Groupe de travail Réseau
Request for Comments : 2539
Catégorie : En cours de normalisation

D. Eastlake, IBM
mars 1999
Traduction Claude Brière de L'Isle

Mémorisation des clés Diffie-Hellman dans le système des noms de domaines (DNS)

Statut du présent 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 décrit une méthode standard pour mémoriser les clés Diffie-Hellman dans le système des noms de domaines qui utilise les enregistrements de ressource KEY du DNS.

Remerciements
Une partie du format des clés Diffie-Hellman et la description qui en découle ont été tirées d'un travail en cours de Ashar Aziz ashar.aziz@eng.sun.com, Tom Markson markson@incog.com, et Hemma Prafullchandra hemma@eng.sun.com, De plus, les personnes suivantes ont fourni des commentaires utiles qui ont été incorporés : Ran Atkinson rja@inet.org, Thomas Narten <narten@raleigh.ibm.com>

Table des matières

1. Introduction

Le système des noms de domaines (DNS, *Domain Name System*) est le système actuel de base de données mondiale hiérarchique dupliquée et répartie pour l'adressage Internet, les mandataires de messagerie, et informations similaires. Le DNS a été étendu pour inclure les signatures numériques et les clés de chiffrement décrites dans la [RFC2535]. Le DNS peut donc être maintenant utilisé pour une distribution sécurisée des clés.

1.1 Sur le document

Le présent document décrit comment mémoriser les clés Diffie-Hellman dans le DNS. Sa lecture suppose de s'être familiarisé avec l'algorithme d'échange de clés Diffie-Hellman décrit dans [Schneier].

1.2 Sur Diffie-Hellman

Diffie-Hellman exige que deux parties interagissent pour déduire les informations de clés qui peuvent alors être utilisées pour l'authentification. Comme les RR SIG du DNS sont principalement utilisés comme authenticateurs mémorisés des informations de zone pour de nombreux résolveurs différents, aucun RR SIG d'algorithme Diffie-Hellman n'est défini. Par exemple, supposons que deux parties ont les secrets locaux "i" et "j". Supposons que chacun calcule respectivement X et Y comme suit :

X = g**i (mod p) Y = g**j (mod p)

Ils échangent ces quantités et chacun calcule alors un Z comme suit :

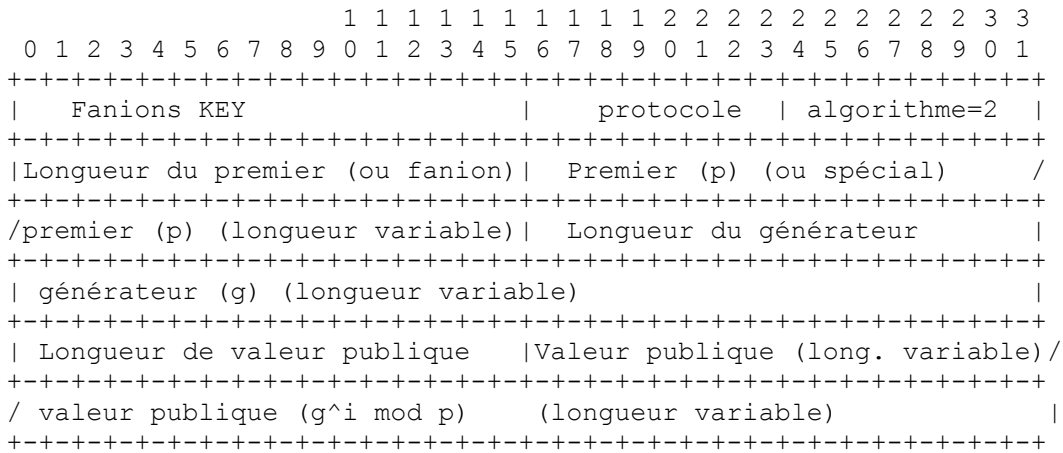
Zi = Y**i (mod p) Zj = X**j (mod p)

qui est le secret partagé entre les deux parties qu'un adversaire qui ne connaît pas i ou j ne sera pas capable de découvrir à partir du message échangé (sauf si l'adversaire peut déduire i ou j en effectuant un logarithme discret modulo p, ce qui est difficile pour des p et g forts).

La clé privée pour chaque partie est leur i (ou j) secret. La clé publique est la paire p et g, qui doit être la même pour les parties, et leur X (ou Y) individuel.

2. Enregistrements de ressource KEY Diffie-Hellman

Les clés Diffie-Hellman sont mémorisées dans le DNS comme des RR KEY utilisant l'algorithme numéro 2. La structure de la portion RDATA de ce RR est donnée ci-dessous. Les quatre premiers octets, incluant les champs de fanions, de protocole, et d'algorithme sont communs à tous les RR KEY, comme décrit dans la [RFC2535]. Le reste, de Longueur du nombre premier à Valeur publique est la partie "clé publique" du RR KEY. La période de validité de la clé n'est pas dans le RR KEY mais elle est indiquée par le ou les RR SIG qui signent et authentifient le ou les RR KEY à ce nom de domaine.



Longueur du premier est la longueur du nombre premier Diffie-Hellman (p) en octets si il est supérieur ou égal à 16. Premier contient la représentation binaire du nombre premier Diffie-Hellman avec l'octet de poids fort en premier (c'est à dire, dans l'ordre du réseau). Si le champ "Longueur du premier" est 1 ou 2, le champ "premier" est en fait un indice non signé dans un tableau de 65 536 paires de premier/générateur et la longueur du générateur DEVRAIT être zéro. Voir à l'Appendice A les entrées définies du tableau et à la Section 4 les informations sur l'allocation d'entrées supplémentaires du tableau. La signification des valeurs de zéro ou 3 à 15 est réservée pour "longueur de premier".

Longueur du générateur est la longueur du générateur (g) en octets. Le générateur est la représentation binaire du générateur avec l'octet de poids fort en premier. Longueur de valeur publique est la longueur de la valeur publique (g**i (mod p)) en octets. Valeur publique est la représentation binaire de la valeur DH publique avec l'octet de poids fort en premier.

L'enregistrement de ressource SIG algorithme=2 correspondant n'est pas utilisé, donc aucun format n'est défini pour lui.

3. Considérations de performances

Les mises en œuvre actuelles du DNS sont optimisée pour les petits transferts, normalement de moins de 512 octets incluant l'en-tête. Bien que de plus gros transferts s'effectuent correctement et que des travaux soient en cours pour rendre plus efficaces de plus gros transferts, il est toujours conseillé de faire des efforts raisonnables pour minimiser la taille des ensembles de RR KEY mémorisés au sein du DNS en cohérence avec la sécurité adéquate. Il faut garder présent à l'esprit que dans une zone sûre, un RR SIG d'authentification sera aussi retourné.

4. Considérations pour l'IANA

L'allocation d'une significations aux valeurs de Longueurs de premier de 0 et de 3 à 15 exige le consensus de l'IETF.

Les paires bien connues de premier/générateur de numéro 0x0000 à 0x07FF ne peuvent être allouées que par action de normalisation de l'IETF et la présente proposition de norme alloue 0x0001 à 0x0002. Les paires numéro 0s0800 à 0xBFFF peuvent être allouées sur la base de la documentation des RFC. Les paires numéro 0xC000 à 0xFFFF sont disponibles pour utilsation privée et ne sont pas coordonnées centralement. L'utilisation de telles paires privées en dehors d'un environnement confiné peut résulter en des conflits.

5. Considérations pour la sécurité

Beaucou des considérations générales de sécurité de la [RFC2535] s'appliquent. Les clés restituées à partir du DNS ne devraient pas être de confiance à moins 1) qu'elles aient été obtenues de manière sûre d'un résolveur sûr ou vérifiées de façon indépendante par l'usager, et (2) que ce résolveur sûr et cette obtention sûre ou sa vérification indépendante se conforment aux politiques de sécurité acceptables pour l'usager. Comme avec tous les algorithmes de chiffrement, évaluer la force nécessaire de la clé est important et dépend de la politique locale.

De plus, les considérations usuelles sur la force des clés Diffie-Hellman s'appliquent. (p-1)/2 devrait aussi être premier, g devrait être premier modulo p, p devrait être "grand", etc. [Schneier]

Références

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

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

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[Schneier] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 1996, John Wiley and Sons

Adresse de l'auteur

Donald E. Eastlake 3rd
Motorola
140 Forest Avenue
Hudson, MA 01749 USA
téléphone : +1 978-562-2827 (h)
+1 508-261-5434 (w)
Fax : +1 508-261-4447 (w)
mél : Donald.Eastlake@motorola.com

Appendice A Paires bien connues de premier/générateur

Ces nombres sont copiés des travaux sur IPSEC où la déduction de ces valeurs est expliquée plus en détails et où des informations supplémentaires sont disponibles. Richard Schroeppel a effectué tout le travail mathématique et de calcul pour le présent appendice.

A.1 Groupe bien connu 1 : un nombre premier de 768 bits

Le nombre premier est 2^768 - 2^704 - 1 + 2^64 * { [2^638 pi] + 149686 }. Sa valeur décimale est :
155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659164
244291000768028886422915080371891804634263272761303128298374438082089019628850917069131659317536746
955176311984337163722100721057791 9

Module du nombre premier : Longueur (mots de 32 bits) : 24, Données (en hexadécimal) :
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD129024E08 8A67CC74 020BBEA6 3B139B22
514A0879 8E3404DDEF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245E485B576 625E7EC6
F44C42E9 A63A3620 FFFFFFFF FFFFFFFF

Générateur : Longueur (mots de 32 bits) : 1, Données (en hexadécimal) : 2

A.2 Groupe bien connu 2 : un nombre premier de 1024 bits

Le nombre premier est 2^1024 - 2^960 - 1 + 2^64 * { [2^894 pi] + 129093 }. Sa valeur décimale est :
179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864925
541502180565485980503646440548199239100050792877003355816639229553136239076508735759914822574862575
007425302077447712589550957937778424442426617334727629299387668709205606050270810842907692932019128
194467627007

Module du nombre premier : Longueur (mots de 32 bits) : 32, Données (en hexadécimal) :
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD129024E08 8A67CC74 020BBEA6 3B139B22
514A0879 8E3404DDEF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245E485B576 625E7EC6
F44C42E9 A637ED6B 0BFF5CB6 F406B7EDEE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651
ECE65381FFFFFFFF FFFFFFFF

Générateur : Longueur (mots de 32 bits) : 1, Données (en hexadécimal) : 2

Déclaration complète de droits de reproduction

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