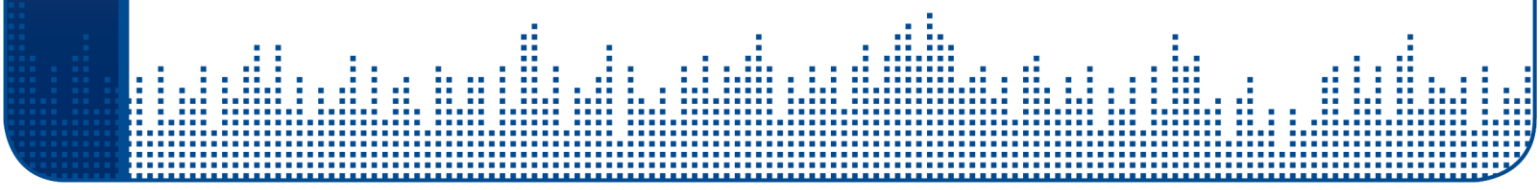
Root of Trust: The Foundation for IT Security

May 2014

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



Root of Trust: The Foundation for IT Security

A tsunami of news reports about data breaches, attacks and hacks has left the security and IT communities reeling – and busy. And a huge number of additional incidents are never reported, or even worse, not detected.

For years, security experts have known of the availability of a hardware root of trust that can anchor core security functions and protect systems, data and networks. But for many reasons, ranging from lack of awareness to difficulty implementing to resistance to change, these solutions have languished while other, reactive tools and solutions took center stage.

Now, security professionals worldwide have woken up and realized that attacking security problems after the fact is not the most effective tactic, and more attention is being paid to a more proactive and holistic approach.

Enter the TPM, or Trusted Platform Module. Typically deployed as a discrete or integrated chip on the circuitry of PCs, servers and embedded systems, the TPM is based on best practices and industry standards for protecting vital security information, such as keys, certificates and passwords. Unlike traditional approaches of storing these items in software that is routinely hacked, these critical bits of data are securely encrypted and stored in the TPM.

The TPM also can measure the "state" of a system and if specific elements of a system have been changed, which often signals malware or boot kits, the system is automatically shut down, or other action taken. While the TPM can be useful in many security applications, we will look at a specific use model in this article.

Connect Only Trusted PCs to the Office Wireless Network

With all the reports of network hacking and the resulting impact on each affected company's business, it does not take much convincing to require password protection for users seeking access to the corporate network. However, a password is only effective for the least experienced hackers.

In contrast, a more secure approach can ensure that only trusted clients connect to the network. This solution does not require anyone to invent, purchase or install new hardware. Based on an open standard developed by the not-for-profit Trusted Computing Group (TCG), the Trusted Platform Module (TPM), a hardware component present in over 500 million enterprise-level computers, can be used to safely connect company PCs to the wireless network in the office.

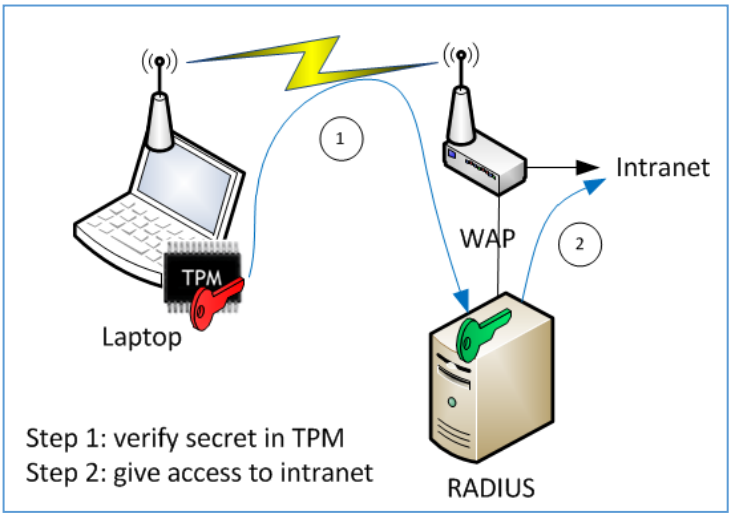
Making the Connection

Laptops mobile computers usually have a Wireless Network adapter that can connect to wireless network access points (WAP). A WAP can be connected to the Internet or to the corporate intranet and it can be configured to authenticate a user. Also, a WAP can provide secured connections to prevent eavesdropping. In a network setup with a single WAP, a Pre Shared Key (password) is configured in the WAP wireless configuration. The same password is entered on the laptop during the wireless network setup. This password is used to authenticate a WAP client and to secure the connection. In networks with multiple WAPs, the configurations and authentication method is centrally managed.

RADIUS

Using only a password does not provide much security. The password must be shared with any user that wants to setup a wireless connection. Also, a password can be easily abstracted from the laptop. A better method is to authenticate the user or the computer to a central server. The central server communicates with the WAP to accept or deny a wireless connection.

Remote Authentication Dial-In User Service (RADIUS) is a standard protocol that can be used to manage secure wireless network connections. The wireless user (that can be a person or the laptop) receives a credential that is used by the RADIUS server to check the identity of the laptop or the user. This credential must be protected to prevent identity theft. The credentials can be protected by a smartcard (persons) or the Trusted Platform Module (computers). Using a smartcard for this purpose has several disadvantages. A user can forget the smartcard PIN or forget or lose the smartcard. Smartcards or the smartcard reader can break and smartcards are expensive to deploy.



Trusted Platform Module

The TPM is a security chip that is soldered on the motherboard of the laptop. Since the TPM chip is inextricable from the laptop, it can be used to store secrets that belong to that laptop only. When a TPM is used to authenticate the laptop to the WAP, no other credentials are required to setup a wireless connection to the intranet and even multiple users on a single computer can use the same computer to access the wireless network. See Sidebar for more TPM insight.

Digital Certificates

A RADIUS server uses Digital Certificates to authenticate a wireless session. Certificates are considered a very secure method to identify and authenticate users or computers. Windows servers and clients have full support for certificates. However, Windows does not provide sufficient protection for the secret component (identity) of the certificate. The secret is stored in the operating system and can be obtained by hacking tools.

A better method is to store that secret in the TPM. The TPM protects these secrets by the special, tamper-resistance construction of the TPM. When the secret is provided by the TPM, the network can verify that it is the company's laptop and not an iPad that is using a stolen secret from the Operating System. Another advantage of the TPM is that it uses the same standard Windows components to create and protect the secret. This will require only one or two minor changes in the RADIUS server configuration.

Setting Up and Managing the TPM

To use the TPM for the protection of Windows secrets, users need to install some type of management software, offered by a number of software vendors. These management tools provide the Cryptographic Service Provider (CSP), a Windows crypto module that will deal with the communication between the TPM, the Wi-Fi adapter and the RADIUS server.

Using the TPM and this software has serveral advantages:

- ✓ Identities are protected by special security hardware (TPM) and can't be stolen
- ✓ The TPM can be used to identify the laptop or;
- ✓ The TPM can be used to identify one or more users (no limitation on the number of users)
- ✓ Al the required software, TPM and RADIUS configurations, TPM management and generation of the digital identities, can be fully automated.
- ✓ Any new laptop in your network automatically connects securely to your intranet without IT management support or end user actions.
- ✓ Support for SMB Wi-Fi Access Points (Linksys, TP-Link, Sitecom, Level One and more) and enterprise class Wi-Fi equipment (Cisco, Juniper, Aruba Networks and others).
- ✓ Scalable from 1-100k+ users.
- ✓ No procurement, personalization and logistics costs for external devices (like smartcards or hardware tokens). The TPM is the most cost-effective solution.

Secure Access When Required

Enterprise security does not have to be compromised by allowing access to authenticated computers and users. The protection provided by available hardware enables a higher level of security and is easily configured to provide other computer and network advantages. With the TPM, network managers can be assured that only trusted PCs are allowed to connect to the office wireless network. Equally important, they can avoid work interruptions knowing that those authorized individuals requiring access will be granted access as required.

Assisted by other available software products, the TPM enables numerous security-enhancing processes as shown in Table 1.

How effective is a TPM at protecting the data on a computer and restricting the unauthorized network access?

The National Institute of Standards and Technology (NIST) has issued directives for ensuring the Basic Input/Output System (BIOS) integrity of computers. The BIOS allows desktop and laptop computers to initialize their hardware during the boot process. Unfortunately, since it is firmware, the BIOS can be altered or reconfigured making the computer vulnerable to a variety of attacks and make the computer an entry point for further attacks on corporate networks.

Application Type
File/Folder Encryption
Full Hard Disk Encryption
Container Encryption
Workgroup Security
High Security User Authentication
Machine Binding
Secured Remote Administration and Mutual Authentication
Client-based Single Log-in
Protected Information Repository
E-mail Integration
Digital Signatures
Enterprise Login
Remote Access
Hardened PKI
TPM System Backup and Recovery
TPM and User Management
Platform Attestation

Table 1. TPM-Compatible Application Software Capabilities

The NIST report mentions and recommends the TPM as a hardware means to establish credible Roots of Trust to ensure that the BIOS has not been compromised. In addition, the report defines attributes that endpoint vendors should provide and minimal essential BIOS integrity measurements for reporting. Working in conjunction with other TCG open standards, including several network access specifications, the TPM can provide a significantly higher degree of network security, especially for wireless access.

For more information on industry efforts to provide a root of trust, go to http://www.trustedcomputinggroup.org/solutions/authentication.

NOTE: Portions of this article were previously published by Sys-con Journal (www.sys-con.com).