Groupe de travail Réseau
Request for Comments : 5304
RFC rendue obsolète : 3567
RFC mise à jour : 1195
Catégorie : En cours de normalisation

T. Li, Redback Networks, Inc.
R. Atkinson, Extreme Networks, Inc.
octobre 2008

Traduction Claude Brière de L'Isle

Authentification cryptographique IS-IS

Résumé
Le présent document décrit l'authentification des unités de données de protocole (PDU) de système intermédiaire à système intermédiaire (IS-IS) qui utilise l'algorithme de code d'authentification de message par hachage de clé – résumé de message n° 5 (HMAC-MD5, *Hashed Message Authentication Code - Message Digest 5*) tel qu'il se trouve dans la RFC 2104. IS-IS est spécifié dans la Norme Internationale 10589 de l'Organisation internationale de normalisation (ISO), avec les extensions pour la prise en charge du protocole Internet version 4 (IPv4) décrites dans la RFC 1195. La spécification de base comporte un mécanisme d'authentification qui permet plusieurs algorithmes d'authentification. La spécification de base ne spécifie que l'algorithme pour des mots de passe en clair. Le présent document remplace la RFC 3567.

Le présent document propose une extension à cette spécification permettant l'utilisation de l'algorithme d'authentification HMAC-MD5 en conjonction avec les mécanismes d'authentification existants.

Table des Matières

1. Introduction

Le protocole IS-IS, tel que spécifié dans la norme [ISO-10589], traite de l'authentification des unités de données de protocole d'état de liaison (LSP, *Link State Protocol*) par l'inclusion des informations d'authentification au titre du LSP. Ces informations d'authentification sont codées comme un tuplet de Type-Longueur-Valeur (TLV). L'utilisation de IS-IS pour les réseaux IPv4 est décrite dans la [RFC1195].

Le type de TLV est spécifié comme étant 10. La longueur du TLV est variable. La valeur du TLV dépend de l'algorithme d'authentification et des secrets en rapport qui sont utilisés. Le premier octet de la valeur est utilisé pour spécifier le type d'authentification. Le type 0 est réservé, le type 1 indique un mot de passe en clair, et le type 255 est utilisé pour les méthodes d'authentification d'acheminement de domaine privé. Le reste des valeurs de TLV est appelé la valeur d'authentification.

Le présent document étend la situation ci-dessus en allouant un nouveau type d'authentification pour HMAC-MD5 et en

spécifiant les algorithmes pour le calcul de la valeur d'authentification. Le présent document décrit aussi les modifications au protocole de base pour assurer que les mécanismes d'authentification décrits dans le présent document sont efficaces.

Le présent document est une publication du groupe de travail IS-IS de l'IETF. Il remplace la [RFC3567], qui est une RFC pour information. Le présent document est en cours de normalisation. Sa Section 3 est révisée, avec l'ajout significatif d'un exposé sur les récentes attaques contre MD5 au paragraphe 3.2. Il comporte aussi l'ajout d'une section de "Considérations relatives à l'IANA" qui crée un registre de codets qui manquait jusqu'à présent.

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

2. Procédures d'authentification

Le type d'authentification utilisé pour HMAC-MD5 est 54 (0x36). La longueur de la valeur d'authentification pour HMAC-MD5 est 16, et le champ Longueur dans le TLV est 17.

L'algorithme HMAC-MD5 exige en entrée une clé K et un texte T [RFC2104]. La clé K est le mot de passe pour le type de PDU, comme spécifié dans la norme ISO 10589. Le texte T est le PDU IS-IS à authentifier avec le champ Valeur d'authentification (à l'intérieur du TLV d'information d'authentification) réglé à zéro. Noter que le type d'authentification est réglé à 54 et la longueur du TLV est réglée à 17 avant le calcul de l'authentification. Lorsque les LSP sont authentifiés, les champs Somme de contrôle et Durée de vie restante sont réglés à zéro (0) avant le calcul de l'authentification. Le résultat de l'algorithme est placé dans le champ Valeur d'authentification.

Lors du calcul du résultat du HMAC-MD5 pour le PDU de numéro de séquence, les PDU de numéro de séquence de niveau 1 DOIVENT utiliser la chaîne d'authentification de zone comme dans les PDU d'état de liaison de niveau 1. Les PDU de numéro de séquence de niveau 2 DOIVENT utiliser la chaîne d'authentification de domaine comme dans les PDU d'état de liaison de niveau 2. Les PDU de Hello IS-IS DOIVENT utiliser la chaîne d'authentification de niveau Liaison, qui PEUT être différente de celle des PDU d'état de liaison. Le résultat du HMAC-MD5 pour les PDU de Hello IS-IS DEVRA être calculé après le bourrage du paquet à la taille de la MTU, si le bourrage n'est pas désactivé. Les mises en œuvre qui prennent en charge la somme de contrôle facultative pour les PDU de numéro de séquence et les PDU de Hello IS-IS NE DOIVENT PAS inclure le TLV de la somme de contrôle.

Pour authentifier un PDU entrant, un système devrait sauvegarder les valeurs du champ Valeur d'authentification, du champ Somme de contrôle, et du champ Durée de vie restante, régler ces champs à zéro, calculer l'authentification, puis restaurer ensuite les valeurs de ces champs.

Une mise en œuvre qui utilise l'authentification HMAC-MD5 et reçoit des informations d'authentification HMAC-MD5 DOIT éliminer la PDU si la Valeur d'authentification est incorrecte.

Une mise en œuvre PEUT avoir un mode de transition dans lequel elle inclut les informations d'authentification HMAC-MD5 dans les PDU mais ne vérifie pas les informations d'authentification HMAC-MD5. C'est une aide transitoire pour les réseaux qui sont en train de développer le processus d'authentification.

Une mise en œuvre PEUT vérifier un ensemble de mots de passe lors de la vérification de la valeur d'authentification. Cela donne un mécanisme pour changer de façon incrémentaire les mots de passe dans un réseau.

Une mise en œuvre qui n'utilise pas l'authentification HMAC-MD5 PEUT accepter une PDU qui contient le type d'authentification HMAC-MD5. Les IS (routeurs) qui mettent en œuvre l'authentification HMAC-MD5 et initient des purges de LSP DOIVENT retirer le corps du LSP et ajouter le TLV d'authentification. Les IS qui mettent en œuvre l'authentification HMAC-MD5 NE DOIVENT PAS accepter des purges non authentifiées. Les IS NE DOIVENT PAS accepter des purges qui contiennent des TLV autres que le TLM d'authentification. Ces restrictions sont nécessaires pour empêcher qu'un système hostile reçoive un LSP, règle le champ Durée de vie restante à zéro, et le diffuse, initiant par là une purge sans connaître le mot de passe d'authentification.

2.1 Considérations de mise en œuvre

Il y a un problème de mise en œuvre qui survient juste après le changement de mot de passe sur un routeur IS-IS et qui peut mériter des commentaires supplémentaires. Immédiatement après le changement du mot de passe sur le routeur, le routeur ou le processus IS-IS peut redémarrer. Si cela arrive, cela cause le redémarrage du numéro de séquence du LSP à la valeur

de 1 en utilisant le nouveau mot de passe. Cependant, les voisins vont rejeter ces nouveaux LSP parce que le numéro de séquence est plus petit. Le routeur ne peut pas augmenter sont propre numéro de séquence de LSP parce qu'il échoue à authentifier son propre vieux LSP que les voisins continuent de lui envoyer. Ainsi le routeur ne peut pas mettre à jour son numéro de séquence de LSP auprès de ses voisins jusqu'à ce que tous les voisins arrivent en fin de temporisation de tous les LSP d'origine. Une solution possible à ce problème est que le processus IS-IS détecte si un LSP entrant avec un échec d'authentification a l'identifiant de système local et a aussi un numéro de séquence supérieur à celui du processus IS-IS. Dans ce cas, le processus IS-IS DEVRAIT augmenter en conséquence son propre numéro de séquence de LSP et rediffuser les LSP. Cependant, comme ce scénario pourrait aussi être déclanché par une attaque active d'un adversaire, il est recommandé de garder un compteur de ces cas pour atténuer le risque découlant d'une telle attaque.

3. Considérations pour la sécurité

Le présent document amélioré la sécurité du protocole d'acheminement IS-IS. Comme un protocole d'acheminement contient des informations qu'il n'est pas nécessaire de garder secrètes, la confidentialité n'est pas une exigence. Cependant, l'authentification des messages au sein du protocole a un intérêt afin de réduire le risque qu'un adversaire compromette le système d'acheminement en injectant délibérément de fausses informations dans ce système.

3.1 Limitations de la sécurité

La technologie du présent document fournit un mécanisme d'authentification pour IS-IS. Le mécanisme décrit ici n'est pas parfait et n'a pas besoin d'être parfait. En fait, ce mécanisme représente une augmentation significative du travail que devra accomplir une attaque adverse contre le protocole IS-IS, tout en ne causant aucune complexité indue de mise en œuvre, de développement ou de fonctionnement. Il procure une sécurité améliorée contre les attaques passives, comme défini dans la [RFC1704], par rapport à l'authentification par un mot de passe en clair.

Ce mécanisme n'empêche pas les attaques par répétition ;cependant, dans la plupart des cas, de telles attaques déclancheraient les mécanismes existants du protocole IS-IS qui rejetteraient effectivement les vieilles informations. Les attaques de déni de service nr sont généralement pas parables par un protocole de réseautage utile [DoS].

Les mécanismes du présent document n'apportent pas de protection contre les routeurs compromis, qui fonctionnent mal, ou sont mal configurés. De tels routeurs peuvent, soit accidentellement, soit délibérément, causer des disfonctionnements qui affectent la totalité du domaine d'acheminement. Le lecteur est invité à consulter la [RFC4593] pour une description plus complète des menaces qui pèsent sur les protocole d'acheminement.

3.2 Assurance

Il faut que les usagers comprennent que la qualité de la sécurité apportée par ce mécanisme dépend entièrement de la force des algorithmes d'authentification mis en œuvre, de la force de la clé utilisée, et de la mise en œuvre correcte du mécanisme de sécurité dans toutes les applications IS-IS qui communiquent. Ce mécanisme dépend aussi de ce que toutes les parties préservent la confidentialité de la clé d'authentification IS-IS. Si un de ces éléments est incorrect ou insuffisamment sécurisé, aucune sécurité réelle ne sera fournie aux utilisateurs de ce mécanisme.

Depuis la publication, il y a une douzaine d'années, de attaques de Dobbertin contre MD5 [Dobb96a] [Dobb96b] [Dobb98], il y a eu des inquiétudes croissantes quant à l'efficacité de la fonction de compression au sein de MD5. Les travaux plus récents de Wang et Yu [WY05] accentuent ces inquiétudes. Cependant, en dépit du résultat de ces recherches, il n'y a pas eu d'attaque publiée jusqu'à présent contre le MD5 à clés ou le HMAC-MD5. Un article récent de Bellare [Bell06a] [Bell06b] donne de nouvelles preuves de la sécurité de HMAC qui exigent moins d'hypothèses que les preuves précédemment publiées pour HMAC. Ces preuves indiquent que les problèmes publiés au sujet de MD5 (et séparément au sujet de SHA-1) ne créent pas de possibilité d'attaque contre HMAC-MD5 (ou HMAC SHA-1). Très récemment, Fouque et d'autres [FLN07] ont publié de nouvelles attaques contre NMAC-MD4, HMAC-MD4, et NMAC-MD5. Cependant, leurs attaques sont loin d'être triviales du point de vue informatique, et ils n'ont pas trouvé d'attaque équivalente contre HMAC-MD5. Aussi, en dépit des inquiétudes publiées sur l'algorithme MD5, il n'y a pas actuellement d'attaque publiée qui s'applique à HMAC-MD5 tel qu'utilisé dans la présente spécification IS-IS. Comme avec toute technique cryptographique, il y a la possibilité que soient à l'avenir découvertes des attaques contre ce mécanisme.

3.3 Configuration de clé

Il convient de noter que le mécanisme de configuration de clé des routeurs peut restreindre les clés qu'il est possible d'utiliser entre des homologues. Il est vivement recommandé qu'une mise en œuvre soit capable de prendre en charge, au minimum, une clé composée d'une chaîne de caractères ASCII imprimables de 80 octets ou moins, selon la pratique

habituelle.

3.4 Autres considérations

Des changements du mécanisme d'authentification décrit ici (principalement : l'ajout d'un champ Key-ID comme celui de OSPFv2 et RIPv2) ont été examinés assez longuement, mais ont été finalement rejetés. Le mécanisme décrit ici a été déjà largement mis en œuvre depuis 1999. Au moment de la rédaction de ce texte, ce mécanisme est très largement répandu chez les utilisateurs intéressés à l'authentification cryptographique de IS-IS. L'amélioration apportés par la proposition de mécanisme révisé n'était pas assez importante pour justifier le changement, étant donné la base installée et le manque d'intérêt des opérateurs pour le développement d'un mécanisme révisé.

Si apparaissait un protocole de gestion de clés qui soit à la fois largement mis en œuvre et facilement déployé pour sécuriser des protocoles d'acheminement tels que IS-IS, un mécanisme d'authentification différent conçu pour être utilisé avec ce schéma de gestion de clés pourrait être ajouté si on le désirait.

3.5 Directions futures

Si on pensait qu'une authentification plus forte serait nécessaire, l'utilisation d'une signature numérique complète [RFC2154] serait alors une approche qu'on pourrait envisager sérieusement. Elle a été rejetée pour le moment parce que la charge de calcul de pleines signatures numériques est estimée être plus que ce qui est raisonnable, étant donné l'environnement actuel des menaces dans le fonctionnement des réseaux commerciaux.

Si des mécanismes supplémentaires d'authentification sont définis, et quand ils le seront (par exemple, de fournir une fonction de hachage plus forte cryptographiquement), il sera aussi nécessaire de définir des mécanismes permettant une transition en douceur des mécanismes existants (tels que définis dans le présent document) à tout mécanisme futur.

4. Considérations relatives à l'IANA

L'IANA a créé un nouveau registre des codes pour administrer le codet de type d'authentification pour le TLV 10. Ce registre fait partie du registre des codets IS-IS existants tel qu'établi par les [RFC3563] et [RFC3359]. Ce registre est géré selon la politique de l'expert désigné telle que décrite dans la [RFC5226] et est appelé "IS-IS Authentication Type Codes for TLV 10" *(Codes de type d'authentification IS-IS pour le TLV 10)*.

Les valeurs du registre "Codes de type d'authentification IS-IS pour le TLV 10"devraient être enregistrées en décimal et ne devraient être approuvées qu'après consultation d'un expert désigné par le directeur de zone de l'IESG. L'intention est que toute allocation soit accompagnée de la publication d'une RFC. Cependant, l'expert désigné peut approuver des allocations une fois qu'il semble clair qu'une RFC sera publiée, permettant l'allocation des valeurs avant que le document ne soit approuvé pour publication comme RFC. De nouveaux éléments devraient être documentés dans une spécification publique et librement disponible. On devrait aussi permettre que des spécifications externes allouent et utilisent les Codes de type d'authentification IS-IS gérés par ce registre.

Les valeurs initiales pour le registre des "Codes de type d'authentification IS-IS pour le TLV 10" sont données ci-dessous ; les allocations futures seront faites au moyen de la révision par expert. Les allocations consistent en un nom de type d'authentification et sa valeur associée.

Code de type d'authentification	Valeur	Référence
Réservé	0	[ISO-10589]
Mot de passe en clair	1	[ISO-10589]
Réservé ISO 10589	2	[ISO-10589]
Authentification HMAC-MD5	54	RFC 5304
Méthode d'authentification d'acheminement de domaine privé	255	[ISO-10589]

5. Remerciements

Les auteurs tiennent à remercier (par ordre alphabétique) Stephen Farrell, Dave Katz, Steven Luong, Tony Przygienda, Nai-Ming Shen, et Henk Smit pour leurs commentaires et suggestions sur le présent document.

6. Références

6.1 Références normatives

[ISO-10589] ISO, "Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", Norme internationale 10589:2002, seconde édition, 2002.

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", RFC 2104, février 1997.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

6.2 Références informatives

[Bell06a] Bellare, M., "New Proofs for NMAC and HMAC: Security without Collision-Resistance", Preliminary Version, in Proceedings of Crypto 2006, Lecture Notes in Computer Science, Vol. 4117, August 2006.

[Bell06b] Bellare, M., "New Proofs for NMAC and HMAC: Security without Collision-Resistance", August 2006, <http://www-cse.ucsd.edu/users/mihir/papers/hmac-new.html>.

[DoS] Voydock, V. and S. Kent, "Security Mechanisms in High-level Networks", ACM Computing Surveys Vol. 15, n° 2, juin 1983.

[Dobb96a] Dobbertin, H., "Cryptanalysis of MD5 Compress", EuroCrypt Rump Session 1996, mai 1996.

[Dobb96b] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes, Vol. 2, n° 2, 1996.

[Dobb98] Dobbertin, H., "Cryptanalysis of MD4", Journal of Cryptology, Vol. 11, n° 4, 1998.

[FLN07] Fouque, P., Leurent, G., and P. Nguyen, "Full Key-Recovery Attacks on HMAC/NMAC-MD5 and NMAC-MD5", Proceedings of Crypto 2007, août 2007.

[RFC1195] R. Callon, "Utilisation de l'IS-IS OSI pour l'acheminement dans les environnements TCP/IP et duels", RFC 1195, décembre 1990.

[RFC1704] N. Haller et R. Atkinson, "Authentification sur l'Internet", RFC 1704, octobre 1994.

[RFC2154] S. Murphy, M. Badger et B. Wellington, "OSPF avec des signatures numériques", RFC 2154, juin 1997.

[RFC3359] T. Przygienda, "Codets de type, longueur et valeur (TLV) réservés de système intermédiaire à système intermédiaire", RFC 3359, août 2002.

[RFC3563] A. Zinin, "Accord de coopération entre l'ISOC/IETF et le comité technique conjoint ISO/IEC 1/sous-comité 6 (JTC1/SC6) sur le développement du protocole d'acheminement IS-IS", RFC 3563, juillet 2003.

[RFC3567] T. Li et R. Atkinson, "Authentification cryptographique de système intermédiaire à système intermédiaire (IS-IS)", RFC 3567, juillet 2003.

[RFC4593] A. Barbir, S. Murphy et Y. Yang, "Menaces génériques contre les protocoles d'acheminement", RFC 4593, octobre 2006.

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 5226, mai 2008.

[WY05] Wang, X. and H. Yu, "How to Break MD5 and Other Hash Functions", Proceedings of EuroCrypt 2005, Lecture Notes in Computer Science, Vol. 3494, 2005.

Adresse des auteurs

Tony Li
Redback Networks, Inc.
300 Holger Way
San Jose, CA 95134
USA
téléphone : +1 408 750 5160
mél : tony.li@tony.li

R. Atkinson
Extreme Networks, Inc.
3585 Monroe St.
Santa Clara, CA 95051
USA
téléphone : +1 408 579 2800
mél : rja@extremenetworks.com

Déclaration complète de droits de reproduction

Propriété intellectuelle