Falsification Prevention and Protection Technologies and Products

NEC's Attitude to "Trusted Computing"

By Takahisa SHIRAKAWA*

ABSTRACT NEC attaches great importance to security for its business PCs (The brand names of NEC's business PCs are Mate and VersaPro). This approach is used because NEC thinks that the PC is a key element in maintaining the security of the overall business system. For example, it has now become necessary to handle secret information by using a PC in various settings in the world of business. This paper introduces NEC opinion on security systems, essentials and viewpoints. It also comments on "Trusted Computing" by discussing the activities of the Trusted Computing Group (TCG) which is the industry organization, and summarizes TCG specifications. In conjunction with the above, the solutions that NEC has achieved by utilizing the Trusted Platform Module (TPM) are introduced.

KEYWORDS **Business PC, Mate, VersaPro, TPM, Encryption-key management, Platform attestation, Platform authentication**

1. INTRODUCTION

The value of information technology (IT) increases more and more to meet the needs of business and social activities. Recent developments in network technologies and the spread of network infrastructures, the Internet, Intranet and the Extranet are all now firmly established as important means of information sharing in the business market. In addition, IT exchanges between companies and their customers that have a direct economic value (ex. e-commerce) will also tend to increase in the future.

So, the role that security technology has, now becomes increasingly important because high value information is always threatened. It is very likely that business and social activities might receive a fatal blow unless we protect both stored and circulated information from such threats.

This paper introduces PC security from the perspective of the trusted platform.

2. PC SECURITY

2.1 The Necessity of PC Security

Processing performances, the quantity of accumulated information and information transmission speeds of PCs are increasing more and more. It must be effected that we use various networks freely and at anytime and in any location and also that we can access any necessary information and be able to freely make use of this ability in our business activities. Therefore one must investigate and solve problems of security at the same time in order to create convenient systems.

Previously, attention to security was apt to be suitable for only server and network. But, poor PC security, which is at the IT interface, lowers the security of the whole system, even if enough security is provided for both server and network. This situation can be compared with providing a weak lock for the gate of a strong fortress.

For example, even if I manage the server side security well and prevent prohibited network logging in, it is often the case that a PC using the server holds important cached data in a local HDD.

In addition a login password might be stolen from a server by means of a proscribed software installation.

Similarly to the above, PC security is indispensable for the security of the whole system.

Below I list NEC's mottos for essential PC security.

- A PC is an entrance (and exit) for secret information.
  (The creation of confidential documents and secret data cache.)
- A PC (mobile laptop) is a secret data store.
  (As well as confidential documents, connection passwords to intranet may also be recorded.)

*Client And Server Division

· A PC is the weakest point of the intranet.
· A PC is in the frontline of authentication.
(In all cases, personal authentication is performed by operating a PC.)

2.2 Overview of PC Security

Of course, as with the security issue, in order to contend with an intensive attack at a weak point, the improvement of the whole system is important. So, I will describe the total security concept based on the threat analysis that is to be pursued for PCs to be used in the business domain.

Figure 1 shows a threats matrix. I distinguish a protective object as being of four kinds, Software, Network, Data file and Hardware. It is probable that PC hardware security, has not been adequately investigated (Physical attack on a PC is easier than for other devices.) I distinguish protected property as being of four kinds, Confidentiality, Availability, Authenticity and Integrity. For example, the "Copying of files illegally" and "Spyware" correspond to a threat (attack) that is related to the "Confidentiality" of a "Data file."

Solutions for these threats are very much connected with each other. I will explain this clearly. From the perspective of leaked information, "Confidentiality" of "Network," "Data file" and "Hardware" are related directly.

Measures that protect against these threats, supplement each other in supporting protection against information leaks. In other words, they form one part of the same castle wall for the same secret information leaks.

As a result, they form a complementary relationship and cannot ignore even one of them in developing the solutions.

No measures for the "Confidentiality" of "Data file" can block access to secret if logged in illegally. Measures for "Authenticity of user (authentication)" of "Software" may be bypassed when software is falsified.

In this way, "Confidentiality" and "Availability" are supported by "Authenticity" and "Integrity," "Authenticity" is supported by "Integrity."

2.3 Viewpoints Peculiar to PC Security

NEC pays attention to the following from the viewpoint of PC security.

(1) Easy of Use for the End User

Security must not obstruct operability (ease-of-use.) Generally, it is often that security capability sacrifices operability. But, poor operability leads to the deterioration of security.

This is because, even if we provided the function of high security and operability is poor, it will not be functional and it becomes not only useless, but also a weak link in the system.

(2) Security Peculiar to a Domain, Not to a Product

Usual threat for PCs

	Software	Network	Date file	Hardware
Confidentiality				
	Reverse engineering	Wiretapping	Copying (printing) files illegally Spyware	Theft of HDD
Availability				
	DoS boot disorder	DoS	Data lost	Damage / loss / theft
Authenticity, Accountability				
	Unjust login private use	Unjust access	denial of accountability infringement of copyright	Theft of PC
Integrity				
	Virus Falsification of software	Falsification of packet (Worm) Illegal device (PC/WLAN-AP...)	Falsification of data	Unjust device connection

Fig. 1 Classification of threats.

For security products for PCs to be marketed extensively, corporate authority for such a product is necessary. In other words, a product is easily got to an illegal user as well as to a company aiming at security improvement. For example, we must not suppose that PC users have Local-admin authority. We must assume in fact that there are PCs brought in illegally. And that these PCs are installed with the same security products set illegally within them.

(3) Interoperability

Each company has a different use environment. On this account, it is necessary to cooperate with a product intended for various scales of application.

3. WHAT IS TRUSTED COMPUTING

3.1 What is TCG

TCG (The Trusted Computing Group,) which was organized in May, 2005 is an industry organization for trusted computing. The forerunner of TCG in which NEC participated was TCPA, which was organized in 1999. TCG has adopted TCPA specifications and aims to both enhance and extend them across multiple platforms such as servers, PDA's, and smart phones.

TCG develops open hardware-based specifications for trusted computing that protect and strengthen the platforms against attack. TCG's specifications have contributed materially to the creation of TPM (Trusted Platform Module).

It has been announced that the TCG/TPM specification (version 1.2) has been adopted for the next generation of PCs. Microsoft will use TPM as the security feature of its next generation OS (Longhorn). And, Intel will support TPM in its next generation CPU technology (LaGrande Technology / Vanderpool Technology). I have also heard that Linux also plans to utilize TPM.

3.2 Aims of Trusted Computing

TCG explains the aims of Trusted Computing as follows.

- Store keys, digital certificates, passwords and data securely in the hardware.
- Enhance network security and protect online commerce transactions.
- Prevent viruses, worms and other malicious attacks.
- Protect digital identities.
- Provide authentication between systems and networks, Allow for single sign-on to systems.
- Enable digital signatures for financial and other transactions.

That is TCG aims at realizing "Confidentiality," "Authenticity" and "Integrity" which was explained in Section 2.2. The reason why TCG pays attention to this point is that it is very difficult (may be impossible) to realize "Integrity" only by software. (Measures based on only software have vulnerable points to these malicious attacks, in any case.) In addition, about "Confidentiality" and "Authenticity," TCG makes up for any weak points of the software.

That is TCG intends to provide markedly strong structures to supplement the overall security function (Confidentiality, Availability, Authenticity and Integrity) by TPM.

3.3 Overview of TPM Feature

Figure 2 is a block diagram of TPM architecture, which shows the major components of a TPM.

The following explains a summary of each component.

- The "Cryptographic Co-Processor" provides cryptographic operations for the TPM. Those operations include RSA key generation, RSA encryption/decryption, SHA-1 hashing and random number generation. The RSA asymmetric algorithm is used for encryption and for digital signatures.
- "Key generation" creates RSA asymmetric key pairs and symmetric keys.

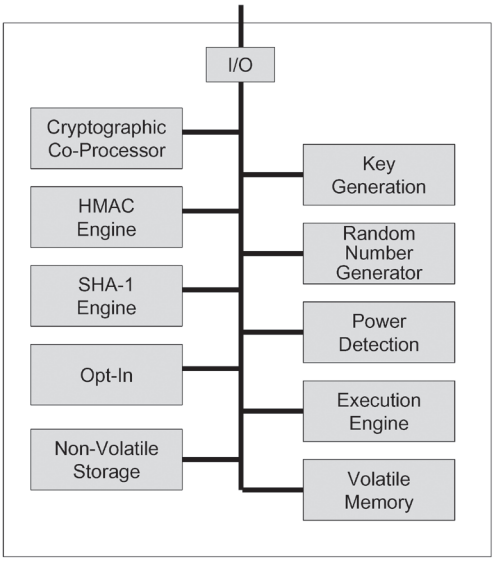

Fig. 2 Major components of a TPM.

- "HMAC Engine" (HMAC: keyed Hashing for Message Authentication Code) provides the detection of falsification of data and the certification of authorization data.
- "Random Number Generator" provides genuine random number for key generation and randomness in signatures and so on.
  Genuine random numbers contribute greatly to the strength of a cryptograph.
- "SHA-1 Engine" is the hash capability of a digital signature. SHA-1 hash algorithm is defined by FIPS-180-1.
- "Power Detection" manages the TPM power states.
- "Opt-in" maintains the state of persistent and volatile flags. It enforces the semantics associated with these flags.
- "Execution Engine" executes the TPM commands from CPU.
- "Non-Volatile Memory" is stored as persistent identity (EK and entities authorized by the TPM owner) in persistent mode.

(NOTE: The existence of these components does not mean that TPM is an accelerator for encryption processing. Software encryption processing by recent CPU is at a higher-speed.)

3.4 Major Data of TPM

The following explains the major data used in TPM.

3.4.1 Platform Configuration Register (PCR)

PCR is a 160bit register for integrity measurements. There is a boot-strapping process by which series of Trusted Subsystem components (BIOS code, OS Loader, OS and Application Software) measure the next component in the chain. It does this measurement by using a cryptographic hash.
(NOTE: The hash property is one-way. This property means that it is almost impossible for an attacker to determine the input message given a PCR value.)

3.4.2 Endorsement Key (EK)

EK is a 2048bit RSA key pair for platform identity mechanisms. Private EK is never revealed outside the TPM (TPM permits the public EK to be read.) It is used for decryption only and cannot perform signatures for security and privacy reasons.

The EK is only available for the following operations: establishing the TPM Owner and Attestation Identity Key values and credentials.

The EK provides the conceptual foundation of Root of Trust for Reporting (RTR). This concept is responsible for the establishment of platform identities, reporting and protecting platform configurations and the establishment of context for attesting to reported values.

3.4.3 Attestation Identity Key (AIK)

The AIK is a 2048bit RSA key pair for the signature of information generated internally by the TPM exclusively. Private AIK is never exposed outside of TPM. For example, the information includes PCR, other keys and TPM status. Because AIK only signs information generated internally, TPM prevents attacks that create data which forge PCRs and so on. It is used for signatures only and cannot provide encryption.

The number of AIKs that can be created virtually has no limit.

The AIK credentials disclose the EK-AIK binding.

3.4.4 Password of Owner

The password of the owner is a shared secret, which is stored in a shielded memory of the TPM. In addition, it is encrypted using the public EK to provide confidentiality. A password attack (which is like a dictionary attack) is not effective so that the collation of a password is done internally on the inside of the TPM.

Whenever a new owner is established, a new Storage Root Key (SRK) is created, and the particulars of the previous owner will not be inherited.

3.4.5 Storage Root Key (SRK)

The storage Root Key is an encryption key for which TPM protects the TPM object (see Section 3.5) stored outside it. A TPM Owner can back up SRK and restore it.

3.5 Key Storage

Figure 3 shows the key storage hierarchy as an example.

Only Storage Root Key is protected by what is stored internally in the TPM. Other keys are stored outside the TPM (in the HDD), and these are protected by using encryption with a key of a higher hierarchy. And finally, secret data are protected by using encryption with leaf-key.

All of the keys of each user form a definite tree, and cannot be decrypted without getting a pass in the collation of each user's password.

This mechanism provides confidentiality and enables the storage of many keys. In contrast, traditional approaches by software methods exclusively and methods to protect the keys by a password have vulnerable points with regard to password attacks.

A TPM Owner can back up all these hierarchies. Each user can back up the lower hierarchy from his/her own user-key. This means that the environment is restored when the maintenance or exchange of a PC Mother-Board is performed.

3.6 Software Interface of TPM

Figure 4 shows a Software stack from the TPM to applications.

The lowest stack, "TPM FW (FirmWare)" runs on the "Execution Engine" of TPM (see Section 3.2). The upper stacks are programs to work on the CPU.

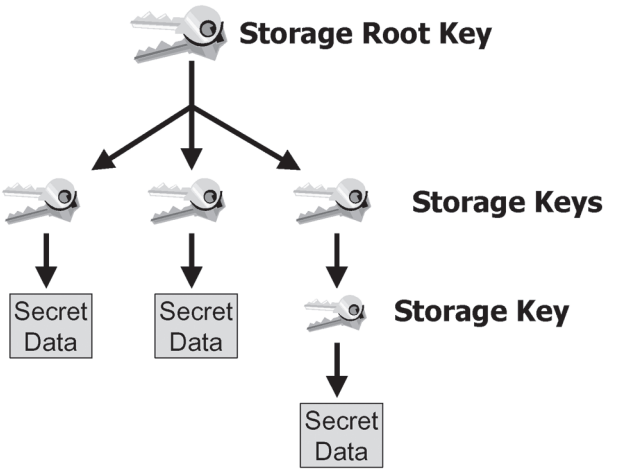

Fig. 3 Key storage hierarchy.

The "TCG Software Stack (TSS)" is a device-driver for the TPM that uses "TPM FW." It provides TSS API for the upper layer. The TCG decides the API and names it "TCG TPM Specification Version 1.x" and the like. Application programs that are compatible with TPM use this interface.

"TPM CSP" is a Cryptograph Service Provider that uses "TSS" through the TSS API. CSP provides Microsoft-Cypto-API (MS-CAPI) and Public-Key-Cryptography-Standards number 11 (PKCS#11) and so on for the upper layer. The application programs for handling TPM abstractly, such as mailer, web-browser and VPN, use these interfaces. Because this API is an interface that has already been introduced to the market for use with a token device such as SmartCard, it is very important that this interface is available at an early stage in order for the application to utilize TPM.

4. NEC TPM EMBEDDED PC

On October 12, 2004, NEC announced a TPM embedded Desktop-PC, Mate slim tower model (highly expandable type).

Photo 1 shows the appearance of this PC. And **Table I** shows its major specifications.

This PC possesses TPM as standard and not as an option. The reason that the TPM is not an option is that NEC has made the issue of customer security more important than a slight increase in the cost of

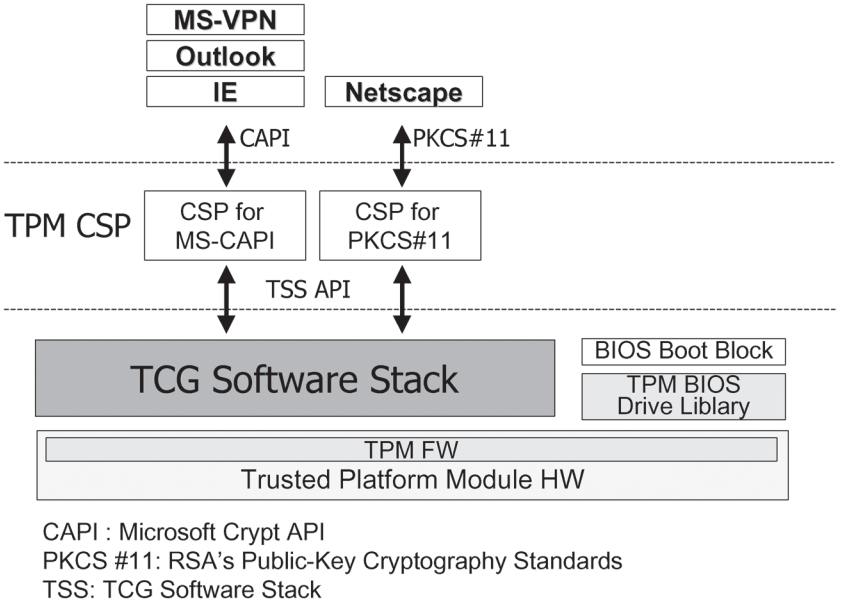

Fig. 4 API of specification of TCG.

Photo 1 The appearance of the PC.

Table I Major specifications of the PC.

Item	Specifications
Base model	MY30Y/G-F
Processor	Intel Pentium 4 530J(3GHz)
Memory	DDR2-SDRAM 256MB ～
Graphic	Intel 915G Express chipset
OS	Windows XP Professional SP2
HDD	40GB
Optical device	24x CD-ROM
FDD	include
Keyboard	PS/2 109keyboard with PS/2 mouse
Network	Gigabit LAN
Display	No Monitor
Shipment	18/10/04
List price	138,000yen

parts. NEC realizes the reinforcement of security in order to conform to the "personal information protection law" that will be enforced in its entirety in April, 2005 by the adoption of Windows XP Professional Service Pack 2 (SP2) with advanced security technologies and the embedding of TPM.

4.1 Security Enhancement to be Attached to the PC

This PC strengthens Windows Encrypting File System (EFS) by using TPM, and reduces the risk of information leaks via theft or loss. The means of achieving this are that TPM can prevent direct access to a private key. In contrast, a traditional private key stored externally by HDD is exposed to illegal access.

In addition, this PC strengthens e-mail security by using TPM, and reduces the risk of wiretapping and forgery. Effectively, this PC can obtain electronic certification for e-mail into TPM from VeriSign for one year gratis. TPM can prevent the prohibited copying of a private key for this certification by storing it. In contrast, the traditional method was effective against attacks on a signal communication path but was powerless against attacks directly on the PC, for example, in cases that a former employee had copied a key. (NOTE: At the implementation level, these keys for EFS and certification are stored in the TPM key storage hierarchy outside the TPM-chip (see Section 3.5)).

4.2 Security Enhancement by Combination

NEC has announced a support plan for TPM security solutions for public information.

The announcement said that various security software such as anti-cyber attack measure "CapsSuite," server firewall software "ServerW@ll" and anti-information-leak measure "InfoCage" will support TPM sequentially after January, 2005.

In the next chapter detailed explanations are provided about features to be provided with this software in the near future.

5. NEC TPM SOLUTION

5.1 Focus on Security Issues

The entire security issue must be considered from the position of an overall solution.

Improvements in connectivity involve uncertain boundaries for computer networks. Improvements in connectivity are likely to advance more and more in the future. The innovative concepts that NEC publishes, such as "Dynamic Collaboration," "Ubiquitous Computing" and "UNIVERGE" can emphasize these trends.

Figure 5 shows these concepts.

"Dynamic collaboration" is collaboration across the company.

"Ubiquitous Computing" utilizes wireless LAN network across a border of traditional intranet. Of course a mobile PC goes outside physical security activity (for example, locking and patrol by a guard).

"UNIVERGE" unifies three different networks, telephone-line, usual intranet and mission critical network, to provide integrated convenience and cost reduction. With unification, a mechanism ensuring that lower communication of an urgent degree does not obstruct a higher communication is necessary. To neglect the implementation of this mechanism widens the damage of current cyber attacks to a network of telephones.

In this way, security issues of recent years are caused by the vagueness of computer network boundaries with regard to improvements in connectivity.

Then, I try looking back at the old days to look for a hint. **Figure 6** shows an example of security in the era of host computing.

Networks of this era had the mechanism of

definitely retaining a border. The terminal is managed by terminal ID. When a terminal is connected to the host, its ID is registered with the terminal registration database in the host. So, a non-registration terminal cannot be connected to the host.

In this way, the access area to the application service, secret information and intranet is limited physically.

The means of personal authentication is added to reinforce this physical limitation.

In contrast, the load now concentrates on the means of personal authentication. It cannot deal with an illegal act by an inside criminal. According to the statistics, 85% of the causes of information leaks are

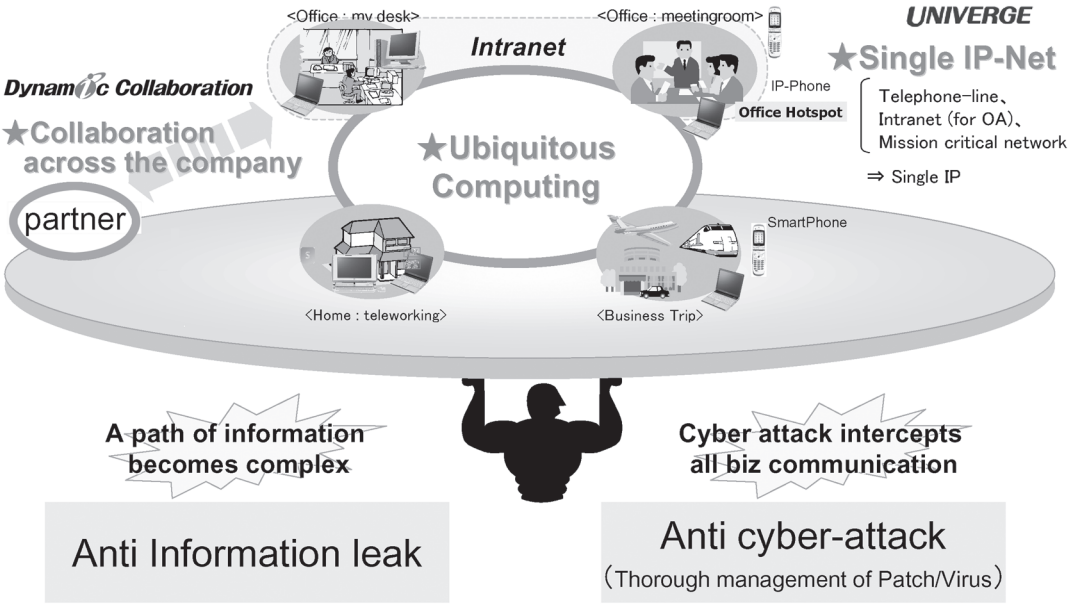

Fig . 5 Concepts of connectivity improvement.

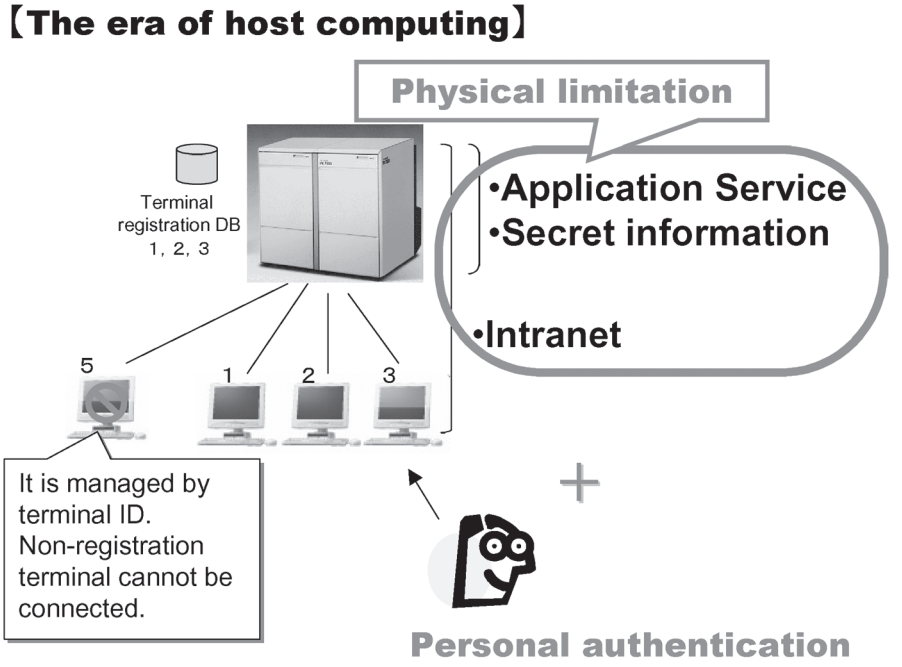

Fig. 6 Taking a lesson from the past.

mistakes or criminal acts by an employee. Theft and loss of a mobile PC are also included in these mistakes. In this case an attack on an encryption key finally becomes a problem (See Section 3.5). This means that the insufficiency is only in the rules.

The means of personal authentication is inadequate for an anti-cyber attack measure. By reasons such as the following, measures by manpower exceed an acceptable limit. Therefore, a management tool was introduced.

- Increase of management input
  - Measures machinery:
    - Gateway only → All network terminal
  - An approach path from the outside:
    - Several places of specification → grasp inability
  - Men:
    - Cracker → +employee, Contracted employee
  - Attack: Crack → +WORM, Spyware
- Moving up of deadline
  - Infection speed : Few days → Dozens of minutes
- Complexity
  - Work of patch adaptation is difficult by instructions in a document.

Unmanaged PCs, which are connected to the intranet obstruct management by this tool. Unmanaged PCs may be private property to be brought in from the outside. It is impossible for a traditional means of personal authentication to distinguish a PC that is private property. And the thoroughness of management collapses.

That is, we need a safer means of key management and a means of applying physical limits at a higher level.

5.2 Limiting PCs Physically by TPM

The recent (and future) networks are not rigidly fixed. A new means of physically limiting the access areas for application services, secret information and intranet may be accommodated by changes to the network. In other words, security levels are maintained abreast of connectivity improvements.

Figure 7 shows the means of limiting PCs physically by TPM.

The terminal ID was a mere number, but the new method uses a digital certificate. When a PC is registered, it receives a digital certificate from the server. The public key of such a digital certificate is automatically registered in the Server.

The certificate offered from a server can precisely distinguish a PC. In other words, the platform authentication keeps a definite border. Means only of software have weak points. Terminal-ID, MAC-address, Product-ID, installation-ID and so on can be falsified. A digital certificate stored in HDD is copied. By combination with a capability of TPM, the platform authentication becomes useful at last.

In addition, the platform authentication with TPM enables thoroughness of management tools by the shutting out of non-managed PCs.

That is TPM can shut out an information leak and cyber attack by controlling physically access to intranet, application servers and secret documents.

Figure 8 shows usage of platform authentication for each solution.

"CapsSuite" can shut out cyber attack by physically controlling access to intranet, so that it has a compelling force for the installation of patches and update of virus pattern.

"ServerW@ll" can shut out cyber attack and an information leaks by physically controlling access to a server, so that it has a compelling force for the installation of patches and updates of virus patterns. It does not accept connection from PCs that are unrelated to the job.

"InfoCage" can shut out an information leak by physically controlling access to a secret file, so that it does not allow connection from PCs that are unrelated to the job.

5.3 Key Management

Recent mobile computing (and ubiquitous computing of the future) increases the risk of theft or the loss of mobile PCs. For these measures, issues of attack to

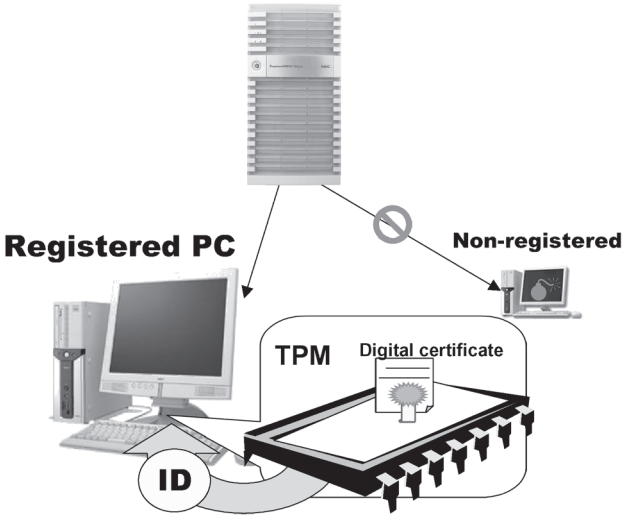

Fig. 7 Platform authentication.

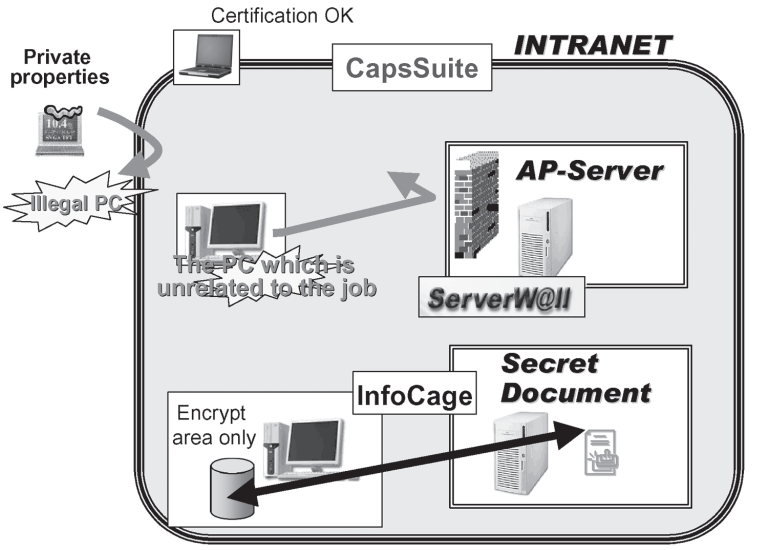

Fig. 8 Image of platform authentication for each solution.

an encryption key must be solved conclusively. In other words, it is essential that the encryption key is not accessed directly.

"InfoCage" can shut out an information leak by physically controlling access directly for private encryption keys of secret files in a PC so that it stores the private encryption keys in TPM.

In the others, TCG announces the software utilizing key management of TPM.

"RSA SoftID" can prevent leak of seed, secret number for remote access systems, so that it stores the seed in TPM.

"Checkpoint Securemote" can prevent illegal copies of digital certificates, so that it stores the private keys of certificates in the TPM.

6. CONCLUSION

This paper introduced important considerations of PC security regarding recent issues relating to solutions by TPM embedded PCs. It also explains about the function, internal structure, data structure and API of TPM.

NEC will continue to attach great importance to ongoing security for business PCs.

To conclude this paper, I thank Software Business Unit for solutions by utilizing the "TPM embedded PC" and all of you for your positive cooperation.

REFERENCE

[1] Trusted Computer Group, http://www.trustedcomputinggroup.org/

---

*Windows is a registered trademark of Microsoft Corporation and used in the USA and other countries.

†Intel is a registered trademark of Intel Corporation and used in the USA and other countries.

‡Other names of companies and products are trademarks or registered trademarks of each company.

Received December 27, 2004

* * * * * * * * * * * * * * * *

Takahisa SHIRAKAWA graduated from the Kyoto Institute of Technology in 1988. He joined NEC Home Electronics Corporation in 1988, and is now Engineering Manager of the Business Client Department, Client And Server Division, NEC Corporation. He is engaged in the planning of Business Client from a solutions viewpoint.