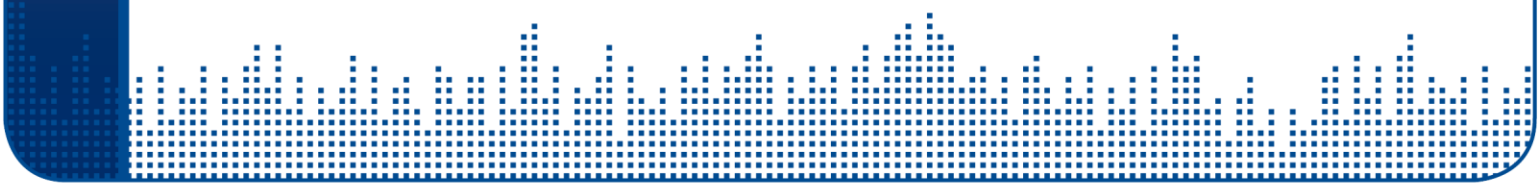
Securing Financial Institutions

November 2009

Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org



TRUSTED COMPUTING GROUP

Securing Financial Institutions

"Because that's where the money is," Willy Sutton, famous 20th century bank robber.

Why do financial institutions need even more protection than other enterprises? Willy Sutton would know the answer. According to Privacy Rights Clearinghouse, banks and credit card companies were the leading targets of the confidential data breaches reported in 2005, representing 20 percent and 18 percent of reported breaches.

• Banks	20%
• Credit Card Companies	18%
• Government Organizations (including universities)	13%
• Healthcare Providers	9%

Table 1. Entities reporting confidential data breaches in 2005.

On average, 40 to 50 percent of the reported confidential data breaches from February 2005 through March 2007 were from stolen laptops. Other causes can include malware attacks, lost or stolen hard drives or data disks and even cell phones and PDAs with confidential data. These other categories could be an increasing cause of concern if appropriate actions are not taken for improved security.

In addition to fines and penalties required by law, the Ponemon Institute's 2005 National Encryption Survey says the cost of a data breach includes:

- Immediate loss of up to 20 percent of clients
- 40 percent consider terminating the relationship
- 5 percent consider legal action

As a result, the estimated average cost per incident is about $14 *million* at the organizational level. While costly, there are laws and regulations that impact organization leaders with personal fines and even jail time for certain type of disclosures/breaches.

Laws and Regulations that Impact Financial Institutions

The business need for network access control is clear: Today's desktop isn't what it used to be; in fact, it may not be a desktop PC at all. As more users telecommute or connect from remote offices, it is more likely to be a laptop that is the machine of choice. These laptops are a threat to corporate networks, and change the network perimeter to one that is very porous and can be easily penetrated when the laptops are sitting in a remote coffee shop or on a hotel network. The first thing that most of these laptops do every morning is to connect to the Internet and grab their corporate email. As the Internet becomes the main business communications pathway, companies need stronger defenses on each user's computer to ensure that they are healthy and not a potential threat to corporate computing resources.

Network access control is a very different kind of security from beefing up your perimeter defenses with a new kind of intrusion prevention appliance, although some intrusion vendors have including various endpoint health assessment tools as part of their product offerings. It also isn't about inventing a better virtual private network, although some VPN vendors have also included endpoint assessment routines in their products. It really is an entirely new way of looking at your network and how machines connect to it, with the understanding that it isn't just the user but also the machine that needs to establish some form of trusted relationship.

Government regulations for privacy, identity theft and more apply directly to financial institutions. Currently, more than 41 breach notification laws exist in the United States. A brief listing of some of the more important ones includes:

- The Financial Services Modernization Act of 1999 (more commonly known as the Gramm-Leach-Bliley Act (or GLB)) is the major federal law that covers privacy for personal financial information.
- The Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- The Fair Credit Reporting Act (FCRA)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

At the federal level, there are or have been a number of significant U.S. bills passed or proposed that impact protection of data.

According to the Federal Trade Commission (FTC), reasonable measures for disposing of consumer report information could include establishing and complying with policies to destroy or erase electronic files or media containing proprietary information so the data cannot be read or reconstructed. A technical solution for preventing unauthorized viewing of confidential files specified in several regulations is full disk encryption (FDE) that provides a safe harbor for owners of lost or stolen hardware.

How is Data Accessed Illegally?

While the problems of easy data access on lost or stolen portable computers or portable drives or data disks without encryption are well known, a more subtle potential data breach problem occurs with hard drives in a data center. When a hard drive with confidential data leaves the data center for failure, maintenance, reconditioning, end of life or any other reason, without inherent protection, the data is easily accessible. An IBM study says that 90 percent of drives returned for problem operation were still readable. So, even a failed drive may not mean inaccessible data, especially to technical expert.

Specific attacks to computers through the internet are one of the major concerns for any computer owner, especially financial organizations. Among the more/most dangerous malware are keystroke logger and rootkits. A keystroke logger captures everything typed on a device (including passwords) and transmits it to unauthorized users. Rootkits attack a computer by modifying the operating system to hide files and run processes from standard security control. This malware provides complete control of connecting device or endpoint, normally with little chance of detection.

A rootkit can produce a network problem called a lying endpoint. If an authorized user accesses a network with a computer infected by a rootkit, the computer will not reveal its true situation or lie about its integrity, gain access to the network and subsequently infect other machines on the network.

A study by Gartner indicates that while hackers and viruses present a constant threat, 90 percent of all security breaches were "self-inflicted" and could have been avoided if the company took the right steps. The right steps include a complete solution that covers all the ways that data can be accessed by unauthorized users.

Trusted Computing Group Solutions

The authentication, data protection and network security for the entire enterprise, protecting desktop computers, portable computers, hard drives, data disks, and other portable devices as well as the enterprise network, can be done on a device by device or system by system basis with the challenge of getting everything to interface properly. Alternatively, protection can be handle using products that were designed based on open specifications intended to provide interconnectivity, compatibility and scalability.

Figure 1 shows how the Trusted Computing Group (TCG) is enabling a security infrastructure that addresses all of the major concerns of large and small organizations. Comprised of major companies that cover the enterprise with connectivity and computing technology, TCG specifications and products developed upon

this work are well positioned to address the security issues that confront financial and other institutions. TCG specifications for Trusted Platform Module (TPM), Trusted Storage and Trusted Network Connect (TNC) provide a starting point for enterprise-wide security that can easily be expanded.

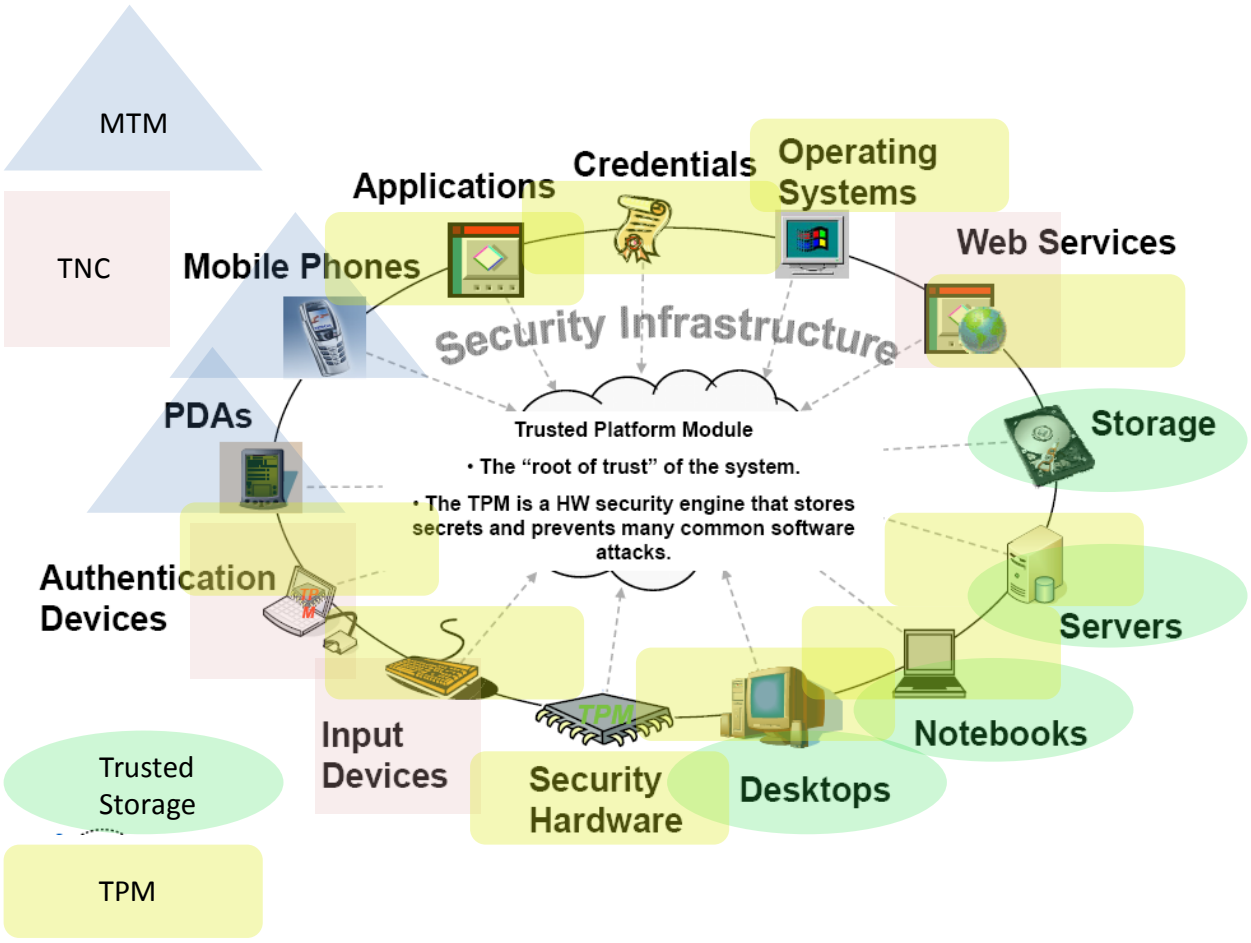


Figure 1. An open architecture system solution for enterprise protection provides compatibility, scalability and cost effectiveness.

Trusted Platform Module

The definition of a hardware component called the Trusted Platform Module (TPM), a computer chip that takes security to a higher level than software alone can achieve, was the initial specification developed by TCG. The TPM can store secrets and encryption keys, enable digital signing and help ensure that the computing platform remains trustworthy. Since most enterprise-level computers contain a TPM (currently approximately 300 million), using the capability provided by the TPM is the first step towards improve security in any enterprise, especially the most frequently targeted by thieves, the financial sector. To do this, the TPM needs to be activated. Once activated, the TPM can provide a hardware based security for machine authentication to networks, VPNs and wireless access points. This solution provides both users and organization with proven hardware authentication and access to local and network information from only the authorized user.

Trusted Storage

TCG's Trusted Storage specification provides an enterprise wide means for implementing full disk encryption. Encryption performed in the drive not only occurs automatically with self-encrypting drives (SEDs), SEDs simplify the enterprise encryption process for handling sensitive data, since all data is encrypted internal to the drive. TCG's specifications for hardware-based encryption does not require user intervention and does not impact system performance like traditional software only encryption schemes that require cycle time from the main processor.

TCG Storage Work Group Security Subsystem Class: Optical Version 1.0 specification extends TCG's industry-standard process of FDE to optical storage disks, making the data on lost or stolen disks useless to the finder since the encrypted data cannot be accessed.

Trusted Network Connect

The TCG's Trusted Network Connect specification provides an open framework for strong user authentication while:

- allowing guest access,
- blocking the access of unsafe endpoints,
- assessing the threat from clientless endpoints such as IP phones, cameras, physical security equipment and printers, and
- deciding proper network access on a collaborative hardware basis.

A Secure Financial Enterprise

In the U.S., government agencies that deal with financial institutions already recognize the benefits of the technologies from the Trusted Computing Group and recommend them to financial institutions. For example,

In Part 3, Technologies To Mitigate Account Hijacking, the Federal Deposit Insurance Corporation (FDIC) identifies and discusses the TPM as one of seven existing authentication technologies to provide increased security. The FDIC also promotes TPM usage to member banks (for more information on Trusted Computing in other sectors of government, see http://www.trustedcomputinggroup.org/solutions/government.

Working in concert, products that implement TCG standards provide authentication, data protection and network security across the financial enterprise to meet government requirements as well as users' expectations for security.