Groupe de travail Réseau
Request for Comments : 2931
RFC mise à jour : 2535
Catégorie : En cours de normalisation

D. Eastlake 3rd, Motorola
septembre 2000

Traduction Claude Brière de L'Isle

Signatures de demandes et de transactions du DNS (SIG(0))

Résumé
Les extensions au système des noms de domaines (DNS, *Domain Name System*) qui sont décrites dans la [RFC2535] fournissent aux résolveurs et applications qui ont des capacités de sécurité l'origine des données, la garantie d'intégrité de la transaction et l'authentification par l'utilisation de signatures numériques chiffrées.

L'expérience de la mise en œuvre a indiqué le besoin de changements mineurs mais non interopérables aux enregistrements de ressource Demande de signature et Transaction de signature (SIG(0)). Ces changements sont précisés ici.

Remerciements
Les personnes suivantes (par ordre alphabétique) sont chaleureusement remerciées pour leurs contributions et suggestions au présent mémoire : Olafur Gudmundsson, Ed Lewis, Erik Nordmark, Brian Wellington.

Table des matières

1. Introduction

Le présent document fait des changements mineurs mais non interopérables à des parties de la [RFC2535], avec laquelle on suppose que le lecteur s'est familiarisé, et il comporte du texte explicatif supplémentaire. Ces changements concernent les enregistrements de ressource (RR, *Resource Record*) SIG qui sont utilisés pour signer numériquement les demandes et réponses de transaction du DNS. Cet enregistrement de ressource, parce qu'il a un champ de type de zéro, est fréquemment appelé SIG(0). Les changements se fondent sur l'expérience de mise en œuvre et de tentatives de mise en œuvre avec TSIG [RFC2845] et la spécification de SIG(0) de la [RFC2535].

Les paragraphes mis à jour de la [RFC2535] sont tout le 4.1.8.1 et une partie de 4.2 et de 4.3. Aucun changement n'est fait ici aux RR qui se rapportent à KEY ou NXT ni aux traitements impliqués par l'origine des données ou le refus

d'authentification pour les données du DNS.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

2. Raison du concept de SIG(0)

SIG(0) pourvoit à la protection des transactions et demandes du DNS qui n'est pas fournie par les RR SIG, KEY, et NXT réguliers spécifiés dans la [RFC2535]. Les services d'origine authentifiée des données du DNS sécurisé fournissent soit des enregistrements de ressource de données protégées soit ils nient de façon authentique leur non existence. Ces services ne fournissent aucune protection pour les enregistrements glu, les demandes au DNS, aucune protection pour les en-têtes de message sur les demandes ou les réponses, et aucune protection de l'intégrité globale d'une réponse.

2.1 Authentification de transaction

Authentification de transaction signifie qu'un demandeur peut être sûr qu'il obtient au moins le message du serveur qu'il a interrogé et que les messages reçus sont en réponse à l'interrogation qu'il a envoyée. Ceci est réalisé par l'ajout facultatif d'un RR TSIG [RFC2845] ou, comme on le décrit ici, d'un enregistrement de ressource SIG(0) à la fin de la réponse, ce qui signe numériquement l'enchaînement de la réponse du serveur et l'interrogation du résolveur correspondante.

2.2 Authentification de demande

Les demandes peuvent aussi être authentifiées en incluant un TSIG ou, comme décrit ici, un RR SIG(0) spécial à la fin de la demande. L'authentification des demandes n'a aucune fonction dans les serveurs DNS qui empiète sur la spécification de mises à jour dynamiques. Les demandes avec une section d'informations supplémentaires non vide produisent une erreur en retour ou peuvent même être ignorées par quelques plus vieux serveurs DNS. Cependant, cette syntaxe pour la signature des demandes est définie pour l'authentification des demandes de mise à jour dynamique [RFC2136], pour les demandes TKEY [RFC2930], ou pour de futures demandes qui exigeraient l'authentification.

2.3 Clés

Les clés privées utilisées dans la sécurité de transaction appartiennent à l'hôte qui compose le message de réponse DNS, et non à la zone impliquée. L'authentification de demande peut aussi impliquer la clé privée de l'hôte ou autre entité qui compose la demande ou d'une zone qui sera affectée par la demande ou d'autres clés privées qui dépendent de l'autorité de demande qu'elle cherche à établir. La ou les clés publiques correspondantes sont normalement mémorisées dans le DNS et restituées à partir de lui pour leur vérification comme RR KEY avec un octet de protocole de 3 (DNSSEC) ou 255 (ANY).

Parce que les demandes et les réponses sont très variables, les SIG d'authentification de message ne peuvent pas être pré calculées. Il sera donc nécessaire de garder la clé privée en ligne, par exemple dans le logiciel ou dans un matériel directement connecté.

2.4 Différences entre TSIG et SIG(0)

Il y a des différences significatives entre TSIG et SIG(0).

Parce que TSIG implique que des clés secrètes soient installées chez le demandeur et chez le serveur, la présence d'une telle clé implique que l'autre partie comprenne TSIG et très vraisemblablement ait la même clé installée. De plus, TSIG utilise des codes d'authentification à hachage à clés qui sont relativement très bon marché à calculer. Il est donc courant d'authentifier des demandes avec TSIG et les réponses sont authentifiées avec TSIG si la demande correspondante est authentifiée.

D'un autre côté, SIG(0) utilise l'authentification avec clé publique, dans laquelle les clés publiques sont mémorisées dans des RR KEY du DNS et une clé privée est mémorisée chez le signataire. L'existence d'un tel RR KEY n'implique pas nécessairement la mise en œuvre de SIG(0). De plus, SIG(0) implique des opérations relativement chères de chiffrement à clé publique qui devraient être minimisées et la vérification d'une SIG(0) implique d'obtenir et de vérifier la KEY correspondante qui peut être une opération longue et coûteuse. Bien sûr, une politique d'utilisation de SIG(0) sur toutes les demandes et sa vérification avant de répondre conduirait, pour certaines configurations, à un cycle mortel avec la tentative d'obtenir et vérifier la KEY nécessaire pour authentifier la demande de SIG(0) résultant en demandes supplémentaires accompagnées par une SIG(0) conduisant à d'autres demandes accompagnées d'une SIG(0), etc. De plus, omettre les SIG(0)

lorsque elles ne sont pas exigées par les demandes diminue de moitié le nombre d'opérations de clé publique exigées par la transaction.

Pour ces raisons, les SIG(0) DEVRAIENT n'être utilisées dans les demandes que lorsque c'est nécessaire pour authentifier que le demandeur a les privilèges ou identités requis. Les SIG(0) sur les réponses sont définies de telle sorte qu'une SIG(0) ne soit pas exigée sur la demande correspondante et fournir quand même la protection de transaction. Pour les autres réponses, qu'elles soient authentifiées par le serveur ou que leur authentification soit exigée par le demandeur DEVRAIT être une option de configuration locale.

3. Enregistrement de ressource SIG(0)

La structure et le numéro de type des enregistrements de ressource SIG sont donnés au paragraphe 4.1 de la [RFC2535]. Cependant, tout le paragraphe 4.1.8.1 et une partie des paragraphes 4.2 et 4.3 qui se rapportent à SIG(0) devraient être considérés comme remplacés par ce qui figure ci-dessus. Tout conflit entre la [RFC2535] et le présent document concernant les enregistrements SIG(0) devraient être résolu en faveur du présent document.

Pour toutes les SIG(0) de transaction, le champ Signataire DOIT être un nom de l'hôte d'origine et il DOIT y avoir un RR KEY à ce nom avec la clé publique correspondant à la clé privée utilisée pour calculer la signature. (Le nom de domaine de l'hôte utilisé peut être le nom de transposition inverse de l'adresse IP pour une adresse IP de l'hôte si la KEY pertinente y est mémorisée.)

Pour tous les RR SIG(0), le nom du possesseur, la classe, le TTL, et le TTL original, n'ont aucune signification. Les champs de TTL DEVRAIENT être à zéro, le champ CLASS DEVRAIT être ANY. Pour conserver l'espace, le nom du possesseur DEVRAIT être une racine (un seul octet à zéro). Lorsque on désire l'authentification SIG(0) sur une réponse, ce RR SIG DOIT être considéré à la plus forte priorité de toute information supplémentaire à inclure dans la réponse. Si le RR SIG(0) ne peut pas être ajouté sans causer la troncature du message, le serveur DOIT altérer la réponse de telle sorte qu'une SIG(0) puisse être incluse. Cette réponse comporte seulement la question et un enregistrement SIG(0), et a le bit TC établi et le RCODE 0 (NOERROR). À ce point, le client devrait re-essayer la demande en utilisant TCP.

3.1 Calcul des signatures de demande et de transaction

Une demande DNS peut facultativement être signée en incluant une SIG(0) à la fin de la section informations supplémentaires de l'interrogation. Une telle SIG est identifiée par le fait qu'elle a un champ "type couvert" de zéro. Elle signe le message de demande DNS précédant en incluant l'en-tête DNS mais elle n'inclut pas l'en-tête UDP/IP et avant que les comptes de RR de demande aient été ajustés pour les inclusions de la SIG(0) de demande.

Elle est calculée en utilisant des "données" (voir au paragraphe 4.1.8 de la [RFC2535]) (1) de la section RDATA de la SIG omettant entièrement (pas en mettant juste à zéro) le sous champ de signature lui-même, (2) des messages d'interrogation du DNS, incluant l'en-tête DNS, mais pas l'en-tête UDP/IP et avant que les comptes de RR de réponse aient été ajustés pour l'inclusion de la SIG(0). C'est à dire :

données = RDATA | demande - SIG(0)

où "|" est la marque de l'enchaînement et RDATA est le RDATA de la SIG(0) qui est calculée moins la signature elle-même.

De même, une SIG(0) peut être utilisée pour sécuriser une réponse et la demande qui l'a produite. De telles signatures de transaction sont calculées en utilisant des "données" de (1) la section RDATA de la SIG en omettant la signature elle-même, (2) du message d'interrogation DNS entier qui a produit cette réponse, incluant l'en-tête DNS de l'interrogation mais pas son en-tête UDP/IP, et (3) du message de réponse DNS entier, incluant l'en-tête DNS mais pas l'en-tête UDP/IP avant que les comptes de RR de réponse aient été ajustés pour l'inclusion de la SIG(0).

C'est à dire :

données = RDATA | interrogation complète | réponse - SIG(0)

où "|" marque l'enchaînement et RDATA est le RDATA de la SIG(0) à calculer moins la signature elle-même.

La vérification d'une SIG(0) de réponse (qui est signée par la clé de l'hôte serveur, et non par la clé de zone) par le résolveur demandeur montre que l'interrogation et sa réponse n'ont pas été altérées dans le transit, que la réponse correspond à l'interrogation prévue, et que la réponse vient du serveur interrogé.

Dans le cas d'un message DNS via TCP, une SIG(0) sur le premier paquet de données est calculée avec des "données" comme ci-dessus et pour chaque paquet suivant, elle est calculée comme suit :

données = RDATA | charge utile DNS - SIG(0) | paquet précédent

où "|" marque l'enchaînement, RDATA est comme ci-dessus, et paquet précédent est la charge utile DNS précédente incluant l'en-tête DNS et la SIG(0) mais pas l'en-tête TCP/IP. La prise en charge de SIG(0) est FACULTATIVE pour TCP. Autrement, TSIG peut être utilisé après, si nécessaire, l'établissement d'une clé avec TKEY [RFC2930].

Sauf lorsque il est nécessaire d'authentifier une mise à jour, TKEY, ou une demande de privilèges similaires, les serveurs ne sont pas obligés de vérifier une SIG(0) de demande.

Note : les demandes et les réponses peuvent avoir une seule TSIG ou une SIG(0) mais pas à la fois une TSIG et une SIG(0).

3.2 Traitement des réponses et des RR SIG(0)

Si un RR SIG se trouve à la fin de la section informations supplémentaires d'une réponse et a un type couvert de zéro, c'est une signature de transaction qui couvre la réponse et l'interrogation qui a produit la réponse. Pour les réponses TKEY, il DOIT être vérifié et le message DOIT être rejeté si la vérification échoue, sauf spécification contraire pour le mode TKEY utilisé. Pour toutes les autres réponses, il PEUT être vérifié et le message PEUT être rejeté en cas d'échec de la vérification.

Si la vérification de la SIG(0) d'une réponse réussit, une telle authentification de transaction SIG n'authentifie pas directement la validité d'un RR de données dans le message. Cependant, elle authentifie qu'elles ont été envoyées par le serveur interrogé et n'ont pas été altérées. (Seul un RR SIG(0) approprié signé par la zone ou un suivi de clé retraçant son autorité jusqu'à la zone ou une configuration de résolveur statique peuvent authentifier directement les RR données, selon la politique de résolveur.) Si un résolveur ou un serveur ne met pas en œuvre les SIG de transaction et/ou de demande, il DOIT les ignorer sans émettre d'erreur lorsque ill sont facultatifs et les traiter comme fautifs lorsque ils sont exigés.

3.3 Durée de vie et expiration de SIG(0)

Les heures de création et d'expiration dans les SIG(0) sont destinées à résister aux attaques en répétition. Elles devraient être réglées de façon à former une plage horaire telle que les messages en dehors de la plage puissent être ignorés. Dans les réseaux IP, cette plage horaire ne devrait normalement pas s'étendre sur plus de 5 minutes dans le passé et 5 minutes vers l'avenir.

4. Considérations pour la sécurité

Aucune considérations sur la sécurité ne s'ajoute à celles de la [RFC2535].

L'inclusion des heures de conception et d'expiration de SIG(0) sous la signature améliore la résistance aux attaques en répétition.

5. Considérations relatives à l'IANA

Aucun nouveau paramètre n'est créé et aucune valeur de paramètre n'est allouée par le présent document.

Références

[RFC1982] R. Elz, R. Bush, "Arithmétique des numéros de série", août 1996. (MàJ RFC1034, RFC1035) *(P.S.)*

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

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

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

RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645) *(P.S.)*

[RFC2930] D. Eastlake 3rd, "Établissement de clés secrètes pour le DNS (TKEY RR)", septembre 2000. *(P.S.)*

Adresse de l'auteur

Donald E. Eastlake 3rd
Motorola
140 Forest Avenue
Hudson, MA 01749 USA
téléphone : 978-562-2827(perso) / 508-261-5434(bureau)
Fax : 978-567-7941(perso) / 508-261-4447(bureau)
mél : Donald.Eastlake@motorola.com

Appendice Changements à SIG(0) depuis la RFC 2535

Ajout d'un texte explicatif sur les différences entre TSIG et SIG(0).

Changement des données sur lesquelles SIG(0) est calculé pour inclure le RDATA SIG(0) autre que la signature elle-même de façon à sécuriser les heures de conception et d'expiration de la signature et résister aux attaques en répétition. Spécification de SIG(0) pour TCP.

Ajout de la discussion des heures appropriées de conception et d'expiration pour SIG(0).

Ajout d'une phrase pour indiquer que soit une TSIG soit une ou plusieurs SIG(0) peuvent être présente mais pas les deux.

Reformulation de certaines phrases pour les rendre plus claires.

Déclaration complète de droits de reproduction

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