Groupe de travail Réseau
Request for Comments : 5310
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Bhatia, Alcatel-Lucent
V. Manral, IP Infusion
T. Li, Redback Networks Inc.
R. Atkinson, Extreme Networks
R. White, Cisco Systems
M. Fanto, Aegis Data Security
février 2009

Authentification cryptographique générique pour IS-IS

Statut de ce 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 propose une extension au protocole de système intermédiaire à système intermédiaire (IS-IS, *Intermediate System to Intermediate System*) pour permettre l'utilisation de tout algorithme d'authentification cryptographique en plus des schémas d'authentification déjà documentés, décrits dans la spécification de base et dans la RFC 5304. IS-IS est spécifié dans la norme internationale ISO 10589, avec les extensions pour la prise en charge du protocole Internet version 4 (IPv4) décrites dans la RFC 1195.

Bien que le présent document ait été écrit spécifiquement pour l'utilisation de la construction de code d'authentification de message haché (HMAC, *Hashed Message Authentication Code*) avec la famille de fonctions de hachage cryptographique d'algorithme de hachage sécurisé (SHA, *Secure Hash Algorithm*) la méthode décrite dans le présent document est générique et peut être utilisée pour étendre à l'avenir IS-IS à la prise en charge de toute fonction de hachage cryptographique.

Table des matières

1. Introduction

La spécification de système intermédiaire à système intermédiaire (IS-IS) ([ISO10589], [RFC1195]) permet l'authentification de ses unités de données de protocole (PDU, *Protocol Data Unit*) via le TLV Authentification (TLV 10)

qui est porté au titre de la PDU. La spécification de base a seulement des dispositions pour les mots de passe en clair et la [RFC5304] augmente cela en fournissant la capacité d'utiliser l'authentification par code d'authentification de message haché – résumé de message n° 5 (HMAC-MD5, *Hashed Message Authentication Code - Message Digest 5*) pour ses PDU.

Le premier octet du champ Valeur du TLV 10 spécifie le type d'authentification à effectuer. Le type 0 est réservé, le type 1 indique un mot de passe en clair, le type 54 indique HMAC MD5, et le type 255 est utilisé pour les méthodes d'authentification de domaine d'acheminement privé. Le reste du champ Valeur contient les données réelles d'authentification, déterminées par la valeur du type d'authentification.

Le présent document propose un nouveau type d'authentification à porter dans le TLV 10, appelé authentification cryptographique générique (CRYPTO_AUTH). Ce peut être utilisé pour spécifier tout algorithme d'authentification pour authentifier et vérifier les PDU IS-IS.

Le présent document explique aussi comment l'authentification HMAC-SHA peut être utilisée dans IS-IS.

Par définition, HMAC ([RFC2104], [FIPS-198]) exige une fonction de hachage cryptographique. On propose d'utiliser SHA-1, SHA-224, SHA-256, SHA-384, ou SHA-512 [FIPS-180-3] pour authentifier les PDU IS-IS.

On propose d'abandonner les clés par interface et d'avoir à la place des identifiants de clés qui se transposent en associations de sécurité (SA, *association de sécurité*) uniques IS-IS.

Bien qu'au moment de la rédaction du présent document il n'y ait aucune attaque ouvertement publiée sur le mécanisme HMAC-MD5, des rapports ([Dobb96a], [Dobb96b]) laissent planer des doutes sur la force ultime de la fonction de hachage cryptographique MD5.

Le mécanisme décrit dans le présent document n'assure pas la confidentialité, car les PDU sont envoyées en clair. Cependant, l'objectif d'un protocole d'acheminement est d'annoncer la topologie d'acheminement, et la confidentialité n'est normalement pas requise pour les protocoles d'acheminement.

1.1 Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Association de sécurité IS-IS

Une association de sécurité IS-IS contient un ensemble de paramètres partagés entre deux locuteurs IS-IS légitimes quelconques.

Paramètres associés à une SA IS-IS :

- Identifiant de clé (Key ID) : c'est un entier non signé de deux octets utilisé pour identifier de façon univoque une SA IS-IS, comme configurée manuellement par l'opérateur du réseau.

  Le receveur détermine la SA active en cherchant le champ Identifiant de clé dans la PDU entrante.

  L'envoyeur, sur la base de la configuration active, choisit l'association de sécurité à utiliser et met la valeur d'identifiant de clé correcte associée à l'association de sécurité dans la PDU IS-IS. Si plusieurs associations de sécurité IS-IS valides et actives existent pour une certaine interface sortante au moment de l'envoi d'une PDU IS-IS, l'envoyeur peut utiliser n'importe laquelle de ces associations de sécurité pour protéger le paquet.

  Utiliser des identifiants de clés rend pratique les changements de clés tout en conservant le fonctionnement du protocole. Chaque identifiant de clé spécifie deux parties indépendantes : le protocole d'authentification et la clé d'authentification, expliqués ci-dessous. Normalement, une mise en œuvre va permettre à l'opérateur de réseau de configurer un ensemble de clés dans une chaîne de clés, chaque clé dans la chaîne ayant une durée de vie fixée. Le fonctionnement réel de ces mécanismes sort du domaine d'application du présent document.

Noter que chaque identifiant de clé indique une clé avec un protocole d'authentification différent. Cela permet que plusieurs mécanismes d'authentification soient utilisés à divers moments sans interrompre l'échange de trafic IS-IS, incluant l'introduction de nouveaux mécanismes d'authentification.

- Algorithme d'authentification : il signifie l'algorithme d'authentification qui va être utilisé avec la SA IS-IS. Cette information n'est jamais envoyée en clair sur le réseau. Parce que cette information n'est pas envoyée sur le réseau, la mise en œuvre choisit une représentation spécifique pour cette information. À présent, les valeurs suivantes sont possibles : HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512.

- Clé d'authentification : cette valeur note la clé d'authentification cryptographique associée à la SA IS-IS. La longueur de cette clé est variable et dépend de l'algorithme d'authentification spécifié par la SA IS-IS.

3. Procédures d'authentification

3.1 TLV Authentification

Un nouveau code d'authentification, 3, indique que le mécanisme CRYPTO_AUTH décrit dans le présent document est utilisé et est inséré dans le premier octet du TLV IS-IS Authentification existant, TLV 10.

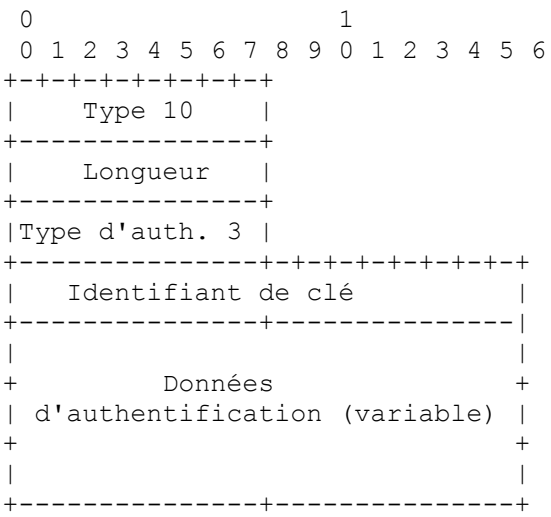

Figure 1

3.2 Processus d'authentification

Lors du calcul du résultat de CRYPTO_AUTH pour les PDU de numéro de séquence, les PDU de numéro de séquence de niveau 1 DEVRONT utiliser la chaîne Authentification de zone, comme dans les PDU d'état de liaison de niveau 1. Les PDU de numéro de séquence de niveau 2 devront utiliser la chaîne d'authentification de domaine, comme dans les PDU d'état de liaison de niveau 2.

Les PDU de HELLO IS-IS DEVRONT utiliser la chaîne d'authentification de niveau liaison, qui PEUT être différente de celle des PDU d'état de liaison. Le résultat de CRYPTO_AUTH pour les PDU de HELLO IS-IS DEVRA être calculé après que la PDU est bourrée 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 Somme de contrôle.

3.3 Aspects cryptographiques

Dans la description d'algorithme ci-dessous, la nomenclature suivante, qui est conforme à [FIPS-198] est utilisée :
H est l'algorithme de hachage (par exemple, SHA-256).
K est le mot de passe pour le type de PDU selon la norme internationale ISO/CEI [ISO10589].
Ko est la clé de chiffrement utilisée avec l'algorithme de hachage.
B est la taille de bloc de H, mesurée en octets plutôt qu'en bits. Noter que B est la taille de bloc interne, et non la taille du hachage. Pour SHA-1 et SHA-256, B == 64. Pou SHA-384 et SHA-512,B == 128.
L est la longueur du hachage, mesurée en octets plutôt qu'en bits.

OUX est l'opération OU exclusif.
Opad est la valeur hexadécimale 0x5c répétée B fois.
Ipad est la valeur hexadécimale 0x36 répétée B fois.
Apad est la valeur hexadécimale 0x878FE1F3 répétée (L/4) fois.

(1) Préparation de la clé
Dans cette application, Ko est toujours long de L octets.
Si la clé d'authentification (K) est longue de L octets, alors Ko est égal à K. Si la clé d'authentification (K) fait plus de L octets de long, alors Ko est réglé à H(K). Si la clé d'authentification (K) fait moins de L octets de long, alors Ko est réglé à la clé d'authentification (K) avec des zéros ajoutés à la fin de la clé d'authentification (K) afin que Ko soit long de L octets.

(2) Premier hachage
D'abord, le champ Données d'authentification du paquet IS-IS est rempli avec la valeur Apad, et le champ Type d'authentification est réglé à 0x3.
Ensuite, un premier hachage, aussi appelé hachage interne, est calculé comme suit :

Premier hachage = H(Ko OUX Ipad || (PDU IS-IS))

(3) Second hachage
Ensuite un second hachage, aussi appelé hachage externe, est calculé comme suit :

Second-hachage = H(Ko OUX Opad || Premier hachage)

(4) Résultat
Le second hachage résultant devient les données d'authentification qui sont envoyées dans le champ Données d'authentification de la PDU IS-IS. La longueur du champ Données d'authentification est toujours identique à la taille de résumé de message de la fonction de hachage spécifique H qui est utilisée.

Cela signifie aussi que l'utilisation des fonctions de hachage avec de plus grandes tailles de résultat va aussi augmenter la taille de la PDU IS-IS qui sera transmise sur le réseau.

3.4 Procédures côté envoyeur

Une SA IS-IS appropriée est choisie pour être utilisée avec une PDU IS-IS sortante. Ceci est fait sur la base de la clé active à ce moment. Si IS-IS est incapable de trouver une clé active, la PDU est alors éliminée.

Si IS-IS est capable de trouver la clé active, la clé fournit alors l'algorithme d'authentification (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, ou HMAC-SHA-512) qui doit être appliqué à la PDU.

Une mise en œuvre DOIT remplir le type d'authentification et la longueur avant que les données d'authentification soient calculées. Les données d'authentification sont calculées comme expliqué au paragraphe précédent. La longueur du TLV est réglée conformément à l'algorithme d'authentification utilisé.

La longueur est réglée à 23 pour HMAC-SHA-1, 31 pour HMAC-SHA-224, 35 pour HMAC-SHA-256, 51 pour HMAC-SHA-384, et 67 pour HMAC-SHA-512. Noter que deux octets ont été ajoutés pour tenir compte de l'identifiant de clé et un octet pour le type d'authentification.

L'identifiant de clé est rempli.

Les champs Somme de contrôle et Durée de vie restante sont réglés à zéro pour les paquets d'état de liaison (LSP, *Link State Packet*) avant que l'authentification soit calculée.

Le résultat de l'algorithme d'authentification est placé dans les données d'authentification, à la suite de l'identifiant de clé.

Les données d'authentification pour les PDU IIH IS-IS DOIVENT être calculées après que le IS-IS Hello (IIH) a été bourré jusqu'à la taille de MTU, si le bourrage n'est pas explicitement désactivé.

3.5 Procédure côté receveur

La SA IS-IS appropriée est identifiée en cherchant l'identifiant de clé provenant du TLV Authentification 10 dans la PDU IS-IS entrante.

Le processus dépendant de l'algorithme d'authentification doit être effectué, en utilisant l'algorithme spécifié par la SA IS-IS appropriée pour le paquet reçu.

Avant qu'une mise en œuvre effectue un traitement, elle doit sauvegarder les valeurs des champs Valeur d'authentification, Somme de contrôle, et Durée de vie restante.

Elle devrait régler le champ Valeur d'authentification avec Apad et les champs Somme de contrôle et Durée de vie restante à zéro avant que les données d'authentification soient calculées. Les données calculées sont comparées avec les données d'authentification reçues dans la PDU, et la PDU est éliminée si les deux ne correspondent pas. Dans ce cas, un événement d'erreur DEVRAIT être enregistré.

Une mise en œuvre PEUT avoir un mode de transition où elle inclut des informations de CRYPTO_AUTH dans les PDU mais ne vérifie pas ces informations. Ceci est à titre de mesure de transition pour les réseaux qui sont en cours de migration vers le nouveau schéma d'authentification fondé sur CRYPTO_AUTH.

4. Considérations sur la sécurité

Le présent document propose des extensions à IS-IS qui le rendent plus sûr qu'il ne l'est aujourd'hui. Il n'assure pas la confidentialité car un protocole d'acheminement contient des informations qui n'ont pas besoin de rester secrètes. Il fournit cependant des moyens d'authentifier l'envoyeur des PDU, ce qui nous intéresse.

On devrait noter que la méthode d'authentification décrite dans le présent document n'est pas utilisée pour authentifier l'origine spécifique d'une PDU, mais qu'elle est plutôt utilisée pour confirmer que la PDU a bien été produite par un système intermédiaire qui a l'accès au mot de passe de zone ou domaine selon le type de PDU.

Le mécanisme décrit ici n'est pas parfait et n'a pas besoin d'être parfait. Ce mécanisme représente plutôt un accroissement significatif de la fonction travail d'un adversaire qui attaque le protocole IS-IS, tout en ne causant pas de complexité indue de mise en œuvre, déploiement, ou fonctionnement.

Le mécanisme détaillé dans le présent document ne protège pas IS-IS contre les attaques en répétition. Un adversaire pourrait en théorie répéter les vieux IIH et détruire l'adjacence [RFC6039] ou répéter les vieilles PDU complètes de numéro de séquence (CSNP, *Complete Sequence Number PDU*) et les PDU de numéro de séquence partielles (PSNP, *Partial Sequence Number PDU*) ce qui causerait une inondation de LSP dans le réseau. Utiliser une sorte de numéros de séquence chiffrés dans les IIH IS-IS et les CSNP/PSNP est une option pour résoudre ce problème. Cette discussion sort du domaine d'application de ce document.

Le présent document déclare que la durée de vie restante du LSP DOIT être réglée à zéro avant de calculer l'authentification, donc ce champ n'est pas authentifié. Ce champ est exclu afin que les LSP puissent être vieillis par les IS intercalés, sans exiger un nouveau calcul des données d'authentification. Ceci peut être exploité par un attaquant.

Un mode de transition est suggéré par lequel les routeurs peuvent ignorer les informations de CRYPTO_AUTH portées dans les PDU. L'opérateur doit s'assurer que ce mode n'est utilisé que quand il migre au nouveau schéma d'authentification fondé sur CRYPTO_AUTH, car cela laisse le routeur vulnérable à une attaque.

Pour assurer une plus grande sécurité, les clés utilisées devraient être changées périodiquement, et les mises en œuvre DOIVENT être capables de mémoriser et utiliser plus d'une clé au même moment. Les opérateurs devraient s'assurer que la clé d'authentification n'est jamais envoyée en clair sur le réseau par tout protocole. Il faudrait aussi veiller à s'assurer que la clé choisie est imprévisible, en évitant toute clé connue pour être faible pour l'algorithme utilisé. La [RFC4086] contient des informations utiles sur les techniques de génération de clés et l'aléa cryptographique.

On devrait noter que la force cryptographique de HMAC dépend de la force cryptographique de la fonction de hachage sous-jacente et de la taille et qualité de la clé.

Si on estime qu'une authentification plus forte doit être exigée, l'utilisation d'une signature numérique complète [RFC2154] serait alors une approche qui devrait être sérieusement envisagée. Elle a été écartée pour l'instant à cause de la charge de calcul de pleines signatures numériques qui est estimée plus lourde qu'il n'est raisonnable compte tenu de l'environnement de menaces actuel dans le fonctionnement des réseaux commerciaux.

5. Remerciements

Les auteurs tiennent à remercier Hugo Krawczyk, Arjen K. Lenstra (Bell Labs), et Eric Grosse (Bell Labs) qui nous ont enseigné les points les plus délicats des mathématiques cryptographiques.

Merci aussi à Bill Burr, Tim Polk, John Kelsey, et Morris Dworkin du (US) NIST pour leur relecture de portions de ce document qui sont directement dérivées du travail étroitement apparenté sur l'authentification cryptographique dans RIPv2 [RFC4822].

Nous nous devons de mentionner la relecture attentive et détaillée de Alfred Hoenes durant le dernier appel.

Enfin, nous tenons à remercier Brian et Stephen Eisenberg de leur soutien continu.

6. Considérations relatives à l'IANA

L'IANA a enregistré la valeur de la méthode CRYPTO_AUTH dans le sous registre des "Codes de type d'authentification IS-IS pour le TLV 10" établi par la [RFC5304]. La valeur 3 note le mécanisme CRYPTO_AUTH pour authentifier les PDU IS-IS.

Code de type d'authentification	**Valeur**	**Référence**
Authentification cryptographique (CRYPTO_AUTH)	3	[RFC5310]

7. Références

7.1 Références normatives

[FIPS-180-3] US National Institute of Standards & Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-3, octobre 2008.

[FIPS-198] US National Institute of Standards & Technology, "The Keyed-Hash Message Authentication Code (HMAC)", FIPS PUB 198, mars 2002.

[ISO10589] Norme internationale ISO 10589, "Technologie de l'information - Télécommunications et échanges d'informations entre systèmes - Protocole d'échange d'informations d'acheminement intra domaine de système intermédiaire à système intermédiaire à utiliser en conjonction avec le protocole de fourniture du service réseau en mode sans connexion(ISO8473)", seconde édition, 2002.

[RFC1195] R. Callon, "Utilisation de l'IS-IS OSI pour l'acheminement dans les environnements TCP/IP et duels", décembre 1990. *(Mise à jour par les* RFC 1349, 5302, 5304*)*

[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. *(MàJ par* RFC8174)

[RFC5304] T. Li et R. Atkinson, "Authentification cryptographique IS-IS", octobre 2008. (*Remplace* RFC3567, MàJ RFC1195) *(PS, MàJ par* RFC6233, RFC6232*)*

7.2 Références pour information

[Dobb96a] Dobbertin, H., "Cryptanalysis of MD5 Compress", Technical Report, mai 1996.

[Dobb96b] Dobbertin, H., "The Status of MD5 After a Recent Attack", Cryptobytes, Volume 2, No 2, Summer 1996.

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

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

[RFC4822] R. Atkinson, M. Fanto, "Authentification cryptographique RIPv2", février 2007. (*Remplace* RFC2082) *(P.S.)*

[RFC6039] V. Manral, M. Bhatia, J. Jaeggli, R. White, "Problèmes des méthodes existantes de protection cryptographique pour les protocoles d'acheminement', octobre 2010. *(Information)*

Adresse des auteurs

Manav Bhatia
Alcatel-Lucent
Bangalore,
India
mél : manav@alcatel-lucent.com

Vishwas Manral
IP Infusion
Almora, Uttarakhand
India
mél : vishwas@ipinfusion.com

Tony Li
Redback Networks Inc.
300 Holger Way
San Jose, CA 95134
mél : tony.li@tony.li

Randall J. Atkinson
Extreme Networks
3585 Monroe Street
Santa Clara, CA 95051
mél : rja@extremenetworks.com

Russ White
Cisco Systems
RTP North Carolina
USA
mél : riw@cisco.com

Matthew J. Fanto
Aegis Data Security
Dearborn, MI
USA
mél : mfanto@aegisdatasecurity.com