

TCPA Security:

By **Marco Scheibe**

Trust your Platform!

Infineon Technologies

E-commerce and E-business seem to be prevalent everywhere in today's computing environment. Everyone seems to want a share of this market with huge marketing campaigns started to promote this new way of doing business. However, people remain wary about using the new services themselves. Compaq, Hewlett-Packard, IBM, Intel and Microsoft have created an Alliance called the Trusted Computing Platform Alliance (TCPA) - an industry working-group focused on increasing the security of computing platforms.

End customers fear for their privacy these days and are increasingly aware of the security breaches that can happen within the Internet. Consequently, there is a reluctance to transmit credit card details via this channel. IT professionals in the business-to-business (B2B) and business-to-employee (B2E) sector are also wary of the security of this new channel as they also have to be sure that they are transmitting their sensitive data to the right person.

To overcome these hurdles, a secure and trusted computing and communication environment must be created. Though current security solutions are well known to the industry, some major topics still remain open: how can the open PC platform be trusted, and how can it be ensured that transactions initiated at the PC are communicated over insecure connections like the Internet in a trustworthy way?

This is the main objective of the Trusted Computing Platform Alliance (TCPA), an industry working-group announced in the fall of 1999 by Compaq, Hewlett-Packard, IBM, Intel and Microsoft. Within the last year, more than 130 companies have joined the TCPA, thus acknowledging the importance of their goals and their approach to reach them.

The TCPA is focused on improving the security of computing platforms through the development of a ubiquitous specification for standardized, platform-based security. This specification can help to minimize security problems while maintaining the inherent flexibility of the platform itself. The main security issues of authenticity, integrity and privacy can be solved for existing applications. At the same time, new opportunities for e-business can be addressed.

A central objective of the TCPA specification is to protect privacy by maintaining owner control over critical data. The owner is able to define what 'critical data' means in this context. This is extremely important since it provides a way to prevent third parties from gaining access to information without the informed consent of its owner.

Another benefit of the TCPA approach is the easy migration path for existing platforms, which add security for a negligible additional cost. Though the specification was initially targeted at PC platforms, it can be readily extended to servers and other connected platforms such as mobile phones and PDAs. TCPA-compliant PCs will enable a secure infrastructure for B2B, B2C and e-commerce applications in a much more cost-effective way.

Trusted Computing

The two main issues of trusted computing are:

- a)** Authenticity - knowing for sure to whom (or to what entity) they are talking.
- b)** Integrity - assurance that all information is transmitted accurately (not changed).

Obviously, an application that can prove its own identity will help develop greater user confidence in areas such as electronic banking, e-cash, networking, platform management, web access and other such applications.

The objective of the TCPA specification is to insert a trusted subsystem into the PC platform and make it a standard part of the platform like a graphics adapter or a modem. The trusted subsystem is then able to extend its trust to other parts of the whole platform by building a 'chain of trust' where each link extends its trust to the next one. In this way, the TCPA subsystem provides the foundation for a fully trusted platform and a basis for extending trusted computing across system and network boundaries.

The root of trust is a small hardware device called a Trusted Platform Module (TPM) which provides features like secure memory, cryptographic sign/verify, and an immutable key pair used to generate anonymous identities. At boot time, this device extends its trust to the BIOS. The trusted BIOS



can extend its own trust to the OS loader, which extends its trust to the OS itself, which in turn can extend its trust to applications. This process ensures that each part of the platform and software running on it can be trusted. It should be noted that using the same mechanism, it is also possible to implement a secure boot functionality which may even restrict access to the platform if something has been changed (for example, new hardware or unknown software).

The root of trust is a small hardware device called a Trusted Platform Module (TPM) which provides features like secure memory, cryptographic sign/verify, and an immutable key pair used to generate anonymous identities.

A question occurs as to whether it is possible to provide adequate security within the operating system alone. The ability to do this in a PC platform is becoming increasingly limited. Even robust operating systems cannot prevent the loading of software before the OS itself is loaded. If such unauthorized software is loaded, it can gain access to certain areas, which

should not be accessible in a trusted environment. For instance, BIOS setup data could be changed. To counter this threat, the PC needs a root of trust that is tightly bound to the platform itself.

To be accepted as a trusted platform, the PC must be trusted by both local and remote entities. This includes users, software, and all other third parties. It must be sure that there are no easy means for tampering with the root of that trust,

the Trusted Platform Module (TPM).

Another concern is privacy. A matter that is extremely important to every business or individual concerned about protecting personal or confidential information. In the computing context, Privacy provides the means to prevent third parties from gaining access to information without the informed consent of its owner. Users are concerned that their credit card data can be observed while doing e-commerce transactions. They may also be concerned that they may be tracked when surfing through the Internet. It is essential that the user can always decide to whom they give what information. The TCPA specification incorporates this principle by making sure that the user has full control over the trusted subsystem. Simply spoken, the subsystem can be made silent, but it never can be made to lie. However, the TPM is not intended to encrypt the complete data stream.

As outlined before, the root of trust is the TPM. This is basically a secure controller with some added cryptographic functionality like hash algorithms and asymmetric key procedures (RSA). Another important feature is the possibility to produce random numbers. Finally, each single

TPM has a unique key that identifies the TPM. This key is also used to check whether the TPM is really a TPM: the manufacturer of the TPM vouches for all TPMs produced (and is thus an integral part of the PKI beneath the platform manufacturer who in turn vouches for the platform).

With these capabilities, the TPM is able to produce a statistically unique "fingerprint" of the BIOS at boot time. This fingerprint is also called an "integrity metric" or "cryptographic digest" in the TCPA specification environment. Once this metric is available, it is saved in a secure memory location. Optionally, it could be compared to some predefined value and the boot process could be aborted on mismatch.

During the boot process, other integrity metrics are collected from the platform, for instance "fingerprints" of the boot loader and the operating system itself. Device drivers may be hashed; even hardware like PCI cards can be detected and identified. Every metric obtained by the TPM is concatenated to the already available metrics. This gives a final metric, which describes the operational state of the whole platform.

A challenger may now ask the platform for these metrics and make informed decisions on whether to trust it based on the metric values obtained. To support the privacy issue, the user of the platform may restrict the TPM in answering to any challenge, but the user is never able to make the TPM report false metrics.

Applications in Access Control and E-Commerce

Of increasing interest is Access Control to PC platforms. This is vital in commercial environments but also becoming more and more an issue for private PC platforms. A promising solution is biometric procedures such as fingerprint recognition.

If the PC would be TCPA compliant, it would be able to authenticate itself to the fingerprint peripheral. This would enable the reader to send the fingerprint data to the PC for further processing without the risk that the data may be used for non-intended purposes. Since the trusted subsystem provides secure storage, it may also store the biometric ID on the platform for later usage. This scenario shows that a TCPA-compliant platform is able to add significant



security to the complete system and may yet optimize the overall system performance.

Another example is the typical e-commerce application. In a vertical supplier-buyer model, the trusted platform features allow the buyer to issue a challenge to the supplier's system to determine whether it is a trusted system as well. This can be done anonymously, thus protecting the buyer's privacy before he really wants to place the order.

The buyer can then digitally sign the contract by using the asymmetric encryption functionality of the TPM. Using digital signatures, non-repudiation can be assured as well as data integrity. This means that the buyer can be sure that his data reaches the supplier unaltered (integrity). In turn, the supplier can be sure that the buyer is not able to deny his purchase order in the future (non-repudiation).

In this context, the TCPA-compliant system gives both partners the confidence that the transaction can be trusted and that it was not altered by malicious software or hacked by third parties.

Conclusion

The TCPA approach can help to alleviate today's security problems in the local and network environment. E-commerce and applications like B2B and B2E benefit from the security and the trustworthiness provided by the TCPA-compliant platform. Since the TCPA solution adds only minimal cost to the platform, it will be able to boost the success of one of the largest market places worldwide – the Internet.

The Infineon Solution

Infineon Technologies is developing a whole family of chips that will be able to act as a TPM. They are all based on the high-security architecture of Infineon's well-known smart card controllers. Basic devices will be available which cover all features needed for a low-cost solution of a TCPA-compliant PC platform. For higher demands, sophisticated solutions are available which add even more security functions to the system like high-speed bulk encryption features and additional interfaces.

Figure 1 shows the block diagram of Infineon's low-cost TPM solution. Based on the high-security architecture of existing smart card controllers, the device provides hardware accelerators for RSA and SHA-1 hashing functions. Optionally, a DES/3DES engine is included to enhance the functionality of the TPM. For easy system integration, the readily available LPC bus is used. The system integration scenario is depicted in Figure 2.

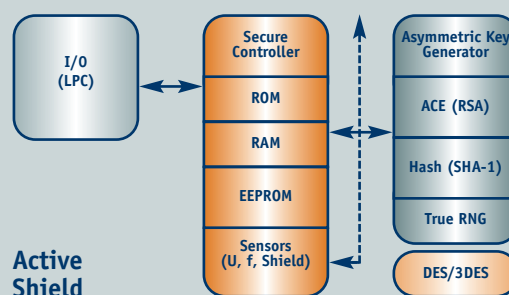


Figure 1: Trusted Platform Module (TPM)

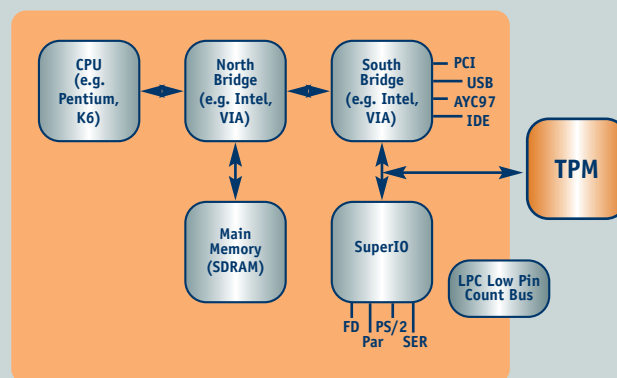
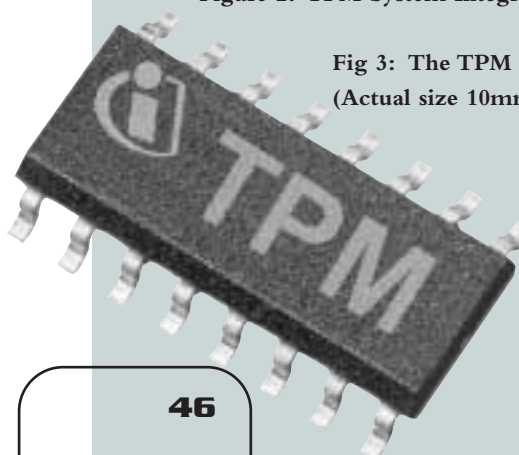


Figure 2: TPM System Integration

Fig 3: The TPM from Infineon
(Actual size 10mm)

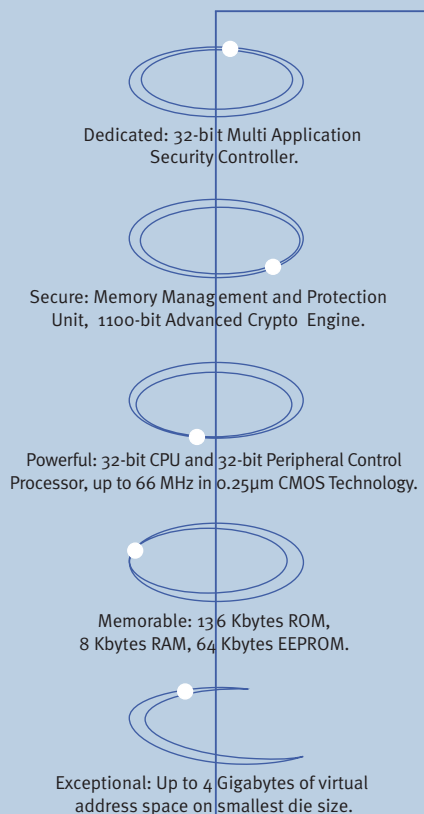


Better to be HUNTER than PREY.

.wtp.

{PERPETUAL THINKING PROCESS}

INFINEON CYCLES



YOU ARE no longer prey to the competition with Infineon's new 32-bit Multi Application Security Controller. You will enjoy market-leading flexibility. And performance that accommodates independent, virtual machine languages such as Java™, Smart Card for Windows™ and Multos™. You will savour the advanced integral security concept that delights everyone – but hackers. And you will profit from top-of-the-food-chain advantages, such as: real multitasking, outstanding cost/performance, up to 512 Kbytes of non-volatile memory (EEPROM/Flash). Plus the talents of a dedicated crypto controller. Whenever you think of high-end chip cards, think of Infineon. Our cutting edge technology has what it takes to make sure you're the hunter – not your competition.

www.infineon.com/88Controller



Never stop thinking.