Groupe de travail Réseau
Request for Comments : 3007
RFC mises à jour : 2535, 2136
RFC rendue obsolète : 2137
Catégorie : En cours de normalisation

B. Wellington, Nominum
novembre 2000

Traduction Claude Brière de L'Isle

Mise à jour dynamique sécurisée du système des noms de domaine (DNS)

Résumé
Le présent document proposes une méthode pour effectuer des mises à jour dynamiques sûres du système des noms de domaine (DNS, *Domain Name System*). La méthode décrite ici est destinée à être souple et utile tout en exigeant aussi peu de changements que possible au protocole. L'authentification du message de mise à jour dynamique est séparée de la validation DNSSEC ultérieure des données. La communication sûre fondée sur des demandes et transactions authentifiées est utilisée pour fournir l'autorisation.

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

1. Introduction

Le présent document définit un moyen pour sécuriser les mises à jour dynamiques du système des noms de domaines (DNS), permettant seulement à des sources autorisés de faire des changements au contenu d'une zone. Les opérations de mise à jour dynamique non sécurisées existantes forment la base du présent travail.

Une certaine familiarité avec le système DNS [RFC1034], [RFC1035] et sa mise à jour dynamique [RFC2136] sera utile et est supposée par le présent document. De plus, la connaissance des extensions de sécurité du DNS [RFC2535], de la sécurité de transaction SIG(0) [RFC2535], [RFC2931], et de la signature de transaction TSIG [RFC2845] est recommandée.

Le présent document met à jour des portions de la [RFC2535], en particulier le paragraphe 3.1.2, et de la [RFC2136]. Le présent document rend obsolète la [RFC2137], autre proposition pour la mise à jour dynamique sécurisée, due à l'expérience de la mise en œuvre.

1.1 Généralités sur la mise à jour dynamique du DNS

La mise à jour dynamique du DNS définit un nouveau code de fonctionnement *(opcode)* du DNS et une nouvelle interprétation du message DNS si cet opcode est utilisé. Une mise à jour peut spécifier des insertions ou suppressions de données, avec les prérequis nécessaires pour que les mises à jour se fassent. Tous les essais et changements pour une demande de mise à jour du DNS sont restreints à une seule zone, et sont effectués au serveur principal pour la zone. Le serveur principal pour une zone dynamique doit incrémenter le numéro de série du début d'autorité (SOA, *Start Of Authority*) de la zone lorsque une mise à jour survient ou avant le prochaine restitution du SOA.

1.2 Généralités sur la sécurité des transactions du DNS

Les échanges de messages DNS qui incluent des enregistrements TSIG [RFC2845] ou SIG(0) [RFC2535], [RFC2931] permettent à deux entités DNS d'authentifier des demandes et réponses DNS envoyées entre elles. Un code d'authentification de message (MAC, *message authentication code*) TSIG est déduit d'un secret partagé, et un SIG(0) est généré à partir d'une clé privée dont la contrepartie publique est mémorisée dans le DNS. Dans les deux cas, un enregistrement contenant la signature/MAC du message est inclus comme enregistrement de ressource final dans un message DNS. Les hachages chiffrés, utilisés dans la TSIG ne coûtent rien à calculer et vérifier. Le chiffrement de clé publique, tel qu'utilisé dans SIG(0), est plus adaptable car les clés publiques sont mémorisées dans le DNS.

1.3 Comparaison de l'authentification des données et du message

L'authentification fondée sur le message, qui utilisé TSIG ou SIG(0), assure la protection du message entier avec une seule signature et une seule vérification qui, dans le cas de TSIG, sont une création et vérification de MAC relativement bon marché. Pour les demandes de mise à jour, cette signature peut établir, sur la base de la politique ou de la négociation de clé, l'autorité pour faire la demande.

Les enregistrements SIG de DNSSEC peuvent être utilisés pour protéger l'intégrité des RR individuels ou des ensembles de RR *(RRset)* dans un message DNS avec l'autorité du propriétaire de la zone. Cependant, cela ne peut pas protéger suffisamment la demande de mise à jour dynamique.

Utiliser les enregistrements SIG pour sécuriser les RRsets dans une demande de mise à jour est incompatible avec la conception de la mise à jour, telle que décrit ci-dessous, et exigerait dans tous les cas plusieurs coûteuses signatures et vérifications de clés publiques .

Les enregistrements SIG ne couvrent pas l'en-tête de message, qui comporte les comptes d'enregistrements. Donc, il est possible à un malveillant d'insérer ou supprimer des RRsets dans une demande de mise à jour sans causer un échec de vérification.

Si des enregistrements SIG étaient utilisés pour protéger la section des prérequis, il serait impossible de déterminer si les SIG eux-mêmes étaient un prérequis ou s'ils étaient simplement utilisés pour la validation.

Dans la section Mise à jour d'une demande de mise à jour, signer les demandes d'ajout d'un RRset est direct, et cette signature pourrait être utilisée en permanence pour protéger les données, comme spécifié dans la [RFC2535]. Cependant, si un RRset est supprimé, une SIG n'a pas de données à couvrir.

1.4 Signatures de données et de message

Comme spécifié dans la [RFC3008], le processus de validation DNSSEC effectué par un résolveur NE DOIT PAS traiter de clé non de zone sauf si la politique locale en décide autrement. Lors d'une mise à jour dynamique sécurisée les données de zone modifiées dans une zone signée DOIVENT être signées par une clé de zone pertinente. Cela dissocie complètement l'authentification d'une demande de mise à jour de l'authentification des données elles-mêmes.

La principale utilité des clés d'hôte et d'utilisateur, par rapport à DNSSEC, est d'authentifier les messages, y compris de mise à jour dynamique. Donc, les clés d'hôte et d'utilisateur PEUVENT être utilisées pour générer des enregistrements SIG(0) pour authentifier les mises à jour et PEUVENT être utilisées dans le processus TKEY [RFC2930] pour générer des secrets TSIG partagés. Dans les deux cas, aucun enregistrement SIG généré par des clés non de zone ne sera utilisé dans un processus de validation DNSSEC sauf si la politique locale l'impose.

L'authentification des données, une fois qu'elles sont présentes dans le DNS, n'implique que les clés de zone DNSSEC et les signatures générées par elles.

1.5 Force de signature

Le paragraphe 3.1.2 de la [RFC2535] définit le champ signataire d'une clé comme les quatre bits finaux du champ Fanions, mais ne définit pas sa valeur. Cette proposition laisse ce champ indéfini. Mettant à jour la [RFC2535], ce champ DEVRAIT être réglé à 0 dans les enregistrements KEY, et DOIT être ignoré.

2. Authentification

Les enregistrements TSIG ou SIG(0) DOIVENT être inclus dans tous les messages de mise à jour dynamique sécurisés. Cela permet au serveur de déterminer de façon vérifiable l'origine d'un message. Si le message contient une authentification sous la forme d'un SIG(0), l'identité de l'envoyeur (c'est-à-dire, le principal) est le propriétaire du RR KEY qui a généré le SIG(0). Si le message contient un TSIG généré par un secret partagé configuré de façon statique, le principal est le même que le nom du secret partagé ou en est déduit. Si le message contient un TSIG généré par un secret partagé configuré de façon dynamique, le principal est le même que celui qui a authentifié le processus TKEY ; si le processus TKEY n'a pas été authentifié, aucune information n'est connue sur le principal, et le secret partagé TSIG associé NE DOIT PAS être utilisé pour une mise à jour dynamique sûre.

Les signatures SIG(0) NE DEVRAIENT PAS être générées par des clés de zone, car les transactions sont initiées par un hôte ou un utilisateur, pas par une zone.

Les enregistrements SIG du DNSSEC (autres que SIG(0)) PEUVENT être inclus dans un message de mise à jour, mais NE DOIVENT PAS être utilisés pour authentifier la demande de mise à jour.

Si une mise à jour échoue parce qu'elle est signée avec une clé non autorisée, le serveur DOIT indiquer l'échec en retournant un message avec le RCODE REFUSÉ. Les autres erreurs de TSIG, SIG(0), or de mise à jour dynamique sont retournées comme spécifié dans la description de protocole appropriée.

3. Politique

Toute politique est configurée par l'administrateur de zone et mise en application par le serveur de noms principal de la zone. La politique dicte les actions autorisées que peut effectuer un principal authentifié. Les vérifications de politique se fondent sur le principal et l'action désirée, où le principal est déduit de la clé de signature du message et appliqué aux messages de mise à jour dynamiques signés avec cette clé.

La politique du serveur définit les critères qui déterminent si la clé utilisée pour signer la mise à jour est autorisée à effectuer les mises à jour demandées. Par défaut, un principal NE DOIT PAS être autorisé à faire de changements aux données de zone ; toutes les permissions DOIVENT être activées par la configuration.

La politique est pleinement mise en œuvre dans la configuration du serveur principal de la zone pour plusieurs raisons. Cela supprime les limitations imposées par la politique de codage à un nombre fixé de bits (comme le champ Signataire du RR KEY). La politique n'est pertinente que dans le serveur qui l'applique, de sorte qu'il n'y a pas de raison de l'exposer. Finalement, un changement de politique ou un nouveau type de politique ne devrait pas affecter le protocole du DNS ou le format des données, et ne devrait pas causer de défaillance d'interopérabilité.

3.1 Politiques standard

Les mises en œuvre DEVRAIENT permettre aux politiques de contrôle d'accès d'utiliser le principal comme un jeton d'autorisation, et PEUVENT aussi permettre aux politiques d'accorder une permission à un message signé sans considération du principal.

Une pratique courante serait de restreindre les permissions d'un principal par nom de domaine. C'est-à-dire qu'il pourrait être permis à un principal d'ajouter, supprimer, ou modifier les entrées correspondant à un ou plusieurs noms de domaine. Les mises en œuvre DEVRAIENT permettre un contrôle d'accès par nom, et DEVRAIENT fournir une représentation concise du nom propre du principal, de ses sous-domaines, et de tous les noms dans la zone.

De plus, un serveur DEVRAIT permettre de restreindre les mises à jour par type de RR, afin qu'un principal puisse ajouter, supprimer, ou modifier des types spécifiques d'enregistrements à certains noms. Les mises en œuvre DEVRAIENT permettre un contrôle d'accès par type, et DEVRAIENT fournir des représentations concises de tous les types et de tous les types "utilisateur", où un type d'utilisateur est défini comme celui qui n'affecte pas le fonctionnement du DNS lui-même.

3.1.1 Types d'utilisateur

Les types d'utilisateur incluent tous les types de données excepté SOA, NS, SIG, et NXT. Les enregistrements SOA et NS NE DEVRAIENT PAS être modifiés par des utilisateurs normaux, car ces types créent ou modifient des points de délégation. L'ajout d'enregistrements SIG peut conduire à des attaques résultant en une charge de travail supplémentaire pour les résolveurs, et la suppression d'enregistrements SIG peut conduire à du travail supplémentaire pour le serveur si la SIG de zone a été supprimée. Noter que ces enregistrements ne sont pas interdits, mais non recommandés pour l'utilisateur normal.

Les enregistrements NXT NE DOIVENT PAS être créés, modifiés, ou supprimés par une mise à jour dynamique, car leur mise à jour cause de l'instabilité dans le protocole. Ceci est une mise à jour de la [RFC2136].

Les questions qui concernent les mises à jour des enregistrements KEY sont discutées dans la section des considérations pour la sécurité.

3.2 Politiques supplémentaires

Les utilisateurs sont libres de mettre en œuvre toutes les politiques. Les politiques peuvent être aussi spécifiques ou générales

que désiré, et aussi complexes qu'on le veut. Elles peuvent dépendre du principal ou de toute autre caractéristique du message signé.

4. Interaction avec DNSSEC

Bien que ce protocole ne change pas la façon dont sont traitées les mises à jour des zones sécurisées, il y a un certain nombre de questions qui devraient être précisées.

4.1 Ajout des SIG

Une demande de mise à jour autorisée PEUT inclure des enregistrements SIG avec chaque RRset. Comme les enregistrements SIG (sauf les enregistrements SIG(0)) NE DOIVENT PAS être utilisés pour l'authentification du message Mise à jour, ils ne sont pas exigés.

Si un principal est autorisé à mettre à jour des enregistrements SIG et si il y a des enregistrements SIG dans la mise à jour, les enregistrements SIG sont ajoutés sans vérification. Le serveur PEUT examiner les enregistrements SIG et éliminer les SIG qui ont leur période de validité temporelle dans le passé.

4.2 Suppression des SIG

Si un principal est autorisé à mettre à jour des enregistrements SIG et si la mise à jour spécifie la suppression des enregistrements SIG, le serveur PEUT choisir d'outrepasser l'autorité et de refuser la mise à jour. Par exemple, le serveur peut permettre que tous les enregistrements SIG qui ne sont pas générés par une clé de zone soient supprimés.

4.3 Mises à jour non explicites des SIG

Si la zone mise à jour est sécurisée, le RRset affecté par une opération de mise à jour DOIT, à l'achèvement de la mise à jour, être signé conformément à la politique de signature de la zone. Cela va normalement exiger qu'un ou plusieurs enregistrements SIG soient générés par une ou plusieurs clés de zone dont les composants privés DOIVENT être en ligne [RFC3008].

Lorsque le contenu d'un RRset est mis à jour, le serveur PEUT supprimer tous les enregistrements SIG associés, car ils ne seront plus valides.

4.4 Effets sur la zone

Si des changements sont faits, le serveur DOIT, si nécessaire, générer un nouvel enregistrement SOA et de nouveaux enregistrements NXT, et les signer avec les clés de zone appropriées. Les changements aux enregistrements NXT par mise à jour dynamique sécurisée sont explicitement interdits. Les mises à jour SOA sont permises, car la maintenance des paramètres de SOA est hors de la portée du protocole du DNS.

5. Considérations pour la sécurité

Le présent document exige qu'une clé de zone et éventuellement d'autre matériel cryptographique secret soit détenu dans un hôte en ligne, connecté au réseau, qui sera très vraisemblablement un serveur de noms. Le secret de clé de matériel est à la merci de la sécurité de l'hôte. Exposer ce secret fait courir aux données du DNS un risque d'attaques déguisées. Les données qui courent un risque sont aussi bien celles servies par la machine que celles déléguées à partir de cette machine.

Permettre les mises à jour des enregistrements KEY peut conduire à des résultats indésirables, car il peut être permis à un principal d'insérer une clé publique sans qu'il détienne la clé privée, et qu'il puisse se faire passer pour le propriétaire de la clé.

6. Remerciements

L'auteur tient à remercier les personnes suivantes pour leur relecture et leur commentaires (en ordre alphabétique) :
Harald Alvestrand, Donald Eastlake, Olafur Gudmundsson, Andreas Gustafsson, Bob Halley, Stuart Kwan, et Ed Lewis.

7. 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. (*MàJ par la* RFC6604)

[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.

[RFC2137] D. Eastlake 3rd, "Mise à jour dynamique sécurisée du système de noms de domaines", avril 1997. *(Remplacée par la présente RFC)*

[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.)*

[RFC2931] D. Eastlake 3rd, "Signatures de demandes et de transactions du DNS (SIG(0))", septembre 2000. *(P.S.)*

[RFC3008] B. Wellington, "Autorité de signature de sécurité du système de noms de domaines (DNSSEC)", novembre 2000. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

8. Adresse de l'auteur

Brian Wellington
Nominum, Inc.
950 Charter Street
Redwood City, CA 94063
USA
téléphone : +1 650 381 6022
mél : Brian.Wellington@nominum.com

9. Déclaration complète de droits de reproduction

Remerciement

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