Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktop Computers

Executive summary

Enterprise-grade servers, laptops, and desktops should be procured with a robust set of security artifacts, configurations, and capabilities. The security artifacts enable several risk mitigation techniques that should be used with an automated Acceptance Test process. This guidance is intended to:

- Encourage the implementation of enterprise Acceptance Testing.
- Inform procurement professionals what provisions will be needed to support Acceptance Testing.
- Inform original equipment manufacturers (OEMs) on what artifacts and capabilities will be needed to support an Acceptance Test.

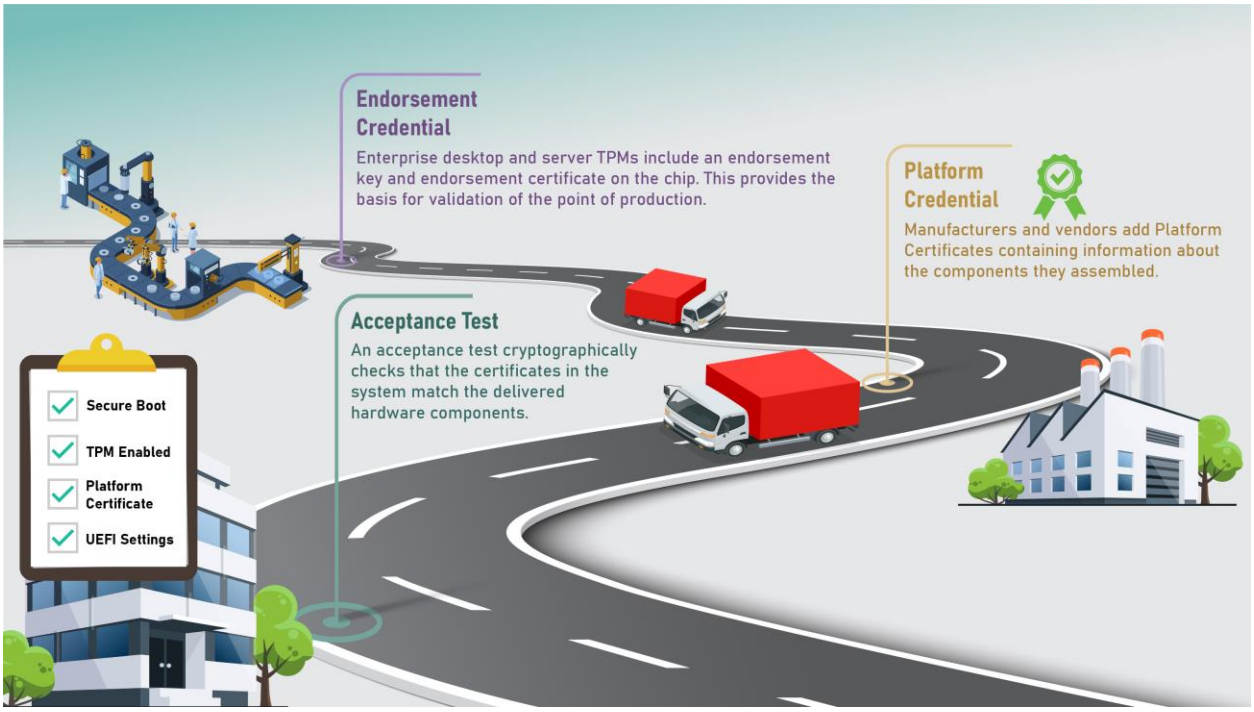

Figure: Acceptance Testing of procured devices.

Whenever an organization receives a server, laptop, or desktop computer, its receiving department should perform an automated Acceptance Test to check that the device

has:

- Secure Boot enabled,
- A Trusted Platform Module (TPM) that is enabled and activated, and
- A valid Platform Certificate that matches the components in the device.

The acceptance process should also configure recommended Unified Extensible Firmware Interface (UEFI) settings. Any devices that fail these tests should be considered defective and returned.

Introduction

The guidance in this cybersecurity information sheet (CSI) assumes that organizations procuring the equipment have already implemented a Supply Chain Risk Management (SCRM) process in accordance with NIST SP 800-161 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations". [1] This guidance is intended to augment those processes with suggested procurement guidance and risk mitigation processes to ensure that enterprise-grade servers, laptops, and desktops are procured with a robust set of security artifacts, configurations, and capabilities.

Enable Secure Boot

All enterprise-grade servers, laptops, and desktop computers contain firmware and firmware-level applications that run outside the purview of the operating system. Almost all of them implement the Unified Extensible Firmware Interface (UEFI) [2] as defined by the UEFI Forum. The UEFI Secure Boot process implements guidance provided by NIST SP 800-147 "BIOS Protection Guidelines" [3] or NIST SP 800-147b "BIOS Protection Guidelines for servers". [4] All UEFI-based devices should be configured with Secure Boot enabled. Enterprise procurements should specify that the manufacturer include and enable Secure Boot as part of device configuration requirements.

Enterprise security monitoring systems should check that Secure Boot is enabled on all UEFI-based devices after every device boot.

Require Trusted Platform Modules

The Trusted Platform Module (TPM), as defined by the Trusted Computing Group (TCG), is a small security coprocessor that can be a standalone component or included as part of another component, such as a microprocessor. Most enterprise-grade laptops and desktops include a TPM version 2.0 since it is required by Microsoft for Windows 8.1 or higher. For servers, the TPM is typically an add-on component that needs to be specified on the ordering manifest by administrators and procurement officials. Procurements of servers should ensure that optional TPMs are included when these devices are ordered. For DoD, DODI 8500.01 "Cybersecurity" [5] requires DoD computer assets to be purchased with a TPM.

DODI 8500.01 also calls for the National Security Agency (NSA) to provide use cases, implementation standards, and plans for DoD to leverage the functionality of the TPM.

This guidance outlines a use case for the validation of the supply chain using an artifact called the Platform Certificate as outlined in the following sections.

Require Platform Certificates

The TCG defines the Platform Certificate as a digital certificate that binds a device to a specific manufacturer, model, and serial number. [6] It also contains a list of internal components that can be considered a hardware bill of materials for the device. The manufacturer creates the certificate during the manufacturing process of a device. The Platform Certificate can be used to detect counterfeit devices, counterfeit internal components, swapped components, and unauthorized configuration changes to the device. This becomes a critical artifact used as part of an Acceptance Test that should be performed when the device arrives at an organization's receiving department.

Procurements of servers, laptops, and desktops should include requirements for the OEM to create the Platform Certificate. Its contents should meet the recommendations specified in the "TCG PC Client Platform Firmware Integrity Measurement". [7]

Platform Certificates have a Delta Platform Certificate that should be created when a value-added reseller (VAR) changes the hardware configuration of a device. For example, the Delta Platform Certificate would record any component upgrades made by the VAR. Each VAR should be required to create Delta Platform Certificates by the procurement contract.

Platform Certificates are currently available from most server, laptop, and desktop OEMs. Some OEMs provide the Platform Certificate as part of their standard offering, while others may provide it as optional item in a similar fashion to the availability of a TPM on enterprise-grade servers. Procurements should ensure that a Platform Certificate is required to be included when the device is ordered.

Establish an enterprise Acceptance Testing process

Ideally, every procured device would be tested upon delivery to an organization. NIST SP 161 section MA-3 item 1 states "the enterprise should deploy Acceptance Testing to verify that the maintenance tools of the ICT [(information and communication technology)] supply chain infrastructure are as expected." Procurement contracts for servers, laptops, and desktop computers should include a clause indicating that devices

procured are required to pass an Acceptance Test and that any devices, which fail those tests, will be considered defective and returned.

When a device is received, the enterprise's receiving department should perform an automated Acceptance Test that validates the Platform Certificate by checking its signature and matching the components it lists against the device itself. Many OEMs will provide a set of tools to perform this check. Several open-source projects (e.g., https://github.com/nsacyber/HIRS [8]) can perform this check as well.

NIST 1800-34C "Validating the Integrity of Computing Devices" is a NIST Cybersecurity Practice Guide that illustrates how to create an Acceptance Test that utilizes the TPM and performs the Platform Certificate checks. [9] Many OEMs for servers, laptops, and desktops participated in the National Cybersecurity Center of Excellence (NCCoE) project that led to the guide.

The enterprise should consider establishing one or more pilot programs to introduce an Acceptance Test before rolling it out to the entire enterprise. Testing a subset of randomly selected devices may be necessary until the testing can be completely automated. The Enterprise should also consider running the Acceptance Test on an isolated network to limit the risk of connecting a potentially compromised device to the Enterprise network. Once the roll out is complete, the Acceptance Test should test every procured device upon delivery.

Post acceptance configuration

NSA guidance for "UEFI Lockdown Quick Guidance" should be followed as a post acceptance configuration lockdown practice to set recommended UEFI configuration settings, including UEFI passwords, boot order, boot options, enabling Secure Boot, and enabling and activating the TPM. [10]

Future technology considerations

Industry is developing the following technologies that appear to be very promising and may be reflected in a future version of this guidance:

Reference Integrity Manifests

The TCG defined a PC Client Reference Integrity Manifest (RIM) that provides a set of signed firmware digests (hashes) that can be used in conjunction with TPM and UEFI

firmware to "Attest" that the firmware has booted the device into a known (trusted) state. [11] Procurements of servers, laptops, and desktops should include requirements to create a TCG PC Client RIM by the OEM. The contents of the Platform Certificate provided by the OEM should meet the recommendations specified in "TCG PC Client Platform Firmware Integrity Measurement". [7]

Cyber resiliency

The TCG is defining a set of cyber-resilient technologies compliant with SP 800-193. [12] Cyber resiliency provides a set of protection, detection, and recovery capabilities above and beyond UEFI Secure Boot. Enterprises should procure servers, laptops, and desktops with cyber-resilient capabilities, and enterprise security management systems should manage the cyber-resiliency mechanisms available in those devices.

Internal component selection

Several security protocols, such as the Security Protocols and Data Models (SPDM) protocol, [13] enable authentication, attestation, and key exchange to assist in enabling enterprise-wide infrastructure security. These protocols are likely to enable attestation of thousands of internal components, such as hard drives, memory sticks, and network cards within different computers. Procurement of servers, laptops, and desktops should include language that provides a preference for components that incorporate standardized security protocols, such as SPDM.

Only accept secure devices

Enterprises should leverage procurement contracts to require the latest security capabilities in their devices and then check that devices meet those requirements upon delivery. Any less, and the organization’s security foundation could be unreliable since the building blocks of its computing infrastructure—the servers, laptops, and desktops themselves—may not be properly secured.▪

Works cited

[1] NIST, SP 800-161 Rev. 1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,” May 2022, https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

[2] UEFI Forum, Inc, "Unified Extensible Firmware Interface (UEFI) Specification,” Release 2.10, August 2022, https://uefi.org/sites/default/files/resources/UEFI_Spec_2_10_Aug29.pdf

[3] NIST, SP 800-147 "BIOS PROTECTION GUIDELINES,” April 2011, https://csrc.nist.gov/publications/detail/sp/800-147/final

[4] NIST, SP 800-147b "BIOS PROTECTION GUIDELINES FOR SERVERS," August 2014, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-147b.pdf

[5] Department of Defense, INSTRUCTION 8500.01 "Cybersecurity," March 2014, Incorporating Change 1, Effective October 7, 2019, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

[6] Trusted Computing Group, "TCG Platform Certificate Profile," Version 1.1 Revision 19, April 2020, https://trustedcomputinggroup.org/wp-content/uploads/IWG_Platform_Certificate_Profile_v1p1_r19_pub_fixed.pdf

[7] Trusted Computing Group, "TCG PC Client Platform Firmware Integrity Measurement" https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_FIM_v1_r40_02dec2020.pdf

[8] NSA, "Host Integrity at Runtime and Startup (HIRS)," https://github.com/nsacyber/HIRS

[9] NIST, 1800-34c "Validating the Integrity of Computing Devices," June 2022, https://www.nccoe.nist.gov/publications/practice-guide/validating-integrity-computing-devices-nist-1800-34-practice- guide

[10] NSA, "UEFI Lockdown Quick Guidance," March 2018, https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional- resources/csi-uefi-lockdown.pdf

[11] Trusted Computing Group, "TCG PC Client Reference Integrity Manifest Specification," Version 1.4 November 2020, https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_RIM_r1p04_pub.pdf

[12] NIST, SP 800-193 "Platform Firmware Resiliency Guidelines," May 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

[13] DMTF, "Security Protocols and Data Models (SPDM)," Version 1.2.1, June 2022, https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.2.1.pdf

Disclaimer of endorsement

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov