PREVIEW

DraftSUMMARY

# TCG Guidance for Securing Network Equipment

# Preview Synopsis

**Version 1.0**
**Revision 3**
**Jun 6, 2016**

Contact: admin@trustedcomputinggroup.org

This synopsis provides a public preview summary of a TCG specification currently under development. All contents are subject to change and formal approval by TCG.

TCG

**TCG Preview**

# Table of Contents

# 1. Executive Summary

The world is interconnected by networks, and those networks have become critical to the operation of a broad range of devices and services, ranging from the World Wide Web to industrial robots and the electric power grid.

Preserving the integrity and security of equipment such as routers, switches, and firewalls used to create the network infrastructure is essential to network reliability, as well as maintaining integrity and privacy of the many kinds of data that transit networks. As increasingly sophisticated attacks[1] are launched on network equipment, strong protection mechanisms for network equipment, both on the device and service level, is required. Trusted Computing is a key security technology to keep networking services free of disruption and to allow for improvements in maintenance processes.

Yet little information is available on how Trusted Computing should be used to secure network equipment and thus the networks that depend on this equipment. TCG’s mission is the creation of security specifications and the promotion of best practices for various application domains. The TCG Network Equipment working group has the expertise to provide good advice in the area of communication devices and the application of Trusted Computing in infrastructure scenarios.

[1] For example, see http://www.legbacore.com/Research_files/HowManyMillionBIOSesWouldYouLikeToInfect_Whitepaper_v1.pdf

The Reference document *TCG Guidance for Securing Network Equipment* provides details of use-cases and implementation approaches to solve these problems, designed to help system designers and network architects get the best security possible from this powerful technology.

## 1.1 Network Equipment Reference Model

Figure 1 shows a simplified reference model for Network Equipment depicting the stakeholder interactions common in communication networks. Special attention to the interconnections between administrative domains and the protection of end user equipment is important in securing networking equipment.

Customer Premise Equipment (CPE) or Residential Gateways are often positioned between administrative domains, and may require special attention for management of access and identity. CPE devices are often under the direct physical access of the respective customers, so secure identities and authentic software are essential security features offered by Trusted Computing.

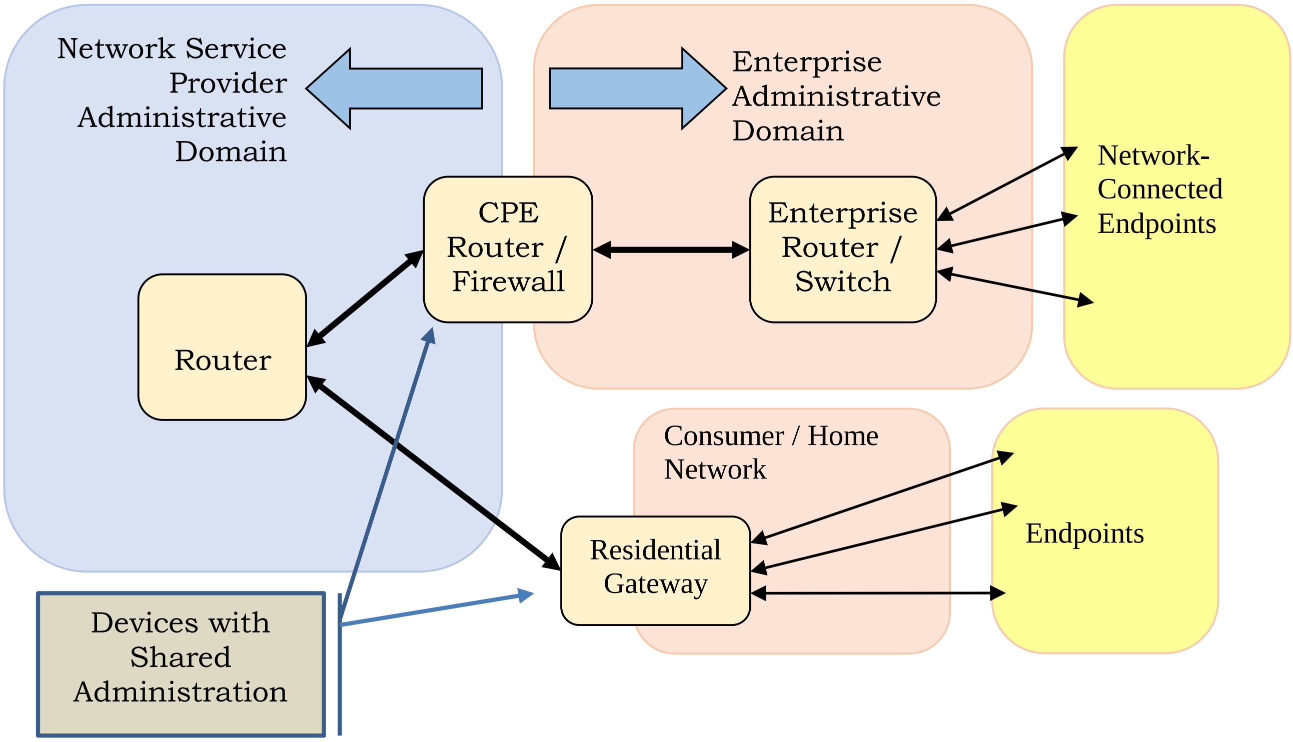
Network Service Provider Administrative Domain
Enterprise Administrative Domain
CPE Router / Firewall
Enterprise Router / Switch
Network-Connected Endpoints
Router
Consumer / Home Network
Residential Gateway
Endpoints
Devices with Shared Administration

**Figure 1: Simplified Network Reference Model**

Traffic transiting from one endpoint to another through networks will often pass through many administrative domains, resulting in a complex trust model. Mechanisms developed by TCG for secure handoff of ownership from one domain to another provide novel security enhancements for the communication industry enhancing the overall robustness of the infrastructure against attackers, and also enabling the detection of common administrative issues.

Further, network administrators normally will not have direct physical connectivity to the device, resulting in a need for authenticated remote access to carry out the management functions. Trusted Computing allows for hardware protected device identities whose security it rooted in a certified design, allowing confident use of these identities in remote access and inventory applications.

## 1.2 Key Differences between Network Equipment and PC Applications

Networking Equipment almost always contains a general-purpose computing environment to configure and manage the device. But there are distinct differences between Networking Equipment and the common PC client and server applications:

- While Network Equipment may be highly modular, it is often shipped as a closed embedded system, integrating hardware and software.
- The chain of security typically does not stop when the OS boots; what matters is security of the networking function that's provided by the unit as a whole
- Network Equipment typically must boot and operate without manual intervention.
- While Network Equipment has an important role in protecting user privacy, the equipment itself typically should not have an ability to hide or mask its own identity.
- Network Equipment often has a long life cycle, and must stay operational in the network for many years.

# 2. Use Cases

TCG technology has a number of applications in Networking Equipment, some of which are common to all computing devices, but others of which are unique to the networking application.

The *TCG Guidance for Securing Network Equipment* document examines each of these use-cases and provides non-normative advice on how existing TCG technology can be put to use.

## 2.1 Device Identity

Providing strong remotely-accessible device identity for each piece of network equipment is a prerequisite for most use cases related to securing network equipment.

Following the IEEE *Standard for Local and Metropolitan Networks – Secure Device Identity*, IEEE Std 802.1AR, the *TCG Guidance for Securing Network Equipment* distinguishes two kinds of device identity: Manufacturer identity and Owner identity.

- The Manufacturer identity for a particular device is established, configured and managed by the Device Manufacturer, although it can also be used (e.g., verified) by the device owner.
- The Owner identity for a device is established by the device Administrator and is generally used only by the Administrator.

Manufacturer identity is generally unique across all products from that manufacturer (e.g., a model number plus a serial number) while Owner identity will be unique only within the Administrator's facility (e.g., an asset number).

The TCG Network Equipment device identity guidance is aligned with Initial and Local Device ID, as specified in IEEE 802.1AR.

Cryptographic device identity has several applications in Networking Equipment

**Identity for Network Access** - Telecommunications companies, cloud and data center operators, hospitals, chemical plants, manufacturing facilities are all examples where the network needs to be tightly controlled, and mechanisms used to ensure that only authorized equipment can be connected. This can be achieved by using cryptographic device identification, with keys stored in tamper-resistant TPMs.

**OEM Device Identity and Counterfeit Protection** - Both network equipment owners and device manufacturers (OEM's) need to verify the authenticity of network equipment, determining whether it is "counterfeit" (made by an unauthorized party or in an unauthorized manner) or "authentic" (made by authorized parties in an authorized manner). Certificates signed by the manufacturer and rooted in a TPM can provide such assurance.

**Secure Autoconfiguration -** There are many cases where a networking device may be shipped with no unique configuration, but must be configured before it can be used with a network. "Autoconfiguration" (also known as Zero Touch Configuration) is an increasingly popular mechanism where the device can identify itself reliably, and communicate through the network, to obtain the configuration information that would specify policy for operational use. As an example, downloaded configuration might enable access to a corporate VPN, or might authorize access to restricted content.

**Remote Device Management** - Network Equipment Owners with a large number of devices often want to manage those devices remotely, including the ability to monitor devices and reconfigure them dynamically. Remote management and reconfiguration is especially important in modern, flexible computing environments that implement Software-Defined Networking (SDN) or Network Function Virtualization (NFV). Reliable identification of each device is critical to remote management.

## 2.2 Securing Secrets

Network equipment often contains secrets such as traffic logs or cryptographic keys (e.g., shared secrets, passwords, VPN keys, SSL keys, and stored data encryption keys). Disclosure of these secrets could result in disclosure of confidential network traffic and privacy-sensitive information or even enable malicious tampering with the network. Network operators (especially Service Providers and Enterprises) must protect these secrets against disclosure to keep their networks secure and reliable and also to meet regulatory or customer requirements for confidentiality and privacy, and can use a variety of TPM mechanisms to ensure that private information stays that way.

## 2.3 Protection of Configuration Data

Network Equipment usually requires configuration, often involving many parameters stored in a variety of files. The equipment Owner may wish to retain control over changes to configuration files on the equipment, with the goal of ensuring that unauthorized configuration changes don't compromise their network. TCG technology can enable an equipment owner to ensure that configuration data can only be applied to the device it's meant for, and can't be snooped along the way.

## 2.4 Licensed Feature Authorization on a Network Device

Device Manufacturers often provide a common baseline version of a product, but want to be able to authorize specific features for individual customers, perhaps as a value-add optional feature. Locking feature authorization to a cryptographic device ID offers a mechanism to ensure that authorization for features on one device can't be transferred to another.

## 2.5 Software Inventory

Most Network devices rely on complex embedded software to enable basic features as well as to enforce security policies. This software is often updated on devices already in the field, using releases and patches usually supplied by the device manufacturer, leaving Network Administrators with the task of keeping track of which devices have been updated to what revision level, sometimes tracking many independent components on a single complex device

Mechanisms can be implemented to allow the Administrator to query devices to find which revision level of what components are installed on each network device in their network.

## 2.6 Attestation of Integrity for Network Devices ("Health Check")

One extension to remote device management enabled by TCG technology allows the management station to monitor the authenticity of software versions and configurations running on each device. This allows owners and auditors to detect deviation from approved software and firmware versions and configurations, potentially identifying infected devices.

## 2.7 Inventory of Composite Devices

Many network devices are composed of one or more control or management units plus optional components like line processing units, feature processing units and other kinds of Field Replaceable Units (FRUs), each of which might contain its own autonomous computing environment. The interaction and tasks of the components are vendor specific, but the behavior of the network device is based upon the composite behavior of individual components. The security posture of the network device is therefore only accurately represented by a composite measure that includes the posture of sub-components.

Many network devices allow FRUs to be replaced without triggering a complete system restart (often called 'hot swap'); for these devices, system-level reboots may be very rare, and the system's security posture must be re-evaluated every time an individual unit is inserted or removed from the system. The *TCG Guidance for Securing Network Equipment* outlines procedures for determining the security posture of these complex machines.

## 2.8 Integrity-Protected Logs

Various processes in the day-to-day operation of network equipment are based on information gathered from the system status of servers, routers and sensors. SACM, SIEM or even legal interception are based on state information of various components. Tampering with this information, mostly existent as log files, can impact the security protection (e.g. by suppressing intrusion-detection (IDS) data) or impact the integrity of information delivered by the legal interception interface.

Integrity-protected log files can be used by the management or external entities by providing information proving the authenticity and integrity of the file.

## 2.9 Entropy Generation

Many networking protocols such as SSH and IPsec have a need for cryptographic-quality random numbers, to avoid the generation of predictable ephemeral session keys.

In addition, the TCP stack for Network Equipment should use good-quality randomness for the TCP window starting point as well as in the selection of ephemeral ports. These help to mitigate SYN and RST attacks against the device.

Most TPMs contain a source of cryptographic entropy, which can be used to improve the security of the many mechanisms that depend on random numbers.

## 2.10 Deprovisioning

Networking Devices often contain information that's considered sensitive by the Administrator, such as customer configurations or routing policies. Once the device is taken out of service, this information must be reliably destroyed.

Confidential information can include TPM keys themselves, or information encrypted by TPM keys. The TPM mechanisms for deleting keys can ensure that the confidential information will become inaccessible.

# 3. Conclusion

Attacks on network equipment are becoming more frequent and more sophisticated. With the growing importance of networking in our lives, especially as IoT becomes commonplace, the security of network equipment is paramount. While securing network equipment is a complex problem, it is clear that Trusted Computing is essential to provide a firm foundation on which higher-layer security mechanisms can be built.

The complete *TCG Guidance for Securing Network Equipment* provides detailed implementation suggestions for all of these use cases, plus related background material. The document is currently available to TCG members for review.

Readers interested in this topic (especially network equipment providers and telecommunications carriers) are encouraged to join TCG to help shape this guidance.

*TCG Guidance for Securing Network Equipment* will be published on the TCG public web site (https://www.trustedcomputinggroup.org/) once member review is complete.

Please contact admin@trustedcomputinggroup.org for more information on TCG membership, or the Working Group, or to offer comments.