Enhancing IT Security

with Trusted Computing Group Standards

An increasingly interconnected global computing environment brings with it myriad threats for enterprises to guard against, including software attacks and theft of both data and physical devices. This article discusses Trusted Computing Group™ security standards that can help enable IT organizations to effectively respond to these challenges.

BY FRANK MOLSBERRY AND BRIAN BERGER

Related Categories:

Enterprise security

Security

Standards

Trusted Platform Module (TPM)

Visit www.dell.com/powersolutions for the complete category index.

Concerns about the security of communications, transactions, and wireless networks—including problems such as data exposure, software attacks, identity theft, and even physical theft of mobile devices—can make it difficult to realize the potential benefits associated with pervasive connectivity and e-commerce. Standards-based security measures can address these issues by helping reduce security risks while also providing interoperability and protecting privacy.

The Trusted Computing Group (TCG) was formed in 2003 to respond to this challenge. TCG is a not-for-profit corporation with international membership and broad industry participation, including more than 135 members. The purpose of TCG is to develop, define, and promote open, vendor-neutral industry specifications for trusted computing and security technologies, including hardware building blocks and software interface specifications across multiple platforms and operating environments. Implementation of these specifications can help enterprises protect their information assets (data, passwords, certificates, keys, digital identities, credit card information, and so on) from software attacks and physical theft; provide mechanisms for proactively establishing trusted relationships for remote access through secure user authentication and computer authentication and attestation; and enable secure computing environments while avoiding compromises in functional integrity, privacy, and individual rights.

Protecting critical information

Products developed based on TCG specifications can help meet the challenges associated with software attacks from sophisticated and automated attack tools, increasing numbers of vulnerabilities, and widespread user mobility. These problems can contribute to the risks of electronic theft of valuable personal or enterprise data—including identity or authentication information that can give hackers access to multiple systems and accounts, thereby compounding the potential damage from the attacks—and to the risks of physical theft of mobile user systems such as notebooks, which can provide another route to sensitive data.

Software-only security mechanisms may not be sufficient to protect information assets. Even firewalls protecting intranet environments can prove inadequate, especially when software attacks bypass the firewall (for example, through e-mail attachments) or originate from internal users. Hardware-based embedded security solutions are therefore an increasingly important element of secure environments. The goal of TCG is to make these protections available across a broad range of computing devices with common software interfaces to facilitate application development and interoperability.

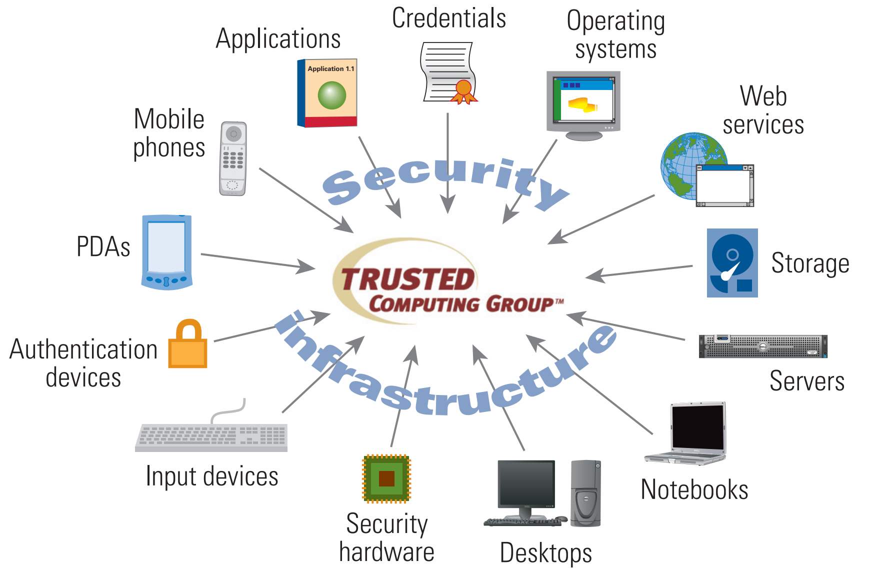

Figure 1. Trusted Computing Group standards as part of a comprehensive security infrastructure

Defining TCG specifications

TCG provides hardware and software interface specifications along with white papers, marketing programs, and other materials to promote awareness, understanding, and adoption of these specifications. Key TCG policies related to specification development include the following:

- **Open platform development model:** TCG is committed to preserving the open development model that enables any party to develop hardware, software, or system platforms based on TCG specifications, and to preserving consumer freedom of choice.
- **Platform owner and user control:** TCG is committed to enabling owners and users of computing platforms to remain in control of their platform, and to requiring platform owners to opt in to enable TCG features.
- **Privacy capabilities:** TCG is committed to including capabilities for securing personally identifiable data in its specifications.

The primary TCG specifications rely on the Trusted Platform Module (TPM) hardware component, which is in widespread deployment, and the TCG Software Stack (TSS), which developers can use as a foundation for various applications. TCG has also released the Trusted Network Connect specifications for network security implementations, and has created additional work groups to develop security standards for storage, mobile devices, servers, infrastructures, and peripherals. Figure 1 illustrates the comprehensive nature of TCG standards as part of a security infrastructure.

Trusted Platform Module

The TPM specification defines the architecture and other standards for TPMs—microcontrollers designed to securely store digital keys, certificates, and passwords to help maintain data confidentiality. TPMs are typically affixed to PC motherboards, but can potentially be used in any computing device that requires these functions. They are designed to protect key operations and other security tasks that might otherwise be performed on unprotected interfaces in unprotected communications, and to protect platform and user authentication information and un-encrypted keys from software-based attacks. TPMs from various semiconductor vendors are included on enterprise desktop and notebook systems from Dell and other vendors.

TCG Software Stack

The TSS specifies a standard software interface to TPM functions that facilitates application development and interoperability across platform types. The TSS includes functions that developers can use to create interfaces for existing cryptography application programming interfaces (APIs), such as Microsoft® CryptoAPI, the Intel® Common Data Security Architecture, and the RSA Security Public-Key Cryptography Standard #11. In this way, the TSS helps enable TPM support for applications using these APIs. Application developers can use the TSS to create interoperable client applications designed to improve tamper-resistant computing by taking advantage of TPM capabilities such as key backup, key migration, platform authentication, and attestation.

Trusted Network Connect

The TNC specifications define an open solution architecture designed to help network administrators protect networks by allowing them to audit endpoint configurations and impose enterprise security policies before establishing network connectivity. The TNC architecture builds on existing industry standards and defines new standards as necessary, with the objective of enabling nonproprietary, interoperable solutions within multivendor environments.

TNC provides a method of measuring and attesting to the characteristics of endpoint devices as they attempt to connect to a network. This method involves collecting endpoint configuration data and user authentication information for comparison with predefined organization access criteria—thereby helping create a security, or *safe computing,* profile for a system—and providing an appropriate level of network access based on the detected level of policy compliance, including full access, partial or directed access, or no access.

TCG work groups

To extend its specifications beyond PCs, TCG has created work groups to define implementation architectures for storage, mobile devices, servers, infrastructures, and peripherals. The Storage Work Group, for example, plans to build on existing TCG technologies and address standards for security services on dedicated storage systems, such as disk drives, removable media drives, flash storage, and multiple storage device systems. One objective is to develop standards and practices for defining the same security services across dedicated storage controller interfaces, including ATA, Serial ATA, SCSI, Internet SCSI (iSCSI), Fibre Channel, USB storage, IEEE 1394, and TCP/IP network attached storage. The Storage Work Group also acts as the TCG liaison to other industry groups that have jurisdiction over these storage interface standards to promote the adoption of TCG technology.

Implementing TCG specifications

When implemented in motherboards, desktop and notebook PCs, servers, and other computing systems, TCG specifications can help provide several important elements of a secure, integrated environment, including the following:

- Secure storage of files, personally identifiable information, and digital secrets, helping protect both data and identities from external software attacks or physical theft
- Strong multifactor user authentication through components such as security tokens, smart cards, passphrases, fingerprint readers, proximity badges, Subscriber Identity Modules, and so on
- Network access control in which an IT organization can control user access based on the organization's policies and security procedures, helping ensure that only secure client systems can access the network
- Exploitation of the latest OS features, such as the BitLocker feature of the Microsoft Windows Vista™ OS, which uses TPMs to measure boot process attributes and store keys for full-volume data encryption

Dell includes TPMs and Wave Systems EMBASSY Trust Suite software on many Dell™ Latitude™ notebooks, Dell OptiPlex™ desktops, and Dell Precision™ workstations. Dell also anticipates eventually incorporating TPM architectures on its servers and storage.

Evolving to meet ongoing security challenges

The open hardware building blocks and software interface specifications developed and promoted by TCG are designed to increase security and trust in computing platforms through hardware-based cryptographic functions, protected storage of user data, mechanisms for secure storage and platform integrity reporting, and platform authentication with multiple attestation identities. Organizations can prepare for a trusted enterprise model by deploying technologies that support TCG standards as they are developed. As threats from software attacks, theft, and other sources increase, TCG anticipates that trusted computing and security technologies will evolve to meet these threats, and plans to work with the IT industry to continue enhancing computing security.

Frank Molsberry is the lead security technologist in the office of the chief technology officer at Dell, and serves as the Dell representative to TCG. He has more than 20 years of experience in advanced systems software development and PC system architectures. Frank is a member of the Computer Security Institute and has a B.A. in Computer Science from the University of Texas at Austin.

Brian Berger is an executive vice president of marketing and sales at Wave Systems as well as a TCG director and chairman of marketing. Brian has a B.A. from California State University, Northridge, and attended the Harvard Business School Executive Education program.

FOR MORE INFORMATION

Trusted Computing Group:
www.trustedcomputinggroup.org