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 29 novembre 2019

N° 4565 /ANSSI/SDE/PSS/CCN

Référence :

ANSSI-CC-NOTE-22_v1.0

NOTE D'APPLICATION

COTATION DE L'UTILISATION D'OPEN SAMPLES/SAMPLES WITH KNOWN SECRETS

Application : Dès son approbation

Diffusion : Publique

Le Sous-directeur « Expertise »
de l'agence nationale de la sécurité
des systèmes d'information

Vincent STRUBEL
[ORIGINAL SIGNÉ]

Suivi des modifications

Editions	Date	Modifications
0.1	22/02/2019	Ebauche.
0.2	18/04/2019	Prise en compte des remarques des développeurs.
1.0	29/11/2019	Document final

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

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

TABLE DES MATIERES

1. Objet de la note

Cette note précise la cotation qui sera appliquée lors de l'utilisation d'*open samples/samples with known secrets* lors des évaluations des domaines « composants électroniques, microélectroniques et logiciels embarqués » et « équipements matériels avec boîtiers sécurisés » au sein du schéma français.

Elle concerne les évaluations Critères communs (CC). Elle s'applique de même aux évaluations Certification de sécurité de premier niveau (CSPN) avec la grille de cotation ad hoc.

2. Références

[CC] Certification Critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version en vigueur.

[CSPN] Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version en vigueur.

[JIWG AP] *Application of Attack Potential to Smartcards*, version en vigueur.

[JIWG SB] *Joint Interpretation Library – Application of attack potential to hardware devices with security boxes*, version en vigueur.

3. Périmètre

Pour déterminer le niveau de résistance (niveau AVA_VAN) atteint par un produit dans le cadre d'une évaluation CC, [JIWG AP] fournit un système de cotation précisant les points associés à plusieurs paramètres impliqués dans la réussite d'une attaque ; cela permet d'établir le potentiel nécessaire à un attaquant pour qu'il puisse la mener à bien.

L'un de ces paramètres correspond à l'utilisation d'échantillons ouverts et d'échantillons avec secrets connus (paramètre *Open Samples/Samples with known secrets*). En effet les évaluations de composants nécessitent parfois des échantillons dont la configuration est dédiée à l'évaluation.

L'accès à ces échantillons doit être à protéger, et le niveau effectif de protection (« *PUBLIC* », « *RESTRICTED* », etc.) est pris en compte dans la cotation des attaques applicables au produit certifié.

4. Problème posé

Lors de cette cotation, il semble difficile a priori de garantir un niveau de protection contre une diffusion à la fois de tels échantillons, mais également de produits aux fonctions similaires, au-delà du niveau « *RESTRICTED* ».

Exemple : cas d'un produit (microcontrôleur ou plateforme) avec un niveau de sécurité lié au suivi de guides de sécurité lors d'une composition sur ledit produit.

Lors de l'évaluation d'une composition sur ce produit, il est généralement difficile de démontrer qu'il n'existe pas une autre composition non certifiée sur le même produit qui n'activerait pas certaines contremesures (par exemple, le cas de contremesures non nécessaires à son problème de sécurité[1]), permettant d'utiliser cette composition comme open sample/sample with known secret,

[1] Au sens de « *security problem* » tel que défini dans [CC].

bien qu'il soit différent de l'échantillon ouvert utilisé lors de l'évaluation. L'existence d'une telle composition et son accès doivent donc être pris en compte lors de la cotation de l'utilisation d'open samples/samples with known secrets.

5. Cotation de l'utilisation d'*open samples/samples with known secrets*

L'utilisation d'*open samples/samples with known secrets* sera cotée par défaut à **0 point** (« *PUBLIC* ») ou **2 points** (« *RESTRICTED* »).

En reprenant l'exemple du chapitre précédent, s'il est trivial de trouver un accès libre à la fonction visée par l'attaque, l'utilisation d'*open samples/samples with known secrets* sera cotée à 0. Un tel accès est dit « trivial » si le CESTI peut démontrer par une recherche rapide l'existence de composition pouvant servir d'*open samples*/*samples with known secrets*. En effet même si le *sample* fourni pour l'attaque n'existe que dans le cadre de l'évaluation, il s'agit de considérer l'accès d'un attaquant à la fonctionnalité et non au *sample* dans son ensemble. En revanche, dans le cas où cet accès est non trivial, l'utilisation d'un tel *sample* sera a priori cotée à 2 points.

Il se peut toutefois qu'un argumentaire convaincant validé par l'ANSSI permette d'attribuer davantage de points à une attaque utilisant des *open samples*/*samples with known secrets*.

Il pourrait par exemple être démontré qu'un microcontrôleur n'est destiné qu'à une composition interne et non pas à être vendu en tant que produit « nu » à un client extérieur, et que la contremesure est toujours activée en composition, même lorsque le problème de sécurité ne l'exige pas. Un autre exemple est le débrayage d'une contremesure inhérente au produit, uniquement sur des échantillons fournis pour des évaluations dans des schémas reconnus EAL1-7 pour le domaine par le SOG-IS.