JANUARY 2018

ARCHITECT'S GUIDE

FOR SECURING NETWORK EQUIPMENT

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

Copyright© 2018 Trusted Computing Group | All Rights Reserved

ARCHITECT'S GUIDE FOR SECURING NETWORK EQUIPMENT

As part of the critical infrastructure of an enterprise, network equipment *(Side Bar 1)* is subject to the same types of attacks and threats as PCs, servers and the network itself.

THESE THREATS INCLUDE:

1. UNAUTHORIZED DEVICES THAT CAN GAIN ACCESS TO NETWORKED DATA
2. UNAUTHORIZED CODE THAT CAN INTERFERE WITH SAFE OPERATION
3. FIRMWARE IMPLANTS THAT CAN RENDER ATTACKS INVISIBLE AND UNREMOVABLE

Preserving the integrity and security of network equipment is essential to maintaining customer privacy and network reliability. Trusted Computing solutions can be used to provide these requirements. This Architect's Guide makes the case for addressing network security and provides some initial guidance from ongoing efforts in this area.

AWARENESS PRIOR TO ACTION

Experts in providing trust to all aspects of an enterprise have found that many designers are not concerned about protecting the low-level, embedded portions of their infrastructure. For example, those people who are interested specifically in network security are extremely concerned about almost all aspects that involve anti-viruses and software but may ignore or forget about risks to the hardware and firmware used in the routers, firewalls, and switches that make up the network—the other attack points in the enterprise. While the bulk of the attack mechanisms today involve stolen passwords, social engineering and similar techniques, a router can also be subverted to make a leak or system breach occur.

It is important to distinguish network security provided by items such as firewalls, VPNs, MPLS domains, access lists, intrusion detection, network access controls, Radius, DMZs and a host of other functions that prevent inappropriate access to networked resources, from Secure Network Equipment. Secure Network Equipment ensures that the network gear itself is doing what it is supposed to be doing, and is resistant to being hacked, since the devices that the network security experts depend on to do their job are themselves vulnerable to boot attacks and other kinds of attacks.

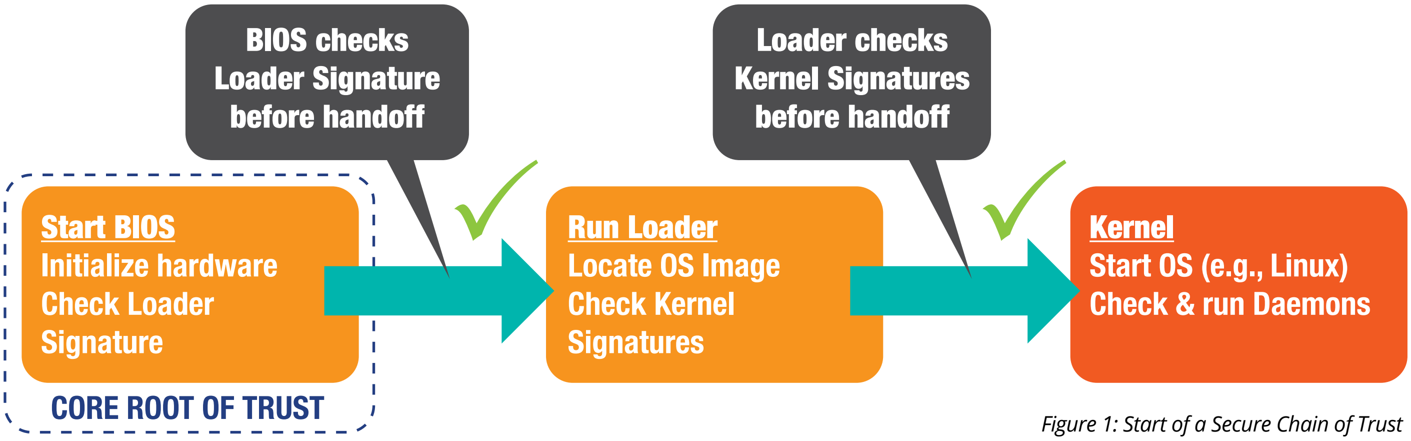

Figure 1: Start of a Secure Chain of Trust

With BIOS trust established, the software that runs routers and other network connected equipment can be secured, allowing that gear to reliably enforce security policies protecting the rest of the network. Figure 2 shows a simplified reference model for network equipment. In this model, customer premise equipment (CPE) or residential gateways are often positioned between administrative domains, and may require special attention for management of access and identity.

Copyright© 2018 Trusted Computing Group | All Rights Reserved

When all the aspects of infrastructure security are analyzed, the shortcomings become more apparent. Network equipment must be on the radar of network planners and of those concerned with overall enterprise security, to avoid being the weak point for future sophisticated, or even not so sophisticated, attacks. While it is not a dominant concern today, it should be part of the total security approach, since hackers' interest and knowledge in this area could accelerate rapidly once a few have successfully breached a corporation's existing defenses. *(See Side Bar 2.)*

With these considerations in mind, the Trusted Computing Group (TCG), which has a long history of seeking out and addressing security issues of all types, has several ongoing efforts to provide increased security and trust for network equipment.

STEPS TO TAKE FOR IMPROVED SECURITY OF NETWORK DEVICES

Most network devices use an embedded processor of some sort to configure and control the device, making software a critical element in correct operation of the device.   Each time the device is powered on, several phases may be executed to initialize the device, each of which must check the integrity of the next for trustworthy operation, forming a 'chain of trust.'

The first link in the chain of trust, boot firmware often referred to as a BIOS, is critical to prevention of persistent firmware attacks. While TCG does not specify how to secure a BIOS, there are two simple steps to ensure trust at this level:

1. Make sure that the OS cannot modify firmware. (This usually needs some kind of hardware help to lock boot flash memory.)

2. Make sure that the BIOS (or U-Boot or other hardware initiation process) requires a valid signature on a new image before it will be accepted as an update.

Using Secure Boot, a security standard developed by experts in the PC industry or other processes such as Verified Boot, can ensure that the device boots an unmodified, authorized image. Specifically, secure boot is achieved by providing an unbroken "chain of trust" from the first instruction executed after Reset through to the OS prompt. Figure 1 shows the start of a secure chain of trust [1].

> *"The chain of security typically does not stop when the OS boots but continues up to application code; what matters is security of the networking function provided by the unit as a whole"*

For those who are not convinced about the reality and impact of failures in network security, two recently documented milestone instances are worth noting.

The first example is the Ukraine power system attack that occurred on December 23, 2015 - the first confirmed hack to take down a power grid [5]. The process involved coordinated attacks on controllers, embedded gear and even the call center. Some networking equipment was permanently disabled as well.

Prior to the day of the attack, the attackers obtained credentials, some of them for the virtual private networks (VPNs) the grid workers used to remotely log in to the supervisory control and data acquisition (SCADA) network in the power plant. The attack took about 30 substations offline, leaving more than 230,000 residents and even system operators in the dark.

The second example is the Dyn cyberattack that occurred on October 21, 2016 [6]. In this incident, hundreds of thousands of connected Internet of Things (IoT) devices (including home routers, printers, Internet protocol (IP) cameras and more) were hijacked and added to a Mirai botnet to mount a distributed denial-of-service (DDoS) attack on Dyn's Domain Name System (DNS) servers. The attack resulted in several hours downtime in large areas of North America and Europe

Copyright© 2018 Trusted Computing Group | All Rights Reserved

CONSIDERING THE SYSTEM AS A WHOLE

While network equipment almost always contains a general-purpose computing environment to configure and manage the device, distinct differences exist between networking equipment and common PC client and server applications. For example:

- Highly modular network equipment is usually shipped as an embedded system with integrated hardware and software
- The chain of security typically does not stop when the OS boots but continues up to application code; what matters is security of the networking function provided by the unit as a whole
- Network equipment typically boots and operates without human intervention so no owner password can be required at boot time

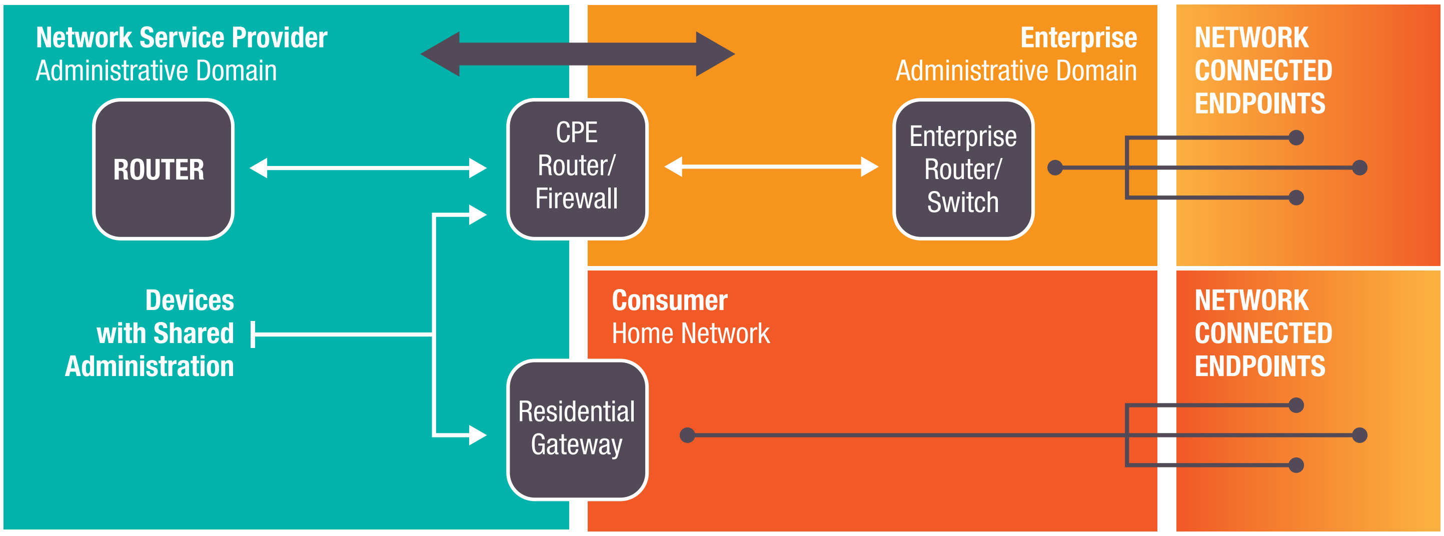

Figure 2: Simplified Network Reference Model

TCG GUIDANCE FOR SECURING NETWORK EQUIPMENT

To address these differences, TCG has developed the TCG Guidance for Securing Network Equipment [2] to provide recommendations and detailed advice on how TCG standards should be used to secure network equipment. TCG Guidance for Securing Network Equipment Preview Synopsis [3] provides an executive summary of the use cases, including:

- Device Identity
- Secure Zero Touch Provisioning
- Securing Secrets
- Protection of Configuration Data
- Remote Device Management
- Software Inventory
- Attestation of Boot Integrity for Network Devices (“Health Check”)
- Integrity-Protected Logs
- Entropy Generation
- Deprovisioning

These use cases address common network functions that require trusted protection, including the destruction of sensitive trust information once the equipment is taken out of service.

Copyright© 2018 Trusted Computing Group | All Rights Reserved

In support of many of these use cases, TCG's Trusted Platform Module (TPM) provides a hardware-based means to provide important security improvements for many products/systems, including network equipment.

For network equipment, device identity can be established using unique per-device identifiers (DevID) defined in the IEEE 802.1AR - 2009, "Standard for Local and Metropolitan Area Networks: Secure Device Identity [4]." Using its Public Key Cryptography capability, the TPM can assert the equipment's identity and then prove that it has possession of a difficult-to-steal private key, stored inside the TPM.

The TPM also contains a cryptographic-quality Random Number Generator (RNG), a critical element for generating cryptographic keys that can't easily be broken, used in protocols such as SSL or IPsec.

In addition to TCG, there are a wide range of topics in this area being discussed at Internet Engineering Task Force (IETF) and other concerned organizations. As awareness and interest in this topic grows, expect to see more considerations and recommendations being offered in conferences, magazines and by various suppliers.

FOR ADDITIONAL INFORMATION

Interested third party developers looking for additional resources should refer frequently to TCG's Network Equipment website page since information will be continuously added as it is available. Other information sources include:

TCG Guidance for Securing Network Equipment, https://trustedcomputinggroup.org/tcg-guidance-securing-network-equipment/

https://trustedcomputinggroup.org/establishing-network-equipment-security/

https://trustedcomputinggroup.org/wp-content/uploads/Establishing-Network-Equipment-Security.pdf

http://trustedcomputinggroup.org/work-groups/embedded-systems/

Infineon Networking and ICT security: https://www.infineon.com/iot-security-ebrochure/en/ict.html

REFERENCES

[1] TCG presentation, "Securing Network Equipment with Trust and Integrity," https://trustedcomputinggroup.org/wp-content/uploads/TCG-on-Securing-Network-Equipment-v2.pdf

[2] "TCG Guidance for Securing Network Equipment," https://trustedcomputinggroup.org/tcg-guidance-securing-network-equipment/

[3] "TCG Guidance for Securing Network Equipment Preview Synopsis," https://www.trustedcomputinggroup.org/wp-content/uploads/NetEq-Synopsis_1_0r3.pdf

[4] IEEE 802.1AR – 2009, "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity," https://standards.ieee.org/findstds/standard/802.1AR-2009.html

[5] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[6] 2016 Dyn cyberattack, https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

Copyright© 2018 Trusted Computing Group | All Rights Reserved