

Virtual TPM on Xen/KVM for Trusted Computing

<http://www.rcis.aist.go.jp/project/knoppix/vmknoppix/index-en.html>

Kuniyasu Suzaki, Toshiki Yagi, Kengo Iijima, Nguyen Anh Quynh
National Institute of Advanced Industrial Science and Technology

Contents

- What is trusted computing? What is TPM?
- virtual TPM
 - Implementation models
 - Requirements for virtual machine
 - BIOS and Device Model for vTPM
 - Current Status of vTPM on Xen and KVM
- Trusted Computing for Guest OS
 - Trusted Boot and Remote Attestation
 - KNOPPIX for Trusted Computing Geeks
- Demo
 - VMKnoppix which integrated vTPM and Trusted Computing
- Future Work
- Conclusions

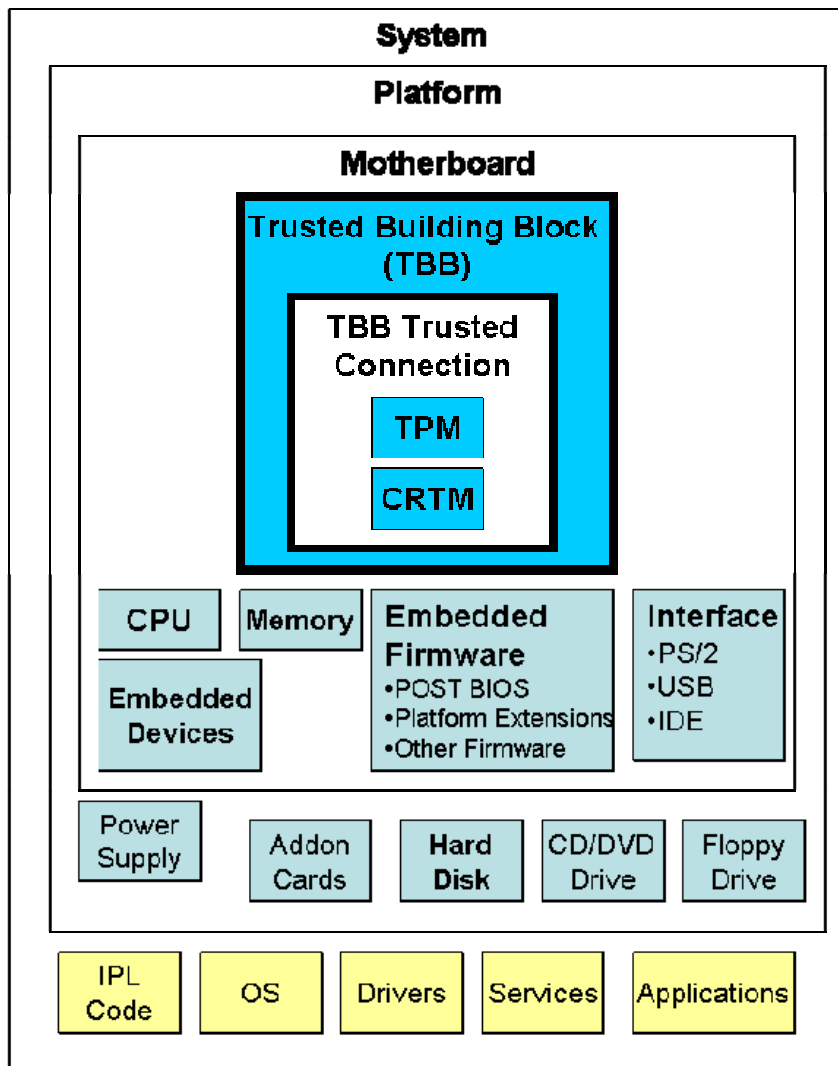
What is Trusted Computing?

- Trusted Computing is a technology to keep the integrity of operating system, which is based on a secure chip such as “TPM (Trusted Platform Module)”.
 - TPM is the hardware-rooted trust.
 - Trusted Boot keeps the “Chain of Trust” from the beginning of power.
- It is developed and promoted by the Trusted Computing Group.
 - <http://www.trustedcomputinggroup.org>
 - Organization
 - Promoter: (send directors to the TCG Board)
 - Intel, HP, IBM, Microsoft, AMD, SUN, Infineon, Lenovo, Fujitsu, Seagate, Wave Systems
 - Contributor: (propose to the organization)
 - Citrix, Phoenix, Dell, Hitachi, NEC, Panasonic, Sony, Toshiba, etc
 - Adaptor: (access selected portions of the web site)

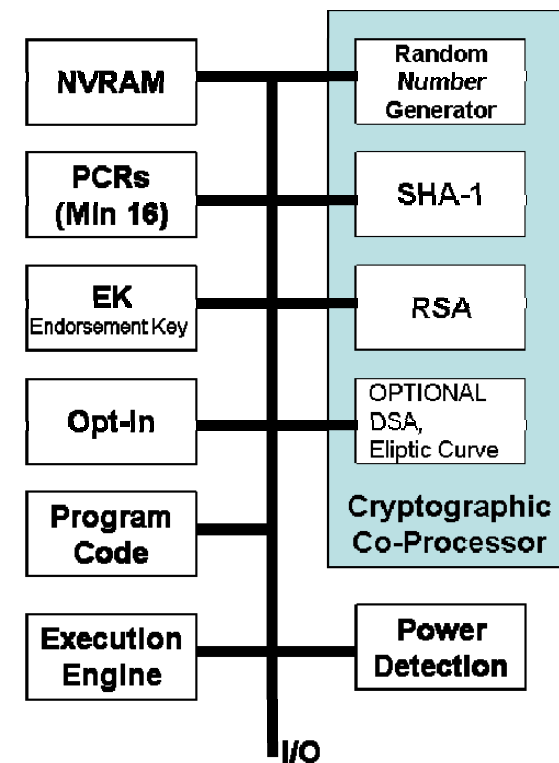


TPM (Trusted Platform Module)

PC: view from TPM



Inside TPM

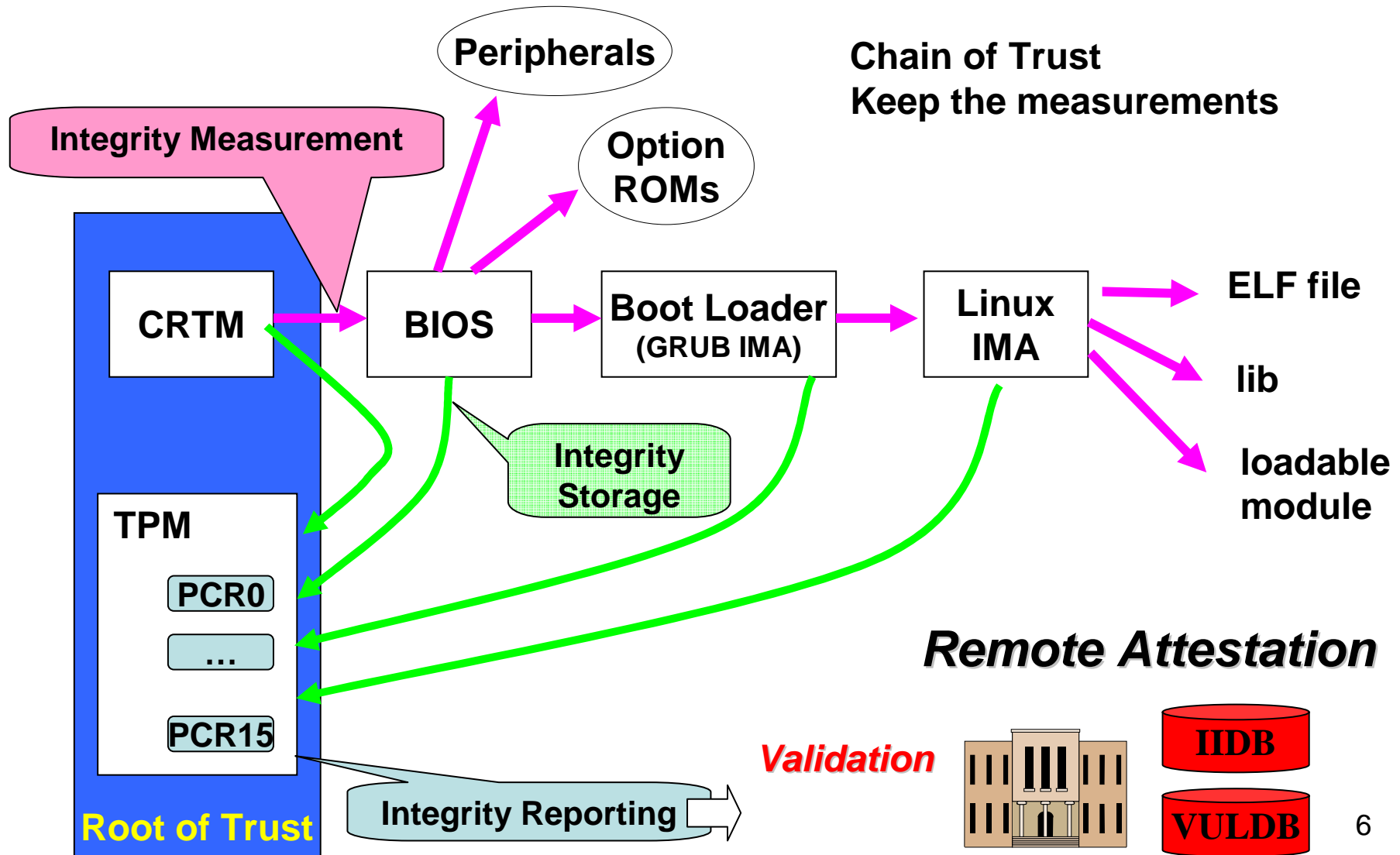


Trusted Boot (1/2)

- TPM is a passive device and has no function to control CPU.
 - The action is triggered by BIOS and the device driver.
- The components (devices and files) which is accessed at boot time are measured and their SHA-1 digest are recorded to PCR (Platform Configuration Register) of TPM with “Extend” operation.
 - **Extend**
 - **PCR=SHA-1(PCR + SHA-1(Component))**
- The usage of PCR is defined by TCG.

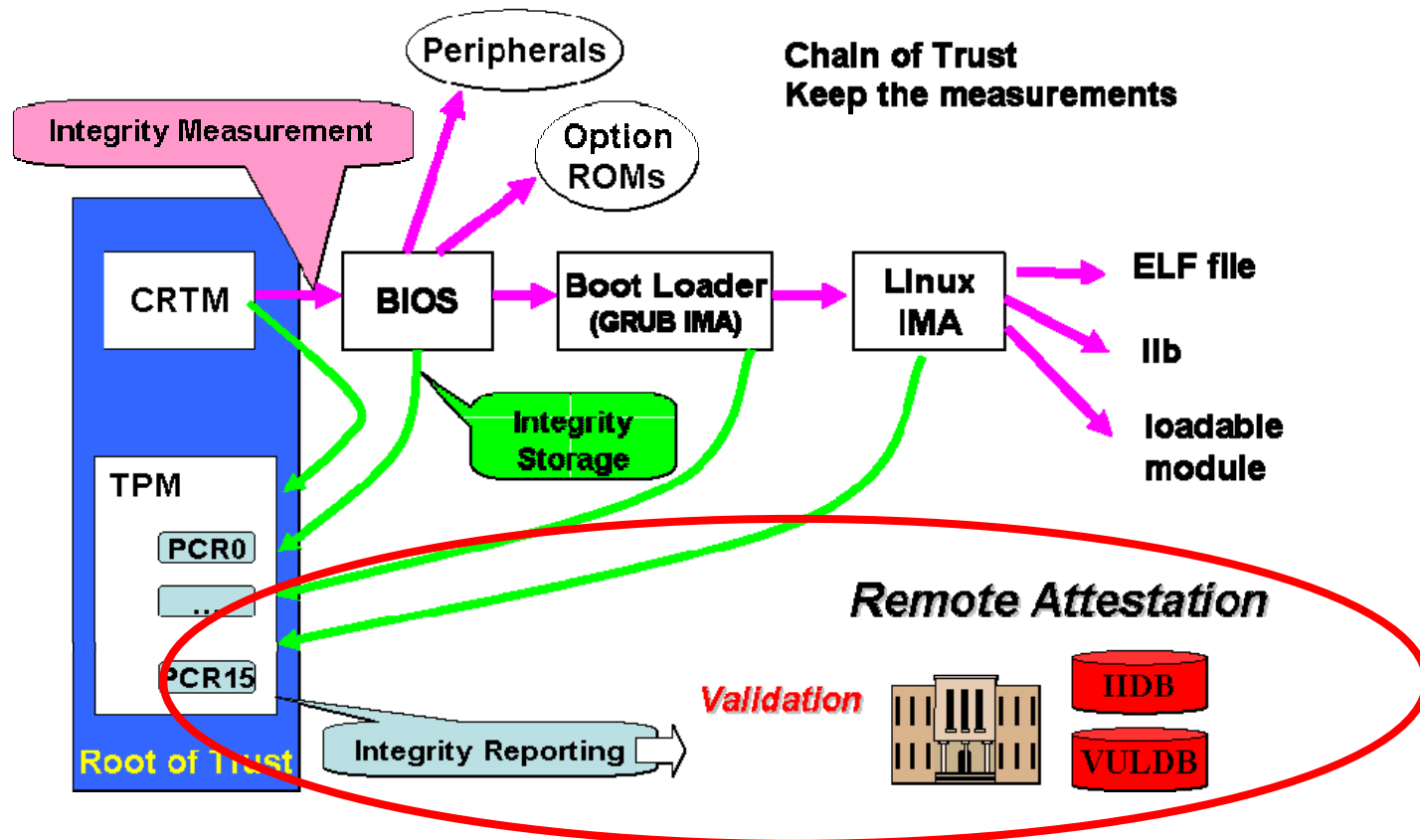
| PCR | Function |
|------|---|
| 0 | CRTM, BIOS, and Platform Extensions |
| 1 | Platform Configuration |
| 2 | Option ROM Code |
| 3 | Optional ROM Configurations and Data |
| 4 | IPL Code (Usually the MBR) |
| 5 | IPL Code Configuration and DATA (for use by the IPL code) |
| 6 | State Transition and Wake Events |
| 7 | Reserved for future usage. Don't use. |
| 8-15 | Flexible use |

The role of TPM for Trusted Boot



Trusted Boot (2/2)

- The PCR values are validated by the Trusted Third Party (Remote Attestation).
- The values of PCR are sealed by the key of the TPM.
 - It is independent of CPU.
- **Remote Attestation detects inclusion of rootkits and malware.**



Contents

- What is trusted computing? What is TPM?
- **virtual TPM**
 - Implementation models
 - Requirements for virtual machine
 - BIOS and Device Model for vTPM
 - Current Status of vTPM on Xen and KVM
- Trusted Computing for Guest OS
 - Trusted Boot and Remote Attestation
 - VMKnoppix which integrated vTPM and Trusted Computing
- Demo
- Future Work
- Conclusions

2 Implementation Models of vTPM

1. Transfer physical TPM to virtual machine
 - Keep the hardware-based root of trust.
 - (USENIX Security Symposium 06, Stefan Berger et al., IBM)
 - Unfortunately there are no open source implementation.
2. Emulate TPM by software
 - Doesn't keep the hardware-based root of trust. It is used for feasibility study.
 - Xen and KVM supports the emulated TPM.
 - TPM Emulator 0.5 (developed and maintained by ETH, Switzerland)
 - <http://tpm-emulator.berlios.de/>

View for Virtual Machine

- In order to enable vTPM, VM must support the interfaces.
 - Device Model
 - Original QEMU-DM has no TPM.
 - Physical TPM is connected to LPC bus
 - Linux kernel communicates TPM **via the device driver**
 - BIOS
 - BIOS must support TCG specification
 - CRTM (Core Root of Trust Measurement)
 - API to communicate TPM (Detail is Next Slide.)
 - » Bootloader communicates TPM **via the API of BIOS**
 - BIOS must support ACPI
 - Guest OS finds the mapped I/O of TPM by ACPI.

TCG-BIOS

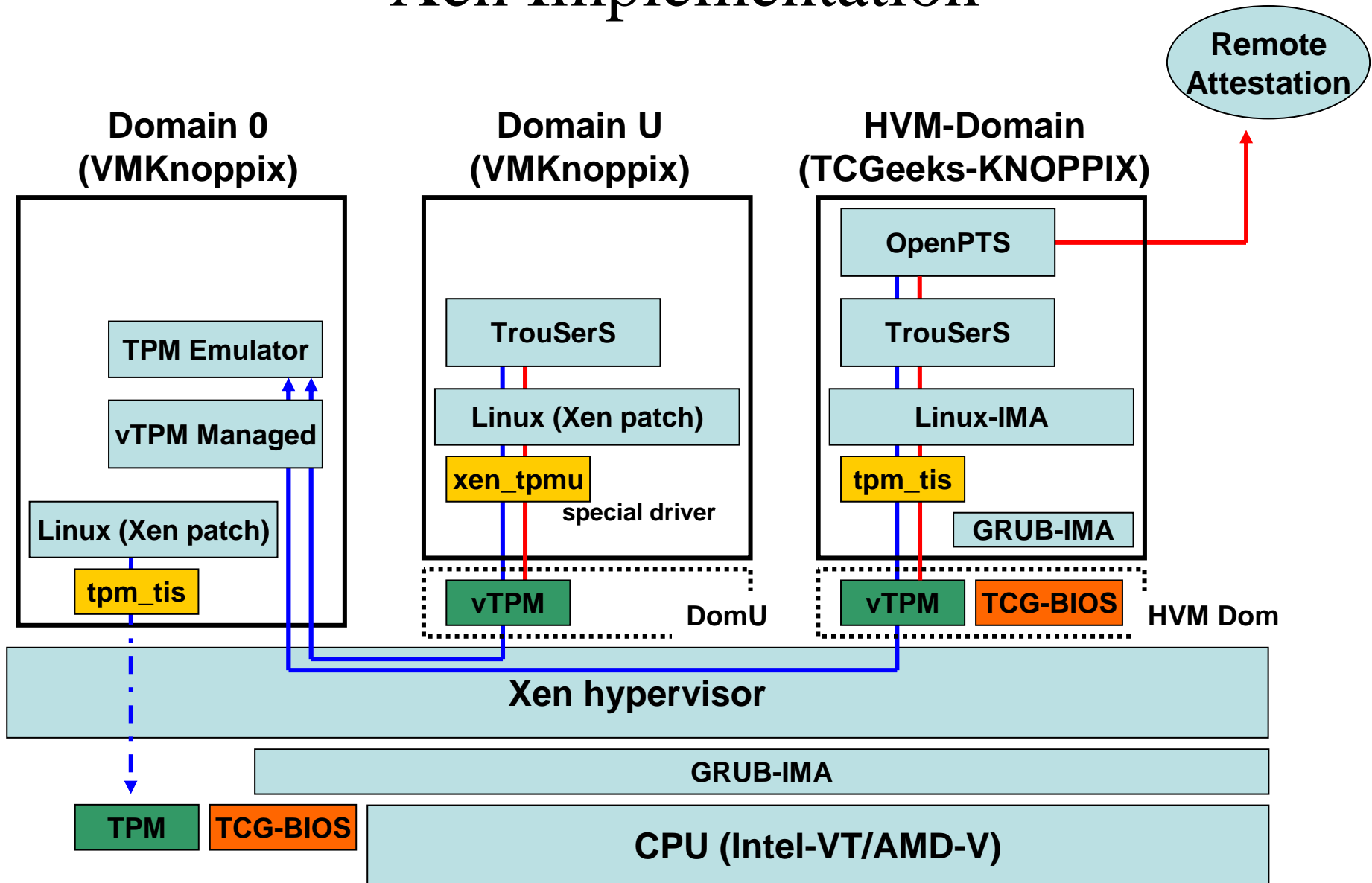
- The BIOS must support interface for Trusted Computing.
 - https://www.trustedcomputinggroup.org/specs/PCClient/TCG_PCClientImplementationforBIOS_1-20_1-00.pdf
 - “INT 0x1Ah” with arguments is used for the TCG Specification.

| Arguments | Name(Function) |
|--------------------|---|
| (AH)=BBh, (AL)=01h | TCG_StatusCheck, Verify the presence of TCG-BIOS |
| (AH)=BBh, (AL)=01h | TCG_HashLogExtendEvent, Extend the events to a PCR |
| (AH)=BBh, (AL)=02h | TCG_PassThroughToTPM, Pass-through the arguments (ES,DI,DS,SI). |
| (AH)=BBh, (AL)=03h | TCG_ShutDownPreBootInterface, Stop response |
| (AH)=BBh, (AL)=04h | TCG_HashLogEvent |
| (AH)=BBh, (AL)=05h | TCG_HashAll, Hash on the input data and returns the resulting hash. |
| (AH)=BBh, (AL)=06h | TCG_TSS |
| (AH)=BBh, (AL)=07h | TCG_CompactHashLogExtendEvent |

vTPM status on Xen (3.4.1)

- DomainU (para virtualization)
 - No BIOS
 - No information about the Platform Integrity on PCRs.
 - vTPM which is emulated by TPM Emulator 0.5
 - Require special driver for TPM (*tmpu.ko*)
 - It can not run trusted boot but it is used for developments of TPM tools (e.g. TrouSerS of TCG Software Stack),
- HVM-Domain (full virtualization)
 - BIOS supports the Interface of TCG-BIOS and ACPI
 - vTPM which is emulated by TPM Emulator 0.5
 - It can run trusted boot.

Xen Implementation

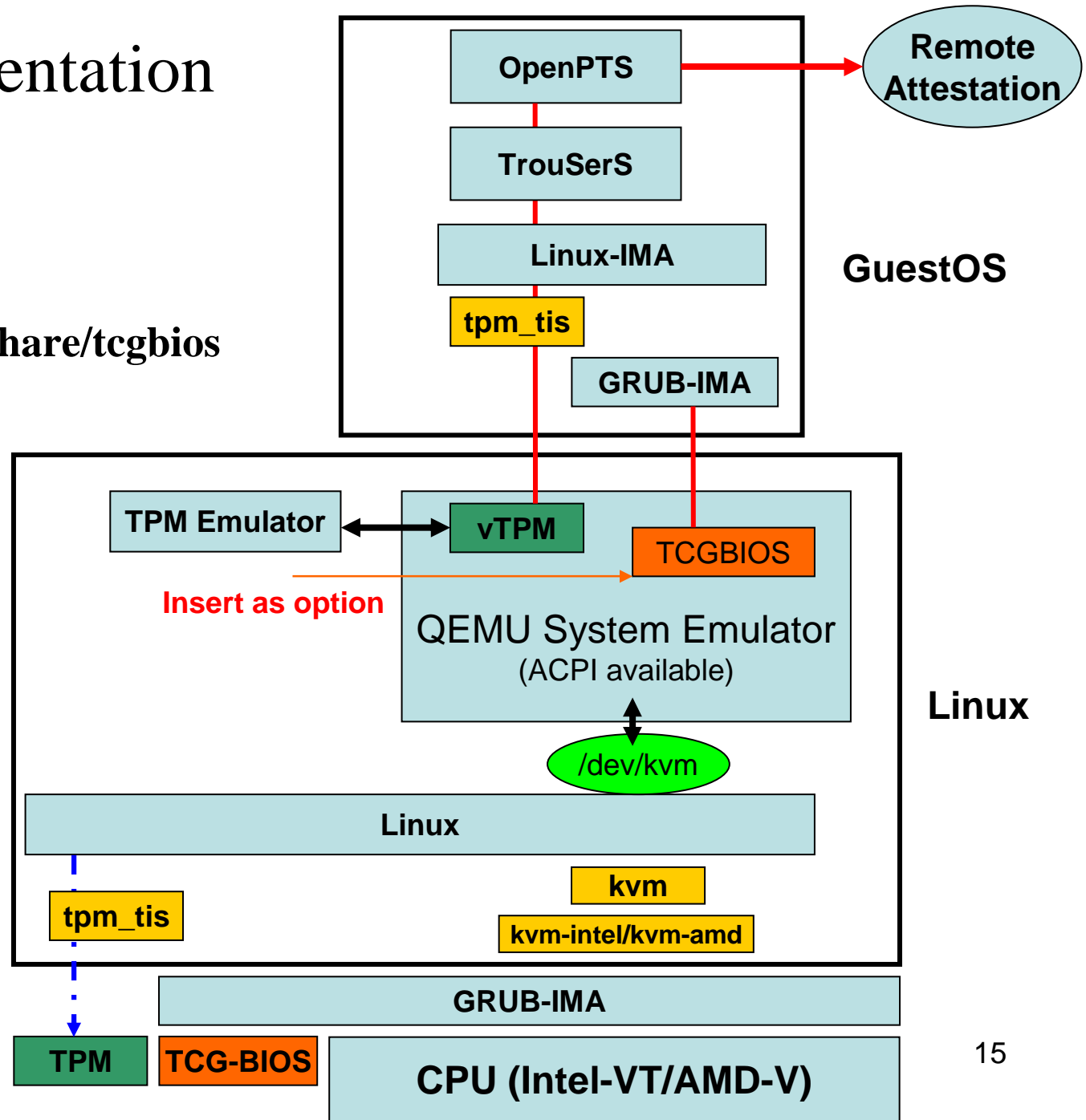


vTPM Status on KVM (60-)

- Original KVM does not support vTPM.
- Nguyen Anh Quynh has customized KVM to enable vTPM. (released soon)
 - TCG-BIOS is inserted as an option.
 - ACPI is available.
 - vTPM is emulated by TPM Emulator 0.5.
 - It will be applied to QEMU.

KVM Implementation

```
# modprobe kvm-intel  
# tpmd  
# kvm -m 512 -L /usr/share/tcgbios  
-cdrom /dev/cdrom
```



Summary of vTPM

| | | Para Virtualization (Xen DomU) | Full Virtualization (Xen HVM) | KVM |
|-----------------------|--|---|--|--|
| Hypervisor/ HostOS | CPU | X86(i686) | Intel-VT/ADM-V | Intel-VT/AMD-V |
| | kernel | Linux 2.6.18 + Xen patch (limit device drivers) | Linux 2.6.18 + Xen patch (limit device drivers) | Least Linux (we can use least drives) |
| | vTPM | TPM Emulator | TPM Emulator | TPM Emulator |
| GuesOS | BIOS | No support | TCG-BIOS | TCG-BIOS |
| | Bootloader | No support | GRUB-IMA | GRUB-IMA |
| | Driver | Xen specific TPM Driver (xen_tpmu) | Normal TPM Driver (tpm_tis) | Normal TPM Driver (tpm_tis) |
| | Kernel | Linux2.6.18 + Xen patch (Limit comes from Host OS) | Any (e.g. Linux2.6.19- IMA) | Any (e.g. Linux2.6.19- IMA) |
| | Validation By Remote Attestation | NG | OK | OK |

Contents

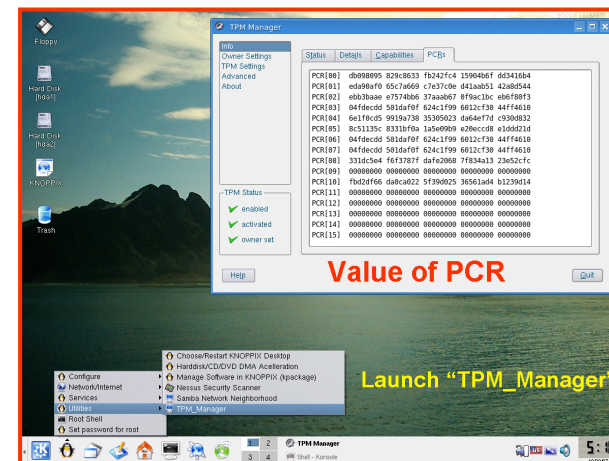
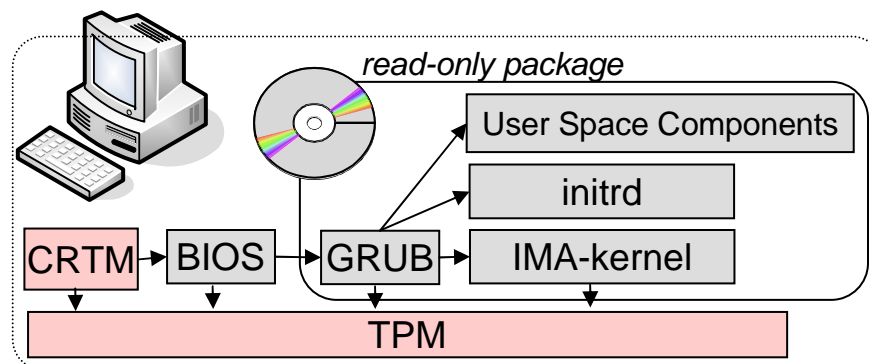
- What is trusted computing? What is TPM?
- virtual TPM
 - Implementation models
 - Requirements for virtual machine
 - BIOS and Device Model for vTPM
 - Current Status of vTPM on Xen and KVM
- **Trusted Computing for Guest OS**
 - Trusted Boot and Remote Attestation
 - VMKnoppix which integrated vTPM and Trusted Computing
- Demo
- Conclusions

Trusted Computing and Remote Attestation

- *Guest OS should utilize the vTPM.*
- We have developed 1CD Linux “**KNOPPIX for Trusted Computing Geeks**” which runs Trusted Computing.
 - The integrity is validated by the Remote Attestation. It also checks the feasibility of vTPM.
- **KNOPPIX for Trusted Computing Geeks** runs Xen-HVM/KVM as a guest OS and checks the feasibility of vTPM.

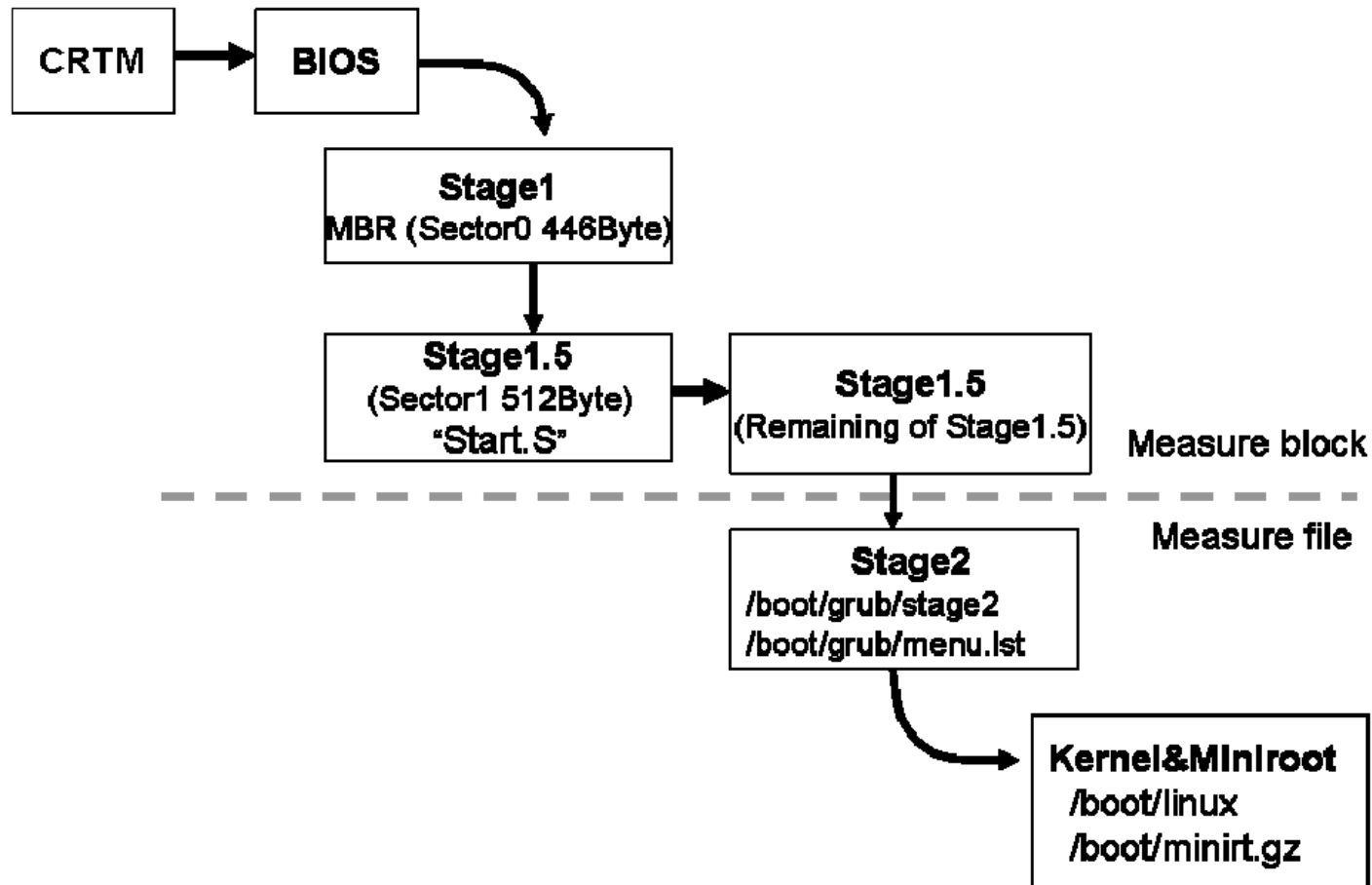
KNOPPIX for Trusted Computing Geeks

- Client
 - GRUB-IMA (Bootloader with Integrity Measurement Architecture)
 - Linux-IMA (kernel with Integrity Measurement Architecture)
 - TrouSerS (Open-source TCG Software Stack)
 - OpenPTS (Open-source Platform Trust Services)
- Server (Remote Attestation)
 - OpenPTS (Open-source Platform Trust Services)
 - Maintain 2 databases
 - IIDB (Integrity Information Data Base)
 - VULDB (Vulnerability Data Base)
 - » which is based on (DSA: Debian Security Advisory)



Measurement by GRUB-IMA

- Extend operation is executed via TCG-BIOS.
- GRUB-IMA takes over the Chain of Trust from the TCG- BIOS.



Log of Trusted Boot by BIOS and bootloader

- /sys/kernel/security/tmp0/ascii_bios_measurements
 - Show **Platform Integrity**.

| PCR | SHA1 | Event |
|-----|------|-------|
| ↓ | ↓ | ↓ |

```
1 017263855c5e8b20f2896a3135b8e4652ab1e708 05 [WAKE EVENT 0]
0 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
1 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
2 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
3 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
5 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
6 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
7 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 c1e25c3f6b0dc78d57296aa2870ca6f782ccf80f 05 [Calling INT 19h]
4 38f30a0a967fcf2bfee1e3b2971de540115048c8 05 [Returned INT 19h]
4 212ba8fde215955b4ed992538900e6b4ca1bd470 05 [Booting BCV Device 00h]
4 946f78edc9a4c8ad1540d4861c4a3690aa096b42 05 [Booting BCV Device 80h]
4 9fd8c23b59cf73d5b101fb189c7f3653aa3b79d6 01 [POST CODE] *** MBR,Stage1 (Sector0, 446 byte)
4 594254f588d95bb1bde243d8b096520df98b7ddb 01 [POST CODE] *** Stage1.5pre (Sector1, 512 byte)
4 4b9db62dddcf93e5d4e9331b7dabf7084fa14b05 01 [POST CODE] *** Stage1.5 remaining
4 ea9e40d3d9a606f847a693519beeb152d522b15a 01 [POST CODE] *** Stage2 "grub/stage2"
5 f8ed9346a86c08aec0a445b92def781cf46b1c66 01 [POST CODE] *** Menu List "grub/menu.lst"
8 27fb6f0e387394ff8a125e225ab0eed21496f773 01 [POST CODE] *** kernel "linux"
8 5c04ae0e736d11b7349eba2a093c1e6c1d0b0731 01 [POST CODE] *** miniroot "minirt.gz"
```

Measurement by Linux-IMA

- Linux-IMA(Integrity Measurement Architecture) measures ELF, Lib, and loadable module when they are used at first time and **extended to PCR** of TPM.
 - Extend operation is executed via TPM driver (tpm_tis.ko).
- Linux-IMA takes over the Chain of Trust from the GRUB-IMA.
 - /sys/kernel/security/ima/ascii_runtime_measurements
 - Show **RunTime Integrity**.

| PCR | SHA1 | Event |
|-----|------|-------|
| ↓ | ↓ | ↓ |

```
10 eeb9e57fc3a66e85858585329c7291a2e138d695 boot_aggregate
10 4cd410cbd7766b0672dfb0b73756c490c1262b6 /static/ash
10 449c076c8bbde638c37e075d63ccd7a6ac6602a0 /static/insmod
10 06dd0a423bd7d35ea2388c481a329b34552db3c0 pas16
10 23a1ba028254b2d5c14f7d6240764706f83bcaa9 psi240i
10 0fa2ec2a67a3e33ea062f4715b1a0d566fe5ce83 t128
10 b55dfa9b2ab368b7f2d839b39dd69613c69a0d56 u14_34f
10 c68b8de398d26abf41989364eb77be153464cd87 wd7000
10 cccf8dc1ff3748dcfa8c4d145a461a3deda6431d usbcore
10 0a2447092eb5d5b337ccfe2afb75dcdae7c40de ehci_hcd
10 bbba6a8dfb5fe4046c4dec4b6d3d98db15067491 uhci_hcd
```

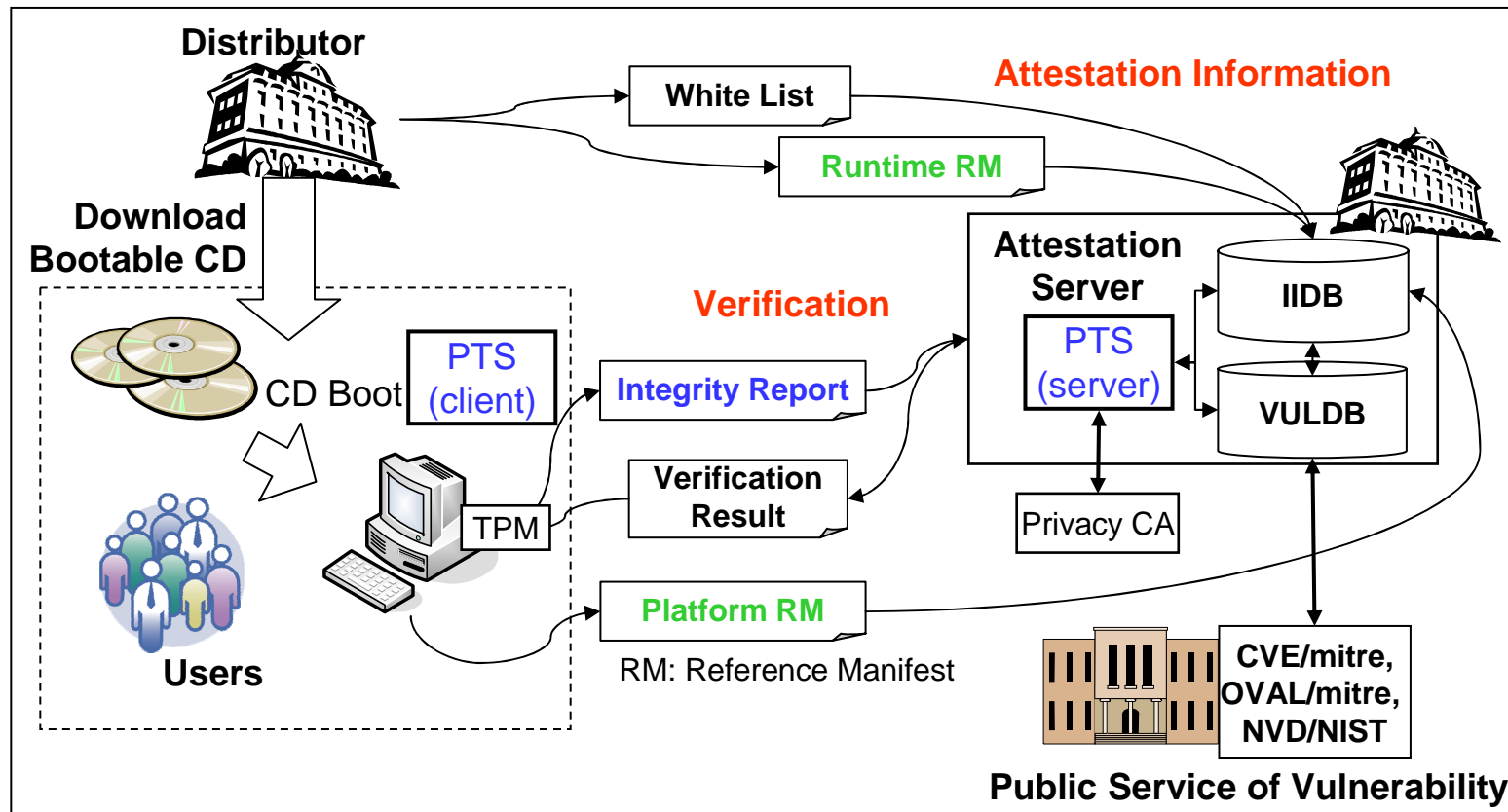
PCR

- `/sys/devices/platform/tpm_atmel/pcrs`

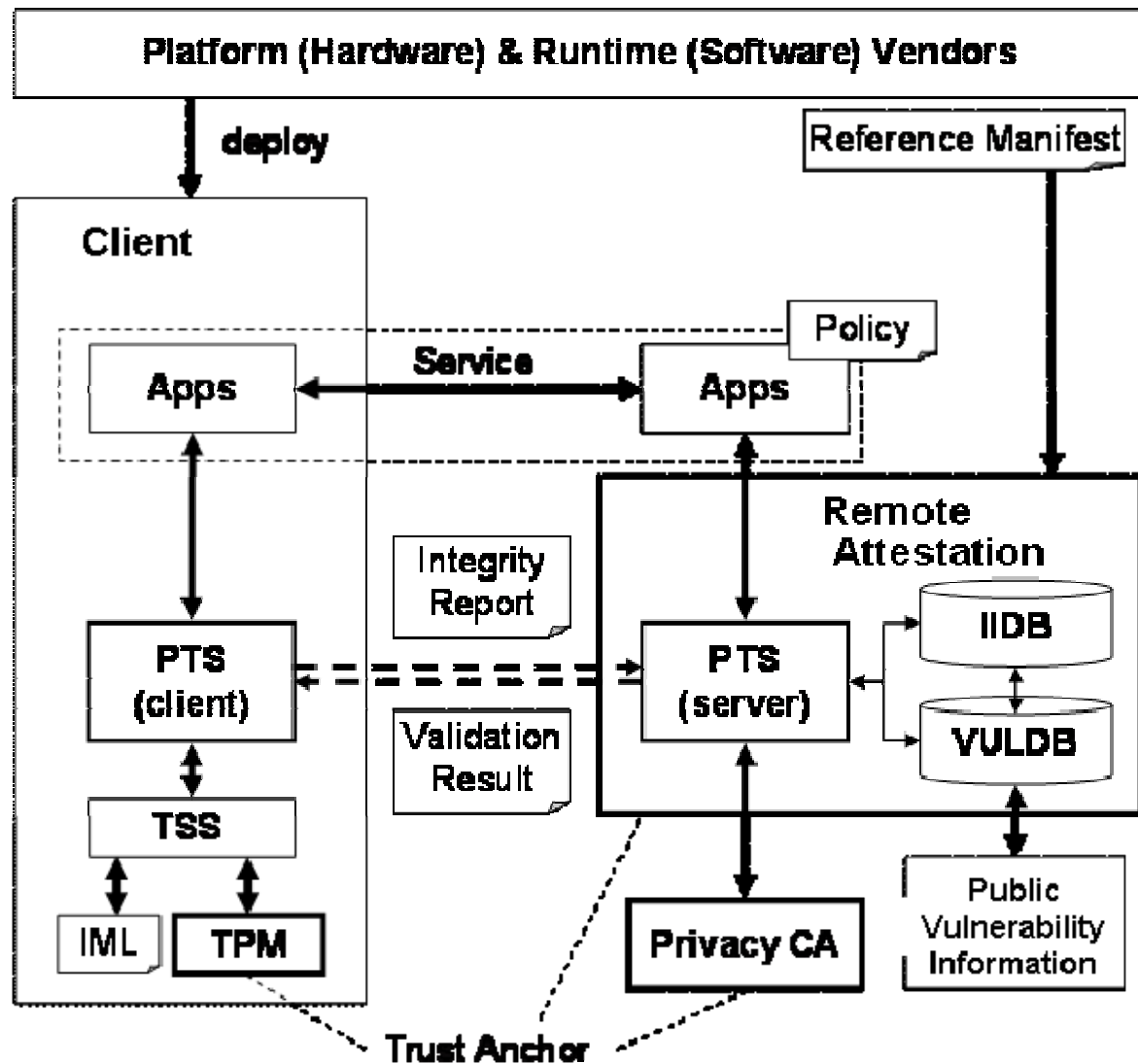
| | | | | | | | | | | | | | | | | | | | | |
|---------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| PCR-00: | 87 | 31 | 03 | 3F | DD | DB | 3F | DA | 05 | F5 | 07 | 63 | 21 | 50 | B9 | 9B | BF | 6D | 45 | 15 |
| PCR-01: | 13 | 02 | B2 | 55 | 28 | E4 | B7 | 06 | 35 | 04 | F2 | 6A | 74 | 6E | D2 | E1 | 1D | 17 | 24 | 3B |
| PCR-02: | EB | B3 | BA | AE | E7 | 57 | 4B | B6 | 37 | AA | AB | 67 | 0F | 9A | C1 | BC | EB | 6F | 80 | F3 |
| PCR-03: | 04 | FD | EC | DD | 50 | 1D | AF | 0F | 62 | 4C | 1F | 99 | 60 | 12 | CF | 30 | 44 | FF | 46 | 10 |
| PCR-04: | 11 | AF | B4 | D2 | CC | 62 | 91 | 18 | 80 | D3 | 3E | 51 | BA | 18 | 8A | EE | E9 | E8 | 0A | D3 |
| PCR-05: | 3D | D4 | 62 | 3E | 57 | 34 | 78 | B1 | EB | A3 | 89 | FE | 24 | 5B | 44 | DB | DO | 79 | 70 | 52 |
| PCR-06: | 04 | FD | EC | DD | 50 | 1D | AF | 0F | 62 | 4C | 1F | 99 | 60 | 12 | CF | 30 | 44 | FF | 46 | 10 |
| PCR-07: | 04 | FD | EC | DD | 50 | 1D | AF | 0F | 62 | 4C | 1F | 99 | 60 | 12 | CF | 30 | 44 | FF | 46 | 10 |
| PCR-08: | 78 | F7 | B8 | 1C | 1B | 69 | DD | 24 | 10 | 4E | 0C | 81 | 59 | 70 | FE | 66 | 1B | DD | 93 | 46 |
| PCR-09: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| PCR-10: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| PCR-11: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| PCR-12: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| PCR-13: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| PCR-14: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| PCR-15: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

OpenPTS (Platform Trust Services)

- OpenPTS is a tool to *send and receive the integrity report* between a client and Remote Attestation.
 - **Platform RM** is integrity information of client PC, which is extended by BIOS and GRUB-IMA.
 - **Runtime RM** is integrity information of software components, which is extended by Linux-IMA.
 - They are registered to Remote Attestation before the validation. Some software components are linked to vulnerability database. When an application becomes vulnerable, the validation is failed.



Software Structure of Attestation



Contents

- What is trusted computing? What is TPM?
- virtual TPM
 - Implementation models
 - Requirements for virtual machine
 - BIOS and Device Model for vTPM
 - Current Status of vTPM on Xen and KVM
- Trusted Computing for Guest OS
 - Trusted Boot and Remote Attestation
 - VMKnoppix which integrated vTPM and Trusted Computing
- **Demo**
- Future Work
- Conclusions

VMKnoppix

- VMKnoppix is 1 CD Linux to correct VM software.
 - Xen (+vTPM), KVM(+vTPM), QEMU, VirtualBox, UserMode Linux, etc.
 - Next version will include
 - “Knoppix for Trusted Computing Geeks”.
 - TCG-BIOS Checker
 - Tool to check the interface of BIOS for Trusted Boot.
Developed by Nguyen Anh Quynh (AIST)

Future Work

- We plan to integrate the trusted computing and virtual TPM to **OS Circular**.
 - OS Circular is a project to distribute the disk image to real and virtual machine.
 - User only has to prepare the bootloader (*“gPXE” or “kexec” which download a kernel and initrd and re-boot with them*) and boots any Linux distribution from the Internet without installation.
 - **BOF “OS Circular”** 24/July(Thursday) 19:30-20:15

Conclusions

- Virtual TPM on Xen/KVM is available on TPM Emulator.
 - The hardware-rooted TPM is not used yet.
- The trusted computing environment is offered by VMKnoppix. It is downloadable from
 - <http://www.rcis.aist.go.jp/project/knoppix/vmknoppix/index-en.html>

Related Presentation

- ASPLOS '08 (Thirteenth International Conference on Architectural Support for Programming Languages and Operating Systems) (Poster)
 - “TPM + Internet Virtual Disk + Platform Trust Services = Internet Client”
- Virtualization Miniconf at Linux.Conf.Au 2007
 - OS Circulation environment “Trusted HTTP-FUSE Xenoppix”
 - http://mirror.linux.org.au/linux.conf.au/2007/video/monday/monday_1450_Virtualisation.pdf
- Linux Kongress2006
 - “Trusted Boot of HTTP-FUSE KNOPPIX”
 - http://www.linux-kongress.org/2006/abstracts.html#4_2_2
- The papers and slides are downloadable form
 - <http://openlab.ring.gr.jp/osircular/>