EXIGENCES DE SÉCURITÉ MATÉRIELLE POUR PLATE-FORMES X86

GUIDE ANSSI

ANSSI-PG-067
08/11/2019

PUBLIC VISÉ :

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

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Exigences de sécurité matérielle pour plate-formes x86 »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab [1].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

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	Version initiale

Table des matières

1
Introduction

Ce guide présente un certain nombre de caractéristiques s'appliquant à des configurations matérielles. Ces caractéristiques sont définies sous formes d'exigences qui peuvent s'appliquer à un fournisseur de ces configurations matérielles.

Elles visent à renforcer la sécurité des matériels acquis par un service informatique. Chaque exigence est accompagnée d'un « objectif de sécurité » qui précise quel est le but recherché.

Les exigences sont regroupées en différentes thématiques :

maîtrise de la plate-forme : ces exigences permettent d'assurer au propriétaires des plate-formes une maîtrise plus importante de celles-ci

caractéristiques matérielles : ces exigences s'appliquent à certains composants matériels spécifiques de la plate-forme

caractéristiques firmware : ces exigences s'appliquent au BIOS et à sa configuration

maintien en condition de sécurité : ces exigences précisent les attendus en terme de mise à jour des composants logiciels

2
Glossaire

Plate-forme : matériel informatique sur architecture x86 ou x86_64, pouvant se décliner sous plusieurs formes : serveurs, PC de bureau, PC portable etc.

Firmware : Nom générique pouvant désigner le BIOS, le firmware UEFI ou tout autre logiciel embarqué dans un composant matériel.

I/OMMU : *Input/Output Memory Management Unit*, composant matériel permettant de filtrer les accès à la mémoire centrale depuis les périphériques.

TPM : *Trusted Platform Module*, composant passif spécifié par le TCG (*Trusted Computing Group*) fournissant des services de mesures d'intégrité et de scellement cryptographique.

Titulaire : Fournisseur des plate-formes matérielles, par exemple issu d'un processus de sélection comme un appel d'offre pour un marché public.

Propriétaire : Le propriétaire des machines ou son représentant (service informatique). Dans le cadre d'un marché public ce serait l'autorité qualifiée.

3
Exigences de sécurité

3.1 Maîtrise de la plate-forme

3.1.1 Inventaire

Pour chaque lot de plates-formes livré et en fonction des options sélectionnées, le titulaire fournit une liste décrivant précisément les composants matériels intégrés. Si un composant est absent de la liste, il doit être absent de la plate-forme livrée. Cette liste comprend notamment :

- la référence du produit (fabricant, modèle, version, etc.) ;
- la liste des composants logiciels actifs liés à ce composant (logiciel s'exécutant indépendamment du système d'exploitation) ;
- la liste des logiciels externes à la plate-forme, mais requis pour permettre leur bon fonctionnement (clients lourds d'administration, par exemple)
- la liste des interfaces de communication (physique ou émulée) exposées par le composant.

Objectif de sécurité : maîtriser les composants de la plate-forme et leurs capacités.

3.1.2 Interfaces sans-fil

Les interfaces de communication sans-fil, si elles sont présentes, devront pouvoir être démontées physiquement sans perturber le bon fonctionnement de la plate-forme et sans influence sur la garantie.

Objectif de sécurité : Limiter la surface d'attaque des plate-formes en permettant de retirer les interfaces inutiles.

3.1.3 Maîtrise du système

La plate-forme n'impose pas l'utilisation d'un système d'exploitation en particulier.

Objectif de sécurité : Permettre la maîtrise du système d'exploitation par le propriétaire.

3.2 Caractéristiques matérielles

3.2.1 I/OMMU

La plate-forme doit disposer d'un système de virtualisation des entrées sorties (I/OMMU), par exemple VT-x (Intel) ou AMD-V (AMD), pouvant être configuré depuis l'interface de configuration du firmware. Il doit être activé par défaut.

Objectif de sécurité : Assurer la protection de la mémoire centrale vis-à-vis des périphériques pour limiter les impacts d'une compromission.

3.2.2 TPM

Si la plate-forme dispose d'un TPM, ce dernier est certifié (au sens des critères communs) au niveau EAL4+ suivant l'un des deux profils de protection suivant :

- *Protection Profile PC Client Specific Trusted Platform Module TPM Family 1.2 1* ;
- *TCG Protection Profile PC Client Specific TPM family 2.0*.

Il ne peut être activé ou désactivé que par le propriétaire (pas par l'utilisateur) de façon sécurisée. La désactivation de ce composant ne doit pas être plus complexe que son activation ; les prérequis à l'activation doivent être suffisants pour la désactivation.

Objectif de sécurité : S'assurer de la robustesse du TPM fourni

3.3 Caractéristiques firmware

3.3.1 Configuration du firmware

L'interface de configuration du firmware doit proposer les fonctionnalités suivantes :

- la protection du démarrage de la plate-forme par un mot de passe ;
- l'activation et la désactivation des interfaces d'entrée-sortie de la plate-forme (par exemple, ports USB) ;
- la modification de l'ordre de sélection des périphériques susceptibles d'amorcer le système ;
- le remplacement des clefs *SecureBoot* du titulaire et des tierces parties par des clefs fournies par le propriétaire ;
- la protection de l'accès à l'interface de configuration du firmware par un mot de passe différent de celui de la séquence de démarrage normale.

Objectif de sécurité : S'assurer de la disponibilité de fonctionnalités minimales pour la sécurisation d'une plate-forme.

3.3.2 Sécurité du firmware

Les mécanismes de sécurité des firmwares listés dans le cadre de l'Exigence 3.1.1 doivent être à l'état de l'art au moment de la livraison. Cela implique notamment de protéger correctement le firmware contre des modifications malveillantes et en particulier contre l'installation d'une version du firmware légitime, mais antérieure à la version courante. Dans ce cas particulier, il est attendu que cette protection, activée par défaut, puisse être désactivée par le propriétaire. L'activation de cette protection ne doit pas être plus complexe que sa désactivation.

Il est demandé au titulaire de fournir un argumentaire décrivant précisément la façon dont les firmwares présents sur les plate-formes satisfont à cette exigence. Cet argumentaire pourra par exemple faire état de l'utilisation de mécanismes matériels, de la procédure de validation des mises à jour, etc.

Objectif de sécurité : Assurer la sécurité de la plate-forme et de ses mises à jour.

3.3.3 Solution d'administration à distance

Il est demandé au candidat de fournir une liste des solutions d'administration à distance proposée par la plate-forme (par exemple, Intel AMT). Ces solutions doivent être désactivées par défaut et ne peuvent être activées que par le propriétaire (et non par l'utilisateur) de façon sécurisée. La désactivation de ces modules ne doit pas être plus complexe que leur activation ; les prérequis à l'activation doivent être suffisants pour la désactivation.

L'accès à distance à l'interface d'administration de ces solutions doit être protégé, notamment par l'utilisation de protocoles conformes au RGS et par l'utilisation d'un mot de passe initial propre à chaque plate-forme.

Objectif de sécurité : Réduire la surface d'attaque de la plate-forme en n'y activant pas par défaut des solutions d'administrations à distance disposant d'importants privilèges.

3.3.4 Inspection du firmware

Les mécanismes de protection contre l'inspection de code doivent soit être absents du firmware, soit être désactivés par défaut. Ces modules ne peuvent être activés que par le propriétaire (pas par l'utilisateur) de façon sécurisée. La désactivation de ces modules ne doit pas être plus complexe que leur activation ; les prérequis à l'activation doivent être suffisants pour la désactivation.

Objectif de sécurité : Permettre l'analyse de sécurité du firmware.

3.4 Maintien en Conditions de Sécurité

3.4.1 Fournitures de correctifs

Le titulaire retenu s'engage à fournir un correctif dans un délai de huit semaines en cas de découverte d'une vulnérabilité critique affectant un composant déclaré dans la liste demandée en

Exigence 3.1.1 du présent document, ou à fournir les informations techniques permettant au propriétaire d'empêcher l'exploitation de ladite vulnérabilité, sans que les contre-mesures aient un impact négatif sur le fonctionnement normal de la plate-forme.

Le délai de huit semaines court à partir du moment où le titulaire est averti de la vulnérabilité.

Objectif de sécurité : S'assurer du maintien en condition de sécurité de la plate-forme après sa livraison

3.4.2 Application des correctifs

Le titulaire s'engage à intégrer les correctifs produits dans le cadre de l'exigence précédente dans les nouvelles plates-formes sous les mêmes délais.

Objectif de sécurité : S'assurer du maintien en condition de sécurité des plates-formes livrées dans le cadre du marché.

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
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