Groupe de travail Réseau
Request for Comments : 4025
Catégorie : En cours de normalisation

M. Richardson, SSW
février 2005
Traduction Claude Brière de L'Isle

Méthode pour mémoriser le matériel de clés IPsec dans le DNS

Résumé
Le présent document décrit un nouvel enregistrement de ressource pour le système des noms de domaines (DNS, *Domain Name System*). Cet enregistrement peut être utilisé pour mémoriser des clés publiques à utiliser dans les systèmes de sécurité IP (IPsec). L'enregistrement comporte aussi des dispositions pour indiquer quel système devrait être contacté lorsque un tunnel IPsec est établi avec l'entité en question.

Cet enregistrement remplace la fonctionnalité du sous-type n° 4 de l'enregistrement de ressource KEY, qui a été rendu obsolète par la RFC 3445.

Table des matières

1. Introduction....1
1.1 Généralités....2
1.2 Utilisation de la transposition d'adresse en nom DNS (IN-ADDR.ARPA et IP6.ARPA)....2
1.3 Critères d'utilisation....2
2. Formats de mémorisation....2
2.1 Format de RDATA IPSECKEY....2
2.2 Format RDATA - préséance....3
2.3 Format RDATA – type de passerelle....3
2.4 Format RDATA – Type d'algorithme....3
2.5 Format RDATA - passerelle....3
2.6 Format RDATA – clés publiques....3
3. Formats de présentation....4
3.1 Représentation des RR IPSECKEY....4
3.2 Exemples....4
4. Considérations pour la sécurité....5
4.1 Attaques actives contre des enregistrements de ressource IPSECKEY non sécurisés....5
4.1.1 Attaques actives contre du matériel de clé IPSECKEY....5
4.1.2 Attaques actives contre du matériel de passerelle IPSECKEY....5
5. Considérations relatives à l'IANA....6
6. Remerciements....6
7. Références....7
7.1 Références normatives....7
7.2 Références pour information....7

1. Introduction

Supposons qu'un hôte souhaite (ou soit obligé par une politique) d'établir un tunnel IPsec avec une entité distante sur le réseau avant de permettre qu'intervienne une communication normale. Dans de nombreux cas, ce système d'extrémité sera capable de déterminer le nom DNS de l'entité distante (soit en ayant le nom DNS qui lui est donné explicitement, en effectuant une interrogation PTR DNS pour une adresse IP particulière, soit par d'autres moyens, par exemple, en extrayant la portion DNS d'un nom "usager@FQDN" pour une entité distante). Dans tous ces cas, l'hôte aura besoin d'obtenir une clé publique pour authentifier l'entité distante, et pourra aussi avoir besoin de quelques lignes directrices pour savoir si elle

devrait contacter l'entité directement ou utiliser un autre nœud comme passerelle vers l'entité cible. Le PP IPSECKEY fournit un mécanisme pour mémoriser de telles informations.

Le numéro de type pour le RR IPSECKEY est 45.

Cet enregistrement remplace la fonctionnalité du sous-type n° 4 de l'enregistrement de ressource KEY, qui a été rendu obsolète par la RFC 3445 [11].

1.1 Généralités

L'enregistrement de ressource (RR) IPSECKEY est utilisé pour annoncer une clé publique à associer à un nom du système des noms de domaines (DNS, *Domain Name System*) [1] à utiliser avec la suite des protocoles IPsec. Ce peut être la clé publique d'un hôte, ou d'une application (dans le cas de chiffrement par accès).

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMENDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la RFC 2119 [3].

1.2 Utilisation de la transposition d'adresse en nom DNS (IN-ADDR.ARPA et IP6.ARPA)

Souvent, une passerelle de sécurité ne donnera accès qu'à l'adresse IP du nœud avec lequel est désirée la communication et elle ne connaîtra aucun des autres noms du nœud cible. À cause de cela, la meilleure façon pour chercher les RR IPSECKEY sera fréquemment d'utiliser l'adresse IP comme un indice dans les arborescences de transposition inverse (IN-ADDR.ARPA pour IPv4 ou IP6.ARPA pour IPv6).

La recherche est faite de la façon usuelle pour les enregistrements PTR. Les octets (IPV4) ou quartets (IPv6) de l'adresse IP sont inversés et la recherche est faite sur le suffixe approprié. Tous les CNAME ou DNAME trouvés DOIVENT être suivis.

Note : même lorsque la fonction IPsec est contenue dans l'hôte d'extrémité, souvent, seule l'application va connaître le nom de transmission utilisé. Bien que le cas où l'application connaît le nom de transmission soit courant, l'utilisateur pourrait facilement avoir tapé une adresse IP littérale. Ce mécanisme de mémorisation n'empêche pas d'utiliser le nom de transmission lorsque il est disponible, mais il ne l'exige pas.

1.3 Critères d'utilisation

Un enregistrement de ressource IPSECKEY DEVRAIT être utilisé en combinaison avec DNSSEC [8] à moins que d'autres moyens d'authentifier l'enregistrement de ressource IPSECKEY ne soient disponibles.

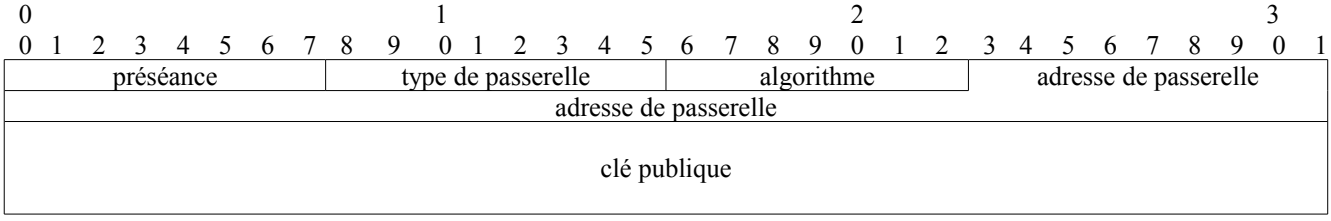
On s'attend à ce qu'il y ait souvent plusieurs enregistrements de ressource IPSECKEY au même nom. Cela sera dû à la présence de plusieurs passerelles et au besoin de clés de retournement.

Cet enregistrement de ressource est indépendant de la classe.

2. Formats de mémorisation

2.1 Format de RDATA IPSECKEY

Le RDATA pour un RR IPSECKEY consiste en une valeur de préséance, un type de passerelle, une clé publique, un type d'algorithme, et une adresse facultative de passerelle.



2.2 Format RDATA - préséance

C'est une préséance de 8 bits pour cet enregistrement. Elle est interprétée de la même façon que le champ PREFERENCE décrit au paragraphe 3.3.9 de la RFC 1035 [2].

Les passerelles figurant dans les enregistrements IPSECKEY avec des préséances inférieures seront essayées en premier. Lorsqu'il y a égalité de préséance, l'ordre devrait être aléatoire.

2.3 Format RDATA – type de passerelle

Le champ type de passerelle indique le format des informations qui sont mémorisées dans le champ passerelle.

Les valeurs suivantes sont définies :
0 aucune passerelle n'est présente.
1 une adresse IPv4 de quatre octets est présente.
2 une adresse IPv6 de seize octets est présente.
3 un nom de domaine à codage incorporé *(wire-encoded)* est présent. Le format à codage incorporé est auto descriptif, de sorte que la longueur est implicite. Le nom de domaine NE DOIT PAS être compressé. (Voir le paragraphe 3.3 de la RFC 1035 [2].)

2.4 Format RDATA – Type d'algorithme

Le champ type d'algorithme identifie l'algorithme cryptographique de clé publique et détermine le format du champ de clé publique.

Une valeur de 0 indique qu'aucune clé n'est présente.

Les valeurs suivantes sont définies :
1 une clé DSA est présente, dans le format défini à la RFC 2536 [9].
2 une clé RSA est présente, dans le format défini à la RFC 3110 [10].

2.5 Format RDATA - passerelle

Le champ passerelle indique une passerelle à laquelle un tunnel IPsec peut être créé afin d'atteindre l'entité nommée par cet enregistrement de ressource.

Il y a trois formats :

Une adresse IPv4 de 32 bits est présente dans le champ passerelle. La portion de données est une adresse IPv4 comme décrit au paragraphe 3.4.1 de la RFC 1035 [2]. C'est un nombre de 32 bits dans l'ordre des octets du réseau.

Une adresse IPv6 de 128 bits est présente dans le champ passerelle. La portion de données est une adresse IPv6 comme décrit au paragraphe 2.2 de la RFC 3596 [12]. C'est un nombre de 128 bits dans l'ordre des octets du réseau.

Le champ passerelle est un nom de domaine normal à codage incorporé, comme décrit au paragraphe 3.3 de la RFC 1035 [2]. La compression NE DOIT PAS être utilisée.

2.6 Format RDATA – clés publiques

Les deux types de clés publiques définis dans le présent document (RSA et DSA) héritent leurs formats de clés publiques des formats RR KEY correspondants. En particulier, le champ de clé publique contient la portion spécifique de l'algorithme du RDATA de RR KEY, qui sont toutes les données du RR KEY après les quatre premiers octets. C'est la même portion du RR KEY qui doit être spécifiée par les documents qui définissent un algorithme DNSSEC. Ces documents spécifient aussi un résumé de message à utiliser pour générer les RR SIG ; cette spécification n'est pas pertinente pour les RR IPSECKEY.

Les algorithmes futurs, si ils doivent être utilisés à la fois pour DNSSEC (dans le RR KEY) et pour IPSECKEY, vont vraisemblablement utiliser les mêmes codages de clé publique dans les deux enregistrements. Sauf spécification contraire, le champ de clé publique IPSECKEY va contenir la portion spécifique de l'algorithme du RDATA de RR KEY pour l'algorithme correspondant. L'algorithme doit encore être conçu pour l'utilisation par IPSECKEY, et un numéro de type d'algorithme IPSECKEY (qui pourrait être différent du numéro d'algorithme DNSSEC) doit lui être alloué.

Le format de clé DSA est défini dans la RFC 2536 [9]

Le format de clé RSA est défini dans la RFC 3110 [10], avec les changements suivants :

La précédente définition de RSA/MD5 dans la RFC 2065 [4] limitait l'exposant et le modulo à une longueur de 2552 bits. La RFC 3110 a étendu cette limite à 4096 bits pour les clés RSA/SHA1. Le RR IPSECKEY n'impose pas de limite de longueur aux clés publiques RSA, autre que la limite de 65 535 imposée par la longueur du codage sur deux octets. Cette extension de longueur n'est applicable qu'à IPSECKEY ; elle n'est pas applicable aux RR KEY.

3. Formats de présentation

3.1 Représentation des RR IPSECKEY

Les RR IPSECKEY peuvent apparaître dans un fichier maître de données de zone. Les champs préséance, type de passerelle, algorithme, et passerelle sont EXIGÉS. Le bloc de clé publique codé en base64 est FACULTATIF ; si il n'est pas présent, le champ clé publique de l'enregistrement de ressource DOIT être construit avec une longueur de zéro octet.

Le champ Algorithme est un entier non signé. Aucun mnémonique n'est défini.

Si aucune passerelle n'est indiquée, le champ Type de passerelle DOIT alors être zéro, et le champ passerelle DOIT être ".".

Le champ Clé publique est représenté comme un codage en Base64 de la clé publique. Les espaces blanches sont admises au sein du texte en Base64. Pour une définition du codage en Base64, voir la RFC 3548 [6], paragraphe 5.2.

La présentation générale de l'enregistrement est la suivante :

```
IN    IPSECKEY ( precedence gateway-type algorithm gateway base64-encoded-public-key )
```

3.2 Exemples

Un exemple d'un nœud, 192.0.2.38, qui va accepter les tunnels IPsec en son nom propre.

```
38.2.0.192.in-addr.arpa. 7200 IN    IPSECKEY ( 10 1 2 192.0.2.38
            AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

Un exemple d'un nœud, 192.0.2.38, qui a seulement publié sa clé.

```
38.2.0.192.in-addr.arpa. 7200 IN    IPSECKEY ( 10 0 2
            .
            AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

Un exemple d'un nœud, 192.0.2.38, qui a délégué l'autorité au nœud 192.0.2.3.

```
38.2.0.192.in-addr.arpa. 7200 IN    IPSECKEY ( 10 1 2 192.0.2.3
            AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

Un exemple d'un nœud, 192.0.1.38 qui a délégué l'autorité au nœud avec l'identité "mygateway.example.com".

```
38.1.0.192.in-addr.arpa. 7200 IN    IPSECKEY ( 10 3 2
            mygateway.example.com.
            AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

Un exemple d'un nœud, 2001:0DB8:0200:1:210:f3ff:fe03:4d0, qui a délégué l'autorité au nœud 2001:0DB8:c000:0200:2::1

```
$ORIGIN 1.0.0.0.0.0.2.8.B.D.0.1.0.0.2.ip6.arpa.
0.d.4.0.3.0.e.f.f.f.3.f.0.1.2.0 7200 IN     IPSECKEY ( 10 2 2
                2001:0DB8:0:8002::2000:1
                AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

4. Considérations pour la sécurité

La totalité du présent mémoire se rapporte aux dispositions concernant le matériel de clés publiques à utiliser par les protocoles de gestion de clés tels que ISAKMP/IKE (RFC 2407) [7].

L'enregistrement de ressource IPSECKEY contient des informations qui DEVRAIENT être communiquées au client final de façon intégrale ; c'est-à-dire, sans aucune modification. La forme de ce canal est à la discrétion du consommateur des données ; il doit y avoir une relations de confiance entre le consommateur final de cet enregistrement de ressource et le serveur. Cette relation peut être une validation DNSSEC de bout en bout, un canal TSIG ou SIG(0) avec une autre source sûre, un canal local sécurisé avec l'hôte, ou une combinaison quelconque des trois.

Le matériel de clés fourni par l'enregistrement de ressource IPSECKEY n'est pas sensible aux attaques passives. Le matériel de clé peut être librement divulgué à tout tiers sans aucun impact sur les propriétés de sécurité de la session IPsec résultante. IPsec et IKE fournissent une défense contre les attaques à la fois actives et passives.

Toute spécification dérivée qui utiliserait cet enregistrement de ressource DOIT documenter soigneusement son modèle de confiance et les raisons pour lesquelles le modèle de confiance de DNSSEC est approprié, si c'est le canal sécurisé utilisé.

Une attaque active contre le DNS qui causerait la restitution d'une mauvaise adresse IP (via une adresse falsifiée), et donc que le mauvais QNAME soit interrogé, aurait aussi pour résultat une attaque par interposition *(man-in-the-middle attack)*. Cette situation ne dépend pas de l'utilisation du RR IPSECKEY.

4.1 Attaques actives contre des enregistrements de ressource IPSECKEY non sécurisés

Ce paragraphe traite des attaques actives contre le DNS. Ces attaques exigent que les demandes et réponses du DNS soient interceptées et changées. DNSSEC est conçu pour défendre contre les attaques de cette sorte. Ce paragraphe traite de la situation dans laquelle DNSSEC n'est pas disponible. Ce n'est pas le scénario de déploiement recommandé.

4.1.1 Attaques actives contre du matériel de clé IPSECKEY

La première sorte d'attaque active est lorsque l'attaquant remplace le matériel de clés soit par une clé sous son contrôle soit par n'importe quoi.

Le champ passerelle est soit non manipulé soit nul. La négociation IKE va donc survenir avec le système d'extrémité d'origine. Pour que cette attaque réussisse, l'attaquant doit effectuer une attaque par interposition contre la négociation IKE. Cette attaque exige que l'attaquant soit capable d'intercepter et de modifier les paquets sur le chemin de transmission entre IKE et les paquets de données.

Si l'attaquant n'est pas capable d'effectuer cette attaque par interposition sur la négociation IKE, il en résultera une attaque de déni de service, car la négociation IKE échouera.

Si l'attaquant est non seulement capable de monter des attaques actives contre le DNS mais aussi en position d'effectuer une attaque par interposition contre les négociations IKE et IPsec, l'attaquant sera alors capable de compromettre le canal IPsec résultant. Noter qu'un attaquant doit être capable d'effectuer des attaques actives contre le DNS sur les deux côtés de la négociation IKE pour que cela réussisse.

4.1.2 Attaques actives contre du matériel de passerelle IPSECKEY

La seconde sorte d'attaque active est celle dans laquelle l'attaquant remplace l'adresse de la passerelle pour qu'elle pointe sur un nœud qui se trouve sous son contrôle. L'attaquant remplace alors la clé publique ou la retire. Si la clé publique a été retirée, l'attaquant pourra alors fournir une clé publique à ses mesures dans un second enregistrement.

Cette seconde forme crée des attaques par interposition simples car l'attaquant peut alors créer un second tunnel vers la destination réelle. Noter que, comme précédemment, cela exige que l'attaquant monte aussi une attaque active contre celui qui répond.

Noter que l'attaque par interposition ne peut pas simplement transmettre des paquets de texte en clair à la destination d'origine. Alors que la destination peut vouloir parler en clair, en répondant à l'envoyeur d'origine, l'envoyeur aura déjà créé un politique qui attend du texte chiffré. Et donc, l'attaquant aura besoin d'intercepter le trafic dans les deux directions. Dans certains cas, l'attaquant peut être capable d'accomplir l'interception complète en utilisant la technologie de la traduction d'adresse/accès réseau (NAT/NAPT, *Network Address/Port Translation*).

Cette attaque est plus facile que la première parce que l'attaquant N'A PAS besoin d'être sur le chemin de transmission de bout en bout. L'attaquant a seulement besoin d'être capable de modifier les réponses du DNS. Cela peut être fait par une modification de paquet, par diverses sortes d'attaques par mise en compétition, ou par des méthodes qui polluent les antémémoires du DNS.

Si l'intégrité de bout en bout du RR IPSECKEY est suspecte, le client terminal DOIT restreindre son utilisation de RR IPSECKEY aux cas où le nom du propriétaire du RR correspond au contenu du champ passerelle. Comme le nom du propriétaire du RR est supposé lorsque le champ passerelle est nul, un champ passerelle nul est considéré comme une correspondance.

Et donc, tout enregistrement obtenu dans des conditions non vérifiées (par exemple, pas de DNSSEC ou de chemin de confiance avec la source) qui a un champ passerelle non nul DOIT être ignoré

Cette restriction élimine les attaques contre le champ passerelle, qui sont considérées comme plus facile, car l'attaque n'a pas besoin d'être sur le chemin de transmission.

Dans le cas d'un RR IPSECKEY avec une valeur de trois dans son champ de type de passerelle, le champ passerelle contient un nom de domaine. L'interrogation suivante exige de traduire ce nom en une adresse IP ou le RR IPSECKEY sera aussi soumis à des attaques par interposition. Si l'intégrité de bout en bout de cette seconde interrogation est suspecte, les dispositions ci-dessus s'appliquent alors aussi. Le RR IPSECKEY DOIT être ignoré chaque fois que la passerelle résultante ne correspond pas au QNAME de l'interrogation du RR IPSECKEY d'origine.

5. Considérations relatives à l'IANA

Le présent document met à jour le registre de l'IANA pour les types d'enregistrement de ressource du DNS en allouant le type 45 à l'enregistrement IPSECKEY.

Le présent document crée deux nouveaux registres IANA, tous deux spécifiques de l'enregistrement de ressource IPSECKEY:

Le présent document crée un registre IANA pour le champ type d'algorithme.

Les valeurs 0, 1, et 2 sont définie au paragraphe 2.4. Les algorithmes numéros 3 à 255 peuvent être alloués par consensus IETF (voir la RFC 2434 [5]).

Le présent document crée un registre IANA pour le champ type de passerelle.

Les valeurs 0, 1, 2, et 3 sont définies au paragraphe 2.3. Les types de passerelle numéros 4 à 255 peuvent être alloués par action de normalisation (voir la RFC 2434 [5]).

6. Remerciements

Tous mes remerciements à Paul Hoffman, Sam Weiler, Jean-Jacques Puig, Rob Austein, et Olafur Gudmundsson, qui ont révisé ce document avec soin. Des remerciements supplémentaires à Olafur Gurmundsson pour sa mise en œuvre de référence.

7. Références

7.1 Références normatives

[1] P. Mockapetris, P., "Noms de domaines - Concepts et facilités", RFC1034, STD 13, novembre 1987.

[2] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", RFC1035, STD 13, novembre 1987.

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

[4] D. Eastlake 3rd, C. Kaufman, "Extensions de sécurité du système de noms de domaines", RFC 2065, janvier 1997. (*Obsolète, voir* RFC2535) (MàJ RFC1034, RFC1035) *(P.S.)*

[5] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", RFC 2434, BCP 26, octobre, 1998. *(Rendue obsolète par la RFC 5226)*

[6] S. Josefsson, "Codages de données Base16, Base32, et Base64", RFC 3548, juillet 2003.

7.2 Références pour information

[7] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", RFC 2407, novembre 1998. *(Obsolète, voir 4306)*

[8] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", RFC 2535, mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[9] D. Eastlake 3rd , "Clés DSA et SIG dans le système des noms de domaines (DNS)", RFC 2536, mars 1999. *(P.S.)*

[10] D. Easlake 3, "SIG RSA/SHA-1 et clés RSA dans le système des noms de domaine (DNS)", RFC 3110, mai 2001.

[11] D. Massey, S. Rose, "Limitation de la portée de l'enregistrement de ressource (RR) KEY", RFC 3445, décembre 2002. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) (MàJ RFC2535) *(P.S.)*

[12] S. Thomson et autres, "Extensions au DNS pour la prise en charge de IPv6", RFC 3596, octobre 2003. *(D.S.)*

Adresse de l'auteur

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA
mél : mcr@sandelman.ottawa.on.ca
URI : http://www.sandelman.ottawa.on.ca/

Déclaration de copyright

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

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