TRUSTED
COMPUTING GROUP™

Backgrounder
November 2006

More Secure Computing

Businesses, governments, academic institutions, and individual users are becoming increasingly interconnected through a variety of wired and wireless communication networks and with a variety of computing devices. Concerns about the security of communications, transactions, and wireless networks are inhibiting realization of benefits associated with pervasive connectivity and electronic commerce. These concerns include exposure of data on systems, system compromise due to software attack, and lack of user identity assurance for authorization. The latter concern is exacerbated by the increasing prevalence of identify theft.

In addition, as users become more mobile, physical theft is becoming a growing concern. Users and IT organizations need the industry to address these issues with standards-based security solutions that reduce the risks associated with participation in an interconnected world while also ensuring interoperability and protecting privacy. Standardization will also enable a more consistent user experience across different device types.

The Trusted Computing Group (TCG) formed in 2003 to respond to this challenge. The purpose of TCG is to develop, define, and promote open, vendor-neutral industry specifications for trusted computing. These include hardware building block and software interface specifications across multiple platforms and operating environments. Implementation of these specifications will help manage data and digital identities more securely, protecting them from external software attack and physical theft. TCG specifications can also provide capabilities that can be used for more secure remote access by the user and enable the user's system to be used as a security token.

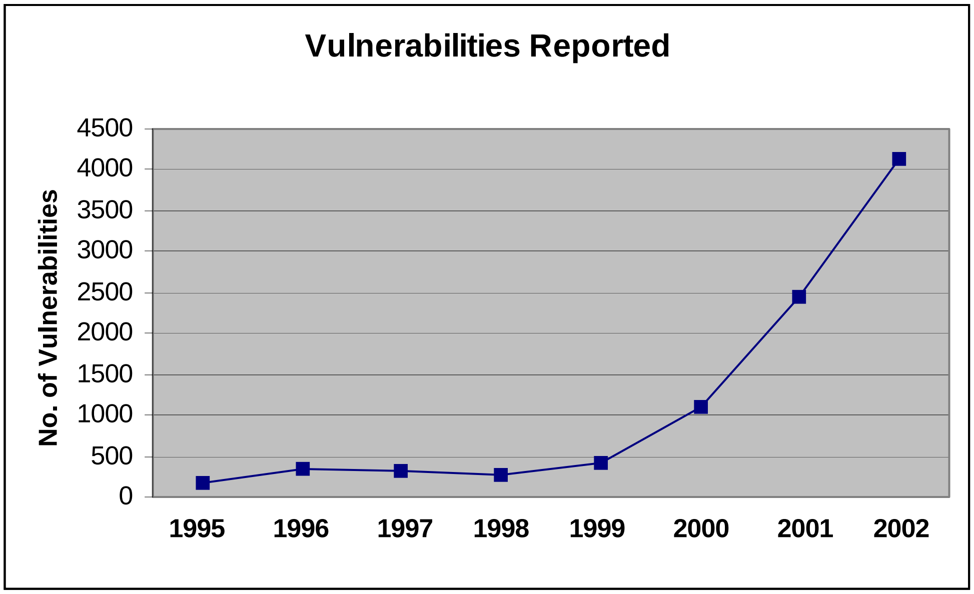
This backgrounder will provide an overview of the threats being addressed by TCG, the user and IT benefits that can be derived from the use of products based on TCG specifications, and the structure and specifications of the organization.

The Threat of Software Attack

A critical problem being addressed by products developed based upon these specifications is the increasing threat of software attack due to a combination of increasingly sophisticated and automated attack tools [1], the rapid increase in the number of vulnerabilities being discovered [1], and the increasing mobility of users.

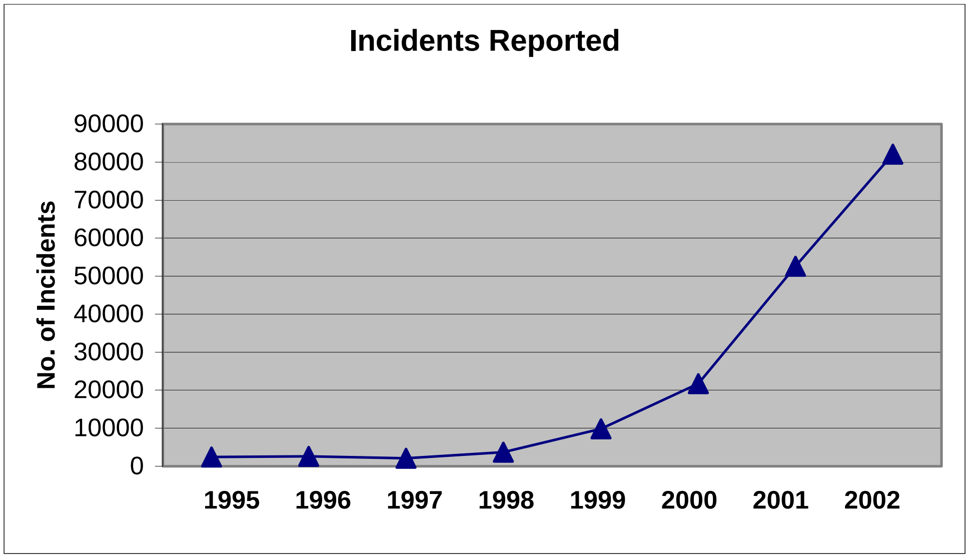
The large number of vulnerabilities is due, in part, to the incredible complexity of modern systems. For example, a typical Unix® or Windows® system, including major applications, represents on the order of 100 million lines of code. Recent studies have shown that typical product level software has roughly one security related bug per thousand lines of source code. Thus, a typical system will potentially have one hundred thousand security bugs.

The reality of this problem can be seen in data on reported vulnerabilities and incidents maintained by the CERT® Coordination Center (CERT) at the federally funded Software Engineering Institute operated by Carnegie Mellon University [2]. For example, reported vulnerabilities have, on average, doubled each year 2000 – 2002. CERT is reporting similar numbers of vulnerabilities reported for 2003 – 2006.



The large and rapidly increasing number of vulnerabilities creates an ideal situation for hackers, as the difficulties associated with keeping up with necessary patches (when available) creates an environment in which most systems will have at least one of the known vulnerabilities. Client systems are particularly vulnerable, as they typically do not have security-aware administrators to keep up with the patches. And, hacker interest in client systems is increasing, due to the valuable information stored on mobile systems and the large number of these systems in use.

The resulting number of incidents reported to CERT below, each of which may represent multiple systems, demonstrates that the problem is indeed very real.



The end result is that the data on systems is at risk. This risk takes several forms. First, there is risk of electronic theft of valuable personal or enterprise data. Second, there is risk of electronic theft of identity / authentication information which can give hackers access to other systems and accounts, thereby compounding the potential damage related to these attacks. In addition, as users become more mobile, there is an increasing risk that data and identity information on user systems may be compromised due to physical theft or loss.

As these risks increase, there is also an increasing recognition that software-only security mechanisms are not sufficient to protect information assets (e.g. user data, passwords, certificates, identity information, keys, credit card numbers, etc.). Even firewalls protecting intranet environments do not provide much comfort, as software attacks are known to originate from users inside these firewalls (e.g. from users on an intranet) and may also bypass these firewalls (e.g. via e-mail attachments), thus attacking from within. The use of hardware-based embedded security solution is an increasingly important approach for protecting information assets from compromise due to these attacks. TCG's goal is to make these protections available across a broad range of computing devices with common software interfaces to facilitate application development and interoperability.

In addition to protecting against compromise, the TCG specifications provide mechanisms for proactively establishing a more trusted relationship for remote access through more secure user authentication and machine authentication and/or attestation.

TCG and the Industry

The Trusted Computing Group is a not-for-profit corporation with international membership and broad industry participation. The purpose of TCG is to develop, define, and promote open specifications for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. By using the building blocks and software interfaces defined by TCG specifications, the industry is addressing a range of security needs without compromising functional integrity, privacy, or individual rights.

TCG was created with an organization structure and governance model, as defined by the TCG bylaws, which is similar to many other computing industry standards bodies. This includes the following:

- An open membership model with multiple membership levels
- A board of directors consisting of Promoters and elected Contributor members
- Multiple work groups that are open to Promoter and Contributor members and seek active participation by these members
- A reciprocal reasonable and non-discriminatory (RAND) patent licensing policy between the members

This structure is designed to enable the expedient development of open, industry-standard specifications with broad industry participation and to foster widespread adoption of the organization's specifications.

The key deliverables of TCG are hardware and software interface specifications, white papers and other materials that facilitate understanding and adoption of the specifications, and marketing programs that promote awareness, capabilities and customer adoption.
Further information on the bylaws and membership levels are available on the web at www.trustedcomputinggroup.org.

User Benefits

When implemented in motherboards, desktop and notebook PCs, and other computing systems, TCG specification can immediately benefit users and enhance confidence in the security of their systems in many ways. Examples are:

- More secure storage of files, personally identifiable information, and digital secrets. This protects both data and identity from compromise due to external software attack or physical theft.
- More secure user authentication by protection of keys used by authentication processes such as 802.1x, S-MIME e-mail, and VPNs. This enhances the security of remote access.
- Lower-cost and stronger user authentication by using systems with Trusted Computing components as a security token along with other types of authentication (pass phrases, fingerprint readers, key fobs, smartcards, proximity badges, SIMs, etc.) to achieve stronger multi-factor user authentication. In this case, the system becomes "what you have" from an authentication standpoint.

Other applications that implement the specifications:

- More secure platform authentication through protection of a key that is associated with the platform.
- Platform authentication with multiple anonymous trusted identities which, when combined with user authentication, will enable additional remote access security while protecting privacy.
- More secure data protection through confirmation of platform integrity prior to decryption.
- More secure platform access through the use of hardware authentication.
- Platform authentication capabilities for user identities that could be either anonymous or identification for secure access to such capabilities as Web Services.
- More secure data access in both a connected network environment and in a standalone client where platform authentication plus data access authentication is desired.
- Network access control in which the IT organization can control user access based upon policies and security procedures, knowing only secure clients have accessed the network.

TCG Specifications

TCG policies that impact specification development are:

- Open platform development model - TCG is committed to preserving the open development model that enables any party to develop hardware, software, or systems based on TCG specifications. Further, TCG is committed to preserving the freedom of choice that consumers enjoy with respect to hardware, software, and platforms.
- Platform owner and user control – TCG is committed to ensuring owners and users of computing platforms remain in full control of their computing platform and to requiring platform owners to opt-in to enable TCG features.
- Privacy effect of TCG specifications – TCG is committed to ensure that TCG specifications provide for an increased capability to secure personally identifiable data.

TCG currently offers specifications for the hardware Trusted Platform Module, which is in widespread deployment – TPMs are available from a number of vendors and implemented in tens of millions of PCs and other systems.

The organization also has published the Trusted Computing Group Software Stack, known as TSS 1.1, which developers are using as a foundation for various applications. Both the current and future TCG specifications will provide backward compatibility with existing specifications. Specifications are not developed exclusively for any specific company products or architectures

To extend the specifications beyond the PC, TCG has work groups for servers, mobile devices, storage, infrastructure and peripherals. A specification for network access control, Trusted Network Connect, has been available to industry for several years, and products to implement it are available from a number of networking equipment and applications providers.

TCG also has released a specification for trusted servers. As with other specifications, this one supports a number of server types and form factors, and as implemented in servers shipping from several vendors, can help protect financial and other sensitive transactions and support Trusted Computing clients already in deployment.

TCG also has started to extend the concepts of the trusted platform to mobile phones. The work group tackling the issue security on handheld systems has published a specification for the Mobile Trusted Module and anticipates additional specifications to follow.

The group also will publish a specification to enable storage security.

.

Trusted Platform Module (TPM) Overview

The Trusted Platform Module (TPM) is a hardware component that securely stores digital keys, certificates and passwords. TPMs protect encryption keys and digital signature keys to maintain data confidentiality. TPM chips are designed to protect key operations and other security tasks that would otherwise be performed on unprotected interfaces in unprotected communications. Especially important, TPMs are specifically designed to protect platform and user authentication information and unencrypted keys from software-based attacks.

TCG Software Stack (TSS) Overview

The TCG Software Stack (TSS) provides a standard software interface for accessing the functions of the TPM in order to facilitate application development and interoperability across platform types. The TSS includes functions that can be used to create interfaces for existing crypto APIs such as Microsoft CryptoAPI (CAPI), CDSA, and PKCS#11, thereby enabling TPM support for current and future applications using these APIs. To make full use of the TPMs' capabilities, including such functions as key backup, key migration, platform authentication and attestation, applications are written directly to the TSS.

Summary

TCG and its member companies are answering the need for increased security and trust in computing platforms. The open hardware building block and software interface specifications developed and promoted by TCG will attain this goal through hardware-based cryptographic functions, protected storage of user data and secrets, mechanisms for secure storage and reporting of platform integrity information, and platform authentication with multiple attestation identities.

As security threats increase, trusted computing and security technologies will evolve. TCG will continue to look for opportunities to work with the industry to make meaningful contributions to enhancing the security of the computing environment.

Information on TCG, member products and specifications is located at www.trustedcomputinggroup.org.

References:

1. CERT Web Site: http://www.cert.org/archive/pdf/attack_trends.pdf [Overview of Attack Trends]
2. CERT Web Site: www.cert.org/stats/cert_stats.html [CERT/CC Statistics]