

Groupe de travail Réseau  
**Request for Comments : 2403**  
Catégorie : En cours de normalisation  
Traduction Claude Brière de L'Isle

C. Madson, Cisco Systems Inc.  
R. Glenn, NIST  
novembre 1998

## Utilisation de HMAC-MD5-96 au sein de ESP et AH

### Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet 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.

### Notice de Copyright

Copyright (C) The Internet Society (1998). Tous droits réservés.

### Résumé

Le présent mémoire décrit l'utilisation de l'algorithme HMAC [RFC2104] en conjonction avec l'algorithme MD5 [RFC1321] comme mécanisme d'authentification au sein de l'encapsulation de charge utile de sécurité IPSEC révisée [RFC2406] et de l'en-tête d'authentification IPsec révisé [RFC2402]. HMAC avec MD5 fournit l'authentification de l'origine des données et la protection de l'intégrité.

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

## 1. Introduction

Le présent mémoire spécifie l'utilisation de MD5 [RFC1321] combiné avec HMAC [RFC2104] comme mécanisme d'authentification par clé dans le contexte de l'encapsulation de charge utile de sécurité et de l'en-tête d'authentification. Le but de HMAC-MD5-96 est d'assurer que le paquet est authentique et ne peut pas être modifié dans le transit.

HMAC est un algorithme d'authentification par clé secrète. L'intégrité des données et l'authentification de l'origine des données fournies par HMAC dépendent de la portée de la distribution de la clé secrète. Si seules la source et la destination connaissent la clé HMAC, cela assure à la fois l'authentification de l'origine des données et la protection de l'intégrité des données pour les paquets envoyés entre les deux parties ; si le HMAC est correct, cela prouve qu'il doit avoir été ajouté par la source.

Dans le présent mémoire, HMAC-MD5-96 est utilisé au sein du contexte de ESP et AH. Pour plus d'informations sur la façon dont les diverses pièces de ESP – y compris le mécanisme de confidentialité – s'assemblent pour assurer les services de sécurité, se référer à la [RFC2406] et la [RFC2411]. Pour plus d'informations sur AH, se référer à la [RFC2402] et 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. Algorithme et mode

La [RFC1321] décrit l'algorithme MD5 sous-jacent, tandis que la [RFC2104] décrit l'algorithme HMAC. L'algorithme HMAC fournit un cadre pour insérer divers algorithmes de hachage, tels que MD5.

HMAC-MD5-96 opère sur des blocs de données de 64 octets de données. Les exigences de bourrage sont spécifiées dans la [RFC1321] et font partie de l'algorithme MD5. Si MD5 est construit conformément à la [RFC1321], il n'est pas besoin d'ajouter de bourrage supplémentaire pour autant que HMAC-MD5-96 est concerné. À l'égard du "bourrage implicite de paquet" défini dans la [RFC2402], aucun bourrage implicite de paquet n'est requis.

HMAC-MD5-96 produit une valeur d'authentifiant de 128 bits. Cette valeur de 128 bits peut être tronquée comme décrit dans la RFC2104. Pour l'utiliser avec ESP ou AH, une valeur tronquée en utilisant les 96 premiers bits DOIT être acceptée. À l'envoi, la valeur tronquée est mémorisée au sein du champ authentificateur. À réception, la valeur entière de 128 bits est

calculée et les 96 premiers bits sont comparés à la valeur mémorisée dans le champ authentificateur. Aucune autre longueur de valeur d'authentificateur n'est acceptée par HMAC-MD5-96.

La longueur de 96 bits a été choisie parce que c'est la longueur d'authentificateur par défaut, comme spécifié dans la [RFC2402] et qu'elle satisfait aux exigences de sécurité décrites dans la [RFC2104]

## 2.1 Performance

[Bellare96a] écrit que "les performances (de HMAC) sont essentiellement celles de la fonction de hachage sous-jacente". La [RFC1810] donne des analyses de performances et des recommandations sur l'utilisation de MD5 avec les protocoles de l'Internet. Au moment de la rédaction de cette note, aucune analyse de performances n'a été faite de HMAC ou de HMAC combiné avec MD5.

La [RFC2104] présente une modification de mise en œuvre qui peut améliorer les performances par paquet sans affecter l'interopérabilité.

## 3. Matériel de clés

HMAC-MD5-96 est un algorithme à clé secrète. Bien qu'aucune longueur fixe de clé ne soit spécifiée dans la [RFC2104], une longueur de clé fixée à 128 bits DOIT être prise en charge dans les utilisations avec ESP ou AH. Les longueurs de clé autres que 128 bits NE DOIVENT PAS être acceptées (c'est à dire que seules les clés de 128 bits sont utilisées par HMAC-MD5-96). La longueur de clé de 128 bits a été choisie sur la base des recommandations de la [RFC2104] (c'est-à-dire que des longueurs de clé inférieures à la longueur de l'authentificateur diminuent la force de la sécurité, et les clés plus longues que l'authentificateur n'augmentent pas la force de la sécurité de façon significative).

La [RFC2104] expose les exigences pour le matériel de clés, et elle inclut une discussion sur les exigences d'un aléa fort. Une fonction pseudo-aléatoire forte DOIT être utilisée pour générer la clé de 128 bits requise.

Au moment de la rédaction du présent mémoire, il n'y a pas de clés faibles spécifiées avec HMAC. Cela ne signifie pas qu'il n'existe pas de clés faibles. Si, à un moment quelconque, un ensemble de clés faibles était identifié pour HMAC, l'utilisation de ces clés faibles devra être rejetée et suivie par une demande de clés de remplacement ou d'une nouvelle négociation d'association de sécurité (SA, *Security Association*).

La [RFC2401] décrit le mécanisme général pour obtenir du matériel de clés lorsque plusieurs clés sont requises pour une seule SA (par exemple, lorsque une SA ESP demande une clé pour la confidentialité et une clé pour l'authentification).

Afin d'assurer l'authentification de l'origine des données, le mécanisme de distribution des clés doit assurer que des clés uniques sont allouées et qu'elles ne sont distribuées qu'aux parties qui participent à la communication.

La [RFC2104] fait les recommandations suivantes à l'égard du changement de clés. Les attaques connues n'indiquent pas qu'il faille recommander une fréquence spécifique pour les changements de clé car ces attaques sont pratiquement infaisables. Cependant, un rafraîchissement périodique des clés est une pratique fondamentale de sécurité qui aide à surmonter les faiblesses potentielles de la fonction et des clés, qui réduit les informations disponibles pour un cryptanalyste, et limite les dommages causés par l'exposition d'une clé.

## 4. Interaction avec le mécanisme de chiffrement d'ESP

Au moment de la rédaction de la présente note, il n'y a pas de problème connu qui empêche l'utilisation de l'algorithme HMAC-MD5-96 avec aucun algorithme de chiffrement spécifique.

## 5. Considérations pour la sécurité

La sécurité assurée par HMAC-MD5-96 se fonde sur la force de HMAC, et à un moindre degré, sur la force de MD5. La [RFC2104] affirme que HMAC ne dépend pas de la propriété de forte résistance à la collision, qu'il est important de considérer quand on évalue l'utilisation de MD5, un algorithme qui s'est, selon des examens récents, révélé beaucoup moins résistant aux collisions qu'il n'était pensé au premier abord. Au moment de la rédaction de la présente note, il n'y a pas eu d'attaque cryptographique pratiquée contre HMAC-MD5-96.

La [RFC2104] déclare que pour des "fonctions de hachage raisonnablement minimalistes", "l'attaque de l'anniversaire", qui est la plus forte attaque connue contre HMAC, est impraticable. Pour un hachage de bloc de 64 octets tels que celui de HMAC-MD5-96, une attaque impliquant le traitement réussi de  $2^{**64}$  blocs serait infaisable sauf à découvrir que le hachage sous-jacent a des collisions après le traitement de  $2^{**30}$  blocs. Un hachage avec une aussi faible résistance aux collisions serait généralement considéré comme inutilisable.

Il est aussi important de considérer qu'alors que MD5 n'a jamais été développé pour être utilisé comme algorithme de hachage à clé, HMAC avait ce critère depuis le début. Bien que l'utilisation de MD5 dans le contexte de la sécurité des données soit en cours de réévaluation, la combinaison de HMAC avec l'algorithme MD5 a soutenu avec succès les épreuves cryptographiques.

La [RFC2104] discute aussi la sécurité additionnelle potentielle qui est fournie par la troncature du hachage résultant. Les spécifications qui incluent HMAC sont vivement encouragées à effectuer cette troncature du hachage.

Comme la [RFC2104] fournit un cadre pour incorporer divers algorithmes de hachage avec HMAC, il est possible de remplacer MD5 par d'autres algorithmes tels que SHA-1. La [RFC2104] contient un exposé détaillé sur les forces et les faiblesses des algorithmes de HMAC.

Comme il est vrai de tous les algorithmes cryptographiques, une partie de sa force réside dans la bonne mise en œuvre de l'algorithme, la sécurité du mécanisme et de la mise en œuvre de la gestion de clés, la force de la clé secrète associée, et de la correction de la mise en œuvre dans tous les systèmes participants. La [RFC2202] contient les vecteurs d'essai et un exemple de code pour aider à vérifier que le code de HMAC-MD5-96 est correct.

## 6. Remerciements

Ce document découle en partie de travaux précédents de Jim Hughes, et des gens qui ont travaillé avec Jim sur les transformations combinées de DES/CBC-MD5 ESP, des participants au groupe ANX, et des membres du groupe de travail IPsec.

Nous souhaitons aussi remercier Hugo Krawczyk de ses commentaires et recommandations en ce qui concerne le teste cryptographique spécifique de ce document.

## 7. Références

- [Bellare96a] Bellare, M., Canetti, R., and H. Krawczyk, "Keying Hash Functions for Message Authentication", Advances in Cryptography, Crypto96 Proceeding, juin 1996.
- [RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992. (*Information*)
- [RFC1810] J. Touch, "Rapport sur les performances de MD5", juin 1995. (*Information*)
- [RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : [Hachage de clés pour l'authentification](#) de message", février 1997.
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2202] P. Cheng et R. Glenn, "Cas d'essai pour HMAC-MD5 et HMAC-SHA-1", septembre 1997. (*Information*)
- [RFC2401] S. Kent et R. Atkinson, "[Architecture de sécurité](#) pour le protocole Internet", novembre 1998. (*Obsolète, voir RFC4301*)
- [RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir RFC4302, 4305*)
- [RFC2406] S. Kent et R. Atkinson, "Encapsulation de [charge utile de sécurité](#) IP (ESP)", novembre 1998. (*Obsolète, voir RFC4303*)
- [RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "[Feuille de route pour la sécurité](#) sur IP", novembre 1998. (*Remplacée par RFC6071*)

## 8. Adresse de l'éditeur

Cheryl Madson  
Cisco Systems, Inc.  
mél : cmadson@cisco.com

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

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

## 9. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1998). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les copyrights définis dans les processus de normes pour Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.