Groupe de travail Réseau
Request for Comments : 4308
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Hoffman, VPN Consortium

décembre 2005

Suites de chiffrement pour IPsec

Résumé
Les protocoles IPsec, échange de clés sur Internet (IKE, *Internet Key Exchange*), et IKEv2 s'appuient sur des algorithmes de sécurité pour assurer la confidentialité et l'authentification entre l'initiateur et celui qui répond. Ces algorithmes sont nombreux, et deux systèmes IPsec ne peuvent interopérer que si ils utilisent les mêmes algorithmes. Le présent document spécifie des suites facultatives d'algorithmes et des attributs qui peuvent être utilisés pour simplifier l'administration de IPsec quand il est utilisé en mode de chiffrement manuel, avec IKEv1 ou avec IKEv2.

1. Introduction

Le présent document accompagne IPsec [RFC2401] et ses deux protocoles d'échange de clés, IKE [RFC2409] et IKEv2 [RFC4306]. Comme la plupart des protocoles de sécurité, IPsec, IKE, et IKEv2 permettent aux utilisateurs de choisir quels algorithmes de chiffrement ils veulent utiliser pour satisfaire leurs besoins de sécurité.

L'expérience de la mise en œuvre de IPsec en mode de clé manuel et de IKE a montré qu'il y a tant de choix pour les administrateurs de système qu'il est difficile de réaliser l'interopérabilité sans un accord préalable. À cause de cela, le groupe de travail IPsec s'est accordé sur un petit nombre de suites désignées qui couvrent les politiques de sécurité normales. Ces suites peuvent être présentées dans l'interface administrative du système IPsec. Ces suites, souvent appelées "suites UI" *(user interface suites)* sont facultatives et n'empêchent pas une mise en œuvre de permettre un choix individuel des algorithmes de sécurité.

Bien que les suites UI mentionnées ici soient de mise en œuvre facultative, le présent document est sur la voie de la normalisation parce que une mise en œuvre qui invoque des suites particulières par le nom utilisé ici doit se conformer aux suites dont la liste figure dans le présent document. Ces suites ne devraient pas être considérées comme des extensions à IPsec, IKE, et IKEv2, mais plutôt comme des méthodes administratives de description d'ensembles de configurations.

Les mots clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", et "PEUT" dans ce document sont à interpréter comme décrit dans la [RFC2119].

2. Suites d'interface d'utilisateur

Cette section fait la liste des suites facultatives, non obligatoires, qui peuvent être présentées aux administrateurs de système pour faciliter le choix parmi les nombreuses options des systèmes IPsec. Ces suites ne peuvent pas couvrir toutes les options parmi lesquelles un administrateur doit faire son choix. On donne plutôt les valeurs d'un sous ensemble des options.

Noter que ces suites UI sont simplement une collection des valeurs de certaines options de IPsec. L'utilisation des suites

UI ne change en aucune façon les protocoles IPsec, IKE, ou IKEv2. Précisément, la sous structure de transformation dans IKE et IKEv2 doit être utilisée pour donner la valeur de chaque option spécifiée sans considération de l'utilisation ou non de suites UI.

Les mises en œuvre qui utilisent des suites UI DEVRAIENT aussi fournir une interface de gestion pour spécifier les valeurs des options de chiffrement individuelles. C'est-à-dire qu'il est peu probable que les suites UI soient une solution complète pour correspondre aux politiques de sécurité de nombreux utilisateurs de IPsec, et donc une interface qui donne un ensemble plus complet d'options devrait aussi être utilisée.

Les mises en œuvre de IPsec qui utilisent ces suites UI DEVRAIENT utiliser les noms de suites qui sont donnés ici. Les mises en œuvre de IPsec NE DEVRAIENT PAS utiliser des noms différents de ceux donnés ici pour les suites décrites, et NE DOIVENT PAS utiliser les noms donnés ici pour des suites qui ne correspondent pas à ces valeurs.Ces exigences sont nécessaires pour l'interopérabilité.

Noter que les suites indiquées ici sont pour l'utilisation de IPsec dans des réseaux virtuels privés. Les autres utilisations de IPsec voudront probablement définir leur propres suites et leur donner des noms différents.

Des suites supplémentaires pourront être définies par des RFC. Les chaînes utilisées pour identifier les suites UI sont enregistrées par l'IANA.

2.1 Suite "VPN-A"

Cette suite correspond à la sécurité couramment utilisée pour le VPN d'entreprise utilisé dans IKEv1 au moment de la publication du présent document.

IPsec :
Protocole : Encapsulation de la charge utile de sécurité (ESP) [RFC2406]
Chiffrement ESP : Triple DES en mode CBC [RFC2451]
Intégrité d'ESP : HMAC-SHA1-96 [RFC2404]

IKE et IKEv2 :
Chiffrement : Triple DES en mode CBC [RFC2451]
Fonction pseudo aléatoire HMAC-SHA1 [RFC2104]
Intégrité : HMAC-SHA1-96 [RFC2404]
Groupe Diffie-Hellman : modulaire exponentiel à 1024 bits (MODP) [RFC2409]

Le changement de clés de phase 2 (pour IKE) ou le CREATE_CHILD_SA (pour IKEv2) DOIT être pris en charge par les deux parties dans cette suite. L'initiateur de cet échange PEUT inclure une nouvelle clé Diffie-Hellman ; si elle est incluse, elle DOIT être du type MODP à 1024 bits. Si l'initiateur de l'échange inclut une clé Diffie-Hellman, celui qui répond DOIT inclure une clé Diffie-Hellman, et elle DOIT être du type MODP à 1024 bits.

2.2 Suite "VPN-B"

Cette suite est ce que de nombreuses personnes attendent de ce que devrait être la sécurité de VPN d'entreprise couramment utilisée dans les quelques années qui viennent.

IPsec :
Protocole : ESP [RFC2406]
Chiffrement ESP : AES avec clés de 128 bits en mode CBC [RFC3602]
Intégrité ESP : AES-XCBC-MAC-96 [RFC3566]

IKE et IKEv2 :
Chiffrement : AES avec clés de 128 bits en mode CBC [RFC3602]
Fonction pseudo aléatoire : AES-XCBC-PRF-128 [RFC3664]
Intégrité : AES-XCBC-MAC-96 [RFC3566]
Groupe Diffie-Hellman : MODP à 2048 bits [RFC3526]

Le changement de clé de phase 2 (pour IKE) ou le CREATE_CHILD_SA (pour IKEv2) DOIT être pris en charge par les deux parties dans cette suite. L'initiateur de cet échange PEUT inclure une nouvelle clé Diffie-Hellman ; si elle est

incluse, elle DOIT être du type MODP à 2048 bits. Si l'initiateur de l'échange inclut une clé Diffie-Hellman, celui qui répond DOIT inclure une clé Diffie-Hellman, et elle DOIT être du type MODP à 2048 bits.

2.3 Durées de vie pour IKEv1

IKEv1 a deux paramètres de sécurité qui n'apparaissent pas dans IKEv2, à savoir la durée de vie de la phase 1 et les associations de sécurité de la phase 2. Les systèmes qui utilisent IKEv1 avec les suites VPN-A ou VPN-B DOIVENT utiliser une durée de vie d'association de sécurité de 86 400 secondes (24 heures) pour la phase 1 et une durée de vie d'association de sécurité de 28 800 secondes (8 heures) pour la phase 2.

3. Remerciements

Beaucoup du texte et des idées de ce document viennent de versions antérieures du document IKEv2 édité par Charlie Kaufman. D'autres textes et idées ont été apportés en contribution par les autres membres du groupe de travail IPsec.

4. Considérations sur la sécurité

Le présent document hérite de toutes les considérations sur la sécurité des documents IPsec, IKE, et IKEv2.

Certaines des options de sécurité spécifiées dans ces suites pourraient à l'avenir se révéler avoir des propriétés significativement plus faibles que ce qui était estimé au moment de la production du présent document.

5. Considérations relatives à l'IANA

L'IANA a créé et va tenir un registre appelé, "Suites de chiffrement pour IKEv1, IKEv2, et IPsec". Le registre consiste en une chaîne de texte et un numéro de RFC qui fait la liste des transformations associées. De nouvelles entrées peuvent être ajoutées au registre après la publication d'une RFC approuvée par un expert désigné par l'IESG.

Les valeurs initiales du nouveau registre sont :

Identifiant	**défini dans**
VPN-A	RFC 4308
VPN-B	RFC 4308

6. Références normatives

[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)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

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

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

[RFC3526] T. Kivinen et M. Kojo, "Groupes supplémentaires d'exponentiation modulaire (MODP) Diffie-Hellman pour l'échange de clés Internet (IKE)", mai 2003.

[RFC3566] S. Frankel, H. Herbert, "L'algorithme AES-XCBC-MAC-96 et son utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3602] S. Frankel, R. Glenn, S. Kelly, "Algorithme de chiffrement AES-CBC et utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3664] P. Hoffman, "Algorithme AES-XCBC-PRF-128 pour le protocole d'échange de clés Internet (IKE)", janvier 2004. (*Obsolète, voir* RFC4434) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

Adresse de l'auteur

Paul Hoffman
VPN Consortium
127 Segre Place
Santa Cruz, CA 95060
USA

mél : paul.hoffman@vpnc.org

Déclaration complète de droits de reproduction

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