Groupe de travail Réseau
**Request for Comments : 2857**

Catégorie : En cours de normalisation

A. Keromytis, University of Pennsylvania
N. Provos, Center for Information Technology Integration
juin 2000
Traduction Claude Brière de L'Isle

# Utilisation de HMAC-RIPEMD-160-96 avec ESP et AH



**Résumé**
Le présent mémoire décrit l'utilisation de l'algorithme HMAC [RFC 2104] en conjonction avec l'algorithme RIPEMD-160 [ISO10118] comme mécanisme d'authentification au sein de l'encapsulation de charge utile de sécurité de IPSEC révisé [RFC2406] et de l'en-tête d'authentification d'IPSEC révisé [RFC2402]. HMAC avec RIPEMD-160 fournit l'authentification de l'origine des données et la protection de l'intégrité.

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

## 1. Introduction

Le présent mémoire spécifie l'utilisation de RIPEMD-160 [ISO10118] combiné avec HMAC [RFC2104] comme mécanisme d'authentification chiffré au sein du contexte de l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) et de l'en-tête d'authentification (AH, *Authentication Header*). Le but de HMAC-RIPEMD-160-96 est de s'assurer que le paquet est authentique et ne peut pas être modifié dans le transit.

HMAC est un algorithme d'authentification à clé secrète. La protection de l'intégrité des données et l'authentification de l'origine des données fournies par HMAC dépend 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 ce mémoire, HMAC-RIPEMD-160-96 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 – se combinent pour fournir les services de sécurité, se référer à la [RFC2402] et la [RFC2411]. Pour plus d'informations sur AH, se référer à la [RFC2402] et la [RFC2411].

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

## 2. Algorithme et mode

La norme [ISO10118] décrit l'algorithme RIPEMD-160 sous-jacent, tandis que la [RFC 2104] décrit l'algorithme HMAC. L'algorithme HMAC fournit un cadre pour l'insertion de divers algorithmes de hachage tels que RIPEMD-160.

HMAC-RIPEMD-160-96 fonctionne sur des blocs de données de 64 octets. Les exigences de bourrage sont spécifiées dans la norme [ISO10118] et font partie de l'algorithme RIPEMD-160. Les bits de bourrage ne sont nécessaires que pour le calcul de la valeur d'authentification du HMAC-RIPEMD-160 et NE DOIVENT PAS être inclus dans le paquet.

HMAC-RIPEMD-160-96 produit une valeur d'authentification de 160 bits. Cette valeur de 160 bits peut être tronquée comme décrit dans la RFC2104. Pour être utilisée avec ESP ou AH, une valeur tronquée utilisant les 96 premiers bits DOIT

être prise en charge. À l'envoi, la valeur tronquée est mémorisée au sein du champ Authentificateur. À réception, la valeur de 160 bits entière 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-RIPEMD-160-96.

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

### 2.1 Performances

[Bellare96a] déclare que "les performances de HMAC sont essentiellement celles de la fonction de hachage sous-jacente". La norme [ISO10118] effectue des analyses de performances. Au moment de la rédaction du présent document, aucune analyse détaillée des performances n'a été effectuée de HMAC ou de HMAC combiné avec RIPEMD-160.

La [RFC 2104] mentionne une modification de mise en œuvre qui peut améliorer les performance par paquet sans affecter l'interopérabilité.

## 3. Matériel de chiffrement

HMAC-RIPEMD-160-96 est un algorithme à clé secrète. Bien qu'aucune longueur fixe de clé ne soit spécifiée dans la [RFC2104], une longueur de clé fixe de 160 bits DOIT être prise en charge pour l'utilisation avec ESP ou AH. Des longueurs de clé autres que 160 bits NE DEVRONT PAS être acceptées. Une longueur de clé de 160 bits a été choisie sur la base des recommandations de la [RFC2104] (c'est-à-dire que des longueurs de clé de moins que la longueur de l'authentificateur diminuent la force de la sécurité et des clés plus longues que la longueur de l'authentificateur n'augmentent pas significativement la force de la sécurité).

La [RFC 2104] expose les exigences pour le matériel de chiffrement, qui incluent un exposé sur les exigences d'une forte aléation. Une fonction pseudo aléatoire forte DOIT être utilisée pour générer la clé de 160 bits requise. Les mises en œuvre devraient se référer à la RFC1750 pour les lignes directrices sur les exigences pour de telles fonctions.

Au moment de la rédaction du présent document, aucune clé faible n'est spécifiée pour être utilisée avec HMAC. Cela ne signifie pas qu'il n'existe pas de clés faibles. Si, à un moment, un ensemble de clés faibles était identifié pour HMAC, l'utilisation de ces clés faibles devrait être rejetée, suivie par une demande de clés de remplacement ou d'une nouvelle négociation d'association de sécurité.

La [RFC2406] décrit le mécanisme général pour obtenir le matériel de chiffrement pour la transformation ESP. La déduction de la clé d'une certaine quantité de matériel de chiffrement n'est pas différente entre les mécanismes manuel et automatique de gestion de clé.

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 [RFC 2104] déclare que pour des "fonctions de hachage raisonnablement minimales" l'attaque de "l'anniversaire" est impraticable. Pour un hachage de bloc de 64 octets tel que HMAC-RIPEMD-160-96, une attaque impliquant le traitement réussi de 2**64 blocs serait infaisable sauf si on découvrait que le hachage sous-jacent produisait des collisions après le traitement de 2**30 blocs. (Un hachage ayant d'aussi faibles caractéristiques de résistance aux collisions serait généralement considéré comme inutilisable.) Aucune attaque fondée sur la durée n'est discutée dans ce document.

Bien qu'il soit cryptographiquement prudent d'effectuer de fréquents changements de clés, la littérature actuelle ne comporte pas de durée de vie recommandée des clés pour HMAC-RIPEMD. Lorsque des recommandations pour la durée de vie des clés HMAC-RIPEMD deviendront disponibles, elles seront incluses dans une version révisée de ce document.

## 4. Interaction avec le mécanisme de chiffrement ESP

Au moment de la rédaction, il n'y a pas de problème connu qui empêche l'utilisation de l'algorithme HMAC-RIPEMD-160-96 avec un algorithme de chiffrement spécifique.

## 5. Considérations pour la sécurité

La sécurité fournie par HMAC-RIPEMD-160-96 se fonde sur la force de HMAC, et à un moindre degré, sur la force de RIPEMD-160. Au moment de la rédaction, il n'y a pas d'attaque cryptographique pratique connue contre RIPEMD-160.

Il est aussi important de considérer qu'alors que RIPEMD-160 n'a jamais été développé pour être utilisé comme algorithme de hachage chiffré, HMAC avait ce critère depuis le début.

La [RFC2104] expose aussi la sécurité supplémentaire potentielle qui est fournie par la troncature du hachage résultant. Les spécifications qui incluent HMAC sont fortement invitées 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 RIPEMD-160 par d'autres algorithmes tels que SHA-1. La [RFC2104] contient un exposé détaillé sur les forces et les faiblesses des algorithmes HMAC.

Comme il est vrai de tout algorithme cryptographique, une partie de sa force réside dans la correction de sa mise en œuvre, dans la sécurité du mécanisme de gestion de la clé et de sa mise en œuvre, dans la force de la clé secrète associée, et dans la correction de la mise en œuvre de tous les systèmes participants. La [RFC2286] contient des vecteurs d'essai et des exemples de code pour aider à vérifier la correction du code HMAC-RIPEMD-160-96.

## 6. Remerciements

Le présent document a bénéficié des apports des travaux de C. Madson et R. Glenn et de travaux antérieurs de Jim Hughes, et des personnes qui ont travaillé avec Jim sur les transformations combinées d'ESP DES/CBC+HMAC-MD5, des participants à la réunion ANX, et des membres du groupe de travail IPsec.

## 7. Références

[Bellare96a] Bellare, M., Canetti, R., Krawczyk, H., "Keying Hash Functions for Message Authentication", Advances in Cryptography, Crypto96 Proceeding, juin 1996.

[ISO10118] ISO/CEI 10118-3:1998, "Technologies de l'information - Techniques de sécurité - fonctions de hachage - Partie 3 : Fonctions de hachage dédiées", Organisation Internationale de Normalisation, Genève, Suisse, 1998.

[RFC1750] D. Eastlake 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Info., remplacée par la* RFC4086)

[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.

[RFC2286] J. Kapp, "Cas d'essai pour HMAC-RIPEMD160 et HMAC-RIPEMD128", février 1998. *(Information)*

[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 des auteurs

Angelos D. Keromytis
Distributed Systems Lab
Computer and Information Science Department
University of Pennsylvania
200 S. 33rd Street
Philadelphia, PA 19104 - 6389
mél : angelos@dsl.cis.upenn.edu

Niels Provos
Center for Information Technology Integration
University of Michigan
519 W. William
Ann Arbor, Michigan 48103 USA
mél : provos@citi.umich.edu

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

Robert Moskowitz
International Computer Security Association
mél : rgm@icsa.net

Ted T'so
VA Linux Systems
mél : tytso@valinux.com

## 9. Déclaration complète de droits de reproduction



**Remerciement**
Le financement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.