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° 4566 /ANSSI/SDE/PSS/CCN

Référence :
ANSSI-CC-NOTE-23_v1.0

NOTE D'APPLICATION

DECISION SUR LA SECURITE ALGORITHMIQUE RESIDUELLE (« REMAINING STRENGTH »)

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	12/03/2019	Création
0.2	26/07/2019	Prise en compte des remarques des développeurs.
1.0	29/11/2019	Signature du document

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

1.1. Objet

Cette note vise à déterminer la sécurité algorithmique résiduelle (« *remaining strength* ») d'un mécanisme en deçà de laquelle une évaluation mène au verdict Echec au sein du schéma français. Elle concerne les évaluations Critères Communs (CC) et les évaluations selon la Certification de sécurité de premier niveau (CSPN).

1.2. Références

[CEM] *Common Methodology for Information Technology Security Evaluation*, version en vigueur.

[CER] Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, 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.

1.3. Périmètre

La sécurité apportée par un algorithme cryptographique dépend de la longueur de la clé utilisée. Les différents types d'attaques cryptographiques (attaques à clair connu, attaques à clair choisi, attaques par canaux auxiliaires, attaques par fautes, etc.) visent le plus souvent à récupérer l'intégralité ou une partie de la clé. Dans le cas où, à l'issue d'une attaque par canaux auxiliaires ou par fautes, seule une partie de la clé est trouvée, l'évaluateur doit déterminer la sécurité algorithmique résiduelle, i.e. la difficulté pour un attaquant de retrouver l'intégralité de la clé ou d'une clé équivalente à partir de la valeur partielle déjà obtenue.

La pratique actuelle consiste généralement à coter l'identification de la clé complète dans la limite du nombre de points correspondant au niveau AVA_VAN visé (potentiel d'attaque), mais aucune règle n'est définie ni dans les référentiels ([CEM]), ni au niveau international permettant d'harmoniser cette cotation entre les CESTI et d'un schéma à l'autre.

2. Décision sur la sécurité algorithmique résiduelle (« *remaining strength* »)

Afin d'homogénéiser les cotations de telles attaques, la règle suivante devra désormais être appliquée lors des évaluations réalisées dans le schéma français : si à l'issue des tests de pénétration du CESTI, la complexité de la finalisation de l'attaque est équivalente ou inférieure à 2^{70} invocations de l'algorithme cryptographique considéré (DES, AES, exponentiation modulaire, multiplication scalaire, etc.), le coût de l'effort de recherche de l'information résiduelle doit être considéré comme nul.