Groupe de travail Réseau
Request for Comments : 4304
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

S. Kent, BBN Technologies

décembre 2005

Addendum du numéro de séquence étendu (ESN) au domaine d'interprétation IPsec (DOI) pour le protocole d'associations de sécurité et de gestion de clé Internet (ISAKMP)

Statut de ce 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.

Résumé
Les protocoles d'en-tête d'authentification (AH, *Authentication Header*) et d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) de la sécurité d'IP (IPsec) utilisent un numéro de séquence pour détecter les répétitions. Le présent document décrit les extensions au domaine d'interprétation de la sécurité de l'Internet pour le protocole de gestion de clé et d'association de sécurité de l'Internet (ISAKMP, *Internet Security Association and Key Management Protocol*). Ces extensions acceptent la négociation de l'utilisation des numéros de séquence traditionnels de 32 bits ou des numéros de séquence étendus (ECN, *extended sequence number*) de 64 bits pour une association de sécurité AH ou ESP particulière.

1. Introduction

Les spécifications de l'en-tête d'authentification (AH, *Authentication Header*) IP [RFC4302] l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IP [RFC4303] décrivent une option à utiliser pour les numéros de séquence étendus (de 64 bits). Cette option permet la transmission de très gros volumes de donnés à grande vitesse sur une association de sécurité IPsec, sans changer de clés pour éviter l'épuisement de l'espace de numéros de séquence. Le présent document décrit l'ajout au DOI IPsec pour ISAKMP [RFC2407] qui est nécessaire pour prendre en charge la négociation de l'option de numéros de séquence étendus (ESN, *extended sequence number*).

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. Attribut Association de sécurité IPsec

La définition d'attribut de SA suivante est utilisée dans la phase II d'une négociation du protocole d'échange de clé Internet (IKE, *Internet Key Exchange*). Le type d'attribut est Basique (B). Le codage de cet attribut est défini dans la spécification de base ISAKMP [RFC2408]. Les attributs décrits comme basiques NE DOIVENT PAS être codés comme variables. Voir dans la [RFC2409] plus d'informations sur le codage d'attribut dans le DOI IPsec. Toutes les restrictions mentionnées dans la [RFC2409] s'appliquent aussi au DOI IPsec et à cet addendum.

Type d'attribut

classe	**valeur**	**type**
Numéro de séquence étendu (64 bits)	11	B

Valeurs de classe : cette classe spécifie que l'association de sécurité va utiliser des numéros de séquence de 64 bits. (Voir dans les [RFC4302] et [RFC4303] la description des numéros de séquence étendus (64 bits).)

Réservé	0
Numéro de séquence à 64 bits	1

3. Négociation d'attribut

Si une mise en œuvre reçoit un attribut DOI IPsec défini (ou valeur d'attribut) qu'elle ne prend pas en charge, un ATTRIBUTES-NOT-SUPPORT DEVRAIT être envoyé et l'établissement de l'association de sécurité DOIT être interrompu.

Si une mise en œuvre reçoit une valeur d'attribut autre que la valeur pour les numéros de séquence à 64 bits, l'établissement de l'association de sécurité DOIT être interrompue.

4. Considérations sur la sécurité

Le présent mémoire relève du protocole d'échange de clé Internet [RFC2409], qui combine ISAKMP [RFC2408] et Oakley [RFC2412] pour assurer la déduction du matériel de chiffrement cryptographique d'une manière sûre et authentifiée. On trouvera un exposé spécifique des divers protocoles de sécurité et des transformations identifiées dans ce document dans les document de base associés et dans les références de chiffrement.

L'ajout de l'attribut ESN ne change pas les caractéristiques de sécurité sous-jacentes de IKE. En utilisant les ESN avec ESP, il est important d'employer un mode de chiffrement sûr quand de très gros volumes de données sont chiffrés sous une seule clé. Donc, par exemple, la norme de chiffrement de données (DES, *Data Encryption Standard*) en mode de chaînage de chiffrement de bloc (CBC, *Cipher Block Chaining*) NE conviendrait PAS pour l'utilisation avec ESN, parce que pas plus de 2^32 blocs ne devraient être chiffrés sous une seule clé DES dans ce mode. De même, l'algorithme d'intégrité utilisé avec ESP ou AH devrait être sûr par rapport au nombre de paquets à protéger. Pour éviter de potentiels problèmes de sécurité imposés par des limitations d'algorithme, la durée de vie de SA peut être réglée à limiter le volume de données protégées par une seule clé, avant d'atteindre la limite de paquet de 2^64 imposée par l'ESN.

5. Considérations relatives à l'IANA

Le présent document contient un numéro "magique" qui est tenu par l'IANA. Aucune valeur de classe supplémentaire ne sera allouée pour cet attribut. L'IANA a alloué la valeur d'attribut de sécurité IPsec pour "Type d'attribut". Cette valeur est mentionnée sous la "valeur" du tableau de la Section 2.

Remerciements

L'auteur tient à remercier les membres du groupe de travail IPsec. Il remercie aussi de ses contributions Karen Seo et de son aide à l'édition de la présente spécification.

Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obs., voir* 4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

Référence pour information

[RFC2412] H. Orman, "Protocole OAKLEY de détermination de clés", novembre 1998. *(Information)*

Adresse de l'auteur

Stephen Kent
BBN Technologies
10 Moulton Street
Cambridge, MA 02138
USA

téléphone : +1 (617) 873-3988
mél : kent@bbn.com

Déclaration complète de droits de reproduction

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