Trusted Computing Platforms, the Next Security Solution

Siani Pearson
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2002-221
November 5th , 2002*

E-mail: Siani.Pearson@hp.com

trusted platform, trusted computing platform, TCPA, root-of-trust, privacy

Would you allow a complete stranger in your house if he couldn't provide an ID? Now would you let him use your computer? Learn how to trust others on the Internet and a network with this exciting technology.

* Internal Accession Date Only
www/informit.com, August, 2002

Approved for External Publication

Trusted Computing Platforms, the Next Security Solution

Siani Pearson

Trusted Systems Lab,
HP Laboratories,
Filton Rd, Bristol. BS34 8QZ. UK.
Siani.Pearson@hp.com

Abstract

Would you allow a complete stranger in your house if he couldn't provide an ID? Now would you let him use your computer? Learn how to trust others on the Internet and a network with this exciting technology.

Introduction

An important new technology has recently been developed that will revolutionize trust and security for online transactions. Based on the concept of incorporating a hardware "root of trust" within PCs and other platforms, it allows users to assess the trustworthiness of computers with which they interact. This article, abstracted from a new book on the subject, explains the key concepts and the exciting potential of Trusted Computing Platforms (often abbreviated to *Trusted Platforms*).

This article covers the following topics:

- Why are Trusted Platforms being developed?
- What are the Trusted Computing Platform Alliance (TCPA) and the TCPA Specification?
- What is a Trusted Platform?
- Basic concepts in the TCPA model
- The main functionalities of a Trusted Platform
- Benefits of using Trusted Platform technology
- Summary of TCPA technology

Why Are Trusted Platforms Being Developed?

Computer platforms are becoming widely available and are central to the growing reliance on electronic business and commerce. In addition, the need to protect information is increasing, particularly on the type of computers we use directly (client platforms such as PCs). Although businesses now use secure operating systems on servers and have physically protected individual server platforms, no overall corresponding improvement in client platforms has occurred, because of the ad hoc way in which client platforms develop, the sheer number of such platforms, and the cost.

The flexibility and openness of the PC platform has enabled phenomenal business growth, and attempts to prohibit that flexibility and openness would meet with resistance. Given a choice between convenience and security, most users opt for convenience. This makes improving confidence in client platforms—PCs in particular—a big challenge.

No single company dictates the architecture of all platforms on the same network or the plan of that network itself. Although other types of platforms are increasingly being used for Internet access, the diversity of software and hardware for PCs continues to mean that the principal client platforms of the Internet are still PC-based. As conventional businesses increasingly depend on PCs and the Internet for their success—even their very existence—the trustworthiness of PCs and other platforms is an increasingly vital issue. The development of e-services and the convenience of using the same computer platform for both personal and business activities mean that users increasingly need to store and use sensitive data on their platforms. Of course, they expect their data to be protected from misuse even when they're connected to the Internet.

However, the ability to protect a PC or other computing platform through software alone has developed as far as it can, and has inherent weaknesses. The degree of confidence in software-only security solutions depends on their correct installation and operation, which can be affected by other software that's installed on the same platform. Even the most robust and tightly controlled software cannot vouch for its own integrity. For example, if malicious software has bypassed the security mechanisms of an operating system (OS) and managed to corrupt the behavior of the OS, by definition it's impossible to expect that the OS will necessarily be aware of this security breach. It's often possible to find out whether software has been modified when you know what modification to look for (for example, a known virus). However, on current computing platform technology, it isn't easy for a local or remote user to test whether a platform is suitable to process and store sensitive information. For example, it's possible to identify an employee accessing a corporate network through a virtual private network (VPN) gateway, but it's impossible to establish with confidence whether the computing

platform used by the employee is a corporate machine, and runs only the required software and configurations.

Experts in information security conclude that some security problems can't be solved by software alone, and even conventional secure operating systems depend on hardware features to enforce separation of user and supervisor modes. Privacy issues have arisen such as the conflict of duty between providing confidence in a computing platform's behavior to the owner of a company PC, and providing confidence in the platform's behavior to the individual user of that PC. Also, differences exist between providing confidence in a platform's behavior to a local user and providing that confidence to a remote entity across a network.

The Trusted Computing Platform Alliance and the TCPA Specification

These issues, coupled with emerging e-business opportunities that demand higher levels of confidence, have led to the Trusted Computing Platform Alliance (TCPA) (http://www.trustedcomputing.org/) designing a specification (http://www.trustedcomputing.org/docs/main v1_1b.pdf) for computing platforms that creates a foundation of trust for software processes, based on a small amount of hardware within such platforms.

The TCPA specification is intended for use in the real world of electronic commerce, electronic business, and corporate infrastructure security. The specification is a mixture of informative comment and normative statements that give a list of all the things that must be done.

What Is a Trusted Platform?

A *Trusted Platform* is a computing platform that has a trusted component, probably in the form of built-in hardware, which it uses to create a foundation of trust for software processes. The computing platforms listed in the TCPA specification are one such type of Trusted Platform. Although different types of Trusted Platforms could be built, we concentrate in particular on the (version 1.1) instantiation specified by the TCPA industry standard.

Converting a platform into a Trusted Platform involves extra hardware roughly equivalent to that of a smart card, with some enhancements.

At the time of writing, secure operating systems use different levels of hardware privilege to logically isolate programs and provide robust platform operation, including security functions.

Converting a platform into a Trusted Platform requires that TCPA *roots of trust* be embedded in the platform, enabling the platform to be trusted by both local and remote

users. In particular, cost-effective security hardware acts as a root of trust in Trusted Platforms. This security hardware contains those security functions that *must* be trusted. The hardware is a root of trust in a process that measures the platform's software environment. In fact, it could also measure the hardware environment, but the software environment is important because the primary issue is knowing what the computing engine is doing. If the software environment is found to be trustworthy enough for some particular purpose, all other security functions—and ordinary software—can operate as normal processes. These roots of trust are core TCPA capabilities.

Adding the full set of TCPA capabilities to a normal, non-secure platform gives it some properties similar to that of a secure computer with roots of trust. The resultant platform has robust security capabilities and robust methods of determining the state of the platform. Among other things, it can prevent access to sensitive data (or secrets) if the platform is not operating as expected. Adding TCPA technology to a platform doesn't change other aspects of platform robustness, so a non-secure platform that's enhanced in the way described above is not a conventional secure computer and probably not as robust as a secure platform that's enhanced in the same way. Nevertheless, we believe that the architectural changes proposed in the TCPA specification are the cheapest way to enhance security in an ordinary, non-secure computing platform. The architectural cost of converting a secure platform into a Trusted Platform is even less, because it requires fewer TCPA functions.

Any type of computing platform—for example, a PC, server, personal digital assistant (PDA), printer, or mobile phone)—can be a Trusted Platform. A Trusted Platform is particularly useful as a connected and / or physically mobile platform, because the need for stronger trust and confidence in computer platforms increases with connectivity and physical mobility. In addition to threats associated with connecting to the Internet, such as the downloading of viruses, physical mobility increases the risk of unauthorized access to the platform—including actual theft. Trusted Platform technology provides mechanisms that are useful in both circumstances.

The first Trusted Platforms containing the new hardware will be desktop or laptop PCs. They'll protect secrets—keys that encrypt files and messages, keys that sign data, and authorization data—using access codes, binding of secrets to a particular physical platform, digital signing using those secrets, plus mechanisms and protocols to ensure that a platform has loaded its software properly. Later, Trusted Platforms will provide more advanced features such as protection of secrets depending on the software that's loaded (for instance, preventing a secret from being accessed if unknown software has been loaded on the platform, such as hacker scripts) and attestation identities for e-services. The technology is certain to evolve in the coming years.

Trusted Platforms are an unfamiliar concept, even to security specialists. However, since the release of TCPA specification v1.0 in February 2001 and its backing by IT organizations and companies, Trusted Platforms are set to become widely available.

The adoption of Trusted Platforms is an important step toward improving confidence in conducting business over the Internet and broadening the scope of e-services. TCPA technology allows existing applications to benefit from enhanced security and encourages the development of new applications or services that require higher security levels than are presently available. Applications and services that would benefit from using Trusted Platforms include electronic cash, email, hot-desking (allowing mobile users to share a pool of computers), platform management, single sign-on (enabling the user to authenticate himself or herself just once when using different applications during the same work session), virtual private networks, Web access, and digital content delivery. The functions of the security hardware are relatively benign as far as product export/import regulations are concerned, and all contentious security functions are implemented as security software and can be changed as required for individual markets.

Another important Trusted Platform property is that the functions of the security hardware operate on small amounts of data, permitting acceptable levels of performance even though the hardware is low cost. In contrast, the normal platform processor is used by a Trusted Platform's security software to manipulate large amounts of data and, as a result, to take advantage of the excellent price-to-performance ratio of normal computer platforms.

Determining the integrity of a platform—trusting a platform—is a critical feature of a Trusted Platform. Security mechanisms (processes or features) are used to provide the information needed to deduce the level of trust in a platform. Only the user who wants to use the platform can make the decision whether to trust the platform. The decision will change according to the intended use of the platform, even if the platform remains unchanged. The user needs to rely on statements by trusted individuals or organizations about the proper behavior of a platform. This aspect ultimately differentiates a Trusted Platform from a conventional secure computer.

Basic Concepts in the Trusted Platform Model

Figure 1 illustrates the general setup for a Trusted Platform Model. The Trusted Computing Platform Alliance has published documents that specify how a Trusted Platform must be constructed. Within each Trusted Platform is a *Trusted (Platform) Subsystem*, which contains a *Trusted Platform Module* (TPM), a *Core Root of Trust for Measurement* (CRTM), and support software (the *Trusted platform Support Service* or TSS). The TPM is a hardware chip that's separate from the main platform CPU(s). The CRTM is the first software to run during the boot process and is preferably physically located within the TPM, although this isn't essential. The TSS performs various functions, such as those necessary for communication with the rest of the platform and with other platforms. The TSS functions don't need to be trustworthy, but are nevertheless required if the platform is to be trusted. In addition to the Trusted Subsystem in the

physical Trusted Platform, Certification Authorities (CAs) are centrally involved in the manufacture and usage of Trusted Platforms (TPs) in order to vouch that the TP is genuine.

Readers with a background in information security know that a *Trusted Computing Base* (TCB) is roughly the set of functions that provide the security properties of a platform (in other words, that enforce the platform's security policy). The TCB in a Trusted Platform is the combination of the Trusted Subsystem (mainly dealing with secrets) and additional functions (mainly dealing with the use of those secrets, such as bulk encryption). As such, the Trusted Subsystem is a subset of the functions of the Trusted Computing Base of conventional secure computers, which would normally include both dealing with secrets and using secrets. Critically, however, the Trusted Subsystem contains some functions not found in a conventional TCB. Conventional secure computers provide formal evidence that a TCB in certain states actually can be trusted. This is done by means of formal assessment and certification of the platform in a particular configuration.

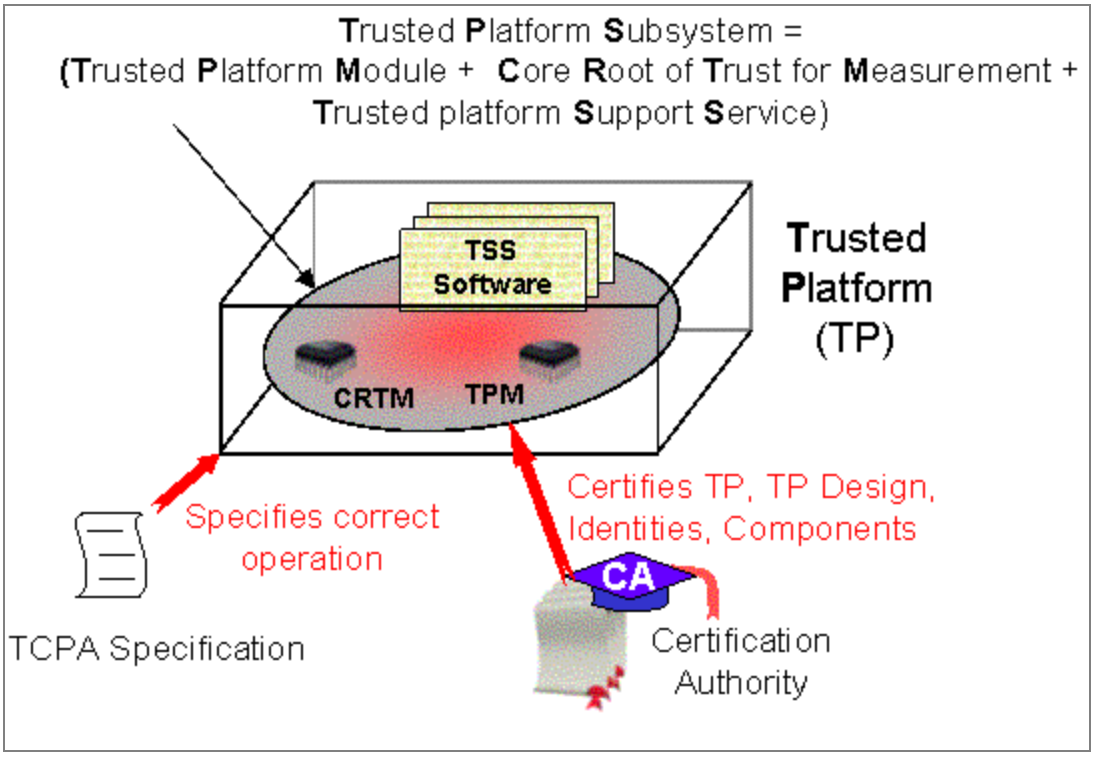

Figure 1

The overall Trusted Computing Platform model.

In contrast, the Trusted Subsystem provides a less formal means of showing that the TCB is both capable of being trusted and actually can be trusted in a variety of configurations. The Trusted Subsystem first demonstrates that *it* can be trusted and

then demonstrates that the *remainder* of the TCB in a Trusted Platform can also be trusted. This involves certification from trusted entities that are prepared to vouch for the platform in various configurations.

Basic Functionalities of a Trusted Platform

A Trusted Platform is a normal open computer platform that has been modified to maintain privacy. It does this by providing the following *basic functionalities*:

- A mechanism for the platform to show that it's executing the expected software
- A mechanism for the platform to prove that it's a Trusted Platform while maintaining anonymity (if required)
- Protection against theft and misuse of secrets held on the platform

We'll consider each of these requirements in turn.

Integrity Measurement and Reporting

Starting from a root of trust in hardware, a Trusted Platform performs a series of measurements that record summaries of software that has executed (or is executing) on a platform. This process is illustrated in Figure 2. Starting with the CRTM, there's a boot-strapping process by which a series of Trusted Subsystem components measure the next component in the chain (and/or other software components) and record the value in the TPM. By these means, each set of software instructions (binary code) is measured and recorded before it's executed. Rogue software cannot hide its presence in a platform because, after it's recorded, the recording cannot be undone until the platform is rebooted. The platform uses cryptographic techniques to communicate the measurements to an interested party, so the recorded values cannot be changed in transit.

Creation of Trusted Identities

It remains, therefore, to prove that the measurements were made reliably. This is the same as proving that a platform is a genuine Trusted Platform. That proof is provided by cryptographic attestation identities, and the process is illustrated in Figure 3. Each identity is created on the individual Trusted Platform, with attestation from a PKI Certification Authority (CA). Each identity has a randomly generated asymmetric cryptographic key and an arbitrary textual string used as an identifier for the pseudonym (chosen by the owner of the platform). To obtain attestation from a CA, the platform's owner sends the CA information that proves that the identity was created by a genuine Trusted Platform. This process uses signed certificates from the manufacturer of the platform and uses a secret installed in the new (in the sense of unique) hardware

in a Trusted Platform; that is, the Trusted Platform Module (TPM). That secret is known only to the Trusted Platform and is used only under control of the owner of the platform. That secret never needs to be divulged to arbitrary third parties; the cryptographic attestation identities are used for such purposes.

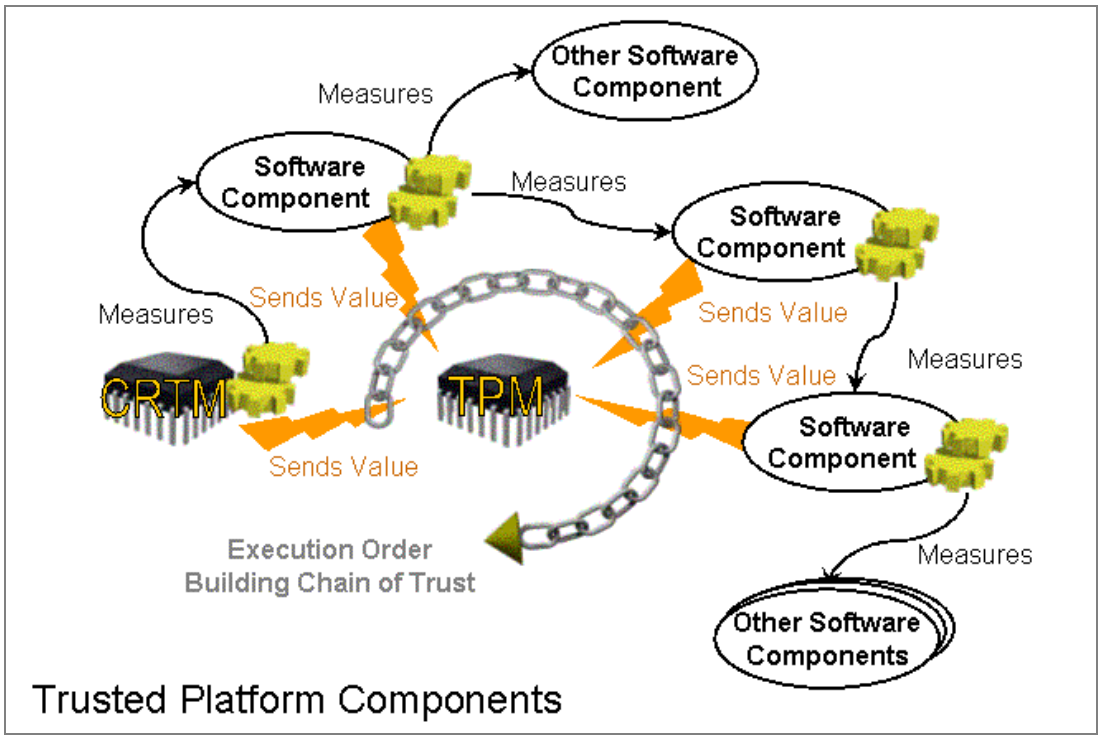

Figure 2

The measurement process for a Trusted Platform.

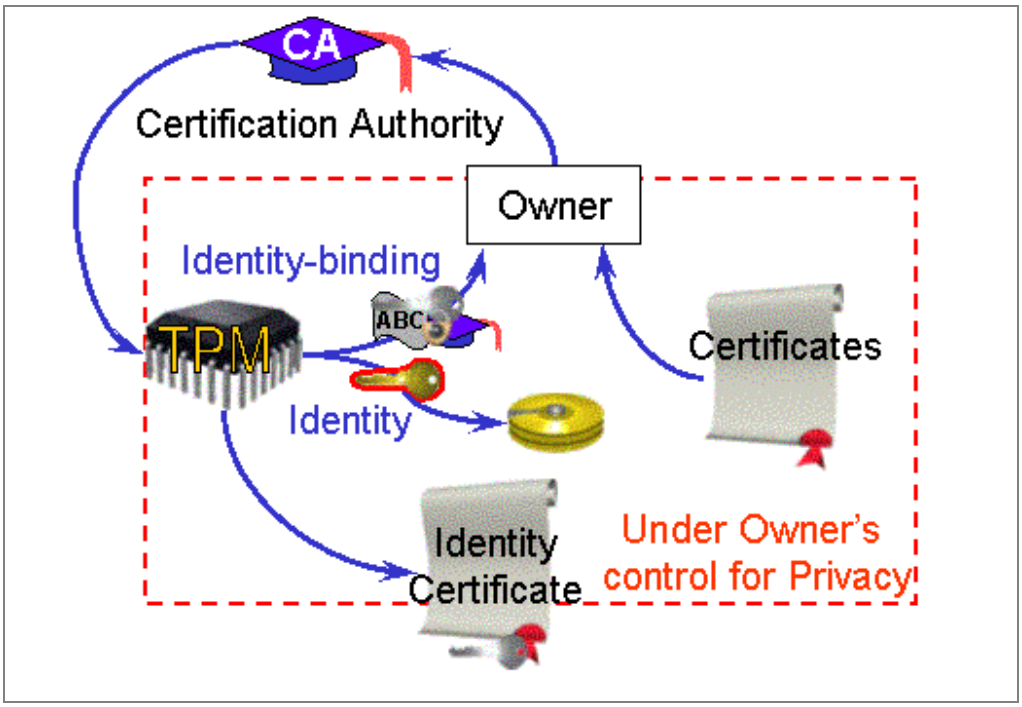

Figure 3

Obtaining proof that a platform is a Trusted Platform.

Protected Storage

A TPM is a secure portal to potentially unlimited amounts of protected storage, although the time to store and retrieve particular information could eventually become large. The portal is intended for keys that encrypt files and messages, keys that sign data, and for authorization secrets. For example, a CPU can obtain a symmetric key from a TPM and use it for bulk encryption, or can present data to a TPM and request the TPM to sign that data. The portal operates as a series of separate operations on individual secrets. Together, these operations make a tree (hierarchy) of *TPM protected objects* (also referred to in the TCPA specification as "blobs of opaque information," which could either be "key blobs" or "data blobs"), each of which contains a secret encrypted ("wrapped") by the key above it in the hierarchy. But the TPM knows nothing of this hierarchy. It's simply presented with a series of commands from untrusted software that manages the hierarchy. An example of such a hierarchy is illustrated in Figure 4.

An important feature that's peculiar to Trusted Platforms is that a TPM protected object can be "sealed" to a particular software state in a platform. When the TPM protected object is created, the creator indicates the software state that must exist if the secret is to be revealed. When a TPM unwraps the TPM protected object (within the TPM and hidden from view), the TPM checks that the current software state matches the

indicated software state. If they match, the TPM permits access to the secret. If they don't match, the TPM denies access to the secret.

Benefits of Using Trusted Computing Technology

Both companies and consumers receive commercial benefits from Trusted Platforms. In this section, we briefly discuss the following:

- Benefits of using Trusted Platforms that will emerge in the short, medium, and long term
- How Trusted Platforms encourage greater customer confidence
- How Trusted Platforms encourage e-business and enhanced e-services

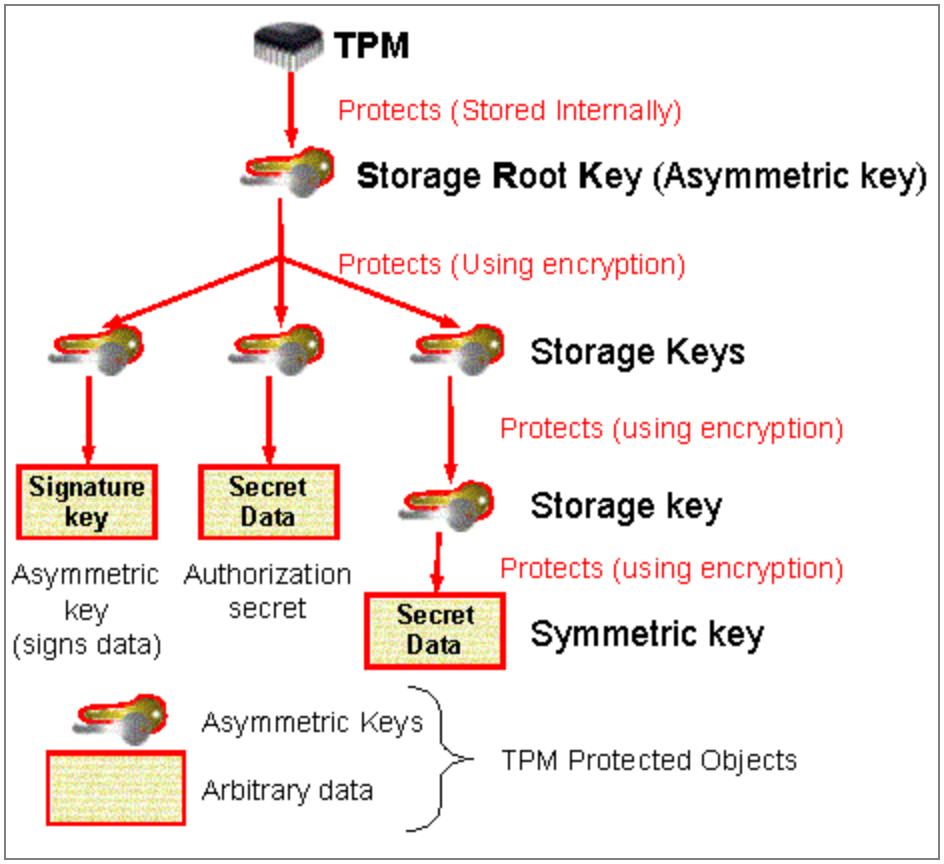

Figure 4

A storage hierarchy.

Benefits to the User

Probably the most important aspect for users is that Trusted Platforms provide a low-cost way to trust a software environment for some particular purpose.

A TP allows users to answer the following questions (see Figure 5):

- Am I appropriately authorized? (platform authentication)
- How can I have confidence that my computing platform will behave in the way I expect? (integrity)
- How can I trust a remote system that's not under my control? (integrity)

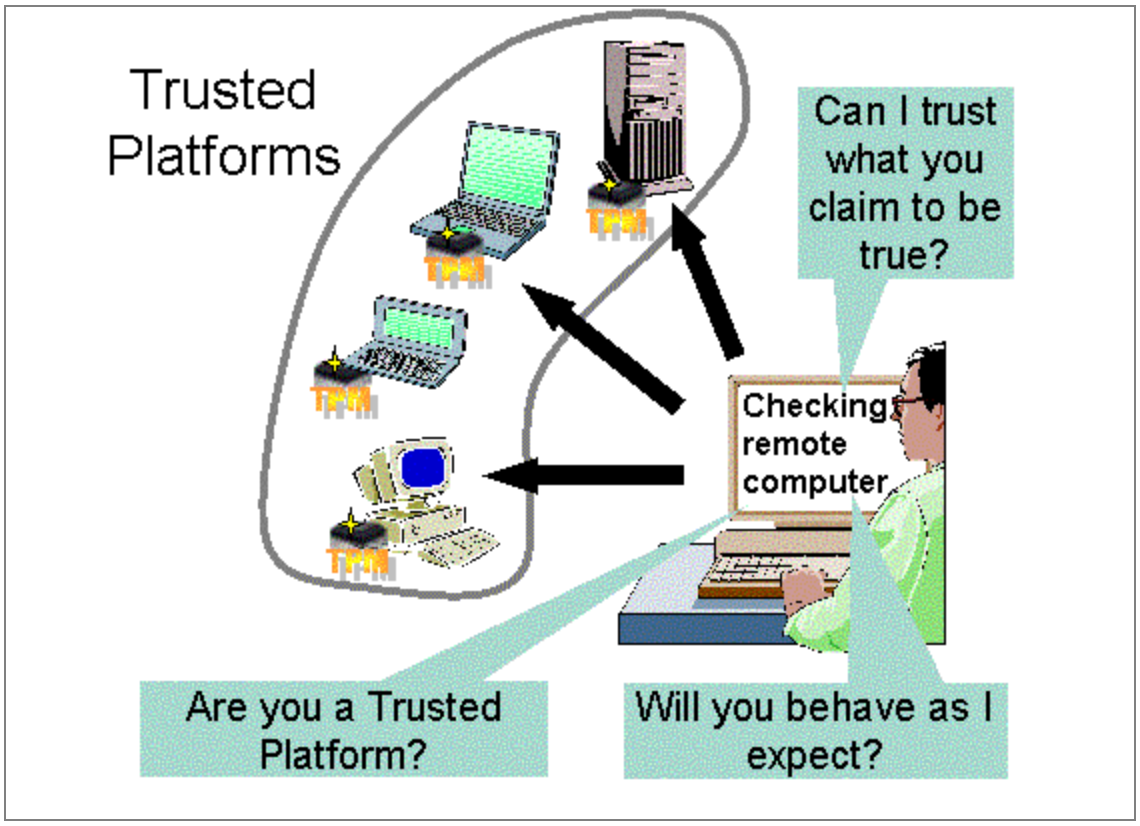

Figure 5

Questions addressed by Trusted Platforms.

In addition, a TP supports any means of user authentication. Therefore, it can support the continuing personalization of web sites and user mobility, such as VPN and hot-desking.

The Trusted Platform architecture is designed to provide immediate, medium-term, and long-term benefits to users. Longer-term benefits are predicated on software improvements: All TPM chips support all TCPA functions, but existing software applications are not designed to take advantage of them. When TCPA platforms are more common, it's anticipated that customers and *Internet service vendors* (ISVs) will start developing applications that use these more advanced functions. The most advanced functions require a public key infrastructure (PKI) and are designed for use by e-services.

Short-Term (Immediate) Benefits

In the short-term, benefits of Trusted Platforms are likely to be based on "protected storage" functions. Customers can use protected storage to protect the confidentiality of data on their hard disks in a way that's fundamentally more secure than pure software solutions. You'll need a basic TCPA implementation with a TPM chip embedded within a platform and associated software provided by the TCPA chip manufacturer.

In providing protected storage, the TPM does the following:

- Acts as a portal to encrypted data
- Provides an option (which doesn't have to be used) such that encrypted data can then be decrypted only on the same platform that encrypted it
- Provides for digital signature keys to be protected and used by the TPM

Medium-Term (Intermediate) Benefits

In the medium term, benefits of Trusted Platforms will probably also involve the measurement of integrity metrics relating to the software environment on the platform, for use by the platform. This scenario is the same as the short-term solution, but it requires additional software. Customers can then protect their sensitive data against hacker scripts, by automatically preventing access to data if unauthorized programs are executed.

The specific mechanism has the following properties:

- It uses the TPM chip.
- It acts as a portal to encrypted data, such that this data can be decrypted only if the platform has a given set of software environment integrity metrics. If a hacker loads a script, the presence of that script changes the state of the software environment and the TPM denies access to any secrets that were linked to that previous software environment. The script still executes, but it can't access any such secrets and can't interpret any information protected by such secrets.

This feature can be exploited through software at different levels in the software stack, ranging from stand-alone applications to a fully TCPA-aware operating system (OS).

Long-Term Benefits

Longer-term benefits of Trusted Platforms involve the reporting of integrity metrics relating to the software environment on the platform, for use by third parties. This benefits e-business. The scenario requires additional public key infrastructure (PKI) support, whether restricted to a corporation or extended across organizational boundaries.

Users and their partners, suppliers, or customers can connect their IT systems and expose only the data that's intended to be exposed.

The specific mechanism has this feature:

- TCPA provides reporting of integrity metrics of the software environment on a specific platform. This allows a remote party to verify the software environment in a TCPA platform *before* sending data to that platform. This provides confidence in the software state and identity of a remote party, enabling higher levels of trust when interacting with this party.

Both trusted clients and trusted servers can use this feature.

How Trusted Platforms Create Better Customer Confidence

Trusted Platforms can help create better customer confidence in several ways, including the following:

- Enhanced security using hardware
- Feedback about trust to the user
- A technological foundation for privacy
- Trustworthy digital signature

Hardware-Based Security

Processes that execute on specialist security hardware are better protected than processes that execute on ordinary computing engines. These protected functions are much more resistant to interference and snooping from logical or physical attack, so there is greater confidence in those processes than in processes that execute on an ordinary computing engine.

In a conventional platform with a conventional crypto co-processor, the co-processor protects all its functions from logical and physical attack but doesn't protect processing on the ordinary CPU. A Trusted Platform provides logical and physical protection for secrets and logical protection for the data protected by those secrets (which is processed on one of the main CPUs). The TPM acts as a conventional co-processor for secrets, and the integrity mechanisms prevent the release of secrets to inappropriate processing environments and permit a local or remote user or computer to verify the trustworthiness of a platform before interacting with that platform. So a Trusted Platform protects a larger number of processes than a conventional platform with a conventional crypto co-processor: A critical few processes—dealing with secrets—are protected by a minimalist crypto co-processor. Other processes on data that uses secrets are less protected than they would be inside a crypto co-processor. This is because no physical protection exists, for example, against deletion. But they're better protected than ordinary processes outside a crypto co-processor because the confidentiality and integrity of the data are protected.

Specifically, a Trusted Platform provides hardware protection for keys and other secrets, which would normally be used to encrypt files or gain access to servers or other networks. The TPM prevents the release of secrets until presentation of an authorization value and / or the presence of a particular TPM and / or the presence of a particular software state in the platform. The TPM prevents inappropriate access to encrypted files and network resources by, for example, snooping around a hard disk, moving a hard disk to another platform, or loading software to snoop on other processes.

Provision of Feedback about Trust to the User

By interacting with Trusted Platforms using smart cards or handheld computers such as personal digital assistants (PDAs), a user can decide whether to trust a computer or computing infrastructure.

A smart card or other handheld computer can be programmed to interrogate a Trusted Platform (local or remote), retrieve identity information and integrity metrics, and compare the identity and integrity metrics with expected values. If they differ, the smart card or handheld computer user can refuse to interact with the Trusted Platform because it's the wrong computer or because it's in an inappropriate software state and not to be trusted for the intended purpose.

This enables a user to access an arbitrary computer platform in an organization or public area, or an arbitrary server, and to determine whether it can be trusted to work on private information and not reveal the private information without authorization from the user.

Provision of a Technological Foundation for Privacy

Both businesses and individuals are increasingly concerned with the privacy of their confidential and personal information, particularly when their computer platforms are connected to networks.

In the computing context, privacy provides a way to prevent others from gaining access to information without the informed consent of its owners. Cell phones, telephone caller ID, credit cards, and the Internet provide people with a dramatic new level of freedoms that can enhance business processes and personal lives, but these innovations come with privacy concerns. All of these systems are capable of providing information, including financial and personal data that most users assume to be private. The TCPA believes that the ability to ensure such privacy is an essential prerequisite of a trusted system. This privacy needs to be as robust as any other aspect of the trust in the system. [TCPA white paper, "TCPA Security and Internet Business: Vital Issues for IT," August 2000 (http://www.trustedcomputing.org/docs/TCPA_IT_WP.pdf)]

Privacy controls should determine whether it's permissible to reveal that the information exists and the circumstances in which the information can be disclosed or used. A credit card number is not secret, for example, but it is private. Only the owner of a credit card has the right to use the credit card number. Others who have been given the credit card number should not disclose, distribute, or use the number in a manner that's not approved by the card owner. It follows that data is rendered private if the owner of the data can control distribution of information about the data, or even knowledge of the existence of that data. Whether particular data should be treated as private data depends on the nature of the data and the opinion of the owner of that data. Some people are not concerned about privacy, and others are. One person may consider that a particular type of data must be private, while another may not.

Any data, even secret data, can have a privacy attribute. Some data associated with Trusted Platforms doesn't require security protection but could be considered privacy-sensitive by some users. The best such examples are public asymmetric keys (such as the public Endorsement key) and X.509 certificates (such as the Endorsement Certificate and identity certificates). To maintain the privacy of such data, the TCPA specification requires that access to such data be under the control of the owner of that data. An owner who's not concerned about privacy can distribute the data or publish its existence to his heart's content. An owner who is concerned about privacy should use whatever mechanisms are provided to prevent others from accessing the data or learning about the data.

TCPA provides a novel form of privacy protection by preventing the revelation of secrets unless the software state of a platform is in an approved state. If secrets are kept on a server built on a Trusted Platform, a user can verify that the server is the expected platform and is operating as expected even before sending private information to the

server. After a user's private information is on a server, the user can be reassured that data in the server will become unavailable if the software environment on the server changes (during a hacker attack, for example). Thus, the secret should never be used in unapproved circumstances.

Some aspects of privacy are expressed in Trusted Platforms through explicit commands or special features of commands or protocols. These commands or enhancements enable the TPM owner to dictate some aspect of a TPM's behavior, such as whether it will do "real work" and whether it will accept an owner. For example, the entire notion of TPM identities exists only to provide privacy when a TPM owner uses a signing key that identifies his platform. A user has multiple trusted attestation identities that are associated with a TPM, which is particularly useful in e-business because different identities can be associated with different types of tasks. The technology prevents someone from building up a profile of the user by combining behavior associated with different identities. A user can use one identity when dealing with a bank, another identity when buying goods, and yet another identity when posting opinions to a newsgroup. An identity can have any arbitrary name or label (even the user's real name, if he or she wishes), yet each identity can prove that it corresponds to a Trusted Platform. A third party can still track the consistency of a user's behavior and benefit from being able to inspect the environment on the associated platform to see if it's trustworthy, but the third party can't correlate activities performed using different identities. (Or, at least, exploiting TCPA mechanisms cannot enable such a correlation.)

TCPA also respects the privacy of a user of a Trusted Platform. TCPA differentiates between the *user* of a Trusted Platform and the *owner* of a Trusted Platform. The owner has certain privileges over a TP, but a user's data is private; even the owner of the platform can't access that data without permission from the user. Hence, a platform could be owned and used by a single owner or user (in the case of a consumer or small business), or owned by one entity and used by another entity. This would be the case in a corporate environment, where the IT department is the owner, and the user is the individual to whom the platform has been issued.

Provision of Trustworthy Digital Signatures

Digital signatures will become more important as they gain greater legal status, and Trusted Platforms can support and enhance the use of digital signatures. Users realize these benefits in the following ways:

- A Trusted Platform protects signature keys using the TPM, never reveals those keys outside the TPM, and uses such keys to digitally sign data submitted to the TPM.

- A Trusted Platform can enhance digital signatures by incorporating integrity metrics that indicate the software state of the platform when data is signed.

- Depending on the implementation of the TPM, a Trusted Platform can further enhance signatures to guarantee that what is signed corresponds to what was seen by the signer.

Benefits to Business

The higher levels of trust that are enabled by Trusted Platforms are valuable to businesses for the following reasons:

- Companies gain by being trustworthy.
- Brand image suffers if there is a breach of trust or privacy.
- Better trust enables more powerful management services.
- Consumers' trust is an important business enabler.
- Improved trust and security are necessary to the delivery of business-critical e-services.

Summary of TCPA Technology

Trusted Platforms get their name from the fact that they enable either a local user or a remotely communicating user to trust a platform for some particular purpose. A behavioral definition of trust has been adopted: *An entity can be trusted if it always behaves in the expected manner for the intended purpose.*

The Trusted Computing Platform Alliance (TCPA) is an industry alliance formed in October 1999 that focuses on developing and standardizing Trusted Platform technology. The TCPA specification, released in February 2001, is designed to be independent of the type of platform (PC, server, PDA, printer, mobile phone, and so on). A single hardware chip (costing about the same as a smart card) will typically perform the TCPA-defined trusted functions. All other functions will be performed by normal software. The TCPA architecture is designed to provide immediate, intermediate, and long-term benefits to users. Some features will be available immediately, while other features require further software development (expected shortly). The most advanced features require a public key infrastructure and are designed for use by e-services.

A TCPA-enabled system offers a low-cost standardized means of embedding security functionality in a platform. As a result, improved levels of security can become ubiquitous. The capabilities provided by a TCPA-compliant platform benefit both consumers and business and have been defined to be independent of a specific market focus. In particular, a Trusted Platform allows users to have confidence that their

computing platform will behave in the way they expect, and also to trust remote systems that are not under their control.

This technology is promoted by major companies such as HP, IBM, Intel, and Microsoft. Trusted Platforms are likely to appear on the market from 2002 onward. These computers can be used as a foundation for many different types of trusted e-service. For example, TCPA-compliant PCs in public places could enable people to authenticate themselves to the network, attest to the trust level of the PC, and then conduct their business in security before leaving. Trusted Platforms can potentially enhance application areas as diverse as manageability, storage, virtual private networks (VPN), and intrusion detection. Therefore, this specification is starting to excite a great deal of interest as security experts and users appreciate its potential and the necessity of this technology for the expansion of e-commerce.

The TCPA home page (http://www.trustedcomputing.org/) is a source of useful information.

Acknowledgements

This article is compiled from material from "Trusted Computing Platforms: TCPA Technology in Context", edited by Siani Pearson, written by Boris Balacheff, Liqun Chen, Siani Pearson, David Plaquin and Graeme Proudler, pub. Prentice Hall, 2002. ISBN 0-13-009220-7.