## Overview

One of the biggest challenges facing computer network administrators today is keeping track of the hosts on their networks. Without this knowledge, it is impossible to keep all hosts patched, up-to-date, and protected from infection and exploitation by malware.

Trusted computing technologies can help administrators take control of their networks so that they can begin to address security problems. Products that leverage these technologies are becoming more and more widely available. Network owners should position themselves to take full advantage of these new products by making sure that they purchase hosts that support the full range of trusted computing technologies.

## Trusted Computing Group

The Trusted Computing Group (TCG) is an industry and government consortium formed to develop and promote standards for trusted computing technologies. They have produced specifications and guidance for—among other things—the hardware TPM, the measured boot and launch of PC operating systems, and the TNC network security architecture.

## Trusted Computing In Action: Host Integrity At Startup

NSA's Research Directorate is currently developing a trusted-computing-based network and host integrity capability called Host Integrity at Startup (HIS). HIS will provide a basic measured launch and reporting capability for commodity operating systems. Measurement reporting is triggered by critical platform events such as user-login, administrative reset, or access to sensitive data. For example, during every user-login from a Trusted Computing-enabled host, the boot time measurements are sent to a central service running on a server. The service compares the new measurement with the host's previous measurement. If the measurement has changed, an administrator could be notified by email. If the system had been patched since the last boot, the changed measurement is a good indicator that the patches "took." If the host had not been patched, then a change might indicate that the host was compromised by malware, or that a user has installed unauthorized software on the system.

Over time, HIS measurements could be expanded to cover not only the operating system kernel, but also applications such as intrusion detection systems and virus scanners—even email clients and web browsers. Ultimately, measurement could be combined with reporting and network access controls to ensure that only fully compliant hosts can have access to operational networks.

For more information about HIS,
Email: hostintegrity@tycho.nsa.gov

System and Network Analysis Center
9800 Savage Rd.
Ft. Meade, MD 20755-6704
410-854-6632 DSN: 244-6632
FAX: 410-854-6604

NSA Creative Imaging 39929 nl Published April 2010

*The* Information Assurance Mission at NSA

# Host and Network Integrity *through* Trusted Computing

# Take Control of your network

## Trusted Platform Module

Trusted Computing Technologies are included in most PC desktop systems sold today. The most common is the Trusted Platform Module (TPM). The TPM is a motherboard-based cryptoprocessor with capabilities that include secure generation and storage of cryptographic keys, and generation of random numbers.

An important capability of the TPM with respect to host integrity is the accumulation and secure storage of system measurements. Measurements are hashes of host software computed by the host and accumulated within the TPM. If the same components are measured at a later time, and the measurements have changed, then the components have changed. This mechanism can be used to detect whether system software has been infected with malware.

## Measured Boot and Measured Launch

Measurement is a powerful capability for generating information about the integrity of software and data. Many hosts that support a TPM include a Trusted Computing Group (TCG)-compliant BIOS that automatically measures the host's pre-boot environment. When compared with prior measurements, this measurement indicates whether the BIOS, boot loader, and other low-level system components have been modified since the last system boot.

Many modern microprocessors support a measured launch capability that can be leveraged to ensure the integrity of a post-boot software environment—such as an operating system kernel or virtual machine hypervisor. The measured launch may be used in conjunction with pre-boot measurements to provide reasonable assurance that critical system components have not been modified since the last launch. This potentially powerful capability is provided by microprocessors that support Intel Trusted Execution Technology (TXT) and AMD-V virtualization.

## Network Access Control

Simply measuring pre- and post-boot environments is not enough to ensure network integrity. In order to actually improve the security of a network, the measurements computed for individual hosts must be collected and acted upon. At the very least, measurements should be reported to system administrators, who can then decide whether action is needed. Ultimately, systems can attest their integrity to a centralized network access-control point using an architecture such as Trusted Network Connect (TNC). The control point can decide whether the host should be allowed on the network.

## Recommendations

Trusted Computing Technologies can provide network administrators with basic information about host integrity without expensive hardware or excessive administrative overhead.

The potential benefits of trusted computing are well worth the minimal investment. While today it is hard to buy a PC that does not come with a TPM, hosts that support measured launch are less common. When purchasing new hosts, (such as Intel's TXT or AMD-V virtualization technology), system owners should look for desktops and servers that include a TPM and support for measured launch and protected execution.

Hosts that support TPMs should have their TPMs turned on and activated from the BIOS. This enables measurement of the pre-boot environment, and is necessary for measured launch. For more information on trusted computing and taking advantage of the TPM, see "How to Use the TPM: A Guide to Hardware-Based Endpoint Security," on the TCG website.

www.trustedcomputinggroup.org

# Enable your Trusted Platform Module