

# Trusted Boot and Platform Trust Services on 1CD Linux

Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, Nguyen Anh Quynh  
Research Center for Information Security,  
National Institute of Advanced Industrial Science and Technology  
{k.suzaki, k-ijima, yagi-toshiki, nguyen.anhquynh}@aist.go.jp

## Abstract

*We developed 1CD Linux which shows the benefit of trusted computing. It includes Trusted Boot and Platform Trust Services and works as a client OS. The integrity of platform and vulnerability of packages are verified by the remote attestation. The 1CD Linux includes Union File System, which keeps the keys of TPM and the updated applications for next boot time. User can customize the OS and check the vulnerability. We also offer the virtual machine “Xen-HVM” which supports a virtual TPM. The virtual machine does not depend on a physical TPM and makes possible to try the feasibility of trusted computing on many PCs. The easy-to-try environment makes easy to understand the trusted computing and increases the awareness.*

## 1. Introduction

Recently, the awareness of computer security is increased and many reports and security patches are issued as quick as possible when problems are found. Most problems however are caused by the rootkit and malware, which are installed without knowing, according to the CSI/FBI Computer Crime and Security Survey [1]. To solve the problem, many security tools are proposed: intrusion detection systems, virus detection tools, digital signature, etc. These tools however are based on software-rooted trust and are not effective against some stealth root-kits and self-evolving malware.

The Trusted Computing Group (TCG) [2] shows an innovative new approach for the problem. The model is hardware-rooted, based on the existence of a specific secure chip called TPM (Trusted Platform Module). A TPM can keep the incident of trusted computing on a client and send the information to a verifier in a reliable manner. The validness of hardware and software components is evaluated by the Platform Validation Authority (PVA), which is called Remote Attestation.

Unfortunately, the trusted computing is not widely spread. One problem is that a few BIOS support the TCG specification which is required for Trusted Boot (e.g. BIOS INT 1Ah/AX=BBxxh must be supported to check the existence of TPM), although current PCs have a TPM chip. Another problem is the lack of understanding of tools and services. Some tools are developed as open source software but the integrations to operating systems are not enough. The public services for vulnerability software are maintained, but they are not related tightly to the trusted computing. The situations prevent the prevalence of trusted computing.

Our project offers the easy-to-try environment of trusted computing and increases the understanding of effectiveness. We developed 1CD Linux which included Trusted Boot and Platform Trust Services. The integrity of platform and vulnerability of packages are verified by the remote attestation. We also offer the virtual machine with a virtual TPM, which does not depend on a physical TPM and works as a trial environment.

The rest of this paper is organized as follows. Section 2 introduces the overview of trusted computing. Section 3 presents the detail of 1CD Linux for trusted computing on a client PC. Section 4 mentions the remote attestation to verify the integrity and vulnerability. Section 5 presents the virtual machine which includes a virtual TPM. Section 6 reports the current status. Section 7 discusses future work and Section 8 concludes this paper.

## 2. Overview of Trusted Computing

This section introduces the overview of trusted computing, which are defined by TCG. Although the trusted computing covers wide area, this section focuses on the measurement of client integrity by trusted boot and the validation by remote attestation.

## 2.1. Measurement of Client Integrity

The trusted bootstrap processes[3] are defined by TCG. The measurement of client integrity is a key concept of trusted boot. It consists of multiple phases: measuring and storing the fingerprints of hardware and software components. When the system is powered on, the immutable bootstrap code, which is called Core Root of Trust for Measurement (CRTM), measures the BIOS and stores the measurement in the TPM before transferring control. The BIOS also measures the peripheral devices, option ROMs and the bootloader before transferring control. The same manner processes are taken over and keep the chain of trust measurement. Figure1 shows the image of the measurement.

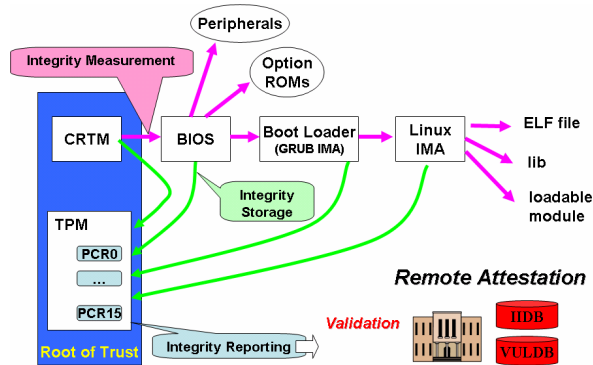


Figure 1. Measurement of Client Integrity

Each measurement uses a SHA-1 hash value of the components. PCR (Platform Configuration Register) in a TPM stores the SHA-1 value with “extend” operation. Extend operation updates PCR with the following manner.

$$\text{PCR} = \text{SHA-1}(\text{PCR} \parallel \text{SHA-1}(\text{Component}))$$

The hash-chain mechanism depends on one way function and detects the inclusion of malicious components because the value becomes strange when an unexpected component is extended.

The trusted bootstrap provides a basis of integrity measurement. The measurement has to be continued in the user space. The Integrity Measurement Architecture (IMA)[4] supports such measurements on Linux kernel. The IMA kernel measures and stores the SHA-1 values of ELF binaries, libraries, and loadable modules to the PCR10.

The measurements are reported to Platform Validation Authority(PVA), i.e. Remote Attestation, to valid the integrity. TCG defines the Platform Integrity Reporting for the PCR values in a reliable manner [3]. In the attestation process, the TPM signs the PCR

values and an external 160-bit challenge using an RSA private key. The confidentiality is guaranteed by the TPM because TPM has own secret keys and the signature can not be forged by the CPU. The platform also sends additional information, such as the measurement log which includes a list of SHA-1 values of components. The remote attestation uses the information to re-calculate the PCR values, since each PCR holds hash-chain which is generated with exponential combination. When the measurement log is wrong or forged, the OS can not be verified with the remote attestation and has a penalty by itself. Namely the validation is two tiered verification systems which are hardware-rooted and software-rooted.

## 2.2. Validation

Platform Validation Authority accepts integrity reports and validates them by the manner of Platform Trust Services (PTS). Unfortunately it has not been defined as TCG specification yet, due to the complexity and variety of the runtime platforms. S.Munetoh et.al [5,6] proposed a realistic approach and this paper follows the architecture.

At first the TCG specification defines Privacy CA (Certification Authority) which issues the credentials for AIKs (Attestation Identity Key) of TPM. AIK is used for making a digital signature of the PCR values and Privacy CA is used for verifying these credentials to make sure that the request comes from a genuine platform with a genuine TPM.

Upon the credential, the TCG specification defines the Integrity Management Model (IMM) [7], to create an infrastructure for managing component integrity. The IMM, together with the integrity measurement and reporting capability of TPM, allows verification of the integrity of the components in a platform. In the specifications, the term “Integrity Measurement” has two meanings. The first is the runtime integrity measurements on a computing platform with TPM. The second is the reference measurements by platform manufacturers. The assertion made by a manufacturer and their integrity metrics (i.e., hash values) is called the Reference Manifest (RM). The RM is compared with the runtime measurements to verify the integrity of the platform configuration.

The IMM defines the PTS as a standard IMM component which provides all the necessary services for integrity measurement. The TCG specification defines both the client-side PTS and the server-side PTS. Figure2 shows the architecture of PTS.

The client-side PTS is an entity which generates Integrity Report (IR), by collecting information from

the Integrity Measurement Log (IML) and the PCR values signed by the TPM with an AIK, through TCG Software Stack (TSS).

The server-side PTS, i.e. Remote Attestation, is an entity which verifies the IRs and returns a Verification Result (VR). The result is one of three values: valid, invalid, or unverified, which means that the IR is verified as trusted, the IR is verified as invalid, or there is not enough information for making a decision, respectively. The server-side PTS verifies IRs with the RM. The integrity of the RM, which represents the expected platform integrity metrics, is protected by the signature issued by the platform vendor or the developer.

The vendors and developers release software with RMs and the software is deployed into the target platforms. The remote attestation maintains the integrity information database (IIDB) and the vulnerability database (VULDB) in order to improve the performance of validation. The IIDB keeps SHA-1 hash values and package information obtained from RMs. The latest vulnerability information for the VULDB are retrieved from public vulnerability databases: e.g., CVE (Common Vulnerabilities and Exposures) [8], OVAL (Open Vulnerability and Assessment Language) [9] and NVD (National Vulnerability Database) [10].

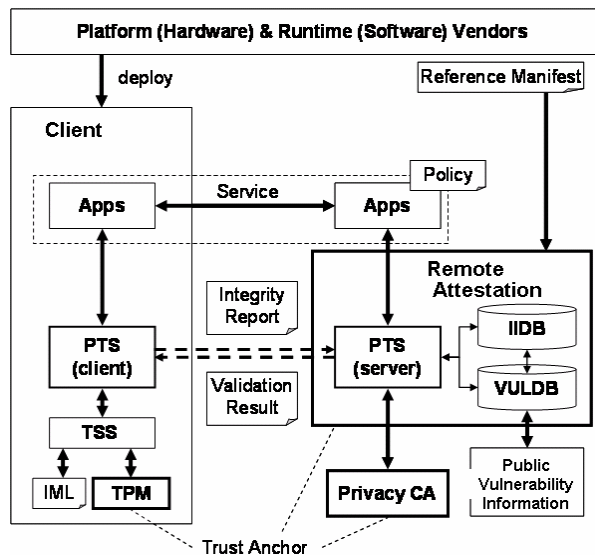


Figure 2. Architecture of Platform Trust Services

### 3. 1CD Linux for Trusted Computing

This section introduces the 1CD Linux for Trusted Computing, which is designed for anonymous PC and works as trusted boot and a client of PTS. The 1CD Linux is based on KNOPPIX and named “KNOPPIX for Trusted Computing Geeks” (From after it is referred to as TCGeeks KNOPPIX).

#### 3.1. KNOPPIX

KNOPPIX is a popular 1CD Linux with a collection of Debian GNU/Linux software. KNOPPIX can be used as a normal desktop Linux because it includes powerful graphical desktop environment (KDE), office software (OpenOffice.org), Web browser (Konqueror, and Mozilla), image manipulation software (GIMP), many games, etc. 1CD Linux is not an exclusive feature of KNOPPIX. There are many distributions: DemoLinux, Mepis, Slax, Adios, etc. Among them, KNOPPIX is the most popular 1CD Linux, because automatic hardware detection/configuration (AutoConfig) function and compressed loopback device (CLOOP) are excellent.

KNOPPIX and other 1CD Linux had a common defect, that could not update the included software because they boot from read only device. Union File System was introduced to solve the problem. It allows files and directories of separate file systems, known as branches, to be transparently overlaid, forming a single coherent file system. Contents of directories which have the same path within the merged branches will be seen together in a single merged directory, within the new virtual file system. It makes a file system appear as writeable, but without actually allowing writes to the file system. The technique is known as COW (copy-on-write).

KNOPPIX uses AuFS (Another Union FS) [11] as a Union File System and makes possible to use Debian package manager. Users can update vulnerable packages via the Internet with “apt-get” command. Furthermore KNOPPIX has a mechanism to re-use the COW image issued by AuFS. The COW image is saved in a file. The image is overlaid on the file system at next boot time to keep the personal update. Therefore the vulnerable application packages, which were updated and stored in the COW image in past time, are automatically overlaid at boot time.

#### 3.2. KNOPPIX for Trusted Computing Geeks

The KNOPPIX is customized for trusted boot and a client of platform trust services. Table 1 shows the

modified and included components. Since normal boot loader and Linux kernel do not support transitive trust chain form CRTM, the GRUB-IMA[12] and Linux-IMA[4,13] are applied. They make possible trusted boot while maintaining the automatic hardware detection/configuration, which is a feature of KNOPPIX. The platform integrity is measured by them. The Integrity of the user land executables and libraries are measured with the Linux-IMA.

The setting of TPM and creating the keys of TPM are managed by the TCG software stack “Trousers” [12] and the user interfaces: TPM tools[12] and TPM Manager[14].

**Table1. Main Components of TCGeeks ONOPPIX**

|            |                                     |
|------------|-------------------------------------|
| Bootloader | Grub 0.97 + Grub-IMA v1.1.0.0[12]   |
| Linux      | Kernel 2.6.19+Linux-IMA[4,13]       |
| TSS        | Trousers v0.2.9.1[12]               |
| CLI        | Tpm-tools v1.2.5.1[12]              |
| GUI        | TPM Manager v0.4[14]                |
| PTS        | OpenPlatformTrustServices v0.1.0[6] |

When the CD-ROM includes vulnerable applications, they must be updated. The union mount keeps the COW image and the persistent mechanism re-uses the image at next boot. We utilize this mechanism to keep the keys of TPM. The keys are encrypted by the SRK (Storage Root Key, RSA 2048 bits) of the TPM, and can be saved in a external storage. The COW image is over laid before the daemon of Trousers, because the keys of TPM must be accessible for the Trousers.

The Platform Integrity Reporting is managed by OpenPTS(OpenPlatformTrustServices)[6], which also depends on Trousers and tpm-tools. OpenPTS creates the Integrity Report on each PC and sends it to the remote attestation. OpenPTS is developed by Java, but JRE can not be included into the CD image because of license. TCGeeks KNOPPIX uses GCJ (GNU Compiler for Java) instead of JRE. It has another merit because the classes on JRE are not measured by Linux-IMA. GCJ creates ELF binary from Java program and shared object form JAR file, which are measured by Linux-IMA.

## 4. Remote Attestation

This section mentions the implementation of the remote attestation for the TCGeeks KNOPPIX.

### 4.1. Verification for Remote Attestation

The validation mechanism on the remote attestation is implemented with OpenPTS[6]. The OpenPTS assumes a finite state machine (FSM) which is a representation of the trusted bootstrap and subsequent measurement processes of the platform. Each state in the behavior model represents a platform state, and each transition represents the integrity of the component that is loaded and executed. This extended capability of the PTS supports efficient verification and management of the integrity of the platform.

## 4.2. Vulnerability Database

The remote attestation has 2 databases: the integrity information database (IIDB) and the vulnerability database (VULDB). Both databases are managed by PostgreSQL 8.1.9.

The IIDB maintains a white list and black list of hash values of the known components. In addition, each entry of the IIDB has a flag that indicates whether there are any known vulnerabilities in the component. The VULDB is the central repository of the known vulnerabilities, by aggregating information from vendors and security advisories. The VULDB synchronizes with the IIDB to update with the latest vulnerability information.

The integrity information of the user land components is stored in the IIDB. We collected the list information for the user-land components from the CD media and store it directly into IIDB, in order to replace the RM creation process and set up the IIDB for the target OS. For the TCGeeks KNOPPIX, the IIDB has integrity information for 84,382 files in 1,415 packages.

The VULDB stores 6,536 entries of CVE data as XML published by NVD [10], and it also includes the corresponding CVSS (Common Vulnerability Scoring System) scores. To validate the TCGeeks KNOPPIX, we obtained the list of Debian Security Advisory (DSA) [15] with the CVE numbers.

## 5. Virtual TPM and Virtual Machine

Current PCs have a TPM chip but a few BIOS support the TCG specification which is required for Trusted Boot (e.g. BIOS INT 1Ah/AX=BBxxh must be supported to check the existence of TPM). The situation prevents the prevalence of Trusted Computing.

To solve this problem, we planned to use virtual machine but most virtual machine did not support TPM. Only Xen [16] hypervisor has a mechanism to support a virtual TPM and TCG-BIOS. Xen has some experimental implementations of virtual

TPM. S.Berger et.al [17] proposed vTPM (virtual TPM) which is linked to physical TPM and passes the chain of trust to a virtual machine. The vTPM is transparently mapped to the physical TPM. The lower PCR [0-8] are used by Xen hypervisor and the upper PCR [9-15] are used for a guest operating system. The other implementation uses a software emulator of TPM which is called TPM Emulator[18]. It can prepare each virtual TPM for each virtual machine.

We adopt software emulator because it does not care a physical TPM and any machine enables to try trusted computing. It is not hardware-rooted and does not keep the chain of trust from the power-on. However it makes possible to try the feasibility of trusted computing on many machines even if a TPM is not integrated e.g., Intel Mac which has no TPM and uses EFI (Extensible Firmware Interface) instead of BIOS.

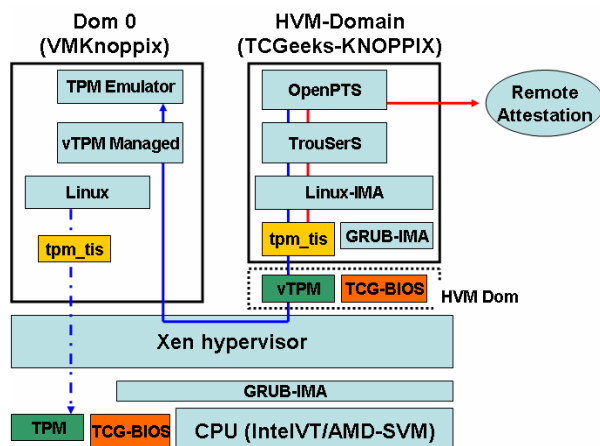


Figure 3. the architecture of vTPM on Xen

Dom 0 of Xen, which works as a host OS, has to prepare vTPM manager daemon to communicate TPM-Emulator because TPM Emulator is independent of Xen and has no interface to Xen. The HVM Domain, which is full virtualized machine on Xen, has a vTPM and the Xen hypervisor intermediates the communication between vTPM and vTPM manager daemon. Figure3 shows the relation of vTPM on Xen.

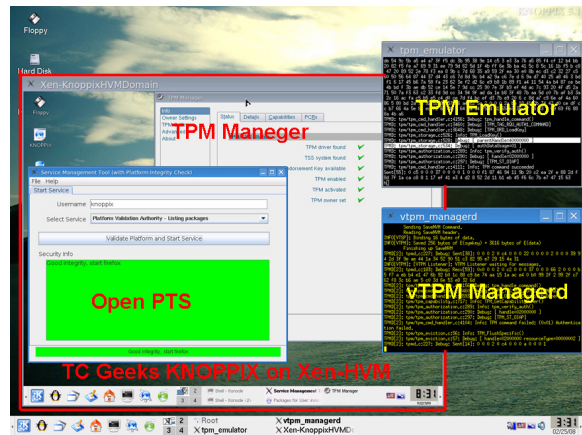


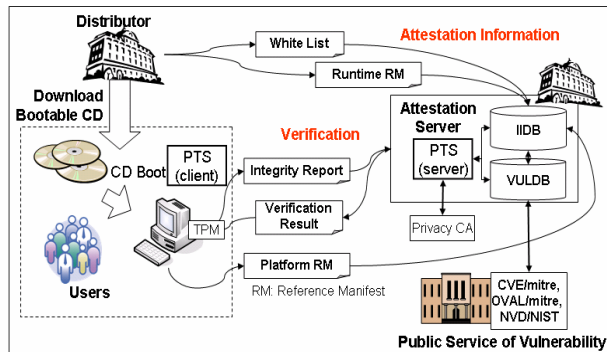
Figure 4. TCGeeks KNOPPIX runs on Xen-HVM with vTPM

The set up of vTPM on Xen is not easy because it is optional implementation. It requires to apply some patched form mailing lists. To boot the TCGeeks KNOPPIX, we have to use the full virtualization, which requires virtualization instructions: Intel VT or AMD-V. We offer ICD Linux which includes Xen-HVM with virtual TPM for convenience, which is called VMKnoppix. Figure4 shows the TCGeeks KNOPPIX is booted on the Xen-HVM which supports vTPM on VMKnoppix.

## 6. Current Status

The TCGeeks KNOPPIX [19] and the VMKnoppix [20] were released and used by anonymous users. The TCGeeks KNOPPIX works well on some PCs, which equips a TPM and TCG-BIOS (e.g. Panasonic LetsNote, IBM ThinkPAD, etc), and Xen-HVM with a vTPM, which is bundled in VMKnoppix. The TCGeeks KNOPPIX includes a vulnerable application (i.e. DSA-1308 Iceweasel package) and the remote attestation can not validate the original one. Namely it is configured that users must update the package. The update is stored to a COW file and overlaid by union FS.

Figure5 shows the Implementation of remote attestation for the TCGeeks KNOPPIX. Current implementation does not use privacy CA because the service is offered by anonymous users and the private information is not managed by us. Therefore the implantation has to assume that credential of AIK is clean.



**Figure 5. Implementation of Platform Trust Services for Trusted KNOPPIX**

To validate the TCGeeks KNOPPIX, we used the Debian Security Advisory [14]. After updating the VULDB, the IIDB was synchronized with VULDB to have the latest vulnerability information. When a user loads the TCGeeks KNOPPIX and tries to validate it the remote attestation, the IML is verified against the RMs and the latest status is also verified according to the databases.

We know that the hash value “e8df910d0bd25ebe7a0b...” is for the file “/usr/lib/iceweasel/firefox-bin” and a part of the “iceweasel-2.0.0.1+dfsg-1” package. This package has several vulnerabilities according to DSA-1308, such as CVE-2007-2871, CVE-2007-2870, CVE-2007-2869, CVE-2007-2868, CVE-2007-2867, and CVE-2007-1362. The CVSS shows the scores from 4.3 to 9.3 in the relevant CVE entries.

We measured the performance on the validation. It took around 1 second (980msec-2593msec) to validate 471 entries with the remote attestation on LAN (1G bps) environment. The validation of vulnerability for 1,415 packages on the TCGeeks KNOPPIX took around 4 seconds. The overhead is acceptable to check the integrity on a client.

## 7. Future Work

### 7.1. Other Linux Distributions

Current TCGeeks KNOPPIX is designed for demonstration, but the basic mechanism is applied to any Linux distributions. The requirement for a client is to include GRUB-IMA, Linux-IMA kernel, Trousers, and OpenPTS. It is not so hard requirement. The most important feature is keeping the correct package database on the remote attestation. TCGeeks KNOPPIX uses the Debian Security Advisory (DSA) because KNOPPIX is consisted of Debian packages. Other distributions also have the public database for the

vulnerable packages. Especially the commercial Red Hat Enterprise Linux has strong support for the packages and reports the vulnerable information to CVE (Common Vulnerabilities and Exposures), which is funded by the National Cyber Security Division of the United States Department of Homeland Security. We should utilize the information to prevent vulnerability. We hope the developers and users use basic mechanism and the infrastructure to keep the integrity of the client.

### 7.2. PreBootLoader

The vulnerable application packages on TCGeeks KNOPPIX are updated using Union FS. The kernel however can not be updated because it is fixed to the 1CD Linux and executed before Union FS. It means the vulnerability of kernel can not be dealt with current framework.

We are developing a PreBoot Loader “InetBoot” [21] to replace the kernel at boot time. InetBoot gets a kernel from the Internet and boots the downloaded kernel with the 1CD Linux. It also downloads a COW image file and vulnerability applications can be overlaid with Union FS.

InetBoot is not a true bootloader. It is a small Linux and reboots a kernel with the Linux system call “kexec”. It works as PreBoot Loader and checks the integrity of whole software before booting. The current development issue is keeping chain of trust. InetBoot will include GRUB-IMA and Linux-IMA kernel. However it looks difficult to include TrouSerS and OpenPTS because InetBoot depends on “BusyBox” which must use the special library “uclibc”. We have to consider the methods to keep chain of trust and reporting mechanism.

### 7.3. Internet Boot

Thin client technology becomes popular to control the updates. However thin client depends on LAN environment, because it uses TFTP to boot an OS and NFS for the root file system. The administration is still charged to each system engineer. Furthermore current thin client has no mechanism to deal with network disconnection. It is not convenient for note PC users.

To solve the problem we have proposed “OS Circular” project[22] to offer an Internet virtual disk. The Internet virtual disks are managed by the distributor and the contents are updated periodically for security. The parts of disk images are cached on a local storage and reusable. Unfortunately the current implementation does not have a mechanism to validate

the integrity. We will integrate the PTS to OS Circular and keep the security.

#### 7.4. Dynamic RTM

Current implementation depends on Static RTM and the chain of trust must start from the power-on. It is not convenient and some applications don't fit to the manner.

Current CPU (i.e. AMD SVM or Intel TXT) has a function to make dynamic RTM and creates the trusted code execution environment for an application at run time. AMD SVM and Intel VT guarantee the code is executed in the isolated environment. OSLO[23] and tboot[24] are bootloaders which use AMD SVM and Intel TXT respectively. Flicker[25] uses AMD SVM and creates an isolated code execution environment on Linux. The technology is valuable but it is also desirable to validate the code by Platform Validation Authority. Our system will be utilized on the technology.

#### 7.5. Hardware rooted vTPM

Current vTPM on Xen is not hardware rooted and the keys of TPM are not certified on the virtual machine. It means the trusted boot on the virtual machine is not guaranteed by trusted third party.

The vTPM should be integrated to hardware rooted TPM for true trusted computing. We are developing another vTPM on the KVM (kernel based Virtual Machine) and plan to implement a hardware rooted vTPM, which is proposed by S.Berger et.al [26].

### 8. Conclusions

TPM chip has a potential to increase computer security with hardware-rooted trust and it is included in a current PC. The utilization however is still quite preliminary. Our project aims to promote the awareness of benefit and increases the understanding of the usage. We offer ICD Linux which includes Trusted Boot and Platform Trust Services to measure the integrity of a platform. The integrity is validated by the remote attestation.

Although the infrastructure is improved, most BIOSes on client PCs do not support trusted boot and prevent the prevailing of the technology. We offered the virtual machine environment with a virtual TPM. It is not hardware-rooted trust but the feasibility of the infrastructure is confirmed.

As the next step, we will integrate the infrastructure to the Internet Thin Client which boots from the disk images on the Internet. It does not depend on hard disk and free from the malware which is stayed in a hard disk. The security update is managed by the distributors and the integrity is also validated by the remote attestation.

### Acknowledgements

We gratefully acknowledge the support and the fruitful discussions with Megumi Nakamura and Seiji Munetoh of IBM Japan about Platform Trust Services.

This study was sponsored by the Ministry of Economy, Trade and Industry, Japan (METI) under contact for the New-Generation Information Security R&D Program.

### References

- [1] CSI/FBI computer crime and security survey 2006.
- [2] Trusted Computing Group, <http://www.trustedcomputinggroup.org/>
- [3] Trusted Computing Group, "TPM Main, version 1.2."
- [4] Reiner Sailer, Xiaolan Zhang, Trent Jaeger and Leendert van Doorn, Design and Implementation of a TCG-based Integrity Measurement Architecture, 13th USENIX Security Symposium, pp. 223–238 (2004).
- [5] Seiji Munetoh, Megumi Nakamura, Sachiko Yoshihama, and Michiharu Kudo, Integrity Management Infrastructure for Trusted Computing, IEICE TRANSACTIONS on Information and Systems, Vol. E91-D No. 5 pp. 1242-1251 (2008).
- [6] OpenPlatformTrustMeasurement: <http://sourceforge.jp/projects/openpts>
- [7] Trusted Computing Group, "TCG Infrastructure Working Group Architecture Part II - Integrity Management, Ver.1.0, Rev. 1.0," November 2006.
- [8] Common Vulnerabilities and Exposures: <http://cve.mitre.org/>
- [9] Open Vulnerability and Assessment Language: <http://oval.mitre.org/>
- [10] National Vulnerability Database: <http://nvd.nist.gov/>
- [11] Another Union File System: <http://aufs.sourceforge.net/>
- [12] TrouSerS: <http://sourceforge.net/projects/trousers>
- [13] Linux-IMA: <http://sourceforge.net/projects/linux-ima>
- [14] TPM Manager: <http://sourceforge.net/projects/tpmmanager>
- [15] Debian Security: <http://www.debian.org/security/>
- [16] Xen hypervisor: <http://www.xen.org/>
- [17] Stefan Berger, Ramón Cáceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, and Leendert van Doorn, vTPM: Virtualizing the Trusted Platform Module, 15th USENIX Security Symposium, pp. 305–320 (2006).
- [18] TPM Emulator: <http://tpm-emulator.berlios.de/>

- [19] KNOPPIX for Trusted Computing Geeks: <http://unit.aist.go.jp/itri/knoppix/index-en.html>
- [20] VMKnoppix: <http://www.rcis.aist.go.jp/project/knoppix/vmknoppix/index-en.html>
- [21] InetBoot: <http://openlab.jp/oscircular/inetboot/>
- [22] Kuniyasu Suzuki, Toshiki Yagi, Kengo Iijima, and Nguyen Anh Quynh, OS Circular: Internet Client for Reference , USENIX 21st Large Installation System Administration conference, pp. 105-116 (LISA'07).
- [23] Bernhard Kauer, OSLO: Improving the security of Trusted Computing, 16th USENIX Security Symposium, pp. 229–237 (2007).
- [24] Joseph Cihula, Trusted Boot: Trusted Boot: Verifying the Xen Launch, Xen Summit 07 Fall.
- [25] Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter and Arvind Seshadri, "How Low Can You Go? Recommendations for Hardware-Supported Minimal TCB Code Execution." In Proceedings of the ACM Conference on Architectural Support for Programming Languages and Operating Systems, (ASPLOS'08).
- [26] Stefan Berger, Ramón Cáceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, and Leendert van Doorn, vTPM: Virtualizing the Trusted Platform Module, 15th USENIX Security Symposium, pp. 305–320 (2006).