory Controller HW
ICH = I/O Controller HW

Hardware Security Context

Hardware-Based Security:

- Protected memory region provided by domain separation
- Memory protection prevents DMA engines from reading or modifying protected memory pages

Software-Based Security

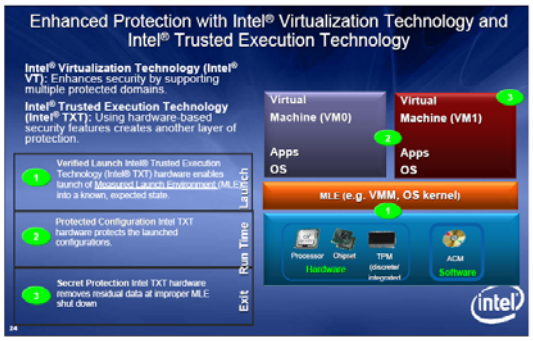
Firewall, virus scanners, encryption software and other security software can provide only so much protection from other malicious software that is running at the same or higher privilege level.

Trusted Computing Challenges

- Protected Execution – Run isolated protected execution environments
- Sealed Storage – Encrypt and store keys and secrets
- Protected Input – Encrypt I/O
- Protected Graphics – Establish a trusted channel
- Attestation – Measure software
- Protected Launch – Controlled launch and registation

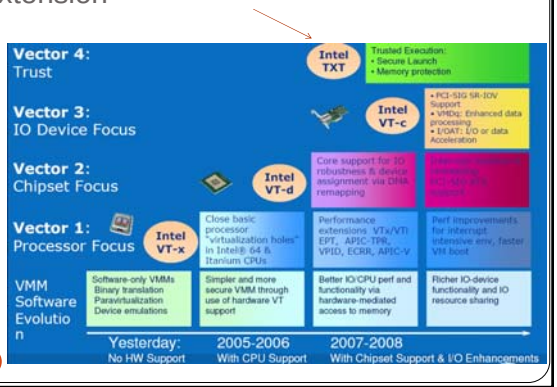
7

Hardware Assisted TXT Technology



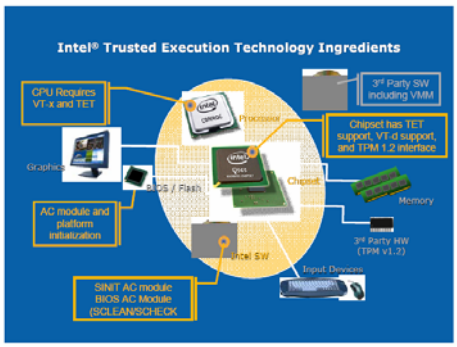
8

Another Hardware Virtualization Extension



9

TXT – TET Integrated Architecture



10

Protection Requirements

- Enable ability to assign a physical memory page to a specific VM and protect the page from other VM and DMA access
- Enable a mechanism that protects keyboard, mouse, and display data from attack while data is in transit
- Protect any secrets with a robust, long-term storage protection mechanism
- Support protection across PC platform corner cases like
  - Reset
  - Initialization
  - Power Management
  - BIOS Configuration

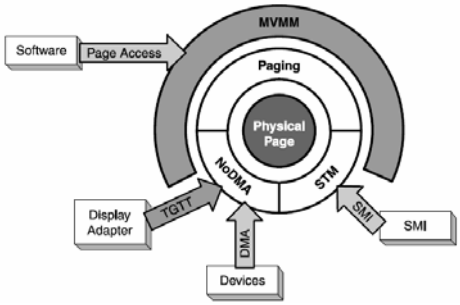
11

Resource Boundary Protections

Entity	Protection Mechanisms	Function or Activities
Physical Page	Rings and Paging	Provide protection from software processes running in the same VM
	Virtualization	Provides protection between VM guests
	NoDMA Table	Provides protection from DMA devices
	STM	Provides protection during SMI events
CPU Resources	MVMM	Protects internal CPU resources from access from VM guest or DMA access
Measurements	SMX	Extensions to ensure the correct and proper measurement of the VMM turning the VMM into a MVMM
	TPM	Provides a storage area for the measurements and a mechanism to report the measurements
Trusted Input	USB host controller or Trusted Mobile Keyboard Controller (TMKBC)	The USB host controller provides protections for messages moving from the controller to the device driver
Trusted Output	TGTT	The TGTT provides a special buffer for the display adapter to obtain display information that has protection from VM guest and DMA access

12

Page Protection Mechanisms



13

Measured Virtual Machine Monitor (MVMM)

- Measurement and Launch of a MVMM must meet the following requirements:
  - All measurement and storage of the measurement must occur prior to passing control
  - Measurement process must defend against spoofing
  - Ensure all processors run the same VMM and start at same entry point
  - No other bus masters, processors, devices, or cache snooping can subvert the VMM measurement or launch
  - No misconfiguration or misinterpretation of processor, chipset, or platform state must be able to subvert the launch
- A major feature of the MVMM is the ability to launch and terminate a Guest Partition and enforce a Policy
  - Memory Access
  - Resource Assignment and Access Virtualization
  - Communication Channel
  - Partitioning Lifecycle
- Implemented via Safer Mode Extensions (SMX)

14

Trusted Computer Group

- Open organization to "develop, define, and promote open standards for hardware-enabled trusted computing and security technologies."
- These secure platform primitives include
  - Platform integrity measurements
  - Measurement attestation
  - Sealed storage
- Can enable
  - Trusted boot (not secure boot)
  - Attestation
- Goals:
  - Ensure absence of malware
  - Detect spyware, viruses, worms, …

15

TPM and Roots of Trust

- Need
  - Roots of Trust for Measurement (RTM)
  - Root of Trust for Reporting (RTR)
  - Root of Trust for Storage (RTS)
- Solution is the Trusted Platform Module (TPM)
  - Slave Device on the LPC bus
  - Performs a set of Defined Commands
    - Validates command bit stream, each parameter, command authorization
    - Creates response packet
  - Secure Hash (SHA-1)
    - Converts string of arbitrary length to fixed length output (20 bytes)
  - 24 + Platform Configuration Registers (PCR)
    - Used to storage measurements reported to the TPM
    - PCR Extension is defined as PCR = SHA-1(PCR old value, new value)

16

TPM Capabilities

The Trusted Platform Module (TPM) is a hardware component that provides four major functions:

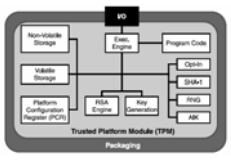
1. Cryptographic functions: RSA, (P)RNG, SHA-1, HMAC
2. Secure storage and reporting of hash values representing a specific platform configuration
3. Key storage and data sealing
4. Initialization and management functions (opt-in)

Auxiliary functions since version 1.2:

- Monotonic counters and timing-ticks
- Non-volatile storage
- Auditing

17

Trusted Processor Module (TPM)



Atmel can optionally provide personalization of the TPMs. During this process, a unique public/private key pair will be created for each TPM and stored inside.

18

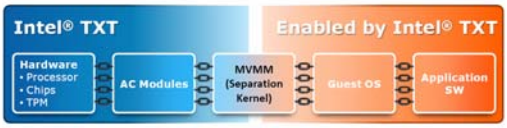
TPM Remote Attestation & Sealed Storage

- Remote attestation (PCRs + AIK)
  - Attestation Identity Keys (AIKs) for signing PCRs
  - Attest to value of integrity measurements to remote party
- Sealed storage (PCRs + SRK)
  - Protected storage + unlock state under a particular integrity measurement (data portability concern)

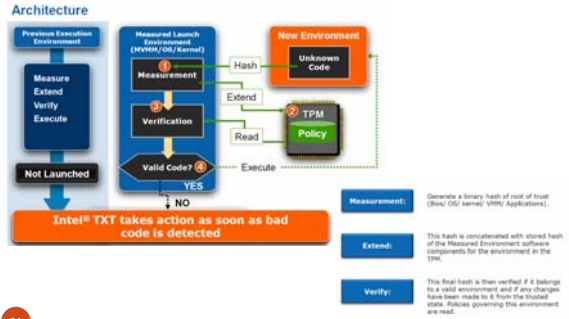
Establishing Root-of-Trust

Intel® TXT builds a chain of trust:

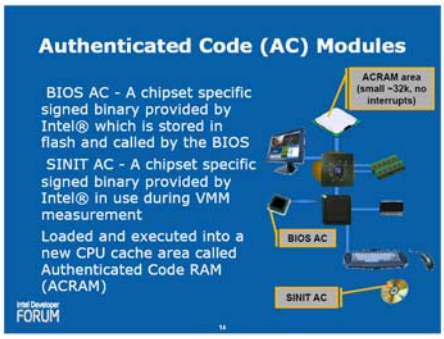
- Power-on Confidence hardware test occurs when power is switched on
- TXT-enabled BIOS prepares the environment and launches BIOS ACM
  - Micro-code built into the processor measures and authenticates the BIOS AC
  - The Root of Trust is now extended to include the BIOS AC
- SINIT AC is launched by the system loader and is used to measure, verify and launch MVMM
  - SINIT is signed by Intel's private key and the chipset has a hash of the public key
- The Root of Trust is now extended to include the MVMM



TXT Environment Enforcement

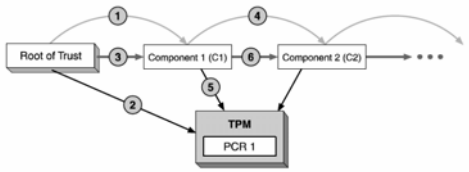


Authenticated Code Modules

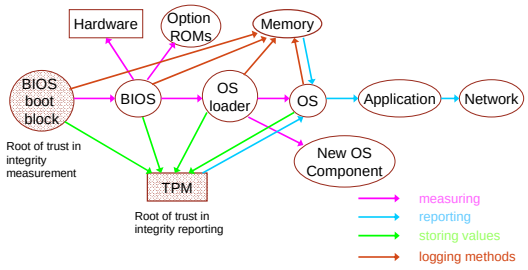


TPM Transitive Trust

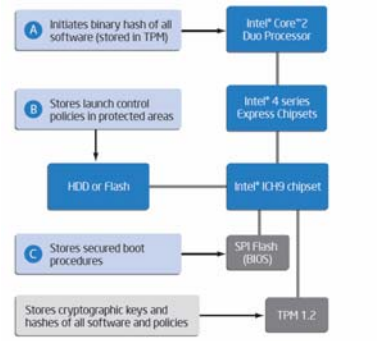
- Provide a way for relying parties to trust a larger circle of entities from a single root of trust:
  1. Measure the next entity and compute Hash
  2. Store the Hash measurement in TPM PCR
  3. Pass control to the measured entity



Bootstrap Sequence



Protected Launch Mechanism



Late Launch

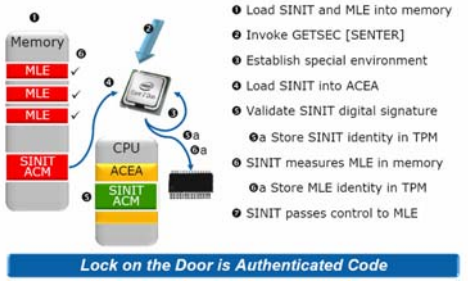
- Create a reboot without doing a complete platform reset
- Enable a Dynamic MVVM1 to MVMM2 transition after initialization at any time
  - Prepare for GETSEC [SENTER]
    - Accurately measure SENTER launch code using Hash
  - Load the MVMM using SINT-AC
  - Pass Control to the MVMM
  - Remove MVMM through GETSEC [SEXIT]
- SENTER is a disruptive event
  - Initiate protections at any time and allow for removal of the partition
  - Make sure all CPUs participate (Multicore and Hyperthreads)
  - Detect any tampering with the launch process
  - Allow multiple invocations of processed partitions without reboot
  - Ensure properly configured hardware

Launching Protected Partition Events

1. IPL loads SINIT Module and MVMM
   - Must be in Ring0, have TXT Chipset, have TPM, no machine checks
   - Controlling entity can be BIOS or OS
   - Neither SINT or MVMM have any protection against modification at this time
2. IPL invokes GETSEC [SENTER]
3. All CPUs Synchronize with ACKs
   - INT, NMI, SMI events are masked, chipset is locked except for ILP
4. IPL loads, launches, and authenticates SINT-AC
   - Chipset manufactures vouches for SINT module and generates a digital signature
   - ILP obtains Chipset Hash and compares with calculated Module Hash to authenticate
   - IPL updates TPM Dynamic PCRs for the measurement of SINIT
5. SINIT Authenticated Code invokes MVMM
   - Establish NoDMA Table
   - IPL Measures and Stores MVMM measurement to the TPM and

Late Launch Control Points

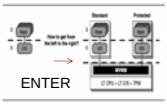
Safe Mode Extensions (SME)

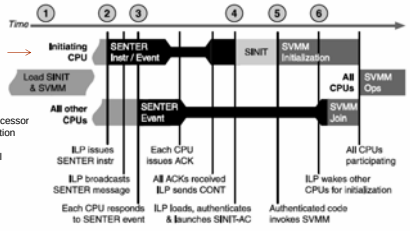


Lock on the Door is Authenticated Code

MLE = Measured Launched Environment , in my charts this is also MVMM and the SVMM

Launching the Protected Partition



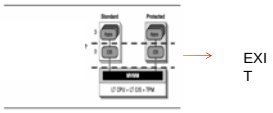


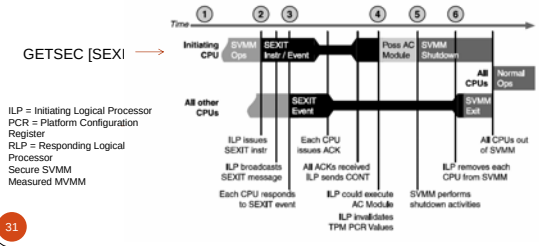
ILP = Initiating Logical Processor
PCR = Platform Configuration Register
RLP = Responding Logical Processor
CONT = SINIT-AC = Secure SVMM Measured MVMM

Exiting the Protected Partition

1. Boot Strap Processor validates the MVMM issued the command
2. Broadcast a message to rendezvous the processors
3. Ensure that all processors respond to the broadcasts
4. Shut down the MVMM
5. Remove all protections and allow normal operations

Exiting the Protected Partition





31

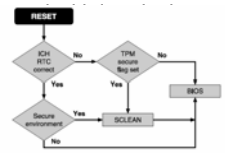
TXT System Design

- Enter VMM mode using GETSEC[SENTER] instruction, measures VMM before transferring control
  - Enables the attestation chain to that point to be discarded, giving a fresh reset. Referred to as Dynamic Root of Trust for Measurement (DRTM)
- CPU provides internal RAM that can execute code after hashing code and verifying against embedded digital signature. Enter Authenticated Code (AC) mode using GETSEC[ENTERACCS] instruction.
  - Will only run software signed by Intel using a private key corresponding to a public key in the chipset itself

32

SCLEAN

- SCLEAN AC Module provides way to remove secrets by erasing selected system memory
  - Writes a data pattern to each byte of memory
- After reset, chipset can request startup code to locate, load, and cause execution of SCLEAN
- Module is an AC Module specific to the chipset embedded in the BIOS and has no reliance on system memory
- RESET Protection is also supp
  block all accesses to system m



33

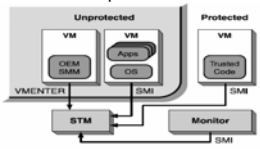
System Management Mode (SMM)

- Operating mode in which all normal execution is suspended including the operating system
  - Special separate software (firmware or a hardware-assisted debugger) is executed in high-privilege mode
- Legacy from the Intel 386 to current processors
- Some uses of SMM are:
  - Handle system events like memory or chipset error, system safety mgmt (temp, power)
  - Emulate or forward calls to a TPM
- SMM is entered via the SMI (system management interrupt), which is caused by:
  - Chipset signaling processor pin, Software SMI, I/O write operation
- By design, the operating system cannot override or disable the SMI
- SMM Vulnerability:
  - New place to hide rootkits
  - No page table means all memory is accessible
  - Hander must have the same trust level as the MVMM

34

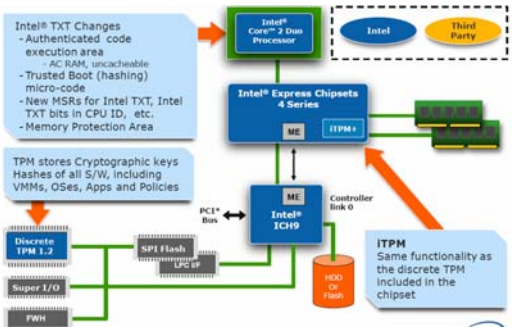
SMM Transfer Module (STM)

- Conceptual mechanism to accept the SMI, invoke the SMM, and ensure no leakage of information to the SMM
- STM requires accurate measurement, reliable storage of the measurement, and verifiable reporting of the measurement
- BIOS holds the SMM code
- Problem:
  - Measurement technique for SINIT and MVMM won't work wi
  - Open tc lat 2009



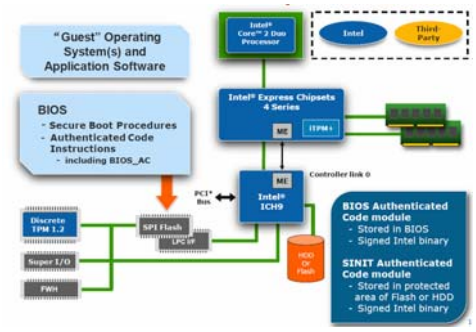
35

TXT Hardware Components

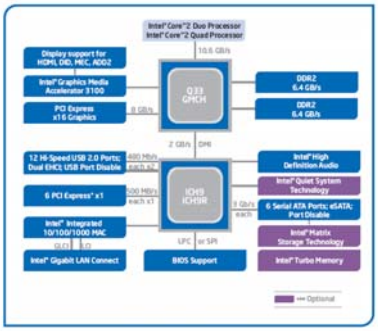


36

TXT Software Components



Q33 TXT Enhanced Chipset



Required Support For TXT Features

Procure Intel® TXT compatible platform components:
- CPU with support for SMX instructions
- Intel® Core 2 Duo Processor (such as: T9400, P8400, SP9300, SL9400, SU9300, E8400, Q9400)
- Intel TXT-enabled chipset
- Intel Express Chipsets 4 Series: (such as: PM45, GM45, GM47, GS45, Q45)
- TPM, TCG 1.2 compliant (IBL doc # 390455) to Intel specifications, available from any of the following Intel approved vendors**
  - Atmel*
  - Broadcom*
  - Infineon*
  - Sinosun*
  - STMicroelectronics*
  - Winbond*

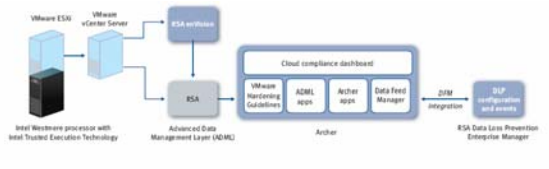
Build Intel TXT-enabled BIOS
- Intel approved BIOS vendors provide Intel TXT enabled BIOS**
  - AMI*
  - Phoenix*
  - Insyde*

Chipset Specific Authenticated Code Module (ACM)
- Available for download from Intel Validation Internet Portal for the chipset specific ACM
- https://platformsw.intel.com/

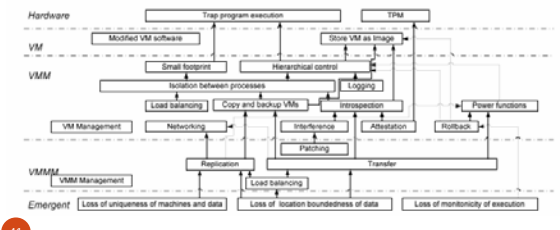
"tboot" is an open-source secure boot loader for Intel® TXT-based systems
- See http://sourceforge.net/projects/tboot

Intel® TXT reference code available for Xen* VMM
- Xen TXT patch available now
- Supports measured launch, Intel® TXT memory protection, teardown, 32/PAE/64bit modes, SMP, etc.

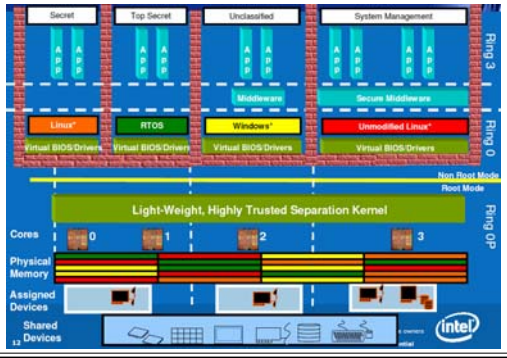
Future = Measuring/Monitoring Clouds



Virtualization Feature Dependencies



Addition of a Trusted Separation Kernel



References Beyond Base Papers

- The Intel Safer Computing Initiative

http://files.rsdn.ru/19450/SECC_100Validation.pdf

My favorite highlight was David Grawrocks section on Secure Launch Recap. He states “I do not understand why you are confused. I have been working on this for many years and do not understand why you cannot pick it up in an hour or so.” [page 208]

- Security Implications of Virtualization: A Literature Study

http://doc.utwente.nl/68164

- Infrastructure Security: Getting to the Bottom of Compliance in the Cloud

http://www.rsa.com/innovation/docs/CCOM_BRF_0310.pdf