New Technology Reports

Trusted Mobile Platform Technology for Secure Terminals

Yu Inamura, Takehiro Nakayama and Atsushi Takeshita

Trusted Mobile Platform is a key technology for increasing the "trust" of mobile terminals such as PDAs. Recently, Intel Corp., IBM Corp. and DoCoMo launched a joint research project to conduct research and development of this key technology.

1. Introduction

Recently, Intel Corp., IBM Corp. and DoCoMo launched a joint research project focusing on "Trusted Mobile Platform," which is a key technology for improving the security of mobile terminals such as Personal Digital Assistants (PDA), and has accomplished a disclosure of a set of technology specifications [1]–[3]. The aim of this joint research is to establish computing environments that can be securely used by terminal users and service providers by improving the "trust" (such as adding functions for checking that hardware/software is functioning normally) of mobile terminals.

We consider that the project has produced excellent results in two aspects in particular: 1) comprehensive security mechanisms were pursued in terms of hardware, software and protocols, and 2) various security classes were defined (**Table 1**). These security classes refer to configurations that achieve good balances in terms of mobile terminals security by using functions and tools listed in the same class simultaneously, rather than being indexes of security strengths, as is often seen in other standard specifications. For example, it is possible to achieve a security level equivalent to the one achieved by functions and tools of class 3 in Table 1 using functions and tools of class 1, by conducting strict examination of software and hardware in advance and placing restrictions on additional upgrading.

Another characteristic of this research is avoiding reinventing the wheel by utilizing various existing technologies such as the Trusted Computing Platform Alliance (TCPA) and Transport Layer Security (TLS), and focused only on the areas required instead.

Table 1 Security classes (excerpt)

Security requirement example	Security class		
	Class 1	Class 2	Class 3
TPM implementation	• Software TPM or equivalent	• Hardware TPM	• Embedded TPM or MCM*6
CPU architecture	—	• MMU*5	• Hardware domain separation
Integrity and attestation	• Minimal integrity checks	• Integrity checks and source authentication (trusted boot)	• Trusted boot • Runtime integrity checks
Domain separation enforcement	• COTS*1 OS separation (user account + process) • Java*2 (JAAS*3 or OSGi*4)	• Hardened OS (mandatory access control) • Encrypted memory system	• Secure processor architecture • Software domain separation
Secure data storage	—	• Through encryption	• Through encryption and domain separation

*1 COTS: Commercial Off The Shelf means products that can be purchased as is.
*2 Java: Object oriented software environment with particular emphasis on network use, promoted by Sun Microsystems, Inc. in the US.
*3 JAAS: Java Authentication and Authorization Service, an optional package to the Java Software Development Kit.
*4 OSGi: Open Service Gateway initiative is an alliance that aims to enable new services and applications for network devices.
*5 MMU: Memory Management Unit that provides physical/logical address conversion functions.
*6 MCM: Multi Chip Module, multiple ICs packaged in an insulated substrate.

The following chapters explain the hardware architecture, software architecture and protocols that constitute the Trusted Mobile Platform technology.

2. Hardware Architecture

The hardware of the Trusted Mobile Platform technology mainly has the following two characteristics.

1) The Trusted Mobile Platform technology was developed as an extension of technologies cultivated by the TCPA for the PC platform [4] by taking the characteristics differences between PCs and mobile terminals into consideration.
2) Security requirements related to input/output devices were newly defined.

The following provides an overview of the Trusted Platform Module (TPM) and input/output devices, which inherit and extend the specifications prescribed by TCPA.

2.1 TPM

The TPM is a tamper-resistant module equipped with its own Central Processing Unit (CPU) and secure memory area; it operates independently of the mobile terminal's CPU and is equipped with various dedicated functions such as cryptographic operations.

Figure 1 shows a function block diagram of the TPM in the minimum configuration.

The TPM has various features; for instance, it provides the cryptographic function required in the trusted boot processing explained in Section 3.1 and has a dedicated memory area called the Platform Configuration Register (PCR) that can only be updated by special update operations. Moreover, it is equipped with digital signature functions based on signature keys that cannot be extracted from the TPM, guaranteeing to third parties that certain data originates from a specific TPM. This is essential in implementing the platform trust status exchange protocol explained in Section 4.1.

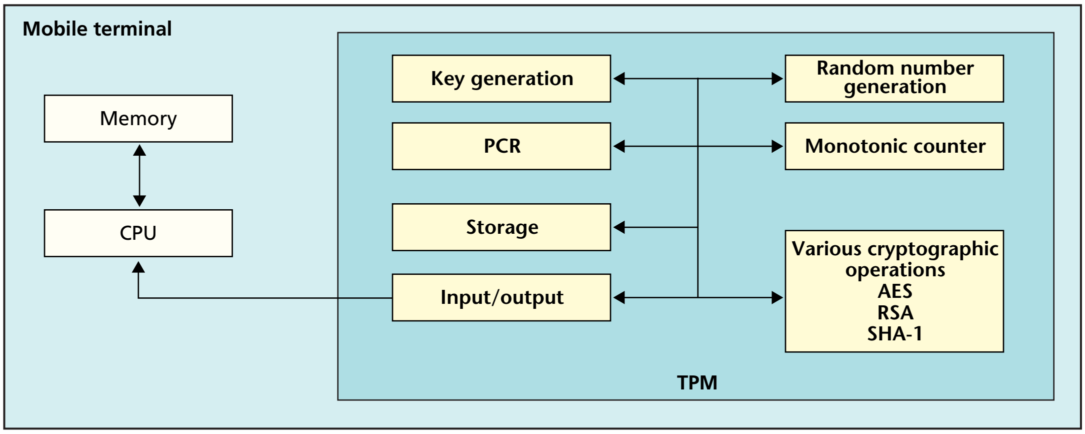
Furthermore, the Trusted Mobile Platform specification requires that a conformant TPM has the Advanced Encryption Standard (AES) functionalities and a monotonic counter, both of which are not specified in the specifications of TCPA.

2.2 Input/Output Device

Even if the mobile terminals themselves are secured, it must not be possible for malicious programs to deceive users to enter important information such as passwords. From that point of view, input/output devices play important roles in terms of security. For this reason, Trusted Mobile Platform prescribes requirements such as that it must be possible to display whether or not a system is in trusted status on the display etc. without being tampered with by applications, and that inputs from the keyboard or other input devices must reach the target application without being modified or tapped.

3. Software Architecture

This chapter introduces the software architecture of Trusted Mobile Platform. The trust required by Trusted Mobile Platform is established and the separated application execution environment is achieved by making effective use of the hardware features explained in Chapter 2.



RSA: Rivest–Shamir–Adleman
SHA-1: Secure Hash Algorithm 1

Figure 1 TPM functional block diagram

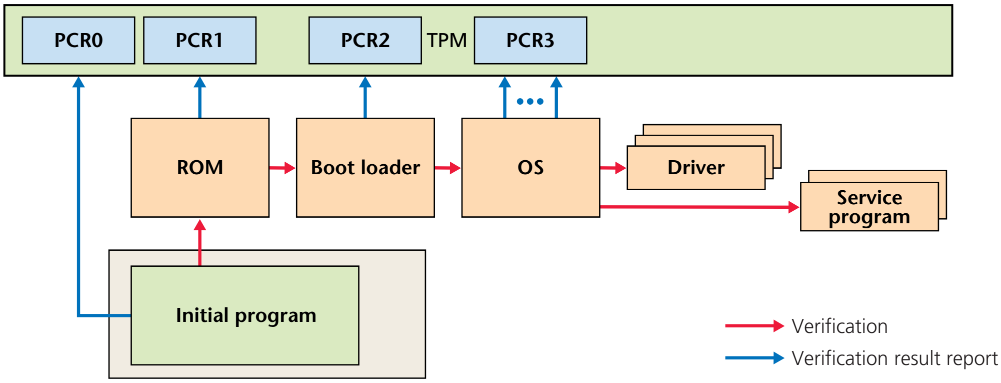


Figure 2 Trusted boot operation

3.1 Trusted Boot

The most significant point is the trusted boot executed when the system is turned on. This is a mechanism proposed by TCPA [4] that allows confirming that the system is in a trusted status according to the procedure after startup. This mechanism makes it possible for the users themselves as well as various servers communicating with a terminal via networks such as the Internet to confirm the trusted status of the terminal.

Figure 2 shows the flow of the trusted boot. In general, a primary initialization procedure is executed when the power is turned on and then higher-level programs are loaded and executed one by one in the order of ROM, boot loader and then OS, each program is activated by lower-level programs in turn. In the trusted boot operation, the lower-level programs verify that the to-be activated higher-level programs are correct. Specifically, data that can uniquely be identified (fingerprint data) is extracted from the file images of higher-level programs, and the PCRs in the TPM are updated using the data.

After being initialized at reset, the PCR can only be updated with values that cannot be deduced immediately from the given data. Thus, when the system is started up as a result of the trusted boot, fingerprint data of the boot loader, OS, drivers and various service programs are stored in the PCRs of the TPM. By comparing these values with expected values that are calculated by the same processing and safely stored in advance, it is possible to check whether the terminal is in a trusted status.

If malicious programs have found their way into the terminal and inserted themselves somewhere between the trusted boot processes, the values stored in the PCRs will be different from the expected values, and since it is not possible to set arbitrary values in the PCRs, the existence of the malicious programs is revealed no matter how smartly they are programmed.

3.2 Domain Separation

It is theoretically possible to keep track of all the system execution states including those of various application programs at any point after activating by following the same method as the trusted boot, but this is unrealistic due to the vastness of the number of combinations of states each program can be in.

To address this issue, Trusted Mobile Platform adopts domain separation to provide protection after the completion of the startup process of the OS. Domain separation is a mechanism that allows various programs to operate only within their own execution environments, and prohibits them from interfering with other applications being executed simultaneously in the system. If this domain separation is enforced strictly, the security of program execution in other domains is guaranteed even if a malicious program is being executed at the same time.

The following three types of domain separation methods can be considered for individual security classes.

1) Application Level

Using a Virtual Machine (VM), as in Java.

2) OS Level

Hardening the current standard OSs. For example, it is recommended to use cryptographic memory systems [5] that protect the data stored in memory by using cryptographic techniques.

3) Hardware Level

Using strict domain separation mechanisms implemented directly in hardware, such as the "ring-1[*]" technology in Intel's architecture.

4. Authentication/Management Protocols and Countermeasures during Operation

This chapter explains the protocols required to allow secure and flexible application building and countermeasures during operation.

4.1 Protocol Overview

We utilized the existing technologies such as Transmission Control Protocol/Internet Protocol (TCP/IP), Secure Sockets Layer (SSL) and TLS and defined custom protocols on top of these protocol stacks in order to supply missing function (**Figure 3**). One of the important common protocols necessary for implementing Trusted Mobile Platform is a platform trust status exchange protocol for exchanging results obtained during the trusted boot with other servers. This allows service providers and contents providers, for example, to provide services only to mobile terminals that can be confirmed to be in trusted status.

Other common protocols include protocols for management applications, for example, protocols for core software download and a key management protocol for delivering encryption keys used in the TPM. For these protocols, it is recommended to use normal SSL/TLS, the extended SSL/TLS, which uses information stored in the TPM, electronic signature and/or other methods.

4.2 Countermeasures during Operation

We also examined possible countermeasures to be taken by

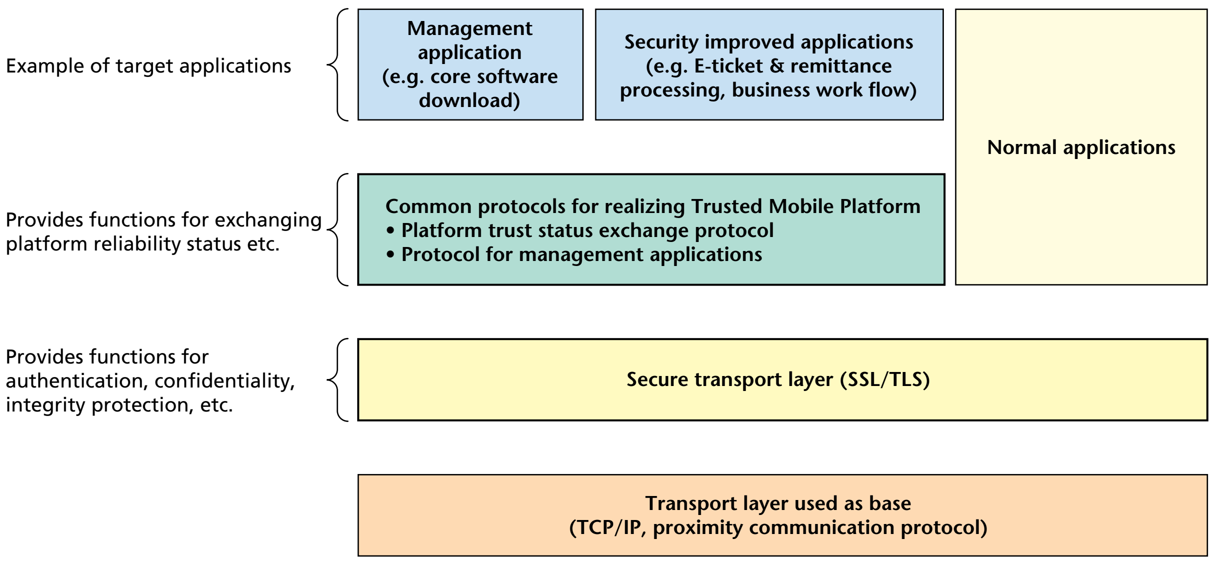

Example of target applications
Management application (e.g. core software download)
Security improved applications (e.g. E-ticket & remittance processing, business work flow)
Normal applications
Provides functions for exchanging platform reliability status etc.
Common protocols for realizing Trusted Mobile Platform
• Platform trust status exchange protocol
• Protocol for management applications
Provides functions for authentication, confidentiality, integrity protection, etc.
Secure transport layer (SSL/TLS)
Transport layer used as base (TCP/IP, proximity communication protocol)

Figure 3 Authentication/management protocols

[*] Ring: Indicates divisions of CPU execution privilege in the Intel architecture. Ring-1 means that a privilege level higher than ring-0, which is used in normal OSs, is provided.

service providers in case security problems are detected in a mobile terminal. Which operation to select is determined by the service characteristics and user type (general or business users), available security technologies and various other conditions.

One example of such countermeasures is to provide services only to the mobile terminals that have taken appropriate countermeasures online. In this case, the possible operations include 1) the requested service is denied or 2) services are only provided under certain restrictions, to terminals for which no measure is taken.

5. Conclusion

This article provided an overview of the Trusted Mobile Platform specifications formulated in a collaboration between Intel Corp., IBM Corp. and DoCoMo. Trusted Mobile Platform adds comprehensive security solutions that involve hardware, software and protocols. Specifically, we explained the mechanism of the trusted boot which is the most characteristic techniques, functions of the TPM that supports it and the protocols used for exchanging information concerning the trusted boot with other devices.

References

[1] "Trusted Mobile Platform Hardware Architecture Description," version 1.0, Jun. 2004; http://www.trusted-mobile.org/

[2] "Trusted Mobile Platform Software Architecture Description," version 1.0, Jun. 2004; http://www.trusted-mobile.org/

[3] "Trusted Mobile Platform Protocol Specification Document," version 1.0, May 2004; http://www.trusted-mobile.org/

[4] S. Pearson et al.: "Trusted Computing Platforms–tcpa technology in context," Prentice Hall PTR, 2003.

[5] Y. Inamura and S. Hongo: "A Proposal for Memory Data Protection Scheme Using Cryptography," Journal of the Information Processing Society of Japan, Vol. 45, No. 7, pp. 1823–1832, Aug. 2004 (in Japanese).

Abbreviations

AES: Advanced Encryption Standard
COTS: Commercial Off The Shelf
CPU: Central Processing Unit
JAAS: Java Authentication and Authorization Service
MCM: Multi Chip Module
MMU: Memory Management Unit
OSGi: Open Service Gateway initiative
PCR: Platform Configuration Register
PDA: Personal Digital Assistant
RSA: Rivest–Shamir–Adleman
SHA-1: Secure Hash Algorithm 1
SSL: Secure Sockets Layer
TCP/IP: Transmission Control Protocol/Internet Protocol
TCPA: Trusted Computing Platform Alliance
TLS: Transport Layer Security
TPM: Trusted Platform Module
VM: Virtual Machine