HARDWARE SECURITY REQUIREMENTS FOR X86 PLATFORMS

GUIDE ANSSI

ANSSI-PG-067-EN
08/11/2019

PUBLIC VISÉ :

Développeur **Administrateur** **RSSI** DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Hardware security requirements for x86 platforms** ». Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	08/11/2019	Initial version

Table des matières

1
Introduction

This guide presents some security features and configuration options applying to hardware devices. These features are defined in the form of requirements and can apply to a provider of these hardware configurations.

The intended goal is to enforce security of new hardware acquired by an IT department. Each requirement is followed by a security objective specifying the goal.

The requirements are consolidated in four themes :

controls over the Platform : these requirements help ensure owners have the best control of their Platform

hardware specifications : these requirements apply to some specifical hardware components

firmware specifications : these requirements apply to BIOS configuration and protection

security Update : these requirements apply to updates of software components

2
Glossary

Plateform : Computing platform based on the x86 hardware architecture (32bit or 64bit), like servers, desktop or mobile PC

Firmware : Low-level software components shipped with the platform, including UEFI and legacy BIOSes or hardware components embedded software.

I/OMMU : *Input/Output Memory Management Unit*, hardware feature allowing for filtering memory accessing issued by peripherals.

TPM : *Trusted Platform Module*, passive hardware component specified by the Trusted Computing Group (TCG) which provides integrity and sealing capabilities.

Contract holder Provider of the hardware platforms, for example choosen after a public tender process.

Owner : Owner of the hardware platform or her delegate (for example the IT department).

3
Security requirements

3.1 Control over the Platform

3.1.1 Inventory

For each platform batch, and in accordance with selected features, the candidates provide a list of the hardware components —the Inventory— which form the platform. In particular, the following information is expected to appear on the Inventory :

- Product references (manufacturer, model version, etc.)
- Details on firmware executed by the hardware component (including version number)
- Details on firmware which interact with the hardware component independently from the platform system software (including version number)
- Communication interfaces exposed by the component

Security objective Ensure the owner has control over the platform they purchase.

3.1.2 Wireless interfaces

Wireless interfaces (e.g., WiFi, 4G), if present, shall remain optional for the platform to operate and physically removable by the owner without any incidents over the platform warranty.

Security Objective : Reduce the platform attack surface by removing unneeded interfaces

3.1.3 System software

The platform does not impose the use of particular system software or operating system

Security objective Make sure the owner has full control over the operating system used on the platform

3.2 Hardware specifications

3.2.1 I/OMMU

The platform exposes an input/output memory management unit, such as VT-x (Intel) or AMD-V (AMD). This feature needs to be enabled by default, and can only be disabled by the owner (not the user of the platform).

Security objective Enforce protection of the main memory against unstrusted peripherals

3.2.2 TPM

In case the platform embeds a TPM, the latter is certified (from a Common Criteria perspective) according to one of the following protection profiles :

- Protection Profile PC Client Specific Trusted Platform Module TPM Family 1.2
- TCG Protection Profile PC Client Specific TPM Family 2.0

Only the owner (not the user) can enable and disable the TPM. Disabling the TPM shall not be more complex than enabling it.

Security objective : Ensure the hardware component quality

3.3 Firmware specifications

3.3.1 Firmware configuration

The firmware configuration interface provides the following features :

- Protecting the access to the firmware configuration interface thanks to a dedicated password
- Locking the boot sequence of the platform thanks to a dedicated password
- Enabling and disabling input/output interfaces (e.g. USB)
- Configuring the boot order (the ordering of the list of devices checked by the BIOS to boot an operating system)
- Replacing default Secure Boot keys with custom keys generated by the owner

Security objective : Ensure the presence of minimal security features.

3.3.2 Firmware integrity

Platform firmwares for components listed at 3.1.1 are expected to ensure their integrity by means of state-of-the-art security mechanisms. This notably includes protecting integrity of the code and

data stored on the Flash Memory. The modification of firmware code should only be the result of a legitimate, signed update. The installation of a signed update older than the version currently installed on the platform *shall be considered illegitimate by default*. However, for the latter case, the firmware configuration interface shall allow the owner to disable this protection.

The candidates shall provide an argument which details the security mechanisms implemented by firmware system to comply with this requirement. This argument shall include the cryptographic protocols used to verify the integrity and legitimacy of updates.

Security objective : Ensure the hardening of the platform against persistent compromises.

3.3.3 Out-of-band management solutions

The candidates shall provide the list of out-of-band management solutions exposed by their platforms. Besides, these solutions shall all be disabled by default, and only the owner can enable them. Disabling these solutions shall not be more complicated than enabling them, and shall not require additional privileges.

Security objective Reduce the attack surface of the platform by enabling highly privileged software components only if necessary.

3.3.4 Firmware Auditability

Mechanisms which prevent firmware code inspection shall be absent or disabled by default. If present, only the owner can enable them, and disabling them shall not be more complex than enabling them, and shall not require any additional privileges.

Security objective Allow for inspecting and auditing firmware code.

3.4 Security updates

3.4.1 Updates availability

The candidates shall provide security updates less then eight weeks after the publication of a critical vulnerability affecting a component declared in the list from 3.1.1. In case this is not possible, the candidate shall provide the technical information enabling the owner to prevent exploitation of the vulnerability without negative impact on the platform normal behavior.

Security objective : Ensure the platform security state accross its entire life

3.4.2 Patch application

The candidates commits to integrate security updates mentionned at the previous requirements in all new platforms in the same delays.

Security objective : Ensure new platforms also include security updates

Bibliographie

[1] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-PG-067-EN
Version 1.0 - 08/11/2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN