

The Evolution of the Trusted PC

By the Trusted Computing Platform Alliance (TCPA)

In today's society we take for granted the technology of Computers; demanding flexible, advanced software programs plus secure ways of interacting with other Users. But this mix of requirements can sometimes be conflicting, and is not necessarily easy for the PC Manufacturers to achieve. This is why the TCPA (Trusted Computing Platform Alliance) was formed by Compaq, HP, IBM, Intel, and Microsoft; to standardize security and privacy levels across the whole industry, without compromising the sophistication and diversity of software.

Computing devices are now no longer restricted to PCs, with the advancement of PDAs, mobile phones and other handheld devices. With the increased interaction between such devices, Users are moving away from their own independent "safe" work stations, and are being networked together, either via the Internet or company networks. While this leads to an increase in transactions and available information, the downside can be a higher incidence of security breaches. It's been estimated that such attacks have affected business losses and computer management expenses by as much as 5.57% of gross revenues in 2000 (Omni Report 2001).

Currently, all that is available to combat security problems are add-on layers such as SSL (Secure Sockets Layer), PKI (Public Key Infrastructure), SET (Secure Electronic Transaction). However these applications are external to the main hardware platform and so do not provide security at the most fundamental level. What is needed is enhanced security at the level of the platform hardware, BIOS system software and operating system.

What is needed is a Trusted Client.

Trusted Client – The New Approach

In the past, manufacturers focused on PC security as an external issue, adding secure applications and software to their systems. Through Trusted Computing, the TCPA promotes a more integral solution, by first ensuring the integrity of the platform and then passing that trust through the different elements of the system.

Trusted Computing requires transactions and computing devices to be:

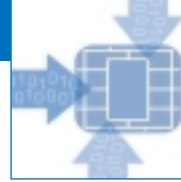
- Trusted — acting in a recognized manner and able to communicate what that manner is supposed to be
- Reliable — readily available for transactions and communications, as well as prepared to act against viruses and other intrusions
- Safe — able to stop unwanted intervention or observation
- Protected — sharing information with only those that need to know within commonly accepted parameters for computer privacy

The Trusted Client is designed to prevent the platform from logical, or software-based, attack. While the Client (or

Subsystem) can still be subverted by physical means, this mode of attack exposes only the secrets of the Subsystem on the local platform, and not on other connected platforms. In other words, if a Computer using a Trusted Client were to receive a virus, it could first of all notify the User that its software has been affected (not to be confused with anti-virus software that identifies and eliminates the virus, which is used as an additional application). Then the Computer could notify all other Computers on the network about the problem, so that no other Computer would access the infected system and spread the virus.

However, Trusted Computing is not only limited to protecting systems from attack, it also:

- Provides protected storage of cryptographic and sensitive data within the TCPA silicon technology
- Authenticates a computing device, verifying its identity to other computing devices
- Supplies owner-defined metrics for reliable, secure network environment access of only other trusted computing devices



How does this work in reality?

The TCPA specification advocates that a separate Subsystem (see Figure 1), can be trusted. The TCPA Subsystem is designed to provide reliable mechanisms for the measurement and reporting of integrity metrics, ensuring that the Client is Trusted. This consists of two building blocks:

- A Trusted Platform Module (TPM) defined as a secure controller (the hardware instantiation of the TCPA specification).
- Software to perform integrity metrics, in conjunction with the TPM.

To ensure system integrity for the Trusted Client, “integrity metrics” are used. These are defined as measurements of key platform characteristics that can be used to establish platform identity, such as BIOS, boot-loader, hardware configuration, OS loader, and the OS security policy. Cryptographic hashing is employed to extend trust from the BIOS to other areas of the platform, in the following simplified sequence:

1. The PC is turned-on.
2. The TCPA-compliant “BIOS Boot Block” and TPM have a “conversation.” This attests that the BIOS can be trusted.
3. BIOS queries to ensure that user is authorized to use the platform.
4. The BIOS then has a “conversation” with the operating system (OS) loader and the TPM. This attests that the OS loader can be trusted.
5. The OS loader then has a “conversation” with the OS kernel. When the OS kernel loads, it knows what software has had access to the system ahead of it. This establishes that whatever happens within the system from that point forward is 100 percent controlled by the OS kernel.

The core elements of trust that are built into the system through the TPM and BIOS extend their trust to the boot loader. The boot loader extends its trust to the OS loader. The OS loader in turn extends its trust to the OS, which can then extend its trust to applications. This process ensures that the initial point of trust (TPM and

BIOS) spreads the trust throughout the whole system, thus resulting in a Trusted Client.

About the TCPA

In 1999, five leading Hi-Tech companies (Compaq, HP, IBM, Intel, and Microsoft) formed an alliance, in order to introduce the concept of a common Trusted Computing Platform within the industry. Now there are over 160 members of the alliance; ranging from OEMs (Original Equipment Manufacturers) and PC Manufacturers to Semiconductor Manufacturers. The alliance is open to any company that can assist in the development and production of the Platform.

The TCPA set out to cover both security and privacy issues in its mandate, with the following mission statement:

“To maintain the privacy of the platform owner while providing a ubiquitous interoperable mechanism to validate the identity and integrity of a computing platform.”

The alliance plans to achieve this goal by issuing White Papers detailing its ideas on Trusted Computing and releas-

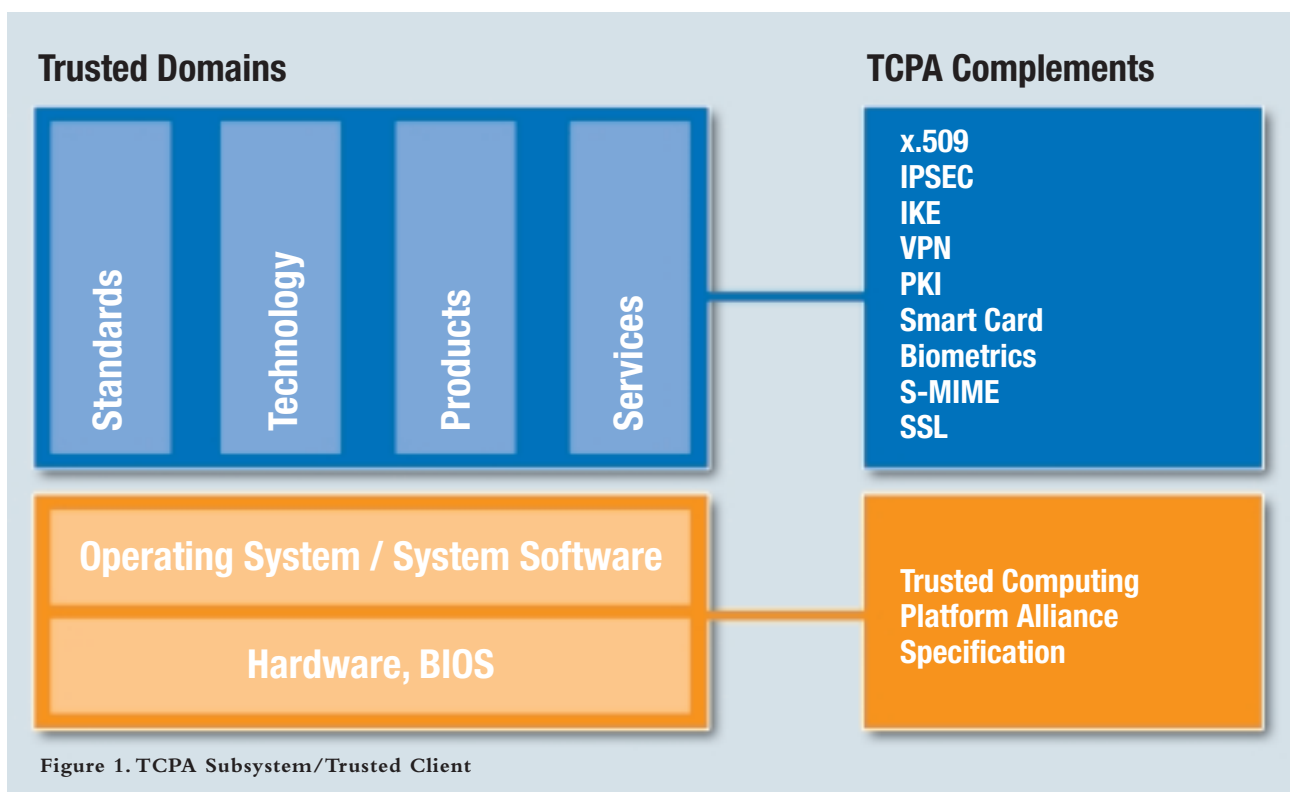
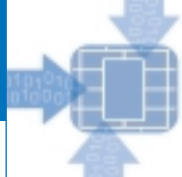


Figure 1. TCPA Subsystem/Trusted Client



ing the Specification for members of the alliance to follow when developing new products. The Specification has moved through different versions over the last year, with the release of Specification 1.1 in November 2001.

Summary

Although the alliance cannot at present guarantee a “hack-proof” system, it has

made significant steps to improve the previous security and privacy shortcomings within the industry.

By bringing together all the major manufacturers, time is no longer wasted on producing competing standards, rather, companies can use the TCPA Trusted Client Specification to enhance their own offerings.

Consumers then benefit from devices that they can trust; reducing the risk of security breaches and ensuring that they are dealing with the intended partner.

It is hoped that this new level of trust will further spur the growth of e-business and e-transactions and lead to a new era of trusted computing.

Examples of “Trust” in action

Remote Attestation in B2B/B2C

TCPA remote attestation allows an application (the “challenger”) to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure.

For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform is trustworthy. The service provider’s platform (the “challenger”) queries the remote platform. During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored.

When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy. If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger make the final decision regarding the trustworthiness of the remote platform.

(Taken from TCPA White Paper: Building a Foundation of Trust for the PC)

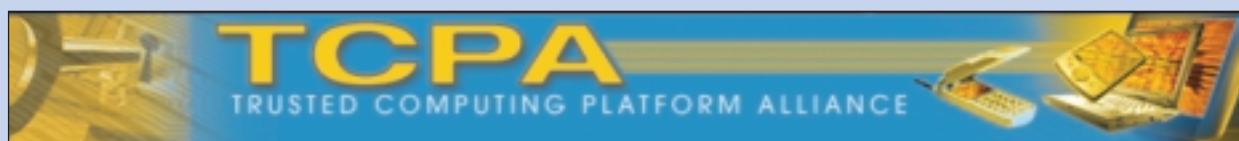
Ensuring Privacy through Authenticated Anonymity

Imagine that the PC has booted as described in the four-step sequence outlined earlier in the article, and that the system can be trusted. It is now possible to present credentials for the system to a third party. In doing so, however, the user exposes the identity of his or her platform to the third party, and possibly runs the risk of providing more information than intended.

An alternative is to use a recognized and trusted entity within the industry that can verify that an identity belongs to a trusted platform. This is termed “anonymous authentication.”

Here is how it works in a TCPA-compliant subsystem:

The user goes to a third-party Authenticated Anonymity Website (AAWS), and requests site verification. Using the TCPA Subsystem, the AAWS provides the user with credentials, known as a “cert” or certification. Those credentials assert that the platform is authenticated by a trusted third party and that the platform can be trusted in certain ways. The AAWS asserts that the platform is unique, but it will not tell someone else anything that can be traced back to the user. For the purposes of the transaction, the platform is reliable, and also anonymous.



For details about the TPM from Infineon Technologies, see page 60.