Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 30 AVR. 2014

N°1760 /ANSSI/SDE/PSS/CCN

Référence : ANSSI-CSPN-NOTE-02/1.0

NOTE D'APPLICATION

METHODOLOGIE POUR L'EVALUATION LOGICIELLE DES TERMINAUX DE RECEPTION NUMERIQUE EN VUE D'UNE CERTIFICATION DE SECURITE DE PREMIER NIVEAU

Application : Dès son approbation.

Diffusion : Publique.

*Le directeur général de l'agence nationale
de la sécurité des systèmes d'information*

Guillaume POUPARD

Suivi des modifications

Editions	Date	Modifications
1.0	30 avril 2014	Création du document dans le cadre du groupe de travail SEMS, à partir des documents [CDS-STB] et de la méthodologie d'évaluation en vue de la CSPN [MET_CSPN]. Prise en compte des évaluations pilotes.

En application du décret n° 2002-535 du 18 avril 2002, la présente procédure a été soumise au comité directeur de la certification, qui a donné un avis favorable.

La présente instruction est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

Remerciements

Cette méthodologie est issue du travail des membres du groupe SEMS (*Security Evaluation Methodology for Set top boxes*) sur la base d'un document rédigé par Sogeti pour Canal +.

Les organismes ayant participé à l'élaboration de ce document sont les suivants :

- Amossys ;
- Bouygues Telecom ;
- Canal + ;
- GIE-CB ;
- Orange ;
- Sagemcom ;
- Sogeti ;
- Thales (TCS – CNES) ;
- Viaccess.

TABLE DES MATIERES

1. Introduction

1.1. Définitions

Chipset	Circuit intégré gérant les flux de données entre le processeur, la mémoire et les périphériques.
Conditional Access System (CAS)	Système de sécurité permettant de limiter l'accès à un contenu du Service aux abonnés autorisés.
Control Word (CW)	Clé de chiffrement du contenu des services
Digital Right Management (DRM)	Mesures techniques permettant de contrôler l'utilisation qui est faite des œuvres numériques.
Personal Video Recorder (PVR)	Système permettant d'enregistrer de la vidéo comme par exemple un magnétoscope numérique.
Service	Ensemble de chaînes.
Service connecté	Service disponible pour l'abonné à partir de son Terminal, et nécessitant la connexion du terminal à un serveur distant fournissant les services.
Télévision de rattrapage (*Catch-up TV*)	Service offrant à un abonné la possibilité de regarder un programme après sa première diffusion pendant une période fixe.
Terminal de réception numérique (*Set top box*, STB)	Système matériel et logiciel permettant de recevoir, désembrouiller, décoder et envoyer vers des équipements d'affichage/sonorisation du contenu distribué sur une plate-forme.
Video on demand (VOD)	Possibilité de visionner un programme d'un service après sa diffusion généralement par téléchargement du contenu sur un serveur (*Pull VoD*).

1.2. Objet de la note et produits visés

La présente note d'application décrit la méthode d'évaluation de la sécurité du logiciel d'un terminal de réception numérique (STB – *Set Top Box*) dans le contexte d'une certification de sécurité de premier niveau (CSPN). La sécurité des aspects matériels n'est pas prise en compte par cette méthodologie.

Cette méthodologie vise les terminaux de réception numérique manipulant les secrets permettant l'affichage des contenus de Pay-TV sur un téléviseur. Elle ne vise pas directement les « box » réseau des opérateurs mais peut être utilisé comme base méthodologique pour l'évaluation de ces équipements et, plus généralement, pour l'évaluation de divers types de boîtiers connectés.

L'évaluation logicielle d'un terminal de réception numérique doit permettre de vérifier qu'il fournit bien les fonctions de sécurité indiquées dans sa cible de sécurité mais également que

toutes les fonctions de sécurité atteignent au moins un niveau intrinsèque de résistance « élémentaire » et qu'aucune vulnérabilité logicielle de la STB n'a pu être exploitée lors de l'évaluation. Cette dernière conclusion doit être prise avec toute la prudence que l'on doit avoir dans le domaine de la sécurité des technologies de l'information. Il n'est en effet pas possible de garantir l'absence de vulnérabilité exploitable dans un produit.

Plus particulièrement, l'évaluation vise à vérifier la bonne manipulation logicielle des secrets contenus dans la STB. Cela comprend les contenus opérateurs ainsi que les données utilisateurs mais également les secrets utilisés pour l'authentification de l'utilisateur auprès de services tiers. A l'inverse, l'évaluation ne prend pas en compte les menaces matérielles sur les composants de la STB ni l'interception des secrets contenus dans la STB lors des transferts entre ces composants.

1.3. Charge d'évaluation

La charge prévue pour la réalisation de l'évaluation des STB est de **40 hommes*jours pour le boîtier** et **10 hommes*jours supplémentaires pour la partie cryptographique** (contre 25 + 10 dans la méthodologie CSPN).

Les DRM ne font pas partie du périmètre de cette méthodologie. Si le commanditaire souhaite les évaluer, une charge supplémentaire de 10 hommes*jours devra y être consacrée. L'évaluation des DRM n'est pas couverte par la présente méthodologie.

La charge d'évaluation peut être revue à la baisse dans le cas d'une réévaluation ou d'une évaluation différentielle. D'une manière générale, toute modification de charge doit être justifiée et validée par l'organisme de certification avant acceptation du démarrage de l'évaluation.

1.4. Aspects spécifiques de cette méthodologie par rapport à la méthodologie CSPN

La présente méthodologie est utilisable sans se référer à la méthodologie CSPN [MET_CSPN]. Pour ce faire, certains travaux à effectuer sont repris de la méthodologie générique et d'autres ont été ajoutés ou raffinés au regard des produits visés.

2. Travaux d'évaluation spécifiques

Ce chapitre décrit le contenu du rapport technique d'évaluation (RTE), dont il reprend la trame, et liste les tâches d'évaluation spécifiques attendues.

2.1. Identification du rapport technique d'évaluation

Nom du projet d'évaluation	Identifiant unique fourni par l'ANSSI
Référence du RTE	Identifiant unique fourni par le CESTI
Auteur	Nom du ou des experts intervenants dans la réalisation de l'analyse
Approbateur	Nom du contrôleur technique
Date de création du RTE	Date de création du RTE
Date de mise à jour du RTE	Date de mise à jour du RTE
N° de version du RTE	
Divers	Texte libre

2.2. Identification du produit évalué

Nom de l'éditeur	
Nom du produit	Nom commercial
N° de version analysée	N° exact (version, release)
Correctifs éventuels appliqués	
Domaine technique CSPN	Terminaux de réception numérique
Divers	

2.3. Fonctionnalités, environnement d'utilisation et de sécurité

Ce chapitre et ses sous-chapitres contiendront une brève description de la STB évaluée ainsi que des différents services concernés par l'évaluation. Ils reprendront également les éléments les plus importants de la cible de sécurité.

La cible de sécurité, fournie par le commanditaire de l'évaluation, devra s'appuyer sur la cible générique pour STB [CDS-STB] et définir clairement le périmètre de l'analyse en particulier vis-à-vis des services distants tiers qui ne pourront faire l'objet d'investigations sans autorisation préalable.

2.3.1. Description générale du produit

L'évaluateur devra faire un rappel de l'architecture général du produit. Notamment il précisera les points suivants :

Chipset	*fournisseur et référence*
Programme de démarrage	*nom et version*
Systèmes d'exploitation	*nom et version*
Middleware	*nom et version*
Navigateur	*nom et version*
Bibliothèques	
CAS	*nom et version*
DRM	*nom et version*
Vidéo à la demande	*nom et version*

Si disponible, un schéma d'architecture générale de la STB devra être fourni par le commanditaire au démarrage de l'évaluation. Ce schéma identifiera les principales entités matérielles et logicielles qui composent la STB, ainsi que leurs interconnexions.

2.3.2. Modes de fonctionnement du produit

Dans cette section, l'évaluateur précisera le mode de fonctionnement du produit et plus particulièrement :

- le fonctionnement de la mise à jour du logiciel embarqué en précisant :
  - les moyens de détection de l'existence d'une nouvelle version ;
  - comment est contraint le passage à une nouvelle version ;
  - les systèmes de protection de la mise à jour ;
- la procédure de démarrage sécurisé en précisant les systèmes de protection mis en place.

2.3.3. Description de la manière d'utiliser le produit

Cette partie contiendra une description de l'utilisation du produit et de son adéquation avec la documentation fournie.

2.3.4. Description de l'environnement d'utilisation prévu

Par défaut, l'environnement d'utilisation prévu devrait correspondre à une utilisation standard (utilisation d'un abonné à son domicile). Dans le cas où il s'agit d'un environnement particulier, l'évaluateur pourra le détailler dans cette section.

2.3.5. Description des hypothèses sur l'environnement

L'évaluateur devra reporter ici l'ensemble des hypothèses sur l'environnement indiqués dans la cible de sécurité, indiquer si certaines de ces hypothèses ne lui paraissent pas pertinentes et identifier les hypothèses couvrant des vulnérabilités découvertes durant l'évaluation.

2.3.6. Description des dépendances

Les dépendances avec des éléments matériels ou logiciels qui ne seraient pas fournis avec le produit devront être indiquées. Notamment, l'évaluateur devra indiquer la méthode de réception du contenu (satellitaire, via le réseau d'un fournisseur d'accès internet, etc.), le matériel nécessaire à la réception (parabole, box réseau, etc.) ainsi que les moyens de raccordements du produit évalué au matériel précité.

2.3.7. Description des utilisateurs typiques concernés

L'utilisateur typique est l'abonné aux services de l'opérateur distribuant le terminal.

2.3.8. Définition du périmètre de l'évaluation

Le périmètre de l'évaluation est la STB avec ses interfaces externes permettant d'utiliser les fonctionnalités de Pay-TV et les accès aux services connectés.

Les attaques matérielles portant sur les composants de la STB ou sur l'interception de secrets entre ces composants n'entrent pas dans le périmètre de l'évaluation.

2.3.9. Inventaire des fonctions de sécurité identifiées

L'évaluateur devra reporter l'ensemble des fonctions de sécurité décrites dans la cible de sécurité et identifier celles qui ont été mises en échec durant l'évaluation.

2.3.10. Inventaire des biens sensibles que le produit doit protéger

L'évaluateur devra reporter l'ensemble des biens sensibles décrits dans la cible de sécurité et identifier ceux qu'il est parvenu à compromettre.

2.3.11. Inventaire des menaces portant sur le produit

L'évaluateur devra reporter l'ensemble des menaces décrites dans la cible de sécurité et identifier celles qu'il est parvenu à mettre en œuvre.

2.4. Installation du produit

Pour permettre l'évaluation du produit, il est nécessaire de s'assurer au minimum de la disponibilité de matériels, logiciels, documents et services accessibles à la STB. C'est au commanditaire de s'assurer que l'évaluateur dispose bien de ces éléments.

2.4.1. Matériels nécessaires à la réalisation de l'évaluation

Pour réaliser son évaluation, l'évaluateur devra disposer :

- d'un terminal de réception numérique (ci-après STB dite « de production ») ;
- d'un terminal de réception numérique en mode « *debug* » offrant un accès console en série, un débuggeur JTAG, etc. (ci-après STB dite « de développement »).

Le terminal de *debug* est nécessaire afin de vérifier si un comportement inopiné du boîtier peut être exploité dans le but d'atteindre en disponibilité, intégrité ou confidentialité les biens à protéger.

De plus, afin d'évaluer la sécurité logicielle du système d'exploitation de la STB, un accès en mode console avec les droits d'administration (de type SSH) est nécessaire sur la STB de développement.

Certaines manipulations peuvent mener à un état instable de la STB. Une procédure de remise en état devra également être mise à disposition (réinitialisation à l'état préalable à l'évaluation, à partir d'une image d'installation par exemple).
Une procédure de remise en état suite à une intrusion sur le boîtier devra également être mise à disposition dans le cas où d'éventuels capteurs bloqueraient le fonctionnement de la STB.

2.4.2. Logiciels et documents nécessaires à la réalisation de l'évaluation

Afin de réaliser l'évaluation, l'évaluateur devra disposer :

- du logiciel embarqué sous forme brute (fichier binaire) déchiffré et du système de fichiers comprenant les éléments de configuration ;
- d'une documentation fonctionnelle (spécifications, informations matérielles, mécanismes cryptographiques, liste des composants et numéros de versions) ;
- d'une chaîne de compilation fonctionnelle.

Dix jours sont prévus pour l'évaluation des mécanismes cryptographiques. Il est donc important pour l'évaluateur d'avoir à disposition l'ensemble des informations nécessaires pour vérifier l'implémentation qui en est faite. Les attendus concernant la documentation des mécanismes cryptographiques sont précisés au chapitre 3.3 du document [CRI_CSPN].

2.4.3. Services nécessaires à la réalisation de l'évaluation

Afin de réaliser l'évaluation, l'évaluateur devra disposer :

- d'un compte par STB fournie pour l'accès aux chaînes chiffrées et protégées ;
- d'un compte *Vidéo à la demande* par STB fournie pour l'achat et la location de films ;
- d'un accès au flux satellite/réseau ;
- de comptes pour l'accès à tous les services faisant partie du périmètre de l'évaluation.

Plus généralement, l'évaluation prenant en compte l'authentification de l'utilisateur auprès de service tiers, le commanditaire devra s'assurer que l'évaluateur dispose de l'ensemble des éléments lui permettant d'étudier ces mécanismes.

2.4.4. Positionnement de l'évaluateur

Afin de vérifier la conformité des fonctionnalités et la résistance des mécanismes mis en œuvre dans le produit, l'évaluateur pourra se positionner sur une plate-forme de test entre le terminal et l'accès internet. Pour cela, la machine de l'évaluateur doit alors être placée entre les deux boîtiers à l'aide, par exemple, d'un concentrateur Ethernet (« Hub ») pour analyser le trafic (des solutions de type pont réseau ou *tap* réseau peuvent être envisagées). Dans tous les cas, l'évaluateur devra décrire précisément la plate-forme d'évaluation.

2.5. Analyse de la conformité

2.5.1. Analyse de la documentation

Le contenu attendu est détaillé dans la partie « Tâches de l'évaluateur » du paragraphe 4.3 de l'instruction ANSSI-CSPN-CER-I.02 (voir [CRI_CSPN]).

2.5.2. Revue du code source (si disponible)

Le contenu attendu est détaillé dans la partie « Tâches de l'évaluateur » du paragraphe 4.4 de l'instruction ANSSI-CSPN-CER-I.02 (voir [CRI_CSPN]).

2.5.3. Fonctionnalités testées

Le contenu attendu est détaillé dans la partie « Tâches de l'évaluateur » du paragraphe 4.5 de l'instruction ANSSI-CSPN-CER-I.02 (voir [CRI_CSPN]).

2.6. Analyse de la résistance des fonctions et mécanismes et des vulnérabilités

Le contenu attendu est détaillé dans la partie « Tâches de l'évaluateur » du paragraphe 4.6 de l'instruction ANSSI-CSPN-CER-I.02 (voir [CRI_CSPN]).

Pour ce type d'équipement, un travail spécifique d'identification des mécanismes et interfaces devra être conduit par l'évaluateur. Ce travail, décrit dans les paragraphes suivants, pourra être fait sur les STB de *debug*. Les tâches du paragraphe 2.6.2 devront être validées sur une STB de production.

Par ailleurs, la cotation de la résistance des mécanismes sera faite sur la STB de *debug* et sur la STB de production.

2.6.1. Analyse des services

2.6.1.1. Identification des points d'entrées

Il est nécessaire d'identifier tous les points d'entrées afin de lister les méthodes d'interaction de l'utilisateur avec le boîtier.
Les points d'entrées peuvent être partagés en plusieurs catégories :

- les points d'entrée logiques : il s'agit principalement des connexions réseaux. On vérifiera par exemple :
  - les connexions réseaux supportées : Ethernet, Wi-Fi, ADSL, Satellite, modem ;
  - les services exposés : TCP/IP, UDP ;
  - les applications utilisées : FTP, navigateur Web, etc. ;
- les points d'entrée physiques : il s'agit principalement des ports disponibles sur la STB afin de connecter des périphériques externes. On vérifiera par exemple les ports disponibles : USB, RS-232 (série), Infrarouge, Firewire ;
- les points d'entrée physiques nécessitant une intrusion du boitier : il s'agit principalement des points d'entrées accessibles uniquement après ouverture du boitier et normalement non-accessible par l'abonné. On vérifiera par exemple :
  - les ports disponibles : ports JTAG ;
  - les supports de stockage de masse : disque dur, disque flash.

2.6.1.2. Identification des services

Pour protéger les données sensibles, que ce soient celles liées à un utilisateur ou à un flux vidéo, l'évaluateur devra identifier tous les transferts de flux.

Pour cela, il est nécessaire de lister l'ensemble des fonctionnalités concernant les services disponibles (chaînes, vidéo à la demande, etc.) :

- la création de compte ;
- l'authentification ;
- l'accès à des espaces personnels ;
- les systèmes de paiements ;
- la location de contenu ;
- l'enregistrement de contenu.

Pour chaque service, l'évaluateur devra noter au moins les informations suivantes :

- le type d'exposition du service :
    - service entrant (du point de vue de la STB) accessible depuis Internet ;
    - service entrant (du point de vue de la STB) accessible depuis le réseau local ;
    - service sortant (du point de vue de la STB) ;
- le déroulement de l'identification du boîtier, de l'utilisateur et du serveur ;
- la méthode de transfert des données (format, protocole, méthode de chiffrement, etc.).

2.6.1.3. Mise à jour du terminal

L'installation par un attaquant d'un logiciel sur le terminal constitue une menace critique. La **gestion des mises à jour**, la **vérification de la signature** du logiciel embarqué et la **chaîne de validation au démarrage** devront être analysées par l'évaluateur. L'évaluateur devra étudier les mécanismes relatifs à la chaîne de démarrage et plus particulièrement la présence d'une vérification d'intégrité reposant sur une signature cryptographique. Ce mécanisme ne doit pas pouvoir être compromis sans rendre le matériel inutilisable.

2.6.1.4. Récapitulatif de l'analyse des services

A la fin de cette étape de récupération des services tournant sur la STB, l'évaluateur devra renseigner une fiche identifiant les points à vérifier en priorité. Les items des tableaux ci-dessous sont présentés à titre illustratif et peuvent être complétés selon le produit évalué.

Entrée	**Présent ?**
Ethernet	Oui/Non
Wi-Fi	Oui/Non
Satellite	Oui/Non
JTAG	Oui/Non
RS-232	Oui/Non

Service réseau	**Port**	**Notes**	**Vulnérabilité publique ?**
Web	80	Apache X.Y	Oui/Non
…	…	…	Oui/Non

Action	**Evénement déclencheur**	**Sécurité**		
		Authentification client	**Authentification Serveur**	**Chiffrement**
DNS	Démarrage et Configuration réseau			
DHCP	Démarrage et Configuration réseau			
FTP	Réinitialisation des paramètres d'usine			
Mise à jour par satellite	Démarrage + vérification 24H			
Montage du disque dur	Branchement USB			

Services	**Fonctionnalités**	**Sécurité**		
		Authentification client	**Authentification Serveur**	**Chiffrement**
Catch-up TV				
	Création de comptes			
	Authentification			
	Espace personnel			
	Visionnage			
	…			
Vidéo à la demande				

2.6.2. Analyse des flux

L'évaluateur devra ici vérifier l'efficacité des mesures de protection mises en œuvre par le terminal.
Les points à vérifier sont par exemple :

- la possibilité pour un utilisateur de se faire passer pour quelqu'un d'autre :
    - pour récupérer un contenu gratuitement ;
    - pour surfacturer un autre utilisateur ;
    - pour récupérer des informations confidentielles ;
    - pour fausser des journaux ;
- la possibilité d'automatiser des requêtes :
    - pour tester des mots de passe faibles par force brute ;
    - pour trouver des numéros de carte valides par force brute ;
    - pour récupérer les informations des utilisateurs.

2.6.2.1. Analyse des flux liés aux services

L'évaluateur devra lister les flux échangés, sans oublier ceux déclenchés automatiquement :

- au démarrage du lien ADSL ;
- au démarrage du boîtier TV ;
- lors des accès aux différents services disponibles :
    - changement de chaîne ;
    - abonnement ;
    - location d'un film de Vidéo à la demande ;
    - rediffusion via le service de *catch-up* TV ;
    - accès à l'espace client ;
- lors d'un retour aux paramètres d'usine.

2.6.2.2. Analyse des flux vidéo

Deux types de contenu doivent être protégés. S'il s'agit d'une chaîne, alors le flux sera récupéré au fur et à mesure. Dans le cas d'un fichier vidéo, le fichier peut être téléchargé en totalité ou en plusieurs parties afin de permettre le visionnage en parallèle du téléchargement. Dans les deux cas, l'évaluateur devra vérifier s'il est possible d'accéder au contenu en clair.

L'évaluateur listera notamment les contenus à disposition ainsi que les mécanismes de protection, dont :

- la présence d'un tunnel chiffré (VPN) protégeant le flux vidéo ;
- l'utilisation de DRM (flux RTP clair avec le contenu chiffré).

Note : Si la sécurité des serveurs tiers ne fait pas partie du périmètre de l'évaluation, l'évaluateur rapportera au commanditaire, après accord de l'ANSSI, tout comportement anormal laissant supposer l'existence de vulnérabilités associées au serveur.

2.6.2.3. Récapitulatif de l'analyse des flux

L'évaluateur devra fournir une description détaillée du fonctionnement de chaque service sous la forme d'un tableau récapitulatif tel que proposé ci-après (les réponses en italiques sont là à titre d'exemple) :

Action	**Evénement déclencheur**	**Sécurité**		
		Authentification du boîtier	**Authentification du serveur**	**Chiffrement**
DNS	Démarrage et Configuration réseau	*néant*	*néant*	*non*
DHCP	Démarrage et Configuration réseau	*néant*	*néant*	*non*
FTP	Réinitialisation des paramètres usines	*néant*	*certificat + signature logiciel embarqué*	*non*
Mise à jour par satellite	Démarrage + vérification 24h	*néant*	*signature logiciel embarqué*	*non*

Service	**Fonctionnalités**	**Sécurité**		
		Authentification client	**Authentification Serveur**	**Chiffrement**
Catch-up TV				
	Création de compte	*non*	***non***	***non***
	Authentification	*login + mot de passe*	***non***	***non***
	Espace personnel	*cookie de session*	***non***	***non***
	Visionnage	*cookie de session*	***certificat***	***AES***
	…			
Vidéo à la demande				
	…			

2.6.3. Analyse logicielle

L'évaluation du logiciel embarqué a pour objectif d'obtenir une vision précise des différents mécanismes de traitement des informations afférentes aux biens à protéger, afin de déterminer si ces derniers peuvent être compromis en disponibilité, intégrité et confidentialité à partir d'une attaque logicielle.

2.6.3.1. Aspects cryptographiques

Dans la mesure où l'évaluation porte sur les aspects logiciels de la STB, le *chipset* et le système de protection de contenu, dès lors que ce dernier repose sur la protection matérielle du *chipset*, sont hors du périmètre de la cotation cryptographique (conformité au RGS) de la STB.

L'étude cryptographique que devra réaliser l'évaluateur comprend l'analyse et la cotation des mécanismes cryptologiques standards du logiciel embarqué, comme par exemple :

- le chiffrement des contenus sur le disque ;
- la communication avec les serveurs distants ;
- la signature du logiciel embarqué.

L'analyse doit permettre de comprendre les mécanismes liés à l'utilisation et au stockage de secrets cryptographiques associés aux traitements du contenu protégé.

L'évaluateur devra :

- détailler les composants logiciels ou matériels en charge de ces traitements ;
- détailler les traitements proprement dits ;
- détailler le fonctionnement du générateur d'aléa utilisé (notamment les sources d'entropie utilisées) ;
- valider la conformité des mécanismes cryptographiques par rapport à l'annexe B du Référentiel Général de Sécurité [RGS] ;
- valider la bonne utilisation d'un composant de confiance pour le stockage et l'utilisation des secrets ;
- valider la présence ou non de vulnérabilités par rapport à l'état de l'art.

Pour chaque faiblesse cryptographique identifiée, l'évaluateur pourra développer une preuve de concept mettant en jeu le mécanisme faible ; il proposera une ou plusieurs actions correctrices.

Ces aspects cryptographiques recouvrent aussi bien les faiblesses protocolaires et algorithmiques (exemple : attaque par oracle sur le « padding » CBC dans TLS) que liées à l'implémentation (exemple : affaiblissement de la signature due à l'utilisation d'un *strncmp* au lieu de *memcmp*, ou encore mauvaise utilisation de ECDSA).

L'évaluateur devra fournir une description détaillée pour chaque vulnérabilité identifiée en s'inspirant de l'exemple ci-après.

Donnée	Composant utilisé	Protocole	Bon traitement des secrets en mémoire	Conformité RGS	Vulnérabilités publiques
Flux vidéo vers TV	*Composant de confiance*	*X.Y.Z*	***OK***	***OK***	
Numéro de CB	*OpenSSL 0.9.6 + libCB 1.1*	*TLS*	***NOK***	***OK***	*Oracle de Bleichenbacher*
Chiffrement des disques USB					

2.6.3.2. Aspects système

2.6.3.2.1 Vérification des bonnes pratiques de durcissement

L'évaluateur vérifiera la présence de mécanismes permettant de durcir la protection des binaires :

- protection de la pile/tas avec des canaris ;
- pile et tas non exécutables ;
- randomisation de la mémoire ;
- application du principe de minimalité : seuls les services, les applications et les modules noyaux nécessaires au fonctionnement de la STB doivent être déployés sur le système ;
- utilisation de mécanismes d'isolation des processus : chroot, conteneurs (VZ ou Vserveur par exemple), droits d'exécution des processus, SECCOMP, *capabilities* des processus ;
- protection réseau : contre le spoofing IP/MAC, DoS, protection de la pile IP.

2.6.3.2.2 Identification des vulnérabilités publiques

L'évaluateur devra examiner les programmes et bibliothèques fournis sous forme non chiffrée pour identifier les composants et leur numéro de version associé (par exemple : zlib 1.2.3), ainsi que l'absence éventuelle des contre-mesures prévues (« cookies de pile », « randomisation », liste blanche de traitement des entrées, etc.).

Il cherchera ensuite quelles sont les vulnérabilités publiques affectant ces composants. Pour chaque vulnérabilité, il étudiera le chemin d'exploitation afin de déterminer si la vulnérabilité est accessible depuis un des points d'entrée précédemment cités. L'écriture d'une preuve de concept mettant en exergue la vulnérabilité et son impact vis-à-vis des biens à protéger et la fourniture d'une ou plusieurs actions correctrices permettant de se prémunir contre la ou les vulnérabilités identifiées ne sont pas obligatoires.

Notons que cette partie peut nécessiter le développement d'outils spécifiques à l'environnement étudié. L'évaluateur pourra fournir au commanditaire et au développeur, après accord de l'ANSSI, l'ensemble ou une partie des outils développés pour lui permettre de reproduire la vulnérabilité et de vérifier sa correction dans une phase ultérieure.

L'évaluateur fournira une description détaillée pour chaque vulnérabilité identifiée en s'inspirant de l'exemple ci-dessous :

Binaire et bibliothèque	Notes	Vulnérable CVE	Privilège restreint	Protection de la pile	Code signé
Serveur Web	*Apache X.Y.Z*				
Navigateur	*Webfront 3.5*	***non***	***oui***	***non***	***non***
libpng	…				

2.6.3.2.3 Recherche de vulnérabilités non publiques

Cette phase s'appuie sur l'expertise de l'évaluateur pour identifier des potentielles vulnérabilités non publiques sur les composants présents ou spécifiques à l'architecture propriétaire en place, et tout particulièrement ceux traitant les données contrôlées par l'attaquant.

Exemples :

- l'utilisation d'IPv6 pour contourner la politique de filtrage ;
- l'exploitation d'une vulnérabilité dans le traitement des métadonnées associées à un téléchargement ;
- une vulnérabilité dans une interface Web (traversée de répertoire, envois de fichiers arbitraires, etc.) ;

Le développement d'une preuve de concept et la proposition d'actions correctives n'est pas requise pour l'évaluateur.

Notons que cette phase peut requérir une extension de la durée de l'évaluation suivant la taille du périmètre et la difficulté d'analyse des composants du système.

2.7. Analyse de la facilité d'emploi

Le contenu attendu est détaillé dans la partie « Tâches de l'évaluateur » du paragraphe 4.9 de l'instruction ANSSI-CSPN-CER-I.02 (voir [CRI_CSPN]).

Il sera indiqué dans le RTE les cas où la sécurité du produit peut être remise en cause dans certains modes d'utilisation ou de configurations du produit. Dans ce cas, il faut recommander, si une telle option existe, une configuration permettant d'atteindre le meilleur niveau de sécurité afin de contrer les menaces identifiées. Une réduction du périmètre fonctionnel du produit (au sens de la sécurité) peut éventuellement être proposée.

2.8. Entretiens avec les développeurs

Cette tâche est facultative.

2.8.1. Résultat des entretiens

L'expert en charge de l'analyse indique les éléments qui lui semblent intéressant à mentionner pour le lecteur.

2.8.2. Avis sur le développeur

Le contenu attendu est détaillé dans la partie « Tâches de l'évaluateur » du paragraphe 4.10 de l'instruction ANSSI-CSPN-CER-I.02 (voir [CRI_CSPN]).

2.9. Synthèse

Un **avis d'expert** synthétise les résultats des tâches précédentes pour un lecteur technique.

Annexe 1 : Références

[CRI_CSPN]	Instruction – Critères pour l'évaluation en vue d'une Certification de sécurité de premier niveau, Référence : ANSSI-CSPN-CER-I-02, version en vigueur.
[MET_CSPN]	Note d'application – Méthodologie pour l'évaluation en vue d'une Certification de sécurité de premier niveau – Contenu du RTE, Référence : ANSSI-CSPN-NOTE-01, version en vigueur.
[CDS-STB]	Exigences de sécurité générales STB conformes à la méthodologie CSPN. Version : 1.2, datée du 26/12/2012. Canal+.
[RGS_B]	Référentiel général de sécurité, annexes B : [RGS_B1] : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. [RGS_B2] : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques. [RGS_B3] : Règles et recommandations concernant les mécanismes d'authentification.