CHAPTER 1

Trusted (Computing) Platforms: An Overview

A platform is any computing device—a PC, server, mobile phone, or any appliance capable of computing and communicating electronically with other platforms. In this chapter, you’ll discover the reasons why Trusted Platforms—also called Trusted Computing Platforms—are being developed and read a summary of the technology and its evolution. The chapter is intended to provide a wide audience with a standalone summary of Trusted Platforms and their context. The conceptual and political framework have been included in this chapter for your convenience. Boxes will be used to highlight important summaries.

This first chapter covers the following points:

- A brief overview of what Trusted Platforms provide
- Consideration of what “trust” means in terms of technology, in order to explain how the technology described in this book can be said to provide “trusted platforms”
- Assessment of the need for Trusted Platforms and why such platforms are important in a business context
- A summary of the main features of Trusted Platforms, including the protection of users’ privacy
- A look ahead to a world in which Trusted Platforms are ubiquitous

Note that this chapter provides motivation and context for the book, so those readers who are familiar with the background to TCPA technology may wish to move on to Chapter 2.
Summary of Trusted Platform Concepts

Before assessing the nature and value of Trusted Platforms in more detail, we summarize the need for Trusted Platforms, how this relates to the Trusted Computing Alliance and its specifications, and the basic concepts behind Trusted Platform technology.

Why Are Trusted Platforms Being Developed?

Computer platforms are ubiquitous; they are central to the growing reliance on electronic business and commerce, and the need for information protection is increasing, particularly on client platforms. Although businesses have deployed Secure Operating Systems on servers (for example, [HP 2001]) 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 them, and the cost.

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

No single company dictates the architecture of all platforms on the network or the plan of the network itself. Although other types of platforms are increasingly being used for Internet access, the diversity of software and hardware available 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 platforms and PCs is an increasingly vital issue. The development of e-services and the convenience of using the same computer platform for both personal and business use mean that users increasingly need to store and use sensitive data on their platforms. Of course, they naturally expect their data to be protected from misuse even when they are 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 execution, which can be affected by other software that has been executed 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 that OS’s behavior, it is by definition impossible to expect that the OS will necessarily be aware of this security breach. It is often possible to find out whether software has been modified when one knows what modification to look for (e.g., looking for a known virus). However, current computing platform technology does not allow a local or remote user to easily test whether a platform is suitable to process and store sensitive information. For example, currently it is possible to identify an employee accessing a corporate network through a virtual private network (VPN) gateway, but it is impossible to establish with confidence whether the computing platform used by the employee is a corporate machine and whether it runs only the required software and configurations.
Experts in information security conclude that some security problems cannot be solved by software alone, for example, trusted hardware is needed as the basis for software security mechanisms such as those described by [Lampson et al., 1992], and even conventional Secure Operating Systems depend on hardware features to enforce separation of user and supervisor modes. Furthermore, 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) designing a specification for computing platforms that creates a foundation of trust for software processes, based on a small amount of hardware within such platforms. A brief history of the Trusted Computing Platform Alliance (the organization set up to develop and standardize Trusted Platform technology), including its organizational structure and objectives, can be found in Appendix A.

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); this book attempts to provide more explanation than is given in the specification.

What Is a Trusted Platform?
A Trusted Platform (TP) is a computing platform that has a trusted component, probably in the form of built-in hardware, and uses this to create a foundation of trust for software processes. The computing platforms specified 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 instantiation specified by the TCPA industry standard. (Note that terms like Trusted Platform are italicized in this chapter because we are using them in a specific way.)

In this book, we concentrate on the issue of converting a platform into a Trusted Platform. The conversion process involves extra hardware roughly equivalent to that of a smart card, with some enhancements.

At the time of this 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, which enable 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 it is the software environment that is important because knowing what the
computing engine is doing is the primary issue.) 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 does not change other aspects of platform robustness, so a non-secure platform that is enhanced in the way described above is not a conventional secure computer and probably not as robust as a secure platform that is enhanced in this way. Nevertheless, we (the authors of this book) claim 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.) We further contrast trust and security mechanisms in the “Trust Versus Security” section later in this chapter.

Any type of computing platform (for example, a PC, server, Personal Digital Assistant or PDA, printer, or mobile phone) can be a TP. A TP 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. Not only are there threats associated with connecting to the Internet, such as the downloading of viruses, but physical mobility increases the risk of unauthorized access to the platform (including physical theft). TP technology provides mechanisms that are useful in both of these circumstances.

The first Trusted Platforms containing the new hardware are expected to be desktop or laptop PCs. They will provide protection of secrets (i.e., keys that encrypt files and messages, keys that sign data, and keys that contain 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, TPs will provide more advanced features such as protection of secrets depending on the software that is loaded (i.e., 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 over the coming years.

Trusted Platforms are an unfamiliar concept, even to security specialists, but since the release of TCPA specification v1.0 in February 2001 and its backing by major industry players, they are set to become widespread. The adoption of Trusted Platforms is a building block to 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 or more ubiquitous security levels than presently available. (Some examples are presented in Chapter 2.) 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 (removing the need for the user to be asked to authenticate himself or herself more than 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 export/import contentious security functions are implemented as security software (and can be changed as required for individual markets). Another important TP 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 TP’s security software to manipulate large amounts of data and, hence, 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 (i.e., processes or features) are used to provide the information needed to deduce the level of trust in a platform. The decision itself can be made only by the user who desires to use the platform, and this 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. It is this aspect that ultimately differentiates a Trusted Platform from a conventional secure computer.

Basic Concepts in the Trusted Platform Model

![Figure 1-1 The overall Trusted Computing Platform model](image-url)
Figure 1-1 illustrates the general setup that we consider in this book. The Trusted Computing Platform Alliance has published documents that specify how a Trusted Platform (TP) 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—TSS). The TPM is a hardware chip that is 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 is not 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 do not themselves need to be trustworthy, but they 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 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 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 TCB 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. The accreditation shows that the platform can operate securely if it is operated in a particular way, but it is said to be unusual for platforms to actually be operated in tested configurations! 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.

<table>
<thead>
<tr>
<th><strong>Basic Definitions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform</strong></td>
</tr>
<tr>
<td><strong>Trusted Computing Platform Alliance (TCPA)</strong></td>
</tr>
<tr>
<td><strong>Trusted (Computing) Platform (TP)</strong></td>
</tr>
<tr>
<td><strong>Trusted Platform Module (TPM)</strong></td>
</tr>
<tr>
<td><strong>Trusted Platform Subsystem</strong></td>
</tr>
<tr>
<td><strong>Certification Authority (CA)</strong></td>
</tr>
</tbody>
</table>
Why Are Trusted Platforms ‘Trusted’?

This section attempts to give a succinct analysis of trust, including consideration of both behavioral and social components. (Further discussion of the nature of trust may be found in Appendix B.) This provides important context for explaining the sense in which TCPA provides trust mechanisms.

Trust: A Complex Notion

Pinning down the meanings of many words can be difficult. Trust is particularly tricky because it is not a simple notion. Typically, we think in terms of Entity A trusting Entity B for something, which is complex for the following reasons (among others):

Not always transitive: If A trusts B and B vouches for C, does A trust C in this case? In other words, is trust a transitive notion? The answer is “not always,” although it can be under specific circumstances.

Dynamic: Trust is dynamic rather than static; there can be differing phases in a relationship such as building trust, ongoing trust (a stable relationship), and declining trust. Trust can be lost quickly, as noted by Nielsen: “[Trust] is hard to build and easy to lose: a single violation of trust can destroy years of slowly accumulated credibility” [Nielsen 1999].

Varying degree and scope: Trust levels differ both in the sense of varying degree and scope of trust: Entities typically trust—or do not trust—one another to fulfill selected obligations or for a particular purpose, rather than for everything. On the other hand, trust in certain areas can transfer to trust more generally, as shown by major brands having an advantage when moving into new areas of business.

However, it is useful to have a succinct definition of trust if at all possible, particularly if you are claiming to provide an increased level of trust in something. Most dictionaries define (at least one use of the word) trust in wording similar to the following: “a firm belief in the reliability or truth or strength, etc., of a person or thing.” However, this is not the end of the story. To date, we have no universally accepted scholarly definition of trust, although “confident expectations” and “a willingness to be vulnerable” are usually viewed as critical components. Evidence from a contemporary, cross-disciplinary collection of scholarly writing suggests that a widely held definition of trust is as follows: “Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another” [Rousseau et al. 1998]. Yet this definition does not fully capture the dynamic and varied subtleties considered above.

In general, we can conclude that it is difficult to define trust because there are different facets of trust. When “trust” is applied in an online business context, these facets include the following:

- A technological basis that is mainly the concern of this book
- A contractual side that includes both laws and underwriting or contracts
Customers’ image that is built up via previous interactions with a company, brand image, publicity, etc.

In Appendix B, some of the major attempts to provide social theories of trust are considered, as well as how such reasoning has been applied to the e-commerce domain. Such background analysis supports further consideration in this section of the extent to which trust is increased by using TCPA technology.

Different Approaches to Trust: Behavioral vs. Social Components

As noted, there are different aspects to trust. The TCPA definition of trust is that something is trusted “if it always behaves in the expected manner for the intended purpose.” A similar approach is adopted in the third part of ISO/IEC 15408 standard: “A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference” [ISO/IEC 15408].

We believe that categorizing trust in terms of behavioral (dynamic) and social (static) components helps in understanding how Trusted Platforms enhance trust.

- The special processes in a Trusted Platform dynamically collect evidence of behavior and provide evidence of behavior. This information provides the means of knowing whether a platform can be trusted.
- The social definition of trust concentrates on what it is to be trustable—capable of behaving properly, i.e., trustworthy in a social sense, when people agree that the trusted thing is good and fair and will do the right things. Social trust in a Trusted Platform is an expression of confidence in behavioral trust, because it is an assurance about the implementation and operation of that Trusted Platform. Trusted Platforms use social trust to provide confidence in the mechanisms that collect and provide evidence of behavior; they also use social trust to provide confidence that particular values of evidence represent a platform that is in a “good” state. This information thus provides the means of knowing whether a platform should be trusted.

Clearly, both aspects of trust are necessary. Processes in a Trusted Platform provide information about the behavior of a platform, but that information cannot be trusted unless someone vouches for the method of providing the information and for the expected value of the information.

The Trust Mechanism Provided by TCPA

Trusted Platforms meet the need for increased confidence in platforms. This (social) confidence comes from declarations by trusted third parties that the platform can be trusted for the intended purpose. These third parties are prepared to endorse a platform because they have assessed the platform and are willing to state that if measurements of the integrity of that platform are such-
and such, it can be trusted for such-and-such purposes. The local user and remote entities trust the judgment of the third parties, so if the platform proves its identity and the measurements match the expected measurements, they trust that the platform will behave in a trustworthy and predictable manner.

For an entity to decide whether a computing platform can be trusted, TCPA specifies a measurement method and a way for the measurement method to show itself to be trustworthy. The first Trusted Platforms have two roots of trust. One root of trust starts the measurement process and is called the Root of Trust for Measurement (RTM). The RTM is very much platform-dependent and can vary by type of platform. The other root of trust stores the results of the measurement processes as they happen, in such a way that measurements cannot be “undone.” It cryptographically reports the current measured values and prevents the release of a secret if the current measured values do not match the values stored with that secret. This root of trust is the Root of Trust for Reporting (RTR), but the term is rarely used because the RTR is independent of platform type, and it is implemented as the Trusted Platform Module (TPM). We argue that the RTM and the TPM are the minimal roots of trust that you need. When any platform starts, you need to form measurements about the way the platform is operating. It is necessary to have a core element that you absolutely trust and that you cannot avoid trusting. The Root of Trust for Measurement must be a computing engine, in order to be able to make measurements and do something with those measurements. In a PC, the RTM is the entire computing platform itself. It consists of some code (inside the BIOS or the BIOS Boot Block in PCs) that starts a series of measurements involving the processor, wiring that is laid down in the printed circuit board, and other components that form part of the computing engine. This code is both critical and essential. The RTM makes the measurements and stores the answers in the TPM. Typically, this is instantiated as a single tamper-resistant chip. What goes on inside the chip cannot be tampered with by the platform, by the user themselves, or by a third party. The TPM is something that is trusted by everyone: Everyone agrees to believe that if something says it comes from a TPM, then what it says can be believed.

**Trusted and Trustable**

How do we trust that these elements are operating in the correct manner—for example, that the code is doing what it should? As far as the TPM is concerned, a so-called endorsement key is embedded into the TPM. This key is signed by the manufacturer and published in the form of a digital certificate. The manufacturer puts its brand name behind guaranteeing that the chip that contains this particular key (to be more specific, that contains a certain asymmetric key pair) is a genuine TPM that will operate as intended. Thereafter, whenever the TPM uses the endorsement key, you know that the resultant data came from a genuine TPM. This is the only way of recognizing a specific genuine TPM, and it uses social trust (“trustable”) as discussed in the preceding subsection. In other words, the reason you trust a specific TPM is that you can inspect the certificate, which is a trustable assertion by the company that made it. Other elements of a Trusted Platform also have certificates. These vouch for the design of a Trusted Platform—that a specific
TPM was incorporated into a TP, that the design of the RTM and TPM meet the TCPA specification, and so on. Any trust in a security system at the end of the day comes back to trust in the individuals, trust in companies, trust in brand names that vouch for the system, and so on.

Clearly, it is necessary to use both aspects of trust (i.e., trusted and trustable). Protocols and services should be designed in such a way that everyone agrees that no gaping holes exist in them and that bad things will not happen when those protocols are used. At the same time, even if someone tells you that a service is trustable, you want to know that it is executed properly. You know this by making measurements and checking the results of these measurements against values that have been created and signed by someone that you trust.

**The Value of Trusted Platforms**

Now that we have described the philosophy behind Trusted Platforms, let’s consider why such platforms are so valuable in cyberspace.

With the demand for commercial advantage and the pace of software development, it is important to evolve the information infrastructure to meet new challenges. Despite real and increasing security threats, security technology in cyberspace is in its infancy. The virtual world lacks the mature methods of physical security that have taken many years to evolve. Critical technology infrastructure such as public key infrastructure and intrusion detection systems are only at early stages of deployment. Legislation in cyberspace is lagging, and fundamental notions such as the “electronic signature” have only just been introduced. The often cross-border nature of cyber activities adds difficulty to the task of ensuring secure interactions. The general public has only limited understanding of cyberspace, and individuals and businesses are often ignorant of the measures they should take to protect their interests. This is why the National Plan for Information Systems Protection in the United States [White House 2000] covers education as
The Value of Trusted Platforms

well as legislation and technology aspects. In summary, threats against information security are real and growing, yet the current computing infrastructure lacks a cheap or ubiquitous method of defense.

In this section, we show how Trusted Platforms can form part of the solution by enhancing trust and confidence in computer platforms. Let’s take a look at the following:

- Security threats
- The limitations of existing security technology
- Why Trusted Platforms are needed
- The benefits of using Trusted Platforms

Security Threats and the Need to Evolve the Current Infrastructure

Figure 1-2 depicts some different types of threats in a typical networked environment. These are some of the more important security threats, for different entities both inside and outside a corporate network:

- Virus and worm introduction, or planting of capabilities to perpetrate or facilitate future attacks (e.g., Trojan horses)
- Software tampering and piracy
- Theft of data, software, and hardware
- Insider threats (reportedly both the most common and most damaging)
- Repudiation (i.e., false denial that previous transactions have occurred)

![](image)

**Figure 1–2 Security threats**
Authorization violation (i.e., inappropriate access by partners and unauthorized log-ins)

Denial of service attack, either intentional or unintentional

Safeguards (often called security services) can be put in place to prevent or deter threats from being realized, or to reduce their impact. Such services include authentication, access control, confidentiality, data integrity, and non-repudiation. However, use of such services will not give total protection. Later in the book, we will show that Trusted Platforms can strengthen existing security services, albeit at the expense of additional Denial Of Service (DOS) attacks. (TPs provide no additional defense against DOS attacks, and because they introduce more complex mechanisms, they actually invite more DOS attacks.)

Security threats are real and growing, as shown in Figure 1-3. Figure 1-4 shows that the acknowledged cost of cyber attacks (as reported in [FBI/CSI 2001]) for 1998, 1999, and 2000 averaged $250 million and is increasing. The cost is probably significantly higher than indicated by the respondents to this survey, because most losses caused by security breaches are considered “company confidential” and are never publicly identified.

![Figure 1–3 Unauthorized usage of computer systems](data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAQAAAABACAYAAAAU59f2AAAACXBIWXMAAAsTAAALEwEAmpwYAAAD1SURBVC1B7f+Xv8AAAAASUVORK5CYII=


Figure 1–3 Unauthorized usage of computer systems
The Value of Trusted Platforms

The Limitations of Existing Security Technology

Trusted Platform technology is not the only approach that aims to enhance confidence in computing platforms. This section discusses current methods and introduces the need for additional technology. Existing security infrastructure consists primarily of the following:

- Firewalls for “boundary protection” [Cheswick & Bellovin 1994]
- Security software, e.g., virus-checking software
- Cryptographic accelerators/co-processors [Smith et al. 1998]
- Security protocols, e.g., the Secure Sockets Layer (SSL) (now called TLS) for confidential communication

We mention briefly each type of existing security technology in the following sections.

Firewalls

Security “firewalls” provide boundary protection for computer networks, but these can become a bottleneck. Furthermore, to enable new functionalities and services, it has become common practice to increase the number of “holes” through firewalls through which dynamic content and programs are “punched” (for outbound or inbound traffic). Thus, an organization is faced with either restricting such new traffic (often an unpopular move) or evolving the firewall to deal with the new situation.

Software Security Programs

A plethora of software programs is available to provide security functionality. These programs might run inside a cryptographic co-processor or on the main platform processor (sometimes embedded in the operating system in the main platform environment) and provide a range of...
functions from straightforward encryption to desktop firewalls. Software that runs on the main processor implicitly assumes that it is running in a safe environment, so maximum confidence is actually delivered only if the software is installed and executing properly. Even then, secrets are stored as normal data, or perhaps in protected files or partitions on the hard disk. When a program executes on the main processor, its secrets are potentially exposed and may be vulnerable to eavesdropping by rogue programs. Data stored on disks may also be vulnerable to eavesdropping.

Software is vulnerable to attack by viruses, of which thousands of varieties exist. The “Nimda” and “Code Red” worms created problems in corporate infrastructures in autumn of 2001, and new strains of viruses are being continually developed and released into the computing and Internet environments. Viruses can attack even security software. Several proprietary applications are available for detecting viruses, preventing their entry and cleaning up if an attack does take place: Symantec’s Norton antivirus toolkit program is one such application. However, virus strains are developing continually, and although parts of the antivirus software are frequently updated, it does not provide reliable protection against unknown viruses.

Cryptographic Co-processors
Another type of existing security product is the cryptographic co-processor, or accelerator (e.g., those provided by Eracom, IBM, Lockheed, nCipher, Thales, Rainbow, and HP). Accelerators such as the IBM4758 are highly credible, self-contained high performance computing engines. These contain specialist hardware and firmware to provide security functions, often faster than can be provided by a general-purpose platform processor. They provide a protected environment for secrets and can include mechanisms that detect attempts to gain access to the secrets. If such an attempt is found, the accelerator can often erase its secrets and disable its functions. A cryptographic accelerator might provide a bulk (symmetric) encryption service, plus generation of keys from a genuinely random source. Prices can be hundreds of U.S. dollars.

IBM currently has PC products with a security chip incorporated on the motherboard. These don’t have “roots of trust” but do have some security functions (primarily “protection of secrets”) provided by a Trusted Platform.

The manner in which Trusted Platform hardware differs from cryptographic co-processors is in both function and integration into the platform architecture. Trusted Platforms require two separate additional functions, one (called a “CRTM”) built into the boot process and the other (called a “TPM”) that communicates with the CRTM and the host platform’s processor: See Chapter 3 for a better introduction to these functions and their technical details.

Carrying out sensitive processing inside a cryptographic co-processor is an entirely acceptable solution to the problem of creating a trusted environment. Moreover, cryptographic co-processors may be preferred over a Trusted Platform in some circumstances, because the co-processor can do bulk encryption in a physically protected environment. However, such specialized hardware is too expensive to be automatically included in all platforms, so it is not possible for ubiquitous platform security to be based on conventional crypto co-processors. The Trusted Platform should be seen as an alternative to the crypto co-processor with its own benefits, including lower cost.
Other Specific Technologies

A number of techniques have been used to enhance levels of confidence in computing platforms: These include compartmentalized mode workstations, embedded software, Boot Integrity Services (Intel), Microsoft security services in their current versions of operating systems (Microsoft Windows 2000) [Microsoft], and the Java “sand box.”

In addition, a great number of security protocols and mechanisms might be implemented in either hardware or software. For example, the Internet Engineering Task Force (IETF) standards include the Transport Layer Security (TLS) and Internet Protocol Security Protocol (IPSEC). Such standards, together with others like Secure Multi-Purpose Internet Mail Extensions (S-MIME), Internet Key Encryption (IKE), and virtual private network (VPN), have been designed to provide different security features, such as user authentication, access control, and confidentiality. [Kohl & Neuman 1993] and [Wobber et al 1994] give some examples of possible solutions. Other technologies that either use or support platform security include digital signatures, watermarking, smart cards, public key infrastructure (PKI), and biometrics. Any of these techniques that involve software executing on the main CPU necessarily rely upon the correct operation of the host computing platform.

Why Do We Need Trusted Platforms?

The increase in online business transactions has created new needs. One of these needs is for cost-effective security hardware that does not fall foul of product export and import regulations. Trusted Platforms can supply this.

The lack of a cheap enabler has been a restraint on the development of solutions/services that could rely on platform security. And the lack of solutions/services that rely on platform security has been a restraint on the development of the platforms themselves.

In this section, we consider why we provide user confidence using trust mechanisms rather than security mechanisms (albeit that the trust mechanisms are provided by security mechanisms) and why an increased need for Trusted Platforms exists. We also look at the main problems that Trusted Platforms are designed to overcome and the advantages that are obtained over a more conventional security approach.

Trust Versus Security

The trust mechanisms in a Trusted Platform reliably generate, store, and report measurements about the software environment in a platform. A user who wants to trust that platform (for some particular purpose) gets the measurements (called “integrity metrics”) about the platform and compares them with expected values. If the measured values are the same as the expected values, the user will interact with the platform (for that particular purpose). Otherwise, he or she should not. (Strictly speaking, only the actual user knows the level of confidence that he requires in order to trust a platform to do a particular job and hence the expected measurement values.) “Social trust” is directly involved because the user trusts other organizations or individuals to say “these particular
values indicate that the platform can safely be used for such-and-such purpose.” The actual required values could differ according to the particular intended use of the platform.

Why are Trusted Platforms preferable to secure platforms? There are several reasons. Technologically, existing secure computers have no way of proving that they are operating as expected. This is a weakness in a world in which platforms are exposed to attack, data is increasingly mobile, and connections are increasingly dynamic. Commercially, trade in information security equipment is still subject to government scrutiny (although perhaps not to the same degree as in the past). The most important answer, however, is that although modern commerce would benefit from a higher level of confidence in platforms, conventional secure platforms are too expensive and too painful to use (untrained users are not sympathetic to the fact that the security is visible to the user!), or perhaps just unnecessary. Secure computers have existed for decades and still are not ubiquitous. Trusted Platforms attempt a different approach.

When people think of information security, they think of secure data. Confidence in secure data relies on confidence in ownership of secrets: The recipient of data trusts it because the recipient knows who owns the underlying secret. It follows that trust in cryptography relies on “social” trust—the statement by some trusted person or organization that such-and-such key belongs to such-and-such entity.

Trusted Platforms may be considered as an attempt to go back to basics, in that they provide confidence by directly exposing the “social trust” that underpins all information security. The distinguishing feature of a Trusted Platform is that it enables someone to vouch for a platform and its integrity. As it turns out, this requires the use of conventional security techniques, but these are simply enablers. The provider of an electronic service, for example, can use a Trusted Platform to prove that a service is the proper service and that the service is operating as the provider expects. This provides greater confidence to both the provider and the user of the service. This is not the whole story, of course. Trusted Platforms must be economically priced and designed to minimize the impact of government regulations on trade in information security equipment. Therefore, TCPA Trusted Platforms include functionality that duplicates the best of currently available similar equipment (confidentiality of data on the platform), functionality that addresses a known problem to which no current solution exists (preventing access to secrets by some types of “bad” code, such as hacker scripts), and functionality that exposes the social trust in a Trusted Platform. This range of functions is intended to convince customers that Trusted Platforms provide useful benefits now and in the future.

Information Integrity and Platform Integrity

The problem of platform integrity is heightened by a changing business environment with a greater reliance on the use of networked computers and an increasing use of PCs. Enhanced trust in the proper operation of local or remote computing platforms is needed if critical business deals are to be carried out online. Such deals would greatly simplify current procedures that must be done offline or “out of band” by other, more trusted, traditional mechanisms.
A computer platform has integrity if the applications running on it execute without interference. Existing security solutions assume the integrity of the platforms on which they operate. In particular, they assume that secrets can be safely stored and used on a computing platform. The owner of a platform may feel satisfied with the integrity of their own platform because the owner is in control of the software environment and history (previous behavior including interactions, physical modification, and software execution) of their platform. However, platforms are increasingly connected and exposed to threats from the Internet. This means that such confidence may be misplaced. A third party is in an entirely different situation to an owner, because the third party usually knows nothing about the environment and history of a remote platform. A third party, therefore, has no explicit confidence in the integrity of a remote platform.

Therefore, if a platform is required to reliably prove its integrity, it follows that there is a need to report integrity measurements and a need for proof that a platform can reliably report integrity measurements. How Trusted Platforms provide such a measurement is explained in the gray section later in this chapter, and in more detail in Chapter 3.

Finally, Trusted Platforms fulfill the need for protected storage for secrets (i.e., protection for cryptographic keys and platform authorization data, for example, that must remain confidential). Trusted Platforms provide a mechanism for encrypting secrets securely using the new hardware in a Trusted Platform (i.e., the TPM). Further, they provide a mechanism for associating encrypted secrets with a physical platform and ensuring that such data is only accessible on that same platform. When such secrets are encrypted, constraints can also be specified about the software environment that must exist in order for the secrets to be released. This last mechanism is not available from existing security solutions.

Using Trust to Simplify Security

A Trusted Platform can provide an alternative solution to using complex conventional security protocols. By way of example, look at the case in which certain security protocols are used to prevent divulgence of sensitive information among parties. These parties must provide sensitive information in order to cooperate, but they do not trust each other with sensitive information. For best confidence, those protocols should operate in trustworthy platform environments. But if these protocols operate in trustworthy environments, why not use a simpler protocol with the knowledge that the platforms can simply be trusted not to reveal the sensitive information to other parties? In particular, a Trusted Platform would be able to provide just as good a solution by ensuring that secrets from multiple parties are not revealed to a platform unless the platform both executes software that performs the desired operation and also does not reveal to any party a secret belonging to another party.

Main Problems: Hardware Cost and Exportability

The main problems that had to be addressed by TCPA were the cost of hardware cryptographic co-processors and the fact that different co-processors could be required for different marketplaces because of product export/import regulations. Governments can (and do) impose restric-
tions on the use of security equipment, so a co-processor that is legal in one country may not be in another. These restrictions apply mainly to strong confidentiality for bulk data (messaging and filing). Countries such as the United States, France and Britain have relaxed their import/export rules in recent years, but it is always possible that those rules will be strengthened again and that other marketplaces have their own security restrictions.

These problems are serious obstacles to the ubiquitous inclusion of security in computer platforms. TCPA hopes to succeed by using simple, low-cost, security hardware with functionality that avoids the import/export trap. TCPA can be regarded, in one sense, as an experiment to test the international marketplace for ubiquitous platform hardware security. To do so, the TCPA sets an industry standard for platform security features and interfaces.

We have already mentioned that ordinary crypto co-processors are too expensive to be fitted “as standard” in the intensely competitive and price-sensitive computer market. Substantial reductions in co-processor cost can be achieved by minimizing the size, functionality, and performance of the co-processor (greater production volumes also decrease cost, but sufficient motivation for this must exist). The problem is that cheap hardware executes symmetric “bulk” encryption (the most common form of encryption used to provide confidentiality for files and messaging) much slower than can be done on a modern central processing unit (CPU). Higher performance specialist hardware is capable of symmetric encryption at the same rate as the main CPU (or even better than the main CPU), but it is unlikely to be as cost-effective because the CPU (obviously) can be used for multiple purposes and because of the numbers in which CPUs are manufactured. If ubiquitous security software existed that relied on hardware protection, it is possible that high performance hardware could be manufactured in such quantities to be cost-effective. However, no such ubiquitous security software exists because no ubiquitous security hardware exists, and no such ubiquitous security hardware exists because no ubiquitous security software exists. This results in deadlock.

TCPA cuts this Gordian knot by inserting simple hardware into a platform, to act as a root of trust for that platform. While a conventional crypto co-processor provides hardware protection for its security processes, a hardware root of trust in an otherwise normal platform provides software protection for the platform’s software processes, at the same time that it maintains all the advantages of a normal, open computing platform. The root of trust enables gathering and reporting of evidence about the trustworthiness of the platform’s main processing environment. The simple TP hardware contains all the functions that must be trusted if the evidence is to be trusted. After it is proven to be trustworthy, the platform’s processing environment can be used for bulk encryption. Serendipitously, it transpires that all the functions that must be trusted are functions that operate on small amounts of data, so the performance of low-cost hardware is acceptable. Furthermore, it transpires that the functions that must be trusted are relatively non-contentious as far as product import and export are concerned. Thus, the hardware can be low-cost, and different versions of hardware for different marketplaces are not required.

TCPA calls “all the things that must be trusted” the Trusted Platform Module (TPM). To be precise, TCPA does not mandate that the TPM be implemented in hardware; it merely specifies the TPM’s properties. Thus, it is possible for an entire computer platform to act as its own
TPM, provided that the platform has the necessary properties. In reality, most TPMs will be hardware devices that are built into a platform. It can be argued that a Trusted Platform is the cheapest way to enhance security in a non-secure platform, because a TPM includes just the minimum functions that must be trusted. This residual hardware cost cannot be eliminated because, as already mentioned, it is axiomatic that the integrity of a platform cannot be proven using software only.

We have already introduced the (logical) concepts of root of trust for measurement and root of trust for reporting. Originally, it was intended that the TPM would be the single physical root of trust in a platform and provide both logical roots of trust. In the first PC implementation specification [TCPA 2001c], however, two physical roots of trust exist because it was considered to be too commercially risky and expensive to integrate the CRTM into a TPM. The CRTM itself is currently specified to be a (physical) root of trust in a memory device that protects it against unauthorized alteration. The TPM is the other root of trust, with more extensive protection mechanisms than the CRTM. Eventually, it is desirable that the CRTM instructions are migrated to the TPM, because the TPM can provide much better control over those instructions. The roots of trust cooperate to enable a process by which integrity metrics can be obtained. Integrity metrics are measurements about the platform and are used to prove that the host platform is in a state in which it can be used to process sensitive data. As will be seen later, integrity metrics can be used to prove to a local user or a third party that a platform is operating as expected and to prevent the release of secrets unless a platform is executing particular software. This feature is new to Trusted Platforms.

In summary, the requirement on enhancing trust and confidence in e-business must satisfy a number of criteria, such as low cost and exportability; otherwise, such security mechanisms will never become ubiquitous. So it is necessary to identify the absolute minimum set of functionality that must be trustworthy if the overall platform is to be trusted, protect those things, and leave the rest “as is.” Trusted Platform functionality is designed to provide the base capabilities essential to the implementation of security solutions, in a low-cost hardware device. The development of software that exploits these capabilities will allow for the strengthening of existing application security and for the development of new applications relying on platform integrity. The potential for ubiquitous availability of TCPA could provide the environment for the development of new security solution architectures (in other words, architectures within which software is trusted to perform operations involving sensitive data).

The Benefits of Using Trusted Computing Technology

You will see that both companies and consumers receive commercial benefits from Trusted Platforms. In this section, we briefly discuss the following:

- The 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

Some of this confidence can be transferred to trust in companies themselves; Appendix B includes a section highlighting reasons why this would benefit companies.
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 Trusted Platform allows users to answer the following questions (see Figure 1-5):

- 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 is not under my control? (integrity)

In addition, a Trusted Platform supports any means of user authentication. Therefore, it can support the continuing personalization of web sites and user mobility, e.g., VPN and hot-desking. A Trusted Client can take part in riskier transactions than might otherwise be possible. For further details, see Chapter 2, which looks at applications of Trusted Platform technology.

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 is 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.

Figure 1–5 Questions addressed by Trusted Platforms
The Value of Trusted Platforms

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 is 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 does not 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 cannot access any such secrets and cannot interpret any information protected by such secrets.

This feature can be exploited through software at different levels in the software stack, ranging from standalone 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 support, whether restricted to a corporation or extended across organizational boundaries.

Users and their partners, suppliers, or customers can connect their IT systems together and expose only the data that is 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 in 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 does not 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 (because no physical protection exists, for example, against deletion), but are better protected than ordinary processes outside a crypto co-processor (because the confidentiality and integrity of the data is 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 snooping around
a hard disk, or moving a hard disk to another platform, or loading software to snoop on other processes, for example.

**Provision of feedback about trust to the user**

By interacting with *Trusted Platforms* using smart cards or handheld computers, 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 are different, the smart card or handheld computer user can refuse to interact with the Trusted Platform because it is the wrong computer or because it is 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 2000b]

Privacy controls should determine whether it is 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 is not approved by the card owner. It follows, therefore, that data is rendered private if the owner of the data can control distribution of information about the data, 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* do not 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 some such data is under the control of the owner of that data. An owner who is not concerned about privacy can still 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 via 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 is trustworthy, but the third party cannot correlate activities performed using different identities. (Or, at least, the correlation cannot be done by exploiting TCPA mechanisms.)

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 Trusted Platform, but a user’s data is private; even the owner of the platform cannot 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 it could be 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.

This issue of privacy is discussed in a more technological context later in this chapter.

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. You’ll realize these benefits:
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. (This issue is considered further in Chapter 14.)

**Support for security services and improved e-services**

TCPA embeds trust and security functionality into computing platforms to properly anchor existing security services; it also provides a basis for improved security services and services that use security. *Trusted Platforms* are deliberately designed to support existing security techniques, even though the TP may lead to the development of improved security techniques that eventually supplant existing techniques. *Trusted Platforms* are even deliberately designed to use existing security techniques to provide the functions of a *Trusted Platform*, and TCPA invents new processes only when necessary. This is critical, and not just a matter of preference: The best security techniques are those that have been subject to study for a long time, yet are still considered to be secure.

The TCPA limits itself to the specification (rather than supply) of *Trusted Platforms* and services derived from *Trusted Platforms*. TCPA *Trusted Platforms* provide the base for software and services at all levels to meet new e-business expectations, whether that base is for platform manufacturers’ products and services or their customers’ own products and services built with/on such platforms.

**The importance of trust for e-commerce**

Consumers’ lack of trust is a major inhibitor to e-commerce, although the expected boom in the use of e-commerce has yet to materialize. There are many contributing factors including brand familiarity, web-site navigation, fulfillment of transactions (i.e., delivery of goods), the lack of sociability of using the Internet to shop, the inability to touch and try goods, and the non-immediacy of receipt of goods. However, according to most surveys on the subject, it appears that consumers’ lack of trust in the Internet is a major reason for not buying online ([Cheskin 1999], [GVU], and [AT&T 1999]). Fears about security are an important aspect of this lack of trust. For example, in order to access an e-service in electronic commerce, you may have to communicate with a platform with which you have had no previous contact. In this case, how can you believe that you are contacting the correct business entity and that the behavior of that entity’s platform is appropriate? How can you even ensure that your local personal computer remains trustworthy, because it may be accessed by remote software during the service?

For e-commerce to be effective, each of the components that combine to make up the system must be trustworthy. Any breach of security at any one of the levels will add to the feeling of distrust that users have toward shopping online. Indeed, it seems that the media’s dramatization of security breaches has already made a substantial contribution toward users’ inherent lack of confidence.
It is not surprising that consumers are worried about the vulnerabilities in the system. On September 13, 1999, British Prime Minister Tony Blair succinctly captured the worries that people have when he said that the biggest barrier to the spread of e-commerce is a cultural one. Companies are worried that they won’t get paid. Customers are concerned that their personal details will be misused. Copyright holders fear piracy, and so on.

On March 20, 1999, former President Clinton expressed the deep concern of consumers in security and privacy, saying that he wanted to work with industry to find ways to give consumers the same protection in the virtual mall that they now have at the shopping mall, and to enhance the security and privacy of financial transactions on the Internet, which he believed to be an increasingly deep concern of citizens everywhere.

Note that neither of them talks about perfect security; instead the goal is to be “as safe as” something else. In the case of Prime Minister Blair, the goal is to be as safe as any country in the world—presumably that implies the U.S. In the case of former President Clinton, the goal is to make the virtual mall as safe as the shopping mall.

The usefulness of Trusted Platforms also extends beyond services traditionally considered as comprising e-commerce. Using TPs, both customers and service providers can have more confidence in business transactions. This has implications in the office environment for hot-desking, in the home environment, in remote management, and in teleworking. Other benefits, such as software distribution, apply to both the home and office environment, albeit with a slightly different focus.

As a result, many business opportunities are expected to be available in providing trust-enhancing services built on top of Trusted Platform technology. For example, the transactional security service market is expected to increase at a compound annual growth rate of 92 percent, from $128 million in 1999 to $3.3 billion in 2004 [IDC 2001].

Corporate responsibilities addressed by Trusted Platform technology
Finally, organizations that use computer platforms will find it easier to maintain good practice if they use Trusted Platforms. Trusted Platforms can maintain confidentiality of the organization’s information. This is currently a major problem.

Attacks occur in these and other ways:

- Information corruption caused by viruses
- Online theft of information (e.g., corporate data being at risk of loss or misuse if an office platform is used at home over a personal Internet connection)
- Offline theft of information (e.g., from a home system used over a personal Internet connection, or information extracted offline from a stolen home or office system)

Information damage has several undesirable effects, including these possibilities:

- Direct financial loss resulting from fraudulent use of secrets
- Loss of business opportunity through disruption of service
- Loss of customer confidence or respect (e.g., via web pages being hacked)
- Costs resulting from uncertainties, e.g., system failures leading to paralyzed transactions leading to dispute resolution
Legislation for digital signatures imposes requirements for trustworthy systems and safeguarding of private keys. Companies could be more comfortable using Trusted Platforms for digital signatures because of the ability to predicate signatures on the software state of the platform, either by checking the state before signing or by incorporating the state into the signature.

### The Value of Trusted Platforms

New business practices drive the need for protected information processing and communication systems.

With increasing and widespread usage of open networks, the need for ubiquitous information protection in computer platforms grows. One solution is the widespread adoption of conventional security techniques but what businesses really want and need is commercial confidence rather than security *per se*. The approach described in this book is that of Trusted Platforms. **Trusted Platforms** are a low-cost method of providing confidence in the protection and processing of information. The trust mechanisms in **Trusted Platforms** use selected security mechanisms, but they are ultimately based upon signed statements of “social trust” made by individuals and organizations.

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 a major business enabler
- Improved trust and security is necessary to the delivery of business-critical e-services

### The Main Features of Trusted Platforms

This section summarizes the capabilities in a **Trusted Platform** that enhances end-users’ confidence in **Trusted Platforms**.

### Design Features of the TCPA Trusted Platform

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Most cryptographic primitives</strong>: But not bulk encryption.</td>
</tr>
<tr>
<td><strong>Privacy</strong>: Fully “opt-in,” with no identity correlation.</td>
</tr>
<tr>
<td><strong>No global secrets</strong>: If a TPM is cracked, it reveals information relating to the associated platform and nothing further.</td>
</tr>
<tr>
<td><strong>Low-cost protected environment outside a crypto co-processor</strong>: It is uneconomic to do bulk processing in a co-processor.</td>
</tr>
<tr>
<td><strong>Ubiquitous security</strong>: Available at the lowest cost and without significant product export/import problems.</td>
</tr>
</tbody>
</table>
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:

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

For further discussion of these capabilities, see Chapter 3.

As stated above, Trusted Platforms use the following definition of trust: An entity can be trusted if it always operates as expected for the intended purpose [TCPA 2000a]. A platform cannot itself decide whether it is trusted because trust depends on the intended use of that platform. Only a user can decide whether the platform is trusted for the purpose intended by that user. So the platform reports information to the user to enable that decision to be made. For further details, see Chapter 12.

An inherent capability of a Trusted Platform is the export of security primitives (except symmetric cryptography) for use by the platform. Trusted Platform Modules (TPMs) export non-deterministic numbers (for keys) together with signing functions, a hash function, and asymmetric encryption. (Readers who are unfamiliar with such cryptographic terms may wish to consult Appendix C for further explanation.) Bulk (symmetric) encryption is not exported by the TPM because of the TCPA’s intent to encourage use of the main CPU for such encryption (for file storage and messaging). Symmetric encryption provided by software on the main CPU is both faster than can be provided by low-cost hardware and easier to tailor for individual markets, thus avoiding the worst of the product import/export regulations.

A Trusted Platform can be used to securely store secrets for conventional security processes operating on the main platform. A Trusted Platform makes no attempt to make secrets difficult to find. Instead, they are rendered unintelligible unless the correct access information is presented and the correct programs are running. A thief can find a secret but cannot reveal it unless the access code is known. Ultimately, the technology could be developed so that a thief can load programs to snoop for secrets that have been revealed by genuine users, but the mere presence of snooping programs prevents the revelation of those secrets. Again, further discussion of this protection capability is provided in Chapter 3.

We now give a summary of the features that Trusted Platform technology provides before moving on to consider privacy issues, the architecture of Trusted Platforms, and some of their main features in more detail.
Privacy

Information protection systems require privacy controls to allow the computer owner to have control over the identity (ID) of the platform and activation of the TPM. Users should have control over the information that they store in the platform.

The owner has complete control over activation of the TCPA Subsystem and generation of attestation identities for the Subsystem. Owner control is preferably expressed by the use of properly authorized commands, but some owner controls must be expressed using physical presence, in which some physical action must be carried out on an actual platform. Physical presence may seem a poor substitute for cryptographically authorized commands, but it is unavoidable in situations such as when the platform is incapable of processing authorized commands, or when the owner has lost his authorization information, or before the owner has had the opportunity to introduce his authorization information to the platform.

The manufacturer, the owner, and the users can all “turn off” a TPM if they so desire. There are mechanisms to disable and deactivate a TPM and prevent a TPM from accepting an owner. Judicious selection of options can enable a virgin platform from the manufacturer to be ready for remote activation as a Trusted Platform or fully blocked from operating as a Trusted Platform, with a range of options in between. After an owner has taken control of a Trusted Platform, he can prevent the TPM from operating until further notice. Users can prevent operation of a TPM until the next boot cycle.

Attestation identities can prove that they correspond to a Trusted Platform, and a specific identity always identifies the same platform. But the origin of a specific identity cannot be tracked further, except by the Certification Authority (CA) that issues a certificate for that attestation identity. So appropriate selection of CAs enables the owner to control traceability from an attestation's identity to the certificates that attest to a specific TPM and a specific platform. Identities can only be correlated with other identities by the CA that certifies these identities, and the owner has sole choice of that CA. So the owner can choose a CA whose policy is not to correlate
identities or whose policy is to correlate identities, according to the wishes of the owner. Different identities are used for different purposes, and separate identities would usually be given to different users of the Trusted Platform. As a result, the mechanisms of the TCPA Subsystem do not worsen the issue of platform privacy (which already exists because of identification of platforms from MAC and IP addresses, for example).

Authorization data is needed in order to gain access to data stored via the TPM. Each user’s data can be kept private, and even the platform owner cannot access that data without the necessary access data. (There is no “superuser.”) Hence, a platform could be owned and used by a single person (which would often happen in the case of consumers or small businesses), or it could be owned by one entity and used by another entity. This would be typical in a corporate environment, where the IT department is the owner, and the user is the individual to whom the platform is issued.

We now move on to look at various aspects of Trusted Platforms in more detail, including proof that a Trusted Platform conforms to the TCPA specification, the platform architecture (including changes to the OS), and the key features that a Trusted Platform provides: hardware-based cryptographic capabilities, integrity measurement and reporting, creation of Trusted Platform identities, and protected storage functionality.

**Meeting the Specification**

A Trusted Platform comes with various “documents” that prove it meets the TCPA specification.

Some “documents” are digitally signed statements by manufacturers that a particular chip is a genuine TPM and that a particular genuine TPM is properly incorporated in a genuine Trusted Platform. Other “documents” are in the form of certificates from an authorized test house to attest that the design of the TPM and platform satisfy the TCPA security requirements. The security requirements are specified in documents called a “Protection Profile” (PP). The particular PPs were written by TCPA in the style required by the International Standard ISO/IEC 15408 “Evaluation criteria for IT security”; the ISO bulletin for June 2000 says that this is also “more commonly known for historical and continuity purposes as ‘Common Criteria’ (CC)” [ISO/IEC 15408]. Another document, called a “Security Target (ST),” is written by the manufacturer and is a statement of how specific equipment satisfies the PP. Each type of TPM must have a Security Target that meets the Protection Profile for TPMs. Each type of platform must have a Security Target that meets the Protection Profile for the CRTM and the connection of the TPM to the platform.

Most customers will buy a standard Trusted Platform and will not concern themselves with these proofs, simply trusting the vendor to sell them a proper Trusted Platform. All STs (or their references) must, however, be provided with a Trusted Platform, in the form of a digital credential that can be checked by a machine, because a CA requires that information in order to issue an attestation identity for a platform. This is because the CA checks that each Trusted Platform meets the TCPA security requirements before attesting to an identity.
To those who are interested in whether a Trusted Platform meets the specifications, the most obvious security aspect of a Trusted Platform is its degree of physical protection. The only parts of a Trusted Platform that need physical protection are the TPM and the RTM (or CRTM in a PC). These would ideally be physically tamper-proof, but absolute resistance to physical attacks is impossible. The best that is possible is tamper-resistance. The amount of tamper-resistance will depend on the level of trust that is required from the platform, which in turn affects the price of the platform. Tamper-resistance can vary from that of an ordinary epoxy-coated chip to that of a sophisticated module with protection against voltage attacks, timing attacks, X-rays, temperature attacks, and so on. Most TPMs will probably have a reasonably sophisticated level of tamper-resistance, equivalent to that of the chips in smart cards. Most CRTMs have a level of tamper-resistance equivalent to at least that of a normal chip. It is currently unclear whether they will be tamper-evident (i.e., reveal that they have been tampered with).

Architectural Summary

Existing security mechanisms can be incrementally fitted to existing platforms, but Trusted Platform functions require a fundamental change to the platform architecture plus attestation by trusted third parties that the platform meets the TCPA specification. This makes it impractical to retrofit existing platforms and convert them into Trusted Platforms.

One part of converting a platform into a Trusted Platform is adding a root of trust for reporting to a platform. This requires the addition of a TPM chip to a platform, but it is potentially more complicated than might be thought. The obvious way is to solder a TPM chip to a motherboard, but this requires motherboards that are specifically designed to be suitable for Trusted Platforms. It may be more cost-effective to use standard motherboards with a “good” connection between the platform and a TPM, in order that the measurements received by the TPM are trustworthy. One way is to use cryptographic techniques to prove to a TPM that incoming measurements originated on a specific platform, but this itself begs the question of safely installing the necessary cryptographic secrets in the motherboard and in the TPM. Another way is to use a socket or connector so that a TPM can be added to standard motherboards when a Trusted Platform is manufactured. However, the connection must be resistant to physical tampering (so it might be necessary to permanently bond the joint), and it must be possible to see whether physical tampering has occurred (so it might be necessary to cover the joint with special seals).

A second part of converting a platform into a Trusted Platform is reliably measuring integrity information. This requires a fundamental alteration to many parts of the software stack, starting with a “Root of Trust for Measurement” (RTM) and probably a chain of subsequent measurement agents. The basic principle is that the RTM does some tasks, measures certain aspects of a platform (including the first measurement agent), and records those measurements in the TPM. Then the RTM passes control to the first measurement agent (which does other tasks), measures certain aspects of the platform (including the second measurement agent), and records those measurements in the TPM. Then the first measurement agent passes control to the
second measurement agent and so on until all software has been measured and loaded. After all software has been loaded, the final measurement agent continues to make measurements of new software and stores them in the TPM before executing that new software. Because all software is measured before it is executed and recordings in the TPM cannot be tampered with, the TPM always contains an accurate summary of the software state of the platform. If, at some point, rogue software is loaded, it cannot hide its presence in the platform, but (of course) all subsequent measurements cannot be trusted.

On a PC, the RTM is the entire platform controlled by the Bios Boot Block (BBB), or by the BIOS itself, provided that nothing untoward can execute before the instructions that comprise the RTM and that acceptable mechanisms are present to prevent unauthorized replacement of the BIOS. The memory device holding the RTM instructions is given a special name—the Core Root of Trust for Measurement (CRTM)—by TCPA because this is the part of the RTM that requires special attention and is subject to constraints described in the TCPA specification. Subsequent measurement agents are the entire platform controlled by some previously measured software. So the OS loader code and the OS must be modified to act as measurement agents.

A third part of converting a platform into a Trusted Platform is storing signed values of predicted integrity measurements, or pointers to those values. Predicted values of a component are values that are made available by the manufacturer of the component so that a comparison can be made between these standard, expected values and those that are actually measured when the platform is being used. Option ROMs might include such information, or such information might be on the hard disk drive (in a PC, for example). This information is needed for a challenger to decide whether he can trust a platform. The challenger must get the actual measured values and compare them with signed predicted values, which is easiest if the predicted values are provided by the challenged platform. If they are the same and the challenger trusts the organization or individual that signed the predicted values, the challenger can then decide to trust the platform for some particular interaction or purpose.

A fourth part of converting a platform into a Trusted Platform does not even involve the platform. Trusted Platforms require a support infrastructure, to provide attestation that the platform is genuine, to provide predicted values of integrity information, and to attest to attestation identities that belong to the platform. In particular, a PKI is required.

The TPM: A Separate Processing Engine Distinct from the Main CPU(s)

The purpose of the TCPA Trusted Subsystem is to detect software attacks on the platform. For both local and remote users to trust the Subsystem, it is necessary to protect the Subsystem against software attacks. The reasoning is obvious: The Subsystem cannot reliably detect software attacks if its software can be subverted. For a remote user to trust the Subsystem, however, protection against hardware attacks is also necessary. This is because a remote user cannot be sure that a local user has not physically tampered with a platform. Preferably, platforms would be protected against a variety of hardware attacks, but that unfortunately dramatically increases
cost. So the Subsystem must resist all software attacks and a given number of hardware attacks. A sense of proportion—cost against threat—is necessary.

In practical terms, a Subsystem needs to protect some secrets and a certain number of capabilities that must be trustworthy. If those capabilities and secrets cannot be trusted, there can be no trust in the Trusted Subsystem. The trusted capabilities and secrets need to be isolated from the rest of the platform to prevent subversion of those capabilities and to prevent eavesdropping and subversion of secrets. The specification does not mandate the embodiment of the trusted capabilities, but does specify the interrelated properties of protected capabilities and shielded locations that any TPM embodiment must satisfy. Having said that, a convenient implementation of the trusted capabilities and secrets takes the form of a single chip. The chip is a self-contained processing engine with specialist capabilities such as generation of non-deterministic numbers, asymmetric key generation, asymmetric encryption, and hashing. Naturally, it also needs communications with the computing engine instantiated by the platform.

A TCPA Trusted Subsystem requires other functions, apart from those in the TPM, but does not need them to be trustworthy. The TCPA mechanisms and protocols are such that if these support functions are broken, they will at worst cause an inconsistency in information that can be detected by another computing platform. Hence, they are implemented as ordinary software executing on one of the main CPUs. The separation is made explicit in the TCPA specifications, in order to minimize the amount of capabilities that must be protected and, hence, minimize the amount of extra hardware that is likely to be required in a TPM. This is vital to minimize costs.

The Operating System

The software that is running after the Trusted Platform has booted, which we will assume is the operating system (OS), still has a vital role to play in a Trusted Platform. The TCPA Subsystem still provides the means to record and report integrity information. The OS, however, must contain a measurement agent that detects execution of software that changes the level of trust in the platform. Like all such measurement agents, this agent detects that software is about to be executed and stores a summary of the software in the TPM and updates a measurement log. The summary is a digest (see Appendix C for an explanation of this term) of the information in the log, and the log is a textual and numeric description of the software. A challenger can retrieve the summary from the TPM and test it as described previously against predicted values. Alternatively, the challenger can retrieve the summary from the TPM and step through the log, deducing and checking the steps taken by the platform.

For an operating system to be TCPA-compatible, the OS needs the following features:

1. It must be able to detect that security-critical changes are being made.
2. It needs a means to decide which events should be recorded and which should not.

Theoretically, all changes to the platform that affect the security state could be recorded, but this makes the measurement log long and more difficult to interpret. It is probably better for
the OS to use a policy to decide which events to record and which not to record. For example, it may check the signature on a new driver or application against an approved list and record the event only if the signature does not appear on the approved list.

Note that code, applets, or drivers used on a TCPA system do not necessarily need to be signed to run. The use of signed components depends on the operating system environment in which the Subsystem operates.

Cryptographic capabilities
A TPM has the following cryptographic capabilities:

- Hashing (SHA-1)
- Random number generation (RNG)
- Asymmetric key generation (RSA)
- Asymmetric encryption/decryption (RSA)

The TCPA specification also requires the use of symmetric encryption/decryption (3DES) during the acquisition of pseudonymous identities, but the TPM does not export that functionality to the platform. Individual TPM manufacturers may, of course, export symmetric encryption from the TPM if they wish, albeit with the risk that such TPMs may cause increased product export/import difficulties.

The Advanced Encryption Standard (AES) [AES]—3DES’s replacement—is not required in v1.1 of the specification, but it may be required in future versions of the specification. These cryptographic capabilities are explained in Appendix C, which provides background to cryptographic concepts for those who are unfamiliar with this material.

Integrity Measurement and Reporting
A Trusted Platform, starting from a root of trust in hardware, 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 1-6. Starting with the CRTM, there is 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 is executed. Rogue software cannot hide its presence in a platform because, after it is recorded, the recording cannot be undone until the platform is rebooted. (This issue is considered in much more detail in Chapters 3 and 6.) 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 1-7. 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 (i.e., 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.
Trusted Platforms: An Overview

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. A CPU can obtain a symmetric key from a TPM and use it for bulk encryption, or a CPU can present data to a TPM and request the TPM to sign that data, for example. The portal operates as a series of 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. The TPM, however, knows nothing of this hierarchy. It is simply presented with a series of commands from untrusted software that manages the hierarchy. An example of such a hierarchy is illustrated in Figure 1-8.

An important feature that is 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 states 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 stated software state. If they do, the TPM permits access to the secret. If they do not match, the TPM denies access to the secret.

![Figure 1-7 Obtaining proof that a platform is a Trusted Platform](image)
When All Platforms Are Trusted Platforms

This section aims to emphasize how Trusted Platform technology is appropriate for all computing platforms. After a brief discussion of laptops, PDAs, and servers, it introduces how an IT infrastructure where all platforms are Trusted Platforms would deliver the full vision of trusted platform technology.

It is very likely that different types of Trusted Platform—and not just Trusted PCs—would form part of a future global computing infrastructure.

Different Types of Trusted Platforms

As discussed already, the generic TCPA specification applies to a wide range of computing platforms including servers, appliances, and cell phones. In particular, the identity creation and usage, reporting mechanisms, etc., can be applied in an analogous way to different types of platforms, although the details for the integrity measurement have not yet been considered for these types of platforms.

Potentially, there can be different types of Trusted Platforms, for which different types of services would be more appropriate. The following are some examples.

PC

A PC would be connected to the network 24 hours a day. It could be connected either to the home network, the Internet, or the intranet in the office. The short-, middle-, and long-term func-
tionalities of Trusted Platforms are targeted at PC deployment. The first target environment would most likely be a corporate one, with provision for protection of sensitive data, identification of corporate platforms, and verification of corporate system configurations.

**Server**

A server is likely to be running in a corporate environment 24 hours a day. A trusted server could have the benefits of protection of sensitive data, greater trustworthiness for those wishing to use the server, and an enhanced relationship with individual client platforms (for example, with better authentication, verification of their configurations, remote management services, etc.). While the initial focus of TCPA has been on the PC/client, the potential for such technology when applied to servers is huge. Because servers are generally the hubs of business-critical servers, the need for such enhanced security mechanisms is probably greater than for the PC.

**Laptop**

A laptop could be standalone, with the potential of being connected to one or more intranets and possibly also to the Internet. Even in the standalone case, a trusted laptop platform would provide better built-in protection of data on the platform, which would be particularly useful due to the pervasive risk of theft of the laptop.

For connected laptops, a secure dial-in service could be provided, by which the physical platform identity would be checked and there would be the possibility to check that this was in the approved corporate (or governmental) software configuration. This would help prevent software hackers from dialing in to a company from unauthorized hardware running hacking software and penetrating the company’s intranet.

**PDAs**

Personal digital assistants (PDAs) are small, lightweight, portable PCs with restricted functionality. They were traditionally standalone but are increasingly being connected to intranets and the Internet. To enable PDAs to become the ultimate personal portal to a connected environment, they must be able to connect to a corporate network and to the Internet. There is no difference today between a corporate PDA and a home-user PDA.

**Ubiquitous Trusted Computers**

*Trusted Platforms* could become fundamental to a global computing infrastructure for the following reasons:

- As already considered, a low-cost approach is necessary for ubiquity and this is what TPs provide. Furthermore, ubiquity and standardization are necessary for a global infrastructure.
- Total security is impossible or not necessarily practical over a wide range of situations. Instead, it is necessary to solve a less serious problem, which is that of providing
technology to enhance trust so that users will use services without fear of consequences.

- **Trusted Platform** technology can be applied to mobile and changing environments. The TCPA specification brings new functionality to client platforms such as PCs, mobile phones, and PDAs. The potential of TCPA will be released in phases, because some features require more supporting software and infrastructure than others.

- Companies improve their performance by stronger collaboration with their customers, suppliers, or partners. This requires dynamic IT relationships between organizations. Sharing data and IT resources in this way is dangerous, yet it is likely that future trusted interactions will increasingly need to be established “on the fly” with a high level of assurance that the risk involved is limited. Such a vision requires platforms with built-in security capabilities; a critical foundation of those security capabilities are the Trusted Platform functionalities of data protection, platform integrity, and platform identity, which are discussed in Chapter 3.

- Finally, the long-term benefits of **Trusted Platforms** discussed above involve a distributed infrastructure.

### Summary

**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 TCPA is an industry alliance formed in October 1999 that focuses on developing and specifying **Trusted Platform** technology. The TCPA specification, released in February 2001, is designed to be independent of the type of platform (e.g., PC, server, PDA, printer, mobile phone, etc.). 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 businesses and have been defined to be independent of a specific market focus. In particular, a TP 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-services. For example, there could be
TCPA-compliant PCs in public places that would 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, VPNs, 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 ([www.trustedcomputing.org](http://www.trustedcomputing.org)) is a source of useful information.