

# TPM + Internet Virtual Disk + Platform Trust Services = Internet Client

<http://www.openlab.jp/oscirclear/>

<sup>†</sup>Kuniyasu Suzaki, <sup>†</sup>Kengo Iijima, <sup>†</sup>Toshiki Yagi, <sup>†</sup>Nguyen Anh Quynh,

<sup>††</sup>Megumi Nakamura, <sup>††</sup>Seiji Muhetoh

<sup>†</sup>National Institute of Advanced Industrial Science and Technology, <sup>††</sup>IBM Japan

## Abstract

We are developing an infrastructure of Internet Client using Platform Trust Services. The Internet Client boots an OS with a minimal boot image which obtains a virtual disk from the Internet. The virtual disk is reconstructed from the downloaded pieces which are saved to block files. The block files are cached at a local storage and reusable for mobile computing. The integrity of the contents and boot procedure are measured and logged at a secure chip TPM. User can send the integrity report to Platform Trust Services and confirm the validness of the boot.

## 1. Introduction of Internet Client

Internet Client boots an OS without installation and makes easy to try new functions of OS. The infrastructure distributes image of OS efficiently and prevents interfusion of malware and vulnerable applications. The image is distributed by Internet Virtual Disk and the validness is check by trusted boot of TPM and Platform Trust Service.

## 2. TPM and Trusted Boot

TPM (Trusted Platform Module) is a secure chip which is equipped in current PC. Trusted boot keeps the boot log at PCRs (Platform Configuration Register) in a TPM with one way function (SHA1). The one way function keeps chain of trust which is passed to BIOS, bootloader (i.e. GRUB-IMA), kernel(i.e.Linux-IMA[1]:Integrity Measurement Architecture), and applications. The log and the value of PCRs are used to valid the platform and contents of the operating system.

## 3. Internet Virtual Disk

We developed Trusted HTTP-FUSE CLOOP[2] for Internet Virtual Disk. A normal block device is split by 256KB and saved to block files. A block file is named by the SHA1 value of its contents. Mapping table has the list of block files and it is used for the driver to reconstruct a block device. Block files are distributed by un-trusted HTTP servers but the contents are validated with the mapping table file. The block files are cached at a local storage and reused. When necessary block files are saved at the local storage, the networking connection is not necessary. It is used for mobile computing environment. The lower part in Figure1 shows the image of Trusted HTTP-FUSE CLOOP.

## 4. PTS: Platform Trust Services

Platform Trust Service checks the integrity of boot procedure on each client. User can confirm the validness even if the disk image is obtained from un-trusted HTTP servers.

We developed OpenPTS[3] for platform trust services. A client of OpenPTS sends Integrity report which includes Platform Manifest and Runtime Manifest. Platform Manifest

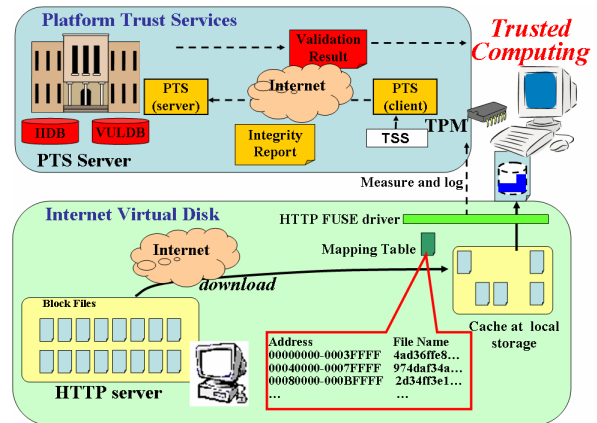


Fig1. Image of Internet Client with TPM, Internet Virtual Disk and Platform Trust Services

is created by the log of BIOS and PCRs of TPM. Runtime Manifest is created by the log of Linux-IMA and PCRs of TPM.

The server of OpenPTS has two types of data base: Integrity Information Data Base (IIDB) and Vulnerability Data Base (VULDB). IIDB checks the platform and VULDB checks the applications and return the validation result. User can confirm the status of the Internet Client. The upper part of Figure1 shows the image of Platform Trust Services.

## 5. Current Status & Future Works

Current Internet Client boots KNOPPIX (Debian GNU/Linux) with GRUB-IMA, Linux-IMA and Trusted HTTP-FUSE CLOOP. OpenPTS checks the integrity of the KNOPPIX. The IIDB has information of platforms which BIOS respond to trusted boot. The VULDB is based on DSA (Debian Security Advisory) and has information for Vulnerable Debian packages.

Near future we will include DRTM(Dynamic Root of Trust Measurement) which is enabled by tboot[4] with Intel TXT and OSLO[5] with AMD-SVM(skinit). The integration makes secure reboot with kexec tools of Linux\*.

## References

- [1] R.Sailer, et al., Design and Implementation of a TCG-based Integrity Measurement Architecture, 13th USENIX Security Symposium (2004)
- [2] K.Suzaki et al., OS Circular: Internet Client for Reference , 21st USENIX LISA (2007)
- [3] OpenPTS: <http://sourceforge.jp/projects/openpts>
- [4] Joseph Cihula, Trusted Boot: Trusted Boot: Verifying the Xen Launch, Xen Summit 07 Fall.
- [5] Bernhard Kauer, OSLO: Improving the security of Trusted Computing, 16th USENIX Security Symposium (2007)

\*Linux is a registered trademark of Linux Torvalds in the United States, other countries, or both.