Groupe de travail Réseau
Request for Comments : 2085
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

M. Oehler, NSA
R. Glenn, NIST
février 1997

Authentification IP HMAC-MD5 avec prévention de la répétition

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit une transformation de clés MD5 à utiliser en conjonction avec l'en-tête d'authentification IP de la [RFC1826]. Cette transformation se fonde sur HMAC-MD5 [RFC2104]. Une option est aussi spécifiée pour se protéger des attaques en répétition.

Table des matières

1. Introduction....1
1.1 Terminologie....1
1.2 Clés....2
1.3 Taille des données....2
2. Format de paquet....2
2.1 Prévention de la répétition....2
2.2 Calcul des données d'authentification....3
3. Considérations pour la sécurité....3

1. Introduction

L'en-tête d'authentification (AH) de la [RFC1826] fournit l'intégrité et l'authentification des datagrammes IP. La transformation spécifiée dans le présent document utilise le mécanisme MD5 à clés de la [RFC2104]. Le mécanisme utilise la fonction de hachage MD5 (sans clé) de la [RFC1321] qui produit un résumé de message. Lorsque il est combiné avec une clé AH, les données d'authentification sont produites. Cette valeur est placée dans le champ Données d'authentification de l'AH [RFC0826]. Cette valeur est aussi la base du service d'intégrité des données offert par le protocole AH.

Pour fournir la protection contre les attaques en répétition, un champ Prévention de répétition est inclus comme option de transformation. Ce champ est utilisé pour aider à empêcher les attaques dans lesquelles un message est mémorisé et réutilisé plus tard, en remplaçant ou en répétant l'original. L'indice de paramètre de sécurité (SPI, *Security Parameter Index*) de la [RFC1825] est utilisé pour déterminer si cette option est incluse dans l'AH.

On supposera que les documents suivants sont familiers au lecteur : "Architecture de sécurité pour le protocole Internet" [RFC1825], "En-tête d'authentification IP" [RFC1826], et "HMAC-MD5 : MD5 à clés pour l'authentification de message" [RFC2104].

Toute mise en œuvre qui revendique la conformité à la spécification d'en-tête d'authentification IP [RFC1826] DOIT mettre en œuvre cette transformation HMAC-MD5.

1.1 Terminologie

Dans ce document, les mots qui sont utilisés pour définir la signification de chaque exigence particulière sont généralement en majuscules. Ces mots sont :

- DOIT
Ce mot ou le participe "EXIGÉ" signifie que l'élément est une exigence absolue de la spécification.

- DEVRAIT
Ce mot ou le participe "RECOMMANDÉ" signifie qu'il peut exister des raisons valables dans des circonstances

particulières pour ignorer cet élément, mais toutes les implications devraient en être comprises et le cas devrait être soupesé avec soin avant de prendre une voie différente.

1.2 Clés

La "clé d'AH" est utilisée comme secret partagé entre deux parties à une communication. La clé n'est pas une "clé de chiffrement" comme on en utilise au sens traditionnel. La clé AH (secret partagé) est plutôt hachée avec les données transmises et donc elle assure qu'un tiers intervenant ne peut pas dupliquer les données d'authentification.

Même si une clé d'AH n'est pas une clé de chiffrement, les problèmes de base des clés de chiffrement s'appliquent. Considérons que l'algorithme et la plus grande partie des données utilisées pour produire le résultat sont connus. La force de la transformation réside dans la transposition particulière de la clé (qui doit être forte) et du datagramme IP (qui est connu) en données d'authentification. Donc, les mises en œuvre devraient, aussi souvent que possible, changer la clé d'AH. Les clés doivent être choisies au hasard, ou générées en utilisant un générateur pseudo aléatoire cryptographiquement fort avec un germe aléatoire [RFC2104]

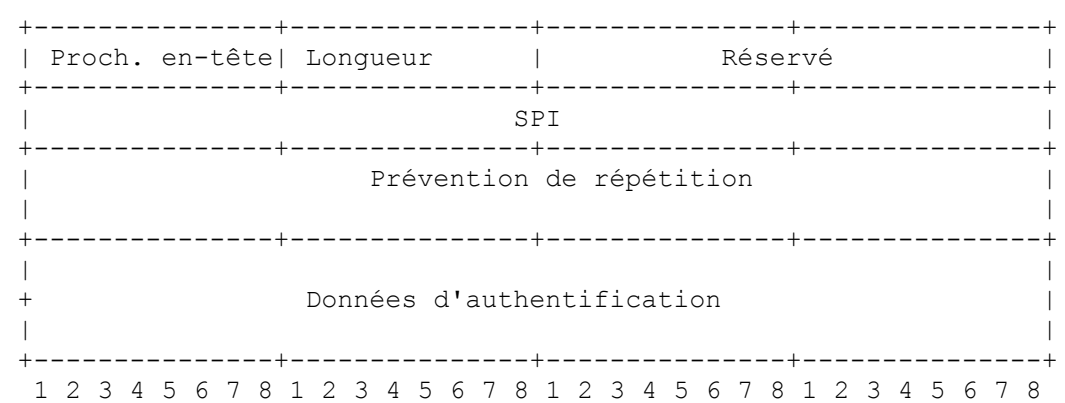
Toute mise en œuvre conforme DOIT prendre en charge une longueur de clé de 128 bits ou moins. Les mises en œuvre DEVRAIENT prendre aussi en charge des longueurs de clé supérieures. Il est recommandé que la longueur de la clé soit choisie comme étant celle du résultat du hachage, qui est 128 bits pour MD5. Pour les autres longueurs de clé, les considérations suivantes DOIVENT être prises en compte :

- Une longueur de clé de zéro est interdite et les mises en œuvre DOIVENT empêcher que des clés de longueur zéro soient utilisées avec cette transformation, car aucune authentification efficace ne pourrait être fournie par une clé de longueur zéro.
- Les clés qui ont une longueur inférieure à 128 bits sont fortement déconseillées car elle diminueraient la force de la sécurité de la fonction.
- Les clés de plus de 128 bits sont acceptables, mais la longueur supplémentaire peut ne pas accroître de façon significative la force de la fonction.
- Une clé plus longue peut être conseillées si le caractère aléatoire de la clé est suspect.
- MD5 fonctionne sur des blocs de 64 octets. Les clés de plus de 64 octets sont d'abord hachées en utilisant MD5. Le hachage résultant est ensuite utilisé pour calculer les données d'authentification.

1.3 Taille des données

MD5 produit une valeur de 128 bits qui est utilisée comme données d'authentification. Elle est naturellement verrouillée sur 64 bits et n'a donc besoin d'aucun bourrage pour les machines avec des doubles mots d'origine.

2. Format de paquet



Les champs Prochain en-tête, Réservé, et SPI sont spécifiés dans la [RFC1826]. Le champ Longueur donne la longueur du champ Prévention de répétition et du champ Données d'authentification en mots de 32 bits.

2.1 Prévention de la répétition

Le champ Prévention de répétition est une valeur de 64 bits utilisée pour garantir que chaque paquet échangé entre deux parties est différent. Chaque association de sécurité IPsec spécifie si la prévention de la répétition est utilisée pour cette association de sécurité. Si la prévention de répétition N'EST PAS utilisée, le champ Données d'authentification va suivre

directement le champ SPI.

Le champ de 64 bits est un compteur ascendant qui commence à 1.

La clé secrète partagée ne doit pas être utilisée pendant une durée qui permette au compteur de revenir à zéro, c'est à dire, d'émettre plus de 2^64 paquets en utilisant une seule clé.

À réception, la valeur de répétition est forcément croissante. La mise en œuvre peut accepter les paquets décalés. Le nombre de paquets décalés à accepter est un détail de mise en œuvre. Si une "fenêtre de décalage" est prise en charge, la mise en œuvre devra s'assurer que tout paquet accepté décalé n'est pas arrivé précédemment. C'est-à-dire que la mise en œuvre n'acceptera chaque paquet qu'une seule fois.

Lorsque l'adresse de destination est une adresse de diffusion groupée, si la protection contre la répétition est utilisée, et si plus d'un envoyeur partage la même association de sécurité IPsec pour cette adresse de destination de diffusion groupée, la protection contre la répétition NE DEVRAIT PAS être activée. Lorsque on désire la protection contre la répétition pour une session de diffusion groupée qui a plusieurs envoyeurs à la même adresse de destination de diffusion groupée, chaque envoyeur DEVRAIT avoir sa propre association de sécurité IPsec.

[ESP-DES-MD5] donne des exemples du code qui met en œuvre une fenêtre de répétition de 32 paquets et un sous programme d'essais pour montrer comment il fonctionne.

2.2 Calcul des données d'authentification

Les données d'authentification sont le résultat de l'algorithme d'authentification (MD5). Cette valeur est calculée sur le datagramme IP entier. Les champs qui sont variables au sein du datagramme durant le transit et le champ Données d'authentification lui-même, doivent ne contenir que des zéros avant le calcul [RFC1826]. Le champ Prévention de répétition, s'il est présent, est inclus dans ce calcul.

La définition et la mise en œuvre de référence de MD5 apparaîssent dans la [RFC1321]. Notons "text" les données auxquelles HMAC-MD5 doit être appliqué et "K" la clé secrète d'authentification du message partagée par les parties. Si K est plus long que 64 octets, il DOIT d'abord être haché en utilisant MD5. Dans ce cas, K est le hachage résultant.

On définit deux chaînes fixes différentes ipad et opad comme suit (le 'i' et le 'o' sont des mnémoniques pour interne et externe) :

ipad = l'octet 0x36 répété 64 fois
opad = l'octet 0x5C répété 64 fois.

Pour calculer HMAC-MD5 sur les données "text", on fait l'opération

MD5(K XOR opad, MD5(K XOR ipad, text))

à savoir ,

(1) ajouter des zéros à la fin de K pour créer une chaîne de 64 octets (par exemple, si K fait 16 octets, on va lui ajouter 48 octets de zéro 0x00) ;
(2) XOR (opération OU exclusif au bit près) la chaîne de 64 octets calculée à l'étape (1) avec ipad ;
(3) ajouter le flux de données "text" à la chaîne de 64 octets résultant de l'étape (2) ;
(4) appliquer MD5 au flux généré à l'étape (3) ;
(5) XOR (opération OU exclusif au bit près) la chaîne de 64 octets calculée à l'étape (1) avec opad ;
(6) ajouter le résultat MD5 de l'étape (4) à la chaîne de 64 octets résultant de l'étape (5) ;
(7) appliquer MD5 au flux généré à l'étape (6) et sortir le résultat.

Ce calcul est décrit plus en détails, avec des exemples de code et des améliorations de performances, dans la [RFC2104]. Pour la mise en œuvre, on devrait consulter la [RFC2104] qui donne plus d'informations sur cette technique pour la fonction de hachage de clés de chiffrement.

3. Considérations pour la sécurité

La sécurité apportée par cette transformation se fonde sur la force de MD5, la justesse de la mise en œuvre de l'algorithme, la sécurité du mécanisme de gestion de clés et sa mise en œuvre, la force de la clé secrète associée, et la justesse de la mise en œuvre de tous les systèmes participants. [RFC2104] contient un exposé détaillé des forces et faiblesses de MD5.

Remerciements

Le présent document s'appuie largement sur le texte rédigé par Hugo Krawczyk. Le format utilisé est dérivé des travaux de William Simpson et Perry Metzger. Le texte sur la prévention des répétitions est directement dérivé des travaux de Jim Hughes.

Références

[RFC1825] R. Atkinson, "Architecture de sécurité pour le protocole Internet", RFC 1825, août 1995. *(Rendue obsolète par la RFC2401)*
[RFC1826] R. Atkinson, "En-tête d'authentification IP", RFC 1826, août 1995. *(Rendue obsolète par la RFC2402)*
[RFC1828] P. Metzger et W. Simpson, "Authentification IP avec du MD5 à clés", août 1995.
[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*
[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", , février 1997.
[ESP-DES-MD5] Hughes, J., "Combined DES-CBC, MD5, and Replay Prevention Security Transform", Travail en cours.

Adresse des auteurs

Michael J. Oehler
National Security Agency
Atn: R23, INFOSEC Research and Development
9800 Savage Road
Fort Meade, MD 20755
mél : mjo@tycho.ncsc.mil

Robert Glenn
NIST
Building 820, Room 455
Gaithersburg, MD 20899
mél : rob.glenn@nist.gov