PROJECT DESCRIPTION

VALIDATING THE INTEGRITY OF SERVERS AND CLIENT DEVICES

Supply Chain Assurance

Tyler Diamond
Nakia Grayson
Celia Paulsen
Tim Polk
Andrew Regenscheid
Murugiah Souppaya
National Institute of Standards and Technology

Christopher Brown
The MITRE Corporation

DRAFT

November 2019

supplychain-nccoe@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://www.nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

Abstract

Product integrity and the ability to distinguish trustworthy products is a critical foundation of Cyber Supply Chain Risk Management (C-SCRM). Authoritative information regarding the provenance and integrity of the components provides a strong basis for trust in a computing device, whether it is a client device, server, or other technology. The goal of this project is to demonstrate how organizations can verify that the internal components of their purchased computing devices are genuine and have not been tampered with or otherwise modified throughout the device's life cycle.

This project addresses several processes: (1) the processes used by original equipment manufacturers (OEMs), platform integrators, and potentially Information Technology departments to create verifiable descriptions of components and platforms; (2) how to verify devices and components within the single transaction between an OEM and a customer; and (3) how to verify devices and components at subsequent stages in the system life cycle in the operational environment. This project will use a combination of commercial and open-source tools to describe the components of a device in a verifiable manner using cryptography. Future builds of this project may cover the other critical phases of the C-SCRM. This project will result in a freely available NIST Cybersecurity Practice Guide.

Keywords

anti-counterfeiting; anti-tampering cyber supply chain risk management; asset management system; computing device; hardware assurance; hardware roots of trust; integrity; server security

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://www.nccoe.nist.gov.

Comments on this publication may be submitted to: supplychain-nccoe@nist.gov.

Public comment period: November 22, 2019 to January 6, 2020

TABLE OF CONTENTS

1 Executive Summary

Purpose

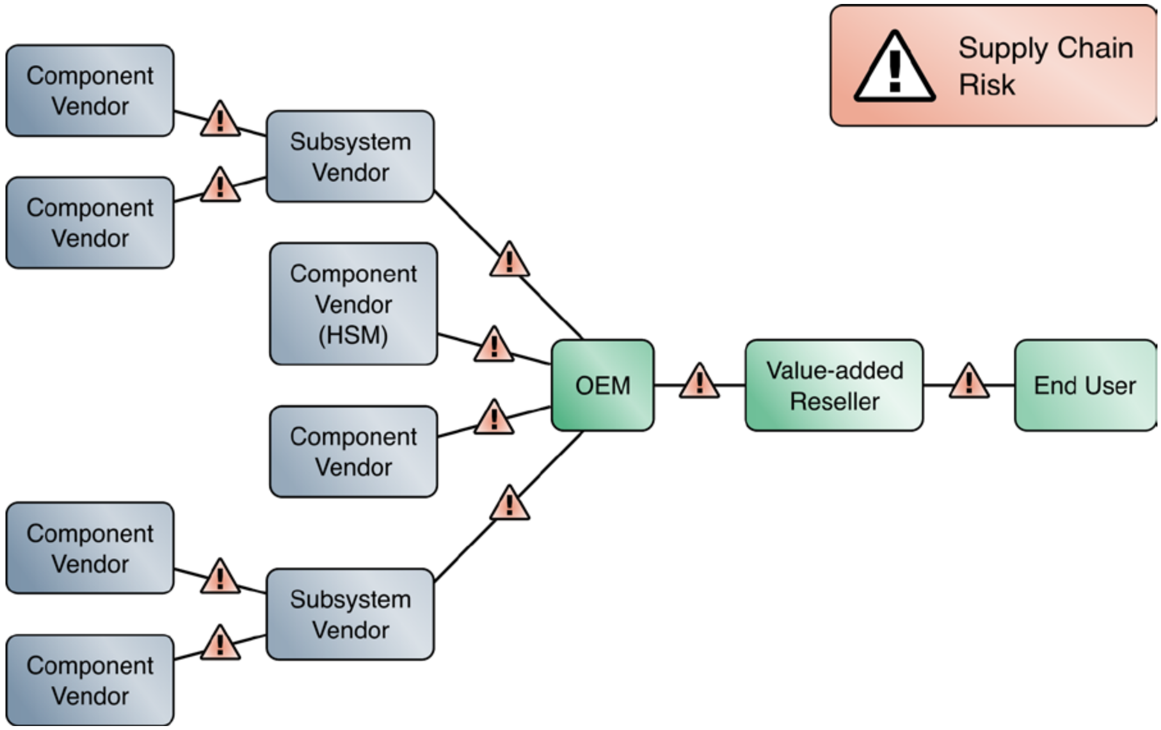
Organizations are increasingly at risk of supply chain compromise, whether intentional or unintentional. Managing cyber supply chain risks requires ensuring the integrity, security, quality, and resilience of the supply chain and its products and services.

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of information and operational technology product and service supply chains. Cyber supply chain risks may include unauthorized production, tampering, theft, and insertion of unexpected software and hardware, as well as poor manufacturing and development practices in the cyber supply chain [1]. C-SCRM presents challenges to many industries and sectors and requires a coordinated set of technical and procedural controls to mitigate cyber supply chain risks throughout manufacturing, acquisition, provisioning, and operations.

This document defines a National Cybersecurity Center of Excellence (NCCoE) project to help organizations decrease the risk of a compromise to products in a specific stage of their supply chain, which may result in risks to the end user. Tampering or misconfiguration in an organization's supply chain is a difficult challenge to effectively solve. Modern supply chains are highly complex, introducing risk of tampering at numerous points, as illustrated in Figure 1-1 Supply Chain Risk. Mitigating this risk is a difficult challenge, one not at all addressed in many cases.

This project will produce example implementations of technical mechanisms that organizations can employ to verify that the internal components of their purchased computing devices are genuine and have not been unexpectedly altered. This project does not address poor manufacturing and development practices in the cyber supply chain. Additionally, it is important to note that components that are genuine and unaltered may still include defects, such as those introduced during design and implementation phases.

Figure 1-1 Supply Chain Risk



To support the stated goals above, this project will leverage verifiable and authentic artifacts that manufacturers produce during the manufacturing and integration process that can support C-SCRM. This may include manufacturer declarations of platform attributes (e.g., serial number, list of hardware components) and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself. For example, these declarations of attributes and measurements could be cryptographically linked to a strong device identity, such as those associated with the Trusted Platform Module (TPM) or Device Identifier Composition Engine. This project will examine a range of different technologies and techniques for establishing device identity and characterizing components as artifacts. Understanding how these technologies and techniques can be combined and leveraged to meet the security objectives of this project will be an important outcome for this project.

In addition, this project will demonstrate how to inspect computing devices to verify that the components in a delivered (or in-use) computing device match the attributes and measurements declared by the manufacturer. Many OEMs have an existing process available for customers to verify the computing devices and components they receive. This project leverages those existing processes and information, in developing a customer-focused practice guide. While the end solution may involve some manual processes, one goal of the project will be to make it as automated and simple as reasonably possible, avoiding human error and leveraging activities many organizations already use when accepting the delivery of a computing device and throughout the operational life cycle of the device.

The National Institute of Standards and Technology (NIST) has an ongoing Roots of Trust project and has produced several publications that describe stronger security assurances, such as highly reliable hardware, firmware, and software components. In particular, NIST has published Special Publication (SP) 800-147 BIOS Protection Guidelines and SP 800-147B *BIOS Protection Guidelines* *for Servers.* NIST is developing SP 800-155 *BIOS Integrity Measurement Guidelines,* which is currently available in draft form. This NCCoE project will demonstrate concepts documented in these publications and result in a publicly available NIST Cybersecurity Practice Guide. A practice guide is a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Scope

The scope of the project is limited to manufacturing and OEM processes that protect against counterfeits, tampering, and insertion of unexpected software and hardware, and the corresponding customer processes that verify that client and server computing devices and components have not been tampered with or otherwise modified. Manufacturing processes that cannot be verified by the customer are explicitly out of scope.

The primary focus is verification of the single transaction between an OEM and a customer. However, the project seeks to provide a method or framework that could potentially be scaled out to verify the provenance, identity, or configurations of many types of components and computing devices throughout their life cycle, regardless of the number of entities involved.

In addition, the scope of the project is limited to verifying attributes that are currently available from one or more OEMs. The project does not address the usefulness of those attributes in addressing specific policy or contractual obligations or best-practice guidance, nor will it produce policy or best-practice recommendations. Rather, it will only provide an example means for verifying attributes that provide assurance as to the identity and integrity of the computing device and its components leveraging automated technical mechanisms.

In this project, a combination of commercial and open source tools are used to:

- establish a strong device identity to support binding artifacts to a specific device
- cryptographically bind devices and their manufacturers to the delivery of a given computer system
- establish assurance for multi-vendor production in which components are embedded at various stages
- provide an acceptance test capability for the recipient organization of the computer system that validates source and integrity of assembled components
- detect unexpected component (firmware) swaps or tampering during the life cycle of the computing device in an operational environment

These activities will augment, not replace, the capabilities of existing acceptance testing tools, asset management systems, and configuration management systems.

Challenges

Verifiable artifacts associated with the computing devices in this project require components that can successfully ingest, interrogate, and validate these data objects. Ideally, the supporting architecture components natively support the artifacts associated with the computing devices. However, additional helper scripts/code may be required to achieve the security characteristics documented here.

Further, heterogeneity in computing devices during the manufacturing process and the drift in configurations once fielded may create challenges for components in the final example implementations. Two illustrations of complications include:

- A computing device may opt to declare fine-grained hardware attributes and measurements in its verifiable artifact. As the number of attributes and measurements increases, the complexity in management also may increase.
- Over the course of a device's life cycle, the configuration will change; hardware may be replaced or firmware updated. These modifications increase the complexity of tracking valid and authorized configuration changes.

Background

Product integrity and the ability to distinguish trustworthy products is a critical foundation of C-SCRM. Authoritative information regarding the provenance and integrity of the components provides a strong basis for trust in a computing device.

Security is a life-cycle issue rather than a discrete state, but most organizations' security processes consider only the visible state of the system. As a general rule, security processes begin after blind acceptance of the delivered product. By incorporating hardware roots of trust into the acquisition and life-cycle management processes, organizations could achieve better visibility into supply chain attacks and detect advanced persistent threats and other advanced attacks. Hardware roots of trust are the foundation upon which the computing system's trust model is built. By leveraging hardware roots of trust as a computing device transverses the supply chain, we can maintain trust in the computing device and throughout the operational life cycle of the device.

Further, unauthorized modification of a product's component firmware by unexpected software constitutes a significant threat because of the potential unique and privileged position of internal components within modern computing architectures. Unexpected modification of components could be part of a sophisticated, targeted attack on an organization—either a permanent denial of service or a persistent malware presence [2]. A measured launch environment (sometimes called measured boot), which measures the identity of components in a device's boot sequence against known good values, and verifiable artifacts from trusted sources are two of the core technologies this project will use to address these threats.

Standards and Best Practices

Hardware roots of trust represent one technique that can thwart these types of attacks to the supply chain. However, OEMs may use different approaches to implement a hardware-roots-of-trust solution because of hardware constraints or other business reasons. The NCCoE encourages OEMs to use standards-based capabilities when implementing hardware roots of trust in devices, to increase the adoption of these technologies by organizations. The remainder of this section discusses one standards-based method designed to provide verifiable artifacts that can be consumed and validated by supporting systems that organizations may already have deployed within their cyber infrastructure. This represents only one technological sample approach for achieving the desired outcome of the project, and this does not imply it is the only way of meeting the objectives of this project.

Trusted Computing Group

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open, vendor-neutral, global industry standards, supportive of a hardware-based roots of trust, for interoperable trusted computing platforms. The TCG developed and maintains the Trusted Platform Module 2.0 specification, which defines a cryptographic microprocessor designed to secure hardware by integrating cryptographic keys and services [3]. The TPM functions as a roots of trust for storage, measurement, and reporting. TPMs are currently included in many computing devices.

This project could apply this foundational technology to address the challenge of operational security by verifying the provenance of delivered systems from the time it leaves the manufacturer until it is introduced in the organization's operational environment. The TPM can be leveraged to measure and validate the state of the system, including:

- binding attributes about the computing device to a strong, cryptographic device identity held by the TPM
- supporting measurement and attestation capabilities that allow an organization to inspect and verify device components and comparing them to those found in the platform attribute credential and OEM-provided reference measurements

Alternative Approaches

Other techniques are available to achieve the same outcome. For example, mobile device manufacturers Apple (iOS) and Google (Android) have documented mechanisms to support a measured launch environment. Apple devices will fail to boot or fail to allow device activation if unauthorized modifications are detected as described in the iOS Security Guide. Android devices support a Verified Boot capability that performs cryptographic checks of the integrity of the system partition [4]. This device-state information can be communicated to an Enterprise Mobility Management system, where a remediation action can be performed if positive device measurements are not satisfied. Android also supports a hardware-backed key attestation to provide proof of its hardware identifiers, such as serial number or International Mobile Equipment Identity [5].

2 SCENARIOS

This project will demonstrate the creation of manufacturing artifacts, verification of components during device acceptance testing, and verification of device state during use of personal computing devices with hardware roots of trust.

Scenario 1: Creation of Verifiable Platform Artifacts

An OEM, value-added reseller, or other authoritative source creates a verifiable artifact that binds reference platform attributes to the identity of the computing device. The platform attributes in this artifact, such as the serial number and other properties, are used by the purchasing organization during acceptance and provisioning of the computing device.

Scenario 2: Verification of Components During Acceptance Testing

In this scenario, an Information Technology (IT) Administrator receives a computing device through non-verifiable channels (e.g., off the shelf at a retailer) and wishes to confirm provenance and authenticity and establish authoritative asset inventory as part of an asset management program. The IT Administrator performs the following steps:

1. As part of the acceptance testing process, the IT Administrator uses tools to extract or obtain the verifiable platform artifact associated with the computing device.
2. This IT Administrator verifies the provenance of the device’s hardware components by validating the source and authenticity of the artifact.

3. The IT Administrator validates the verifiable artifact by interrogating the device to obtain platform attributes that can be compared against those listed in the artifact.
4. The computing device is provisioned into the physical asset management system and is associated with a unique enterprise identifier.

Scenario 3: Verification of Components During Use

In this scenario, the computing device has been accepted by the organization (Scenario 2) and has been provisioned for the end user.

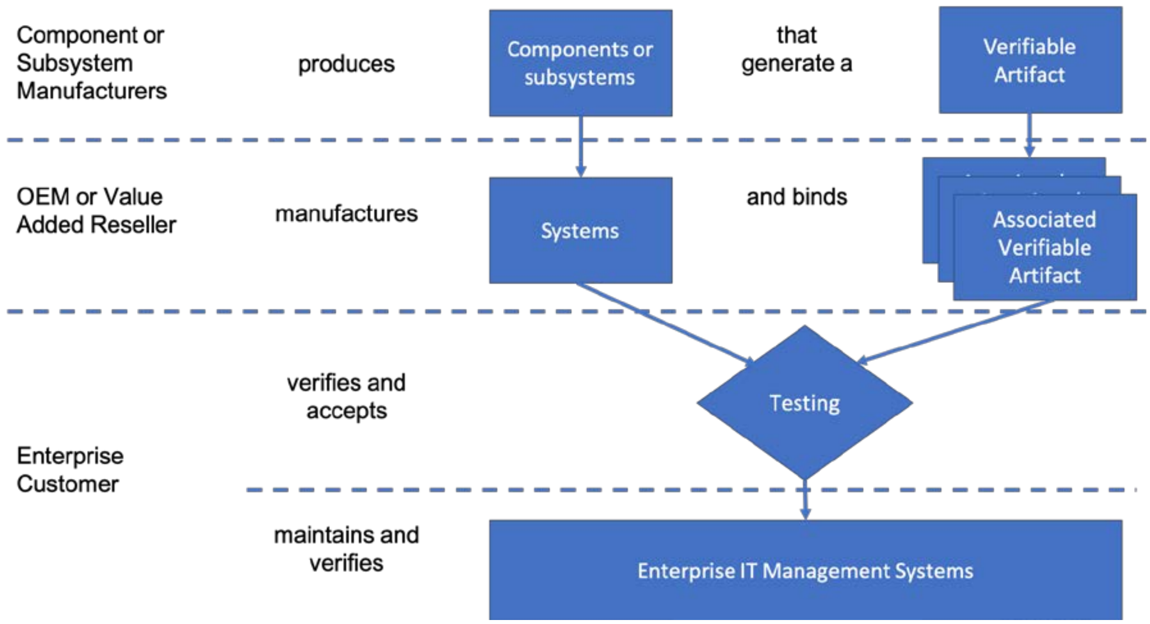
1. The end user takes ownership of the computing device from the IT department, performing daily work tasks within the scope of normal duties.
2. The computing device creates a report that attests to the platform attributes, such as device identity, hardware components, and firmware measurements that can be identified by interrogating the platform.
3. The attestation is consumed and validated by existing configuration management systems used by the IT organization as part of a continuous monitoring program.
4. The measured state of the device is maintained and updated as the authorized components of the device are being maintained and associated firmware updated throughout the operational life cycle of the device.
5. Optionally, the IT Administrator takes remediation action against the computing device if it is deemed out of compliance. For example, the computing device could be restricted from certain corporate network resources.

3 HIGH-LEVEL ARCHITECTURE

Figure 3-1 Architecture shows a notional, high-level architecture for an organization incorporating C-SCRM technologies into an existing infrastructure. A descriptive component list follows.

The architecture depicts a manufacturer that creates a hardware-root-of-trust-backed verifiable artifact associated with a computing device. The verifiable artifacts are then associated with existing asset and configuration management systems during the provisioning process. Finally, an inspection component measures and reports on hardware attributes and firmware measurements during acceptance testing and operational use.

Figure 3-1 Notional Architecture



Component List

The high-level architecture will include the following components:

- **Computing devices** – client and server devices associated with verifiable artifacts
- **Enterprise IT Management Systems**
    - **Asset discovery and management systems** – components that help organizations ensure that critical assets are uniquely identified using known identifiers and device attributes [6]. This component could include discovery tools that identify endpoints and interrogate the platform for device attributes.
    - **Configuration management systems** – components that enforce corporate governance and policies through actions such as applying software patches and updates, removing blacklisted software, and automatically updating configurations [7]. These components may also assist in the management and remediation of firmware vulnerabilities.
    - **Security information and event management tools** – components that provide real-time analysis of alerts and notifications generated by organizational information systems [8].
- **Certificate Authority** (not pictured) – the trusted entity that issues and revokes public key certificates [9].

4 Relevant Standards, Guidelines, and Open Source Projects

The references, standards, and guidelines that are applicable to this project are listed below.

- National Institute of Standards and Technology, *ITL Bulletin October 2014, Release of NIST Special Publication 800-147B, BIOS Protection Guidelines for Servers*
- National Institute of Standards and Technology, Special Publication 800-147B *BIOS Protection Guidelines for Servers*
- National Institute of Standards and Technology, *ITL Bulletin June 2011, Guidelines for Protecting Basic Input/Output System (BIOS) Firmware*
- National Institute of Standards and Technology, Special Publication 800-147 *BIOS Protection Guidelines*
- National Institute of Standards and Technology, Special Publication 800-155 *(DRAFT) BIOS Integrity Measurement Guidelines*
- National Institute of Standards and Technology, Special Publication 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- Trusted Computing Group, *TPM 2.0 Library Specification*
- Open Attestation Project, *GitHub Repository*
- NSA Cybersecurity, *Host Integrity at Runtime and Start-up (HIRS) Project*

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge of operational security to the applicable standards and best practices described in Special Publication 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 5-1 Security Control Mapping

Cybersecurity Framework (CSF) v1.1			
Function	**Category**	**Subcategory**	**SP800-53R4**
Identify (ID)	Supply Chain Risk Management (ID.SC)	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations, to confirm they are meeting their contractual obligations.	AU-2, AU-6, SA-19
	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.	CM-8, AU-10

Cybersecurity Framework (CSF) v1.1			
Function	**Category**	**Subcategory**	**SP800-53R4**
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	IA-4
	Data Security (PR.DS)	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7, SA-10, SA-18
		PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity	
Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	PE-20

317 # APPENDIX A REFERENCES

[1] National Institute of Standards and Technology, [Online]. Available: https://csrc.nist.gov/projects/supply-chain-risk-management/. [Accessed 23 April 2019].

[2] D. Cooper, W. Polk, A. Regenscheid and M. Souppaya, *Special Publication 800-147 BIOS Protection Guidelines,* National Institute of Standards and Technology, 2011.

[3] Trusted Computing Group, "About TCG," [Online]. Available: https://trustedcomputinggroup.org/about. [Accessed 23 April 2019].

[4] The MITRE Corporation, "Modify System Partition," [Online]. Available: https://attack.mitre.org/techniques/T1400/. [Accessed 23 April 2019].

[5] Android, "Key and ID Attestation," [Online]. Available: https://source.android.com/security/keystore/attestation. [Accessed 23 April 2019].

[6] A. Johnson, K. Dempsey, R. Ross, S. Gupta, D. Bailey, *Special Publication 800-128 Guide for Security-Focused Configuration Management of Information Systems*, National Institute of Standards and Technology, 2011.

[7] M. Stone, L. Kauffman, C. Irrechukwu, H. Perper and D. Wynne, "NIST SP 1800-5B IT Asset Management," National Institute of Standards and Technology, 2018.

[8] National Institute of Standards and Technology, "SI-4 Information System Monitoring," [Online]. Available: https://nvd.nist.gov/800-53/Rev4/control/SI-4. [Accessed 23 Aprfil 2019].

[9] National Institute of Standards and Technology, "Computer Security Resource Center," [Online]. Available: https://csrc.nist.gov/glossary/term/Certificate-Authority. [Accessed 1 05 2019].

APPENDIX B ACRONYMS AND ABBREVIATIONS

C-SCRM	Cyber Supply Chain Risk Management
DE	Detect
ID	Identify
IT	Information Technology
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PR	Protect
SP	Special Publication
TCG	Trusted Computing Group
TPM	Trusted Platform Module