Groupe de travail Réseau
Request for Comments : 2410
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

R. Glenn, NIST
S. Kent, BBN Corp
novembre 1998

Algorithme de chiffrement NULL et son utilisation avec IPsec

Résumé
Le présent mémoire définit l'algorithme de chiffrement NULL et son utilisation avec l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IPsec. NULL ne fait rien pour altérer les données de texte en clair. En fait, NULL, par lui-même, ne fait rien. NULL donne le moyen à ESP de fournir l'authentification et la protection de l'intégrité sans celle de la confidentialité.

Plus d'informations sur les autres composants nécessaires pour les mises en œuvre de ESP sont fournies dans [RFC2406] et [RFC2411].

1. Introduction

Le présent mémoire définit l'algorithme de chiffrement NULL et son utilisation avec l'encapsulation de charge utile de sécurité (ESP) IPsec [RFC2406] pour fournir l'authentification et la protection de l'intégrité sans la confidentialité.

NULL est un chiffrement de bloc dont l'origine se perd dans la nuit des temps. En dépit de rumeurs comme quoi l'Agence National de Sécurité aurait supprimé la publication de cet algorithme, il n'y a aucune preuve d'une telle action de sa part. Il y aurait plutôt des preuves archéologiques récentes qui suggèrent que l'algorithme NULL a été développé à l'époque romaine, comme solution de remplacement exportable aux chiffrements de César. Cependant, comme les chiffres romains n'ont pas de symbole pour zéro, les traces écrites du développement de l'algorithme ont été perdues pour les historiens pendant près de deux millénaires.

La [RFC2406] spécifie l'utilisation d'un algorithme de chiffrement facultatif pour assurer la confidentialité et l'utilisation d'un algorithme d'authentification pour assurer l'authentification et la protection de l'intégrité. L'algorithme de chiffrement NULL est une façon pratique de représenter l'option de ne pas appliquer de chiffrement. Ceci est appelé ESP_NULL dans la [RFC2408].

La spécification de l'en-tête d'authentification IPsec [RFC2402] fournit un service similaire, en calculant les données d'authentification qui couvrent la portion de données d'un paquet ainsi celle qui est intangible dans les portions en transit de l'en-tête IP. ESP_NULL n'inclut pas l'en-tête IP dans le calcul des données d'authentification. Cela peut être utile pour fournir les services IPsec à travers des appareils de réseau non IP. La discussion de la façon dont ESP_NULL pourrait être utilisé avec des appareils de réseau non IP sort du domaine d'application du présent document.

Dans le présent mémoire, NULL est utilisé dans le contexte de ESP. Pour plus d'informations sur la façon dont les diverses pièces de ESP s'assemblent pour fournir des services de sécurité, se référer à la [RFC2406] et à la [RFC2411].

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

2. Définition de l'algorithme

NULL est défini mathématiquement par l'utilisation de la fonction Identité I appliquée à un bloc de données b tel que :

NULL(b) = I(b) = b

2.1 Matériel de clés

Comme les autres chiffrements modernes, par exemple, RC5 [RFC2040], l'algorithme de chiffrement NULL peut faire usage de clés de longueurs variables. Cependant, aucun accroissement mesurable de la sécurité n'est apporté par l'usage de plus grandes longueurs de clé.

2.2 Synchronisation cryptographique

À cause de la nature sans état de l'algorithme de chiffrement NULL, il n'est pas nécessaire de transmettre un vecteur d'initialisation (IV) ou de données de synchronisation cryptographique similaires paquet par paquet (ou même par SA). L'algorithme de chiffrement NULL combine beaucoup des meilleures caractéristiques des chiffrements de bloc et de flux, tout en exigeant pas la transmission d'un IV ou de données de synchronisation cryptographique analogiques.

2.3 Bourrage

NULL a une taille de bloc de 1 octet, et donc, le bourrage n'est pas nécessaire.

2.4 Performances

L'algorithme de chiffrement NULL est significativement plus rapide que les autres algorithmes de chiffrement symétriques couramment utilisés et les mises en œuvre de l'algorithme de base sont disponibles sur tous les matériels et plates-formes de système d'exploitation couramment utilisés.

2.5 Vecteurs d'essai

Voici un ensemble de vecteurs d'essai pour faciliter le développement de mises en œuvre NULL interopérables .

cas_d'essai = 1
données = 0x123456789abcdef
longueur_des_données = 8
données_NULL = 0x123456789abcdef

cas_d'essai = 2
données = "Les gens de la sécurité des réseau ont un étrange sens de l'humour"
longueur_des_données = 53
données_NULL = "Les gens de la sécurité des réseau ont un étrange sens de l'humour"

3. Exigences pour le fonctionnement de ESP_NULL

ESP_NULL est défini par l'utilisation de NULL dans le contexte de ESP. La présente section définit ESP_NULL en mentionnant les exigences des paramètres opérationnels particuliers.

Pour les besoins de l'extraction de clé IKE [RFC2409], la taille de clé pour cet algorithme DOIT être de zéro (0) bit, pour faciliter l'interopérabilité et pour éviter tout problème potentiel de contrôle d'exportation.

Pour faciliter l'interopérabilité, la taille d'IV pour cet algorithme DOIT être zéro (0) bit.

Un bourrage PEUT être inclus dans les paquets sortants, comme spécifié dans la [RFC2406].

4. Considérations pour la sécurité

L'algorithme de chiffrement NULL n'offre par de protection de la confidentialité ni aucun autre service de sécurité. Il est simplement une façon pratique de représenter l'utilisation facultative de l'application du chiffrement au sein de ESP. ESP peut alors être utilisé pour assurer l'authentification et la protection de l'intégrité sans la confidentialité. À la différence de AH, ces services ne sont appliqués à aucune partie de l'en-tête IP. Au moment de la rédaction du présent mémoire, il n'y a aucune preuve que la prise en charge de ESP_NULL soit moins sûre que AH lorsque on utilisé le même algorithme d'authentification (c'est-à-dire, un paquet sécurisé en utilisant ESP_NULL avec un algorithme d'authentification est aussi sûr cryptographiquement qu'un paquet sécurisé en utilisant AH avec le même algorithme d'authentification).

Comme mentionné dans la [RFC2406], bien que l'utilisation des algorithmes de chiffrement et des algorithmes d'authentification soit facultative dans ESP, il est impératif qu'une SA ESP spécifie l'utilisation d'au moins un algorithme de chiffrement cryptographiquement fort ou un algorithme d'authentification cryptographiquement fort ou un de chaque.

Au moment de la rédaction du présent mémoire, il n'y a pas de loi connue qui empêche l'exportation de NULL avec une longueur de clé de zéro (0) bit.

5. Droits de propriété intellectuelle

Conformément aux dispositions de la [RFC2026], les auteurs déclarent qu'ils n'ont divulgué l'existence d'aucun brevet ou droit de propriété intellectuelle dans cette contribution qui soit raisonnablement et personnellement connu des auteurs. Les auteurs ne prétendent pas connaître personnellement tous les propriétaires potentiellement pertinents et les droits de propriété intellectuelle détenus ou revendiqués par les organisations qu'ils représentent ou de tiers.

6. Remerciements

Steve Bellova suggéré et fourni le texte de la section Droits de propriété intellectuelle.

Il est aussi nécessaire de mettre au crédit des participants à l'atelier d'interopérabilité IPsec & IKE Cisco/ICSA de mars 1998 que c'est là que l'idée de la nécessité du présent document est apparue.

7. Références

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303*)*

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Remplacée par* RFC6071*)*

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306*)*

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306*)*

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. *(Remplace* RFC1602, RFC1871) (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378, RFC6410)

[RFC2040] R. Baldwin et R. Rivest, "Algorithmes RC5, RC5-CBC, RC5-CBC-Pad, et RC5-CTS", octobre 1996. *(Information)*

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

6. Adresse des éditeurs

Rob Glenn
NIST
mél : rob.glenn@nist.gov

Stephen Kent
BBN Corporation
mél : kent@bbn.com

Le groupe de travail IPsec peut être contacté par ses présidents :

Robert Moskowitz
ICSA
mél : rgm@icsa.net

Ted T'so
Massachusetts Institute of Technology
mél : tytso@mit.edu

7. Déclaration complète de droits de reproduction