

# **TCPA Security and Internet Business: Vital Issues for IT**

*The Trusted Computing Platform Alliance*

August 2000



<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
<b>WHAT IS TRUSTED COMPUTING? .....</b>	<b>4</b>
<b>BENEFITS OF TCPA SUBSYSTEMS .....</b>	<b>5</b>
<b>EXAMPLE 1: B2B .....</b>	<b>6</b>
<b>EXAMPLE 2: B2E.....</b>	<b>7</b>
<b>EXAMPLE 3: WEB ADMINISTRATION .....</b>	<b>8</b>
<b>COMPLEMENTING EXISTING STANDARDS .....</b>	<b>8</b>
<b>CAN'T WE PROVIDE SECURITY IN SOFTWARE? .....</b>	<b>9</b>
<b>PRIVACY AND USER CONTROL.....</b>	<b>9</b>
<b>CONCLUSION.....</b>	<b>10</b>

## **TCPA Security and Internet Business: Vital Issues for IT**

### **Executive summary**

PCs are designed to be open computing systems, and the Internet is designed as an open network infrastructure. In supplier/buyer e-Business applications, corporate Intranets, and Web portals, this quality of openness has provided IT organizations and PC users with the flexibility they need to communicate, collaborate, and conduct transactions in important new ways. As a result, Business-to-Business (B2B), Business-to-Employee (B2E), and Business-to-Consumer (B2C) applications enable IT to reach a global base of customers and partners with tremendous economies of scale.

For IT managers, this quality of openness can be a two-edged sword, because it can render e-Business systems vulnerable to malicious parties and hackers. In the opinion of industry analysts, security issues pose a significant barrier to the ubiquitous adoption of Internet-based e-Business applications<sup>1</sup>. Overcoming this hurdle requires the creation and maintenance of a secure and trusted computing and communication infrastructure. While today's trusted computing environments use security components that are well known within the industry, two core issues remain for IT managers to tackle:

- 1) How to trust the PC as the primary vehicle for initiating e-Business transactions.
- 2) How to ensure that e-Business transactions initiated at the PC are communicated over the Internet in a trustworthy way.

IT organizations can benefit from a specification that provides a ubiquitous and standardized means to address trustworthiness of the PC platform, improve the authenticity, integrity, and privacy of Internet-based communications and commerce, and maintain broad exportability and ubiquity over time. These are the goals of the Trusted Computing Platform Alliance (TCPA), a PC industry working group announced in the fall of 1999 by Compaq, Hewlett-Packard, IBM, Intel and Microsoft. Acknowledging the

## TCPA Security and Internet Business: Vital Issues for IT

importance of these goals and the approach taken by the promoting companies, the TCPA membership has rapidly grown to more than 135 companies in less than nine months.

The TCPA is focused on improving trust and security of computing platforms through the development of a ubiquitous specification for standardized, *platform-based* security. The TCPA specification can help minimize the security problem for IT managers by enhancing the trustworthiness of the PC and associated e-Business transactions, while preserving the inherent flexibility of the platform itself. By focusing on the fundamentals of authenticity, integrity, and privacy, the TCPA specification can help secure existing communications and applications, as well as create opportunities for new e-Business. A central objective of the TCPA specification is to protect privacy by maintaining owner control over critical data, while reducing the costs of deployment and ownership. Privacy is extremely important, because it provides a way to prevent others from gaining access to information without the informed consent of its owners.

Another principal benefit of the TCPA specification is its ability to integrate trust and privacy modalities into a platform for negligible incremental cost. The interoperable TCPA platform baseline can be utilized by a variety of applications to support the continuing evolution of B2B, B2C, and e-Commerce. While it is initially targeted at PC platforms, the TCPA specification is designed for ultimate extension to servers and other connected computing platforms. TCPA-compliant PCs will allow IT managers to improve their security infrastructures through easy deployment of cost effective, secure solutions.

### **What is trusted computing?**

Trusted computing has three primary characteristics:

- 1) Users of a computer system are confident that they know to whom and to what entity they are talking (authenticity).
- 2) They have assurance that the information is transmitted accurately (integrity).
- 3) They are confident that the (privacy) of the information is respected.

## TCPA Security and Internet Business: Vital Issues for IT

An application that invokes proof of identity can support greater user confidence in areas including electronic cash, e-mail, free seating, networking, platform management, single sign-on, Virtual Private Networks (VPNs), Web access, and digital content delivery.

The objective of the TCPA specification is to make a trusted *subsystem* just as much a standard part of the PC platform as memory or graphics are today. Through a TCPA-compliant subsystem, core elements of trust are integrated into the platform. These elements extend trust to the PC's BIOS, which extends its trust to the OS loader, which extends its trust to the OS, which in turn can extend its trust to applications. In this way, the TCPA subsystem provides the foundation for a fully trusted PC platform and a foundation for IT managers to extend trusted computing across systems and networks for multiple users. The trusted system maintains authenticity, integrity, and privacy, while maintaining the freedom of choice that is central to the PC usage model.

### **Benefits of TCPA subsystems**

A TCPA subsystem provides reliable information about the software environment in a target platform, and provides an identity, or set of identities, which can be used as platform identities. A trusted subsystem also provides a foundation for data storage methods that can prevent access to the information if the software environment in the platform is altered.

Connected platforms benefit the most from a TCPA subsystem. In the general case of a client-server connection, the client can check that the software environment in the TCPA-enabled server is what it is expected to be, and check that the data relating to the client that is held in the server is accessible only if the software environment in the server is as it is expected to be. This enables the client to check the server before sending new personal information to the server. In addition, it enables the client to have confidence that existing personal data in the server is better protected. In the event of an attack on the server by a hacker, a suitably designed operating system can register the fact that the software environment has changed. This enables a client to detect the software change and refuse to deal with the server. At the same time, the client knows that old personal

## TCPA Security and Internet Business: Vital Issues for IT

data already on the server cannot be accessed by the hacker, because the software environment has changed. Moreover, a hacker who attacks a TCPA-hardened server cannot access customer data stored in the server.

A TCPA-enabled client provides advantages to the server and client alike. For example, the server can use the subsystem's identity to verify that the client is the correct client and that the client is working as expected. The client can use different identities for different transactions, and can take part in more “adventurous” transactions than might otherwise be possible. In addition, a TCPA subsystem provides a relatively low-cost way to transform a platform into a trusted software environment, without requiring the purchase of a dedicated crypto-coprocessor.

Following are three examples of how a TCPA subsystem can enhance security in B2B, B2E, and Web administration applications.

### **Example 1: B2B**

The following scenario illustrates how a TCPA-compliant system adds to the authenticity, integrity and privacy of a B2B Public Key Infrastructure (PKI) deployment.

In a vertical supplier/buyer e-Commerce model, TCPA capability enables a buyer to issue a challenge to the supplier platform to determine that it is a trusted system. This can be accomplished using an application that ensures that the transaction is correct to proceed. This challenge can be provided anonymously, in order to protect user privacy. For example, this capability can allow a TCPA-enabled PC user to browse anonymously, perhaps looking for the best prices among suppliers.

After deciding on a supplier, the buyer can challenge the server to determine that it is operating properly. The buyer can then utilize the TCPA subsystem to “digitally sign” the sales contract and send it to the seller. Digital signatures can provide assurance of the source of the data and that the received data is the same as the sent data. Digital signatures also prevent the data source from denying that the data was created by the

## TCPA Security and Internet Business: Vital Issues for IT

source (a feature known as ‘non-repudiation’). If the TCPA-enabled system is digitally signing the contract, the identity used for the signature can be simultaneously reliable and anonymous. In this context, the TCPA-enabled system ensures that the transaction was not compromised by unauthorized hardware or software designed to spoof or hack the transaction. The result is a fully trusted transaction.

### **Example 2: B2E**

Today IT managers can have serious issues with authentication systems based on passwords, and rogue viruses are being introduced that can make difficult to be sure that the platform environment can be trusted. The TCPA system can be used to support an enterprise virtual private network, in order to enable access by employees located in remote sites. This scenario would employ 2-factor authentication devices (e.g., Smart Cards and/or biometrics) utilizing a TCPA-enabled system. This process, known as “remote attestation,” allows an application (the “challenger”) to trust a remote platform. This trust is built by obtaining “integrity metrics” in the remote platform, securely storing these metrics in the remote platform, and then ensuring that the reporting of the metrics from the remote platform is secure.

For example, before making content available to a remote user, it is likely that a provider will need to know that the remote platform is trustworthy. The provider’s platform (the “challenger”) queries the remote platform. During system boot, the challenged platform creates a series of cryptographic digests (integrity metrics) that represent the method used to build the software environment in the challenged platform. These digests are statistically unique indications of the platform environment, yet they will occur in all platforms with the same software environment.

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. The TCPA

## TCPA Security and Internet Business: Vital Issues for IT

system reports the metrics and lets the challenger make the final decision regarding the trustworthiness of the remote platform. Based upon the reported integrity metrics, the challenger can determine if the platform is configured in a trusted state.

### **Example 3: Web administration**

Today, an e-Business website doesn't really know that it can trust interactions with unknown parties. TCPA provides new capabilities to address this potentially costly issue. The following scenario illustrates how an e-Business website can trust interactions with unknown parties over the Internet by using a recognized and trusted third-party that can verify to the interactions are coming from 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 Web site (AAWS), which could be provided by a PKI (Public Key Infrastructure) vendor, to request site verification. Using the TCPA Subsystem, the AAWS provides the user with certification credentials. These credentials assert that the user's 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 disclose anything that can be traced back to the user. For the purposes of the transaction, the platform is reliable, and also anonymous. The user can store private data in a TCPA-compliant system and then select when to disclose the information. This improves existing applications that use security, including Web browsers with SSL and e-mail using S-MIME (Secure Multi-Purpose Internet Mail Extensions).

### **Complementing existing standards**

Today's PCs already provide some degree of trustworthiness to users. For example, businesses routinely depend on the ability to trust PC functions such as Secure Sockets Layer (SSL) to help transact online business with security. The TCPA specification goes further to enhance security at the level of the platform hardware, BIOS, system software,



and the operating system. The TCPA specification is designed to complement existing standards, including the X.509 standard for digital certificates, PKCS11, IPSEC (Internet Protocol Security Protocol), IKE (Internet Key Encryption), VPN (Virtual Private Network), PKI, the PC/SC Specification for smart cards, biometrics, S-MIME, SSL and SET (Secure Electronic Transaction).

### **Can't we provide security in software?**

The ability to protect the integrity of a PC system through application software alone is becoming increasingly limited. This is because even the most robust PC operating systems cannot prevent unauthorized software from loading, before the operating system itself loads. Once such unauthorized software has loaded, it has access to areas of the system that should not be accessible in a trusted environment. To counter this threat, the PC needs a foundation of trust based in the PC platform.

The TCPA specification establishes a "TCPA subsystem" that makes security functionality integral to the PC platform. Once integrated in the PC, the TCPA specification enables trusted storage subsystems to raise the level of security in all subsequent layers. To be defined as "trusted platform" a PC must be trusted by local users and remote entities, including users, software, websites, and all third parties. The TCPA subsystem provides complete owner control over how the subsystem is configured. As mentioned in the "B2E" example above, while platform integrity metrics are provided by the subsystem, users maintain control over what to do with the information.

### **Privacy and user control**

Privacy is extremely important to every business and individual concerned about protecting confidential and personal information. 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

## TCPA Security and Internet Business: Vital Issues for IT

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 systems allow the PC owner to maintain complete control over information contained and offered by the system.

By providing a standardized means of user authentication, the TCPA compliant platform will support the continuing personalization of Web sites, as well as the concept of user mobility. In the future, airports might feature TCPA compliant PCs that would enable business travelers to authenticate themselves to the network, attest to the trust level of the PC, conduct their business in security, and then depart.

### **Conclusion**

The continuing success of e-Commerce and e-Business applications will depend on trusted computing, including the ability to provide authenticated owners with access to authorized information and to keep unauthorized persons out. The mission of the TCPA, through the collaboration of platform, software, and technology vendors, is to develop a specification for an enhanced trusted computing platform that strengthens the user's trusted domains.

The objective of the TCPA is to make a standardized trusted *subsystem* an integral part of the PC platform. The TCPA subsystem will enhance platform-based authenticity, integrity, and privacy and provide functions that can be used by operating systems and applications. The approach will enable PC platforms to retain their inherent flexibility, but at a much higher level of security. Stronger platform authentication and network integrity will enable IT managers to raise the level of trust for internal networks, as well as the Internet. By defining a baseline set of security features and capabilities, the TCPA specification will help make security solutions easier for IT organizations to deploy, use, and manage.

## TCPA Security and Internet Business: Vital Issues for IT

As security becomes increasingly refined through layers of the infrastructure, the hard and soft costs of deploying high-value applications can be expected to decrease substantially. The TCPA specification will assist in driving deployment costs and cost of ownership downward, while helping IT organizations realize the untapped potential of Internet business applications.

# # #

<sup>1</sup>International Data Corporation, “PC Vendors Look to Build a Solid Foundation for Security” by Abner Germanow, *IDCFLASH* 1999.