

SECURING NETWORK-BASED CLIENT COMPUTING: USER AND MACHINE SECURITY



The IT industry is addressing two complementary aspects of securing client computers on “untrusted” networks: user security and machine security. In this white paper, we explain the concepts of user and machine security and distinguish between the two. We compare two relevant technologies: smart cards, which address user security (or *who* can access network resources), and the Trusted Platform Module (TPM), which addresses machine security (or what *hardware* can access network resources). We explain how these technologies fit into an industry vision of a “trusted computing” platform.

What is User Security?

For the purposes of this paper, user security refers to methods used to establish the identity of (or “authenticate”) a user who is logging onto a computer system or network. The method used can be as simple as a username and password or it can rely on a token¹ such as a

User Authentication Methods

User authentication methods are commonly described as:

- “What you know” — Requires the user to remember a password or personal identification number (PIN).
- “What you have” — Requires the user to carry a “token” such as a smart card.
- “What you are” — Identifies user based on fingerprint, iris scan, and so forth.

Multifactor authentication combines more than one authentication method to provide increased security. Typical multifactor approaches combine “what you have” with “what you know” or “what you are.” For example, a token device such as a smart card (“what you have”) is usually combined with a user password or PIN (“what you know”). In this way, if the smart card is lost, it cannot be used without knowing the password.

smart card in combination with a username and password or biometric method. (See sidebar, “User Authentication Methods.”)

A smart card is a credit card-sized electronic device with a built-in microprocessor and memory that is used for user identification. User information and credentials, including digital certificates and encryption keys, are securely stored within the card. Because of their versatility, smart cards are increasingly being issued to employees of large companies and organizations. Smart cards are multifunctional: they can be used to log on the corporate network or gain entry to a building that is secured with badge readers at exterior doors. To log on the network, the employee inserts the smart card into a smart card reader that may be attached to or integrated into the computer, or embedded in the computer keyboard. The reader exchanges data with an authentication server (such as a RADIUS server) to complete the authentication handshake. The network infrastructure then enforces resource access based on the authenticated identity that has been established.

What is Machine Security?

In contrast to user security, machine security refers to measures designed to authenticate the computer system, rather than the user. For example, the following two scenarios require some level of machine security:

- **IP Security (IPsec)²** — The IPsec protocol used on IP networks can be configured to require a networked computer to authenticate its identity to the network prior to generalized network access to resources. The computer uses a digital certificate to

1. A token is a security device in the possession of an authorized user. The best known token device is the smart card, a credit-card sized device with an integrated microprocessor and memory.

2. IPsec is a security protocol from the Internet Engineering Task Force (IETF) that provides authentication and encryption over the Internet or a private IP network. Unlike the Secure Sockets Layer (SSL) protocol, which provides services at the application layer—layer 4—of the Open System Interconnection (OSI) network model and secures two applications, IPsec works at the network layer—layer 3—and secures everything in the network.

establish its identity to an authentication server before the computer attempts to use any network-available resources. In this way, network administrators can allow only supported client machines to access network resources.

- **File Encryption on Local Drive** — Computer credentials can also be used to encrypt files stored on the local hard drive, thus "locking" the files to a particular machine. The machine's credentials are required to unlock the files and access their content.

These scenarios and others require that the local system be able to generate and store the secret encryption keys used to encrypt and decrypt data, digitally sign documents, and authenticate systems. The problem with the current PC platform is that there is no standardized way to securely store keys that are used for machine identity so that the keys cannot be discovered if the system is stolen or otherwise compromised. The Trusted Platform Module (TPM) is an emerging technology that is designed to address this weakness in current platforms.

Trusted Platform Module

TPM is an initial step toward the goal of standardizing a more-secure "trusted PC platform." The TPM can be thought of as a smart card that is embedded on the system board and acts as a smart card for the machine.

The TPM is based on specifications developed by the Trusted Computing Group (TCG). The TCG is an industry standards group formed to "develop, define, and promote open standards for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices."³ Members include Microsoft, Intel, Dell, HP, and IBM. Current TPM implementations are based on the TCG 1.1 specification. TPM implementations based on the next-generation version, TCG 1.2, are expected in 2005.

The TPM has two components. The first is a secure microcontroller with cryptographic capabilities that is very similar to the microcontrollers in smart cards. The sec-

ond component is a proprietary software interface between the functions of the microcontroller and security-aware applications.

The TPM provides the following cryptographic capabilities: hashing, random number generation, asymmetric key generation, and asymmetric encryption/decryption. Each TPM has a unique root key that is initialized during the silicon manufacturing process. However, before a

Smart cards are best suited for user credential storage. The Trusted Platform Module (TPM) is best suited for host credential storage.

TPM can be enabled, its "owner" must be established. The end user establishes ownership of the computer system and its TPM via BIOS setup commands. These commands cannot be issued remotely; instead, the TCG specification requires that the end user issue the commands at

the local computer system. When completed successfully, the TPM has a unique owner, a "trust bond" is established, and the TPM can be used by TPM-aware software for security purposes. When coupled with software that can take advantage of its features, the TPM provides security that can be stronger than that contained in the system BIOS, operating system, or non-TPM applications.

Security implementations that rely on the TPM must also include "key escrow" services to securely back up and manage the unique keys associated with the TPM on each computer system. In this way, if something happens to the system, its full TPM-enabled identity can be restored. Without this capability, it would be impossible, for instance, to unencrypt files encrypted with the TPM key. Key escrow services are provided by public key infrastructure (PKI) systems that manage asymmetric key exchanges.

Smart Cards Vs. TPMs

It can be seen that smart card-based user authentication and TPM-based machine authentication are complementary, rather than competing, technologies. Table 1 presents appropriate uses of smart cards and TPM.

3. www.trustedcomputinggroup.org

User/Machine Authentication Scenarios	Smart Card	Trusted Platform Module (TPM)
User ID for virtual private network (VPN) access	Yes	No
User ID for domain logon	Yes	No
User ID for building access	Yes	No
User ID for secured e-mail	Yes	No
Host computer ID for VPN access	No	Yes
Host computer ID for domain access	No	Yes
Host computer ID for attestation (that is, authentication of software applications)	No	Yes

Table 1. Suitable Uses of TPM and Smart Cards

Future Secure Computing Platform

The TPM is only one piece of an industry vision of a future secure computing platform. Ideally, this platform cannot be compromised or accessed by unauthorized users or machines. The platform provides robust user authentication and protects data stored on the local drive. This vision implies secure software and built-in security hardware.

The future secure computing platform must encompass more than the secure generation and storage of encryption keys provided by the TPM. A complete standard solution must also encompass the client operating system, the CPU and chip set, and methods to secure client system I/O devices such as keyboards, displays, and mouse devices. A number of initiatives are under way to begin to address these components.

Microsoft® Windows® Next Generation Secure Computing Base (NGSCB)

The NGSCB is the future Microsoft secure operating system component of this vision. NGSCB consists of a set of software components that are currently scheduled for release beginning with the Microsoft next-generation operating system, "Longhorn."

NGSCB security is designed to allow an application or part of an application to be run in a trusted environment called "Nexus mode." The application is authenticated by the NGSCB infrastructure and runs in protected virtual memory space that is separate from other applications. Data stored to the hard drive is encrypted and I/O data (keyboard, monitor, and so forth) is also encrypted.

NGSCB is expected to leverage the next-generation TPM hardware, based on the TCG 1.2 specification. It

may also require modified CPU, video, keyboard, and USB hardware.

Secure CPU and Chip Set

The Intel® LaGrande technology (LT) will provide hardware support for the parallel, protected execution environments that are integral to the NGSCB architecture. According to Intel, LT consists of processor, chip set, keyboard and mouse I/O, and graphics subsystem enhancements that provide the following capabilities:

- Protected and isolated execution environments with dedicated resources managed by the processor, chip set, and operating system kernel. These protected environments will run parallel to standard execution environments.
- Support for a hardware-based mechanism such as TPM to provide sealed storage of encryption keys and other secret data.
- Protected communication between applications and USB keyboard and mouse devices.
- Protected communications between applications and display output.
- "Attestation" services, which provide authentication of software applications.

Figure 1 depicts a sample future Intel LaGrande platform architecture that includes the TPM and supports the NGSCB. The CPU and chip set are key areas affected by the new security initiatives.

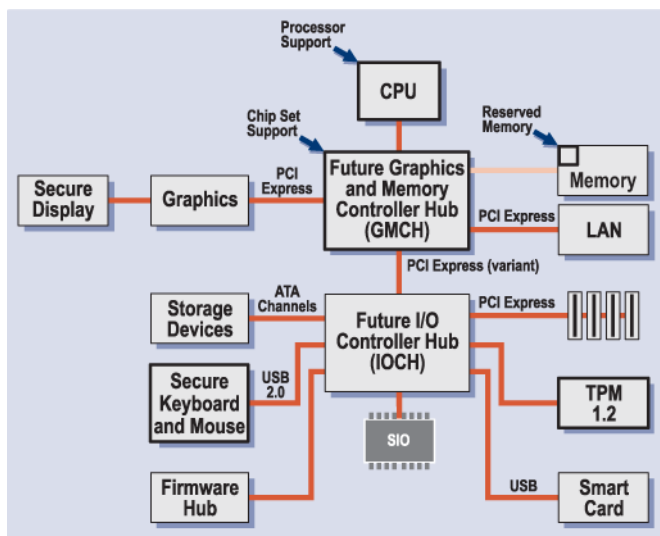


Figure 1. Sample LaGrande Platform Architecture That Includes the TPM and Supports NGSCB

Conclusion

The industry is making progress toward a robust, standards-based machine authentication security solution. This solution includes comprehensive TPM functionality, native operating system support, and PKI infrastructure on the network. It is unclear when all of these elements will be in place and mature enough for end-to-end solutions to be routinely deployed. Meanwhile, a TPM-based solution to provide baseline machine authentication may be appropriate in environments such as defense, finance, and medical industries where platform security is extremely important. In addition to the TPM module, this solution must include mature TPM-aware software and supporting server infrastructure, including PKI. This *machine* authentication must be accompanied by a robust and mature *user* authentication method.

Native TPM support in Microsoft operating systems will not be available until the NGSCB is released, beginning with Longhorn. NGSCB will not support the current TPM 1.1. Instead, it will natively support the next-generation TPM 1.2. Dell plans to offer a TPM 1.2 option in Summer 2005. Dell recommends this option for customers who will require native NGSCB support or the additional features of TPM 1.2.

For customers who require an interim TPM option, Dell will offer TPM 1.1 on selected Dell™ OptiPlex™ desktop, Dell Precision™ mobile workstation, and Latitude™ notebook systems in early 2005. Dell also offers a range of user authentication technologies in OptiPlex, Dell Precision workstation, and Latitude notebook systems. These offerings include smart cards, Dell USB keyboards with a built-in smart-card reader, and third-party biometric authentication devices.

Standardization is the key to making security a pervasive technology feature on computer platforms. Dell will continue to participate in major industry standards initiatives and to offer relevant standards-based security technology in Dell products. This approach protects customer investments in Dell systems and allows the systems to be deployed flexibly in a variety of platform and user security environments.

For More Information

- Dell security website: www.dell.com/security
- Trusted Computing Group:
www.trustedcomputinggroup.org
- Microsoft NGSCB technology:
www.microsoft.com/technet/security/news/ngscb.mspx
- Intel LaGrande Technology:
www.intel.com/technology/security

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2004 Dell Inc. All rights reserved.

Trademarks used in this text: *Dell*, the *DELL* logo, *OptiPlex*, *Dell Precision*, and *Latitude* are trademarks of Dell Inc.; *Intel* is a registered trademark of Intel Corporation; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.