Groupe de travail Réseau
Request for Comments : 4986
Catégorie : Information

Traduction Claude Brière de L'Isle

H. Eland, Afilias Limited
R. Mundy, SPARTA, Inc.
S. Crocker, Shinkuro Inc.
S. Krishnaswamy, SPARTA, Inc.
août 2007

Exigences relatives au changement des ancres de confiance de la sécurité du DNS (DNSSEC)

Résumé
Chaque résolveur DNS à capacité de sécurité doit avoir au moins une ancre de confiance à utiliser comme base pour la validation des réponses provenant des zones signées du DNS. Pour diverses raisons, la plupart des résolveurs DNS à capacité de sécurité sont supposés avoir plusieurs ancres de confiance. Pour certaines opérations, la surveillance et la mise à jour manuelle des ancres de confiance peut être faisable, mais de nombreuses opérations vont exiger des méthodes automatisées pour la mise à jour de leurs ancres de sécurité dans leurs résolveurs à capacité de sécurité. Le présent document identifie les exigences qui doivent être satisfaites par une solution de changement automatisé des ancres de confiance pour les résolveurs DNS à capacité de sécurité.

Table des Matières

1. Introduction....1
2. Terminologie....2
3. Fondements....2
4. Définitions....2
5. Exigences....3
5.1 Adaptabilité....3
5.2 Pas de droits de propriété intellectuelle connus....4
5.3 Applicabilité générale....4
5.4 Prise en charge des réseaux privés....4
5.5 Détection des ancres de confiance périmées....4
5.6 Permetttre les opérations manuelles....4
5.7 Changements planifiés et non planifiés....4
5.8 Contraintes de temps....4
5.9 Grande disponibilité....5
5.10. Nouveaux types de RR....5
5.11 Prise en charge des opérations de maintenance d'ancre de confiance....5
5.12 Récupération de compromission....5
5.13 Non dégradation de la confiance....5
6. Considérations sur la sécurité....5
7. Remerciements....5
8. Références normatives....5
Adresse des auteurs....6
Déclaration complète de droits de reproduction....6

1. Introduction

Les extensions de sécurité du système des noms de domaine (DNSSEC, *Domain Name System Security Extensions*) telles que décrites dans les [RFC4033], [RFC4034], et [RFC4035], définissent de nouveaux enregistrements et modifications du protocole au DNS qui permettent aux résolveurs à capacité de sécurité de valider les enregistrements de ressource (RR,

resource record) provenant d'une ou plusieurs ancres de confiance détenues par ces résolveurs à capacité de sécurité.

Les résolveurs à capacité de sécurité devront initialement obtenir leurs ancres de confiance d'une manière digne de confiance pour s'assurer que les ancres de confiance sont correctes et valides. Cette étape initiale peut être accomplie de diverses façons ; cependant, les détails de cette étape sortent du domaine d'application du présent document. Une fois qu'un opérateur a obtenu des ancres de confiance, entrer initialement les ancres de confiance dans leurs résolveurs à capacité de sécurité va être dans de nombreuses instances une opération manuelle.

Pour certains environnements de fonctionnement, la gestion manuelle des ancres de confiance pourrait être une approche viable. Cependant, de nombreux environnements de fonctionnement vont exiger une méthode plus automatique, fondée sur la spécification, pour mettre à jour et gérer les ancres de confiance. Le présent document donne une liste d'exigences qui peuvent être utilisées pour mesurer de façon cohérente l'efficacité de tout mécanisme de changement automatique d'ancre de confiance proposé.

2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

L'utilisation des termes de la RFC 2119 dans les exigences est destinée à décrire sans ambiguïté une exigence. Si un compromis doit être fait entre des exigences en conflit lors du choix d'une solution, l'exigence avec un terme DOIT aura le pas sur une préférence dont l'exigence est marquée DEVRAIT, PEUT, ou RECOMMANDÉE. Il est entendu qu'un compromis peut devoir être fait entre des exigences qui contiennent toutes deux le langage de la RFC 2119.

3. Fondements

Les résolveurs du DNS ont besoin d'avoir un ou plusieurs points de départ à utiliser pour obtenir des réponses du DNS. Les points de départ pour les résolveurs d'extrémité sont normalement les adresses IP d'un ou plusieurs serveurs de noms récurrents. Les points de départ pour les serveurs de noms récurrents sont normalement les adresses IP des serveurs racine de noms du DNS. De même, les résolveurs à capacité de sécurité doivent avoir un ou plusieurs points de départ à utiliser pour construire la chaîne authentifiée pour valider une réponse signée du DNS. Au lieu des adresses IP, DNSSEC exige que chaque résolveur fasse confiance à un ou plusieurs RR DNSKEY ou RR DS comme point de départ. Chacun de ces points de départ est appelé une ancre de confiance.

On devrait noter que les RR DNSKEY et les RR DS ne sont pas des ancres de confiance quand ils sont créés par l'opérateur de zone signée ni ne sont des ancres de confiance parce que les enregistrements sont publiés dans la zone signée. Un RR DNSKEY ou un RR DS devient une ancre de confiance quand un opérateur d'un résolveur à capacité de sécurité détermine que la clé publique ou le hachage va être utilisé comme ancre de confiance. Donc, l'opérateur de zone signée qui a créé et/ou publié ces RR peut ne pas savoir si un des RR DNSKEY ou RR DS associé à sa zone est utilisé comme ancre de confiance par les résolveurs à capacité de sécurité. Les exceptions évidentes sont les RR DNSKEY pour la zone racine, qui vont être utilisés comme ancres de confiance par de nombreux résolveurs à capacité de sécurité. Pour diverses raisons, les RR DNSKEY ou les RR DS provenant de zones autres que racine peuvent être utilisés par les opérateurs de résolveurs à capacité de sécurité comme ancres de confiance. Il s'ensuit que la responsabilité incombe à l'opérateur du résolveur à capacité de sécurité de s'assurer que les RR DNSKEY et/ou DS qu'ils ont choisi d'utiliser comme ancres de confiance sont valides au moment où ils sont utilisés par le résolveur à capacité de sécurité comme point de départ pour la construction de la chaîne d'authentification pour valider une réponse DNS signée.

Quand les opérateurs de résolveurs à capacité de sécurité choisissent une ou plusieurs ancres de confiance, ils doivent aussi déterminer la ou les méthodes qu'ils vont utiliser pour s'assurer qu'ils utilisent des RR valides et qu'ils sont capables de déterminer quand les RR utilisés comme ancres de confiance devraient être remplacés ou supprimés. Les premiers qui ont adopté les zones signées du DNS ont publié des informations sur les processus et méthodes qu'ils utilisent quand leurs RR DNSKEY et/ou RR DS changent de sorte que les opérateurs de résolveurs à capacité de sécurité puisssent changer manuellement les ancres de confiance au moment approprié. Cette approche manuelle n'est pas adaptée, et conduit donc au besoin d'une approche automatisée, fondée sur la spécification pour le changement des ancres de confiance pour les résolveurs à capacité de sécurité.

4. Définitions

Le présent document utilise les définitions contenues à la Section 2 de la RFC 4033, plus les définitions supplémentaires suivantes :

Ancre de confiance : d'après la RFC 4033, "Un hachage configuré de RR DNSKEY ou de RR DS d'un RR DNSKEY. Un résolveur à capacité de sécurité validant utilise cette clé publique ou son hachage comme point de départ pour construire une chaîne d'authentification à une réponse DNS signée". De plus, un RR DNSKEY ou un RR DS est associé à précisément un point dans la hiérarchie du DNS, c'est-à-dire, une zone du DNS. Plusieurs ancres de confiance PEUVENT être associées à chaque zone du DNS et PEUVENT être détenues pas un nombre quelconque de résolveurs à capacité de sécurité. Les résolveurs à capacité de sécurité PEUVENT avoir des ancres de confiance provenant de multiples zones du DNS. Les responsables du fonctionnement des résolveurs à capacité de sécurité sont responsables de la détermination de l'ensemble des RR qui vont être utilisés comme ancres de confiance par ce résolveur.

Relation initiale de confiance : les opérateurs de résolveurs à capacité de sécurité doivent s'assurer qu'ils obtiennent initialement toutes les ancres de confiance d'une manière digne de confiance. Par exemple, la correction des RR DNSKEY de la zone racine pourrait être vérifiée en comparant ce que l'opérateur estime être la ou les ancres de confiance racines avec plusieurs sources "bien connues, comme le site de la Toile de l'IANA, les zones racines publiées du DNS, et la publication de la clé publique dans les formes sur papier bien connues. Pour les autres ancres de confiance, l'opérateur doit s'assurer de la précision et de la validité des RR DNSKEY et/ou DS avant de les désigner comme ancres de confiance. Cela pourrait être réalisé par une combinaison de relations techniques, procédurales, et contractuelles, ou l'utilisation d'autres relations de confiance existantes en dehors du protocole DNS actuel.

Distribution d'ancre de confiance : la ou les méthodes utilisées pour porter le ou les RR DNSKEY et/ou DS entre l'opérateur de zone signée et l'opérateur de résolveur à capacité de sécurité. La ou les méthodes DOIVENT être réputées suffisamment dignes de confiance par l'opérateur du résolveur à capacité de sécurité pour assurer l'authenticité de la source et l'intégrité des nouveaux RR pour maintenir la relation initiale de confiance requise pour désigner ces RR comme ancres de confiance.

Maintenance d'ancre de confiance : tout changement dans un résolveur à capacité de sécurité validant pour ajouter une nouvelle ancre de confiance, supprimer une ancre de confiance existante, ou remplacer une ancre de confiance existante par une autre. Ce changement pourrait être réalisé manuellement ou d'une manière automatique. Le responsable du fonctionnement du résolveur à capacité de sécurité est chargé d'établir des politiques et procédures pour s'assurer qu'une relation de confiance initiale suffisante est en place avant d'ajouter des ancres de confiance pour une zone DNS particulière à la configuration de son résolveur à capacité de sécurité.

Révocation et suppression d'ancre de confiance : l'invalidation d'une ancre de confiance particulière qui résulte quand l'opérateur de la zone signée révoque ou supprime un RR DNSKEY ou DS qui est utilisé comme ancre de confiance par tout résolveur à capacité de sécurité. Il est possible qu'un administrateur de zone invalide plus d'un RR à un moment donné ; donc, il DOIT être clair à l'administrateur de zone et au résolveur à capacité de sécurité quels RR exacts sont révoqués ou supprimés afin que la ou les ancres de confiance appropriées soient supprimées.

Changement d'ancre de confiance : la ou les méthodes nécessaires pour le remplacement sûr d'une ou plusieurs ancres de confiance détenues par les résolveurs à capacité de sécurité. Le changement d'ancre de confiance devrait être considéré comme un sous ensemble de la maintenance d'ancre de confiance.

Changement d'ancre de confiance normal ou pré-programmé : l'opérateur d'une zone DNSSEC signée a produit un ou des nouveaux RR DNSKEY et/ou DS au titre d'une routine de fonctionnement.

Changement d'ancre de confiance d'urgence ou non-programmé : l'opérateur d'une zone signée a produit un ou des nouveaux RR DNSKEY et/ou DS au titre d'un événement exceptionnel.

Révocation d'urgence d'ancre de confiance : l'opérateur d'une zone signée souhaite indiquer que le ou les RR DNSKEY et/ou DS courants ne sont plus valides au titre d'un événement exceptionnel.

5. Exigences

Les exigences pour le changement automatique d'ancre de confiance pour DNSSEC fondé sur la spécification figurent ci-

après.

5.1 Adaptabilité

La solution automatisée de changement d'ancre de confiance DOIT être capable de s'adapter à un usage à l'échelle de l'Internet. Le plus grand nombre probable d'instances de résolveurs à capacité de sécurité ayant besoin de changer une ancre de confiance vont être celles qui utilisent les clés publiques pour la zone racine comme ancres de confiance. Ce nombre pourrait être extrêmement grand si un certain nombre d'applications ont des résolveurs à capacité de sécurité incorporés.

La solution automatisée de changement d'ancre de confiance DOIT être capable de prendre en charge des ancres de confiance pour plusieurs zones et plusieurs ancres de confiance pour chaque zone du DNS. Le nombre d'ancres de confiance qui pourraient être configurées dans tout résolveur à capacité de sécurité validant n'est pas connu avec certitude pour l'instant ; dans la plupart des cas, il va être inférieur à 20 mais il peut même aller jusqu'à un millier.

5.2 Pas de droits de propriété intellectuelle connus

Parce que le changement d'ancre de confiance va probablement être "de mise en œuvre obligatoire", la Section 8 de la [RFC3979] exige que la solution technique choisie soit connue pour n'être pas grevée de droits de licence ou être disponible sans royalties.

À cette fin, "sans royalties" est défini comme suit : droit mondial, irrévocable et perpétuel d'utiliser sans redevances, dans le commerce ou autrement, où "utiliser" inclut les descriptions d'algorithmes, la distribution et/ou l'utilisation de mises en œuvre matérielle, la distribution et/ou l'utilisation de systèmes logiciels en forme source et/ou binaire, dans toutes les applications du DNS ou de DNSSEC incluant le service de registre, registraire, nom de domaines incluant d'autorité, récurrent, de mise en mémoire tampon, de transmission, de résolveur d'extrémité, ou similaire.

En résumé, aucune mise en œuvre, aucun distributeur, ou opérateur de la technologie choisie pour la gestion d'ancre de confiance ne devra être supposé ou tenu de payer de droit à tout détendeur de droits de propriété intellectuelle pour le droit de mettre en œuvre, distribuer, ou faire fonctionner un système qui inclut la solution de mise en œuvre obligatoire choisie.

5.3 Applicabilité générale

La solution DOIT fournir la capacité de maintenir les ancres de confiance dans les résolveurs à capacité de sécurité pour toute zone du DNS.

5.4 Prise en charge des réseaux privés

La solution DOIT prendre en charge les réseaux privés avec leur propre hiérarchie du DNS.

5.5 Détection des ancres de confiance périmées

La solution de changement d'ancre de confiance DOIT permettre à un résolveur à capacité de sécurité validant d'être capable de détecter si le ou les RR DNSKEY et/ou DS ne peuvent plus être mis à jour étant donné l'ensemble courant d'ancres de confiance actuelles. Dans ce cas, le résolveur devrait informer l'opérateur de la nécessité de rétablir la confiance initiale.

5.6 Permetttre les opérations manuelles

L'opérateur d'un résolveur à capacité de sécurité peut choisir le changement manuel ou automatisé, mais le protocole de changement doit permettre à la mise en œuvre de prendre en charge les deux opérations automatisée et manuelle de maintenance d'ancre de confiance. La mise en œuvre du protocole de changement va probablement être obligatoire, mais cela sort du domaine d'application de ce document d'exigences.

5.7 Changements planifiés et non planifiés

La solution DOIT permettre des changements d'ancres de confiance aussi bien prévus (pré-programmés) que non prévus (non programmés). La prise en charge de la fourniture d'une relation de confiance initiale est FACULTATIVE.

5.8 Contraintes de temps

Les enregistrements de ressource utilisés comme ancres de confiance DEVRAIENT être capables d'être distribués aux résolveurs à capacité de sécurité en temps utile.

Les résolveurs à capacité de sécurité ont besoin d'acquérir de nouveaux RR DNSKEY et/ou DS et de supprimer ceux qui sont révoqués qui sont utilisés comme ancres de confiance pour une zone afin qu'aucun vieux RR ne soit utilisé comme ancre de confiance après que la zone a produit de nouveaux RR ou révoqué les RR existants.

5.9 Grande disponibilité

Les informations sur la vue de l'administrateur de zone de l'état des enregistrements de ressource utilisés comme ancres de confiance DEVRAIENT être disponibles de façon fiable à tout moment aux résolveurs à capacité de sécurité. Les informations sur les enregistrements de ressource qu'un administrateur de zone a invalidés et qui sont connus pour être utilisés comme ancres de confiance devraient être disponibles de façon fiable pendant une durée raisonnable.

5.10. Nouveaux types de RR

Si une solution de changement d'ancre de confiance exige de nouveaux types de RR ou des modifications de protocole, cela devrait être pris en compte dans l'évaluation des solutions. Le groupe de travail devra déterminer si ces changements sont une bonne chose, une mauvaise chose ou autre chose.

5.11 Prise en charge des opérations de maintenance d'ancre de confiance

La solution de changement d'ancre de confiance DOIT prendre en charge les opérations qui permettent à un résolveur à capacité de sécurité validant d'ajouter une nouvelle ancre de confiance, de supprimer une ancre de confiance existante, ou de remplacer par une autre une ancre de confiance existante.

5.12 Récupération de compromission

La solution de changement d'ancre de confiance DOIT permettre à un résolveur à capacité de sécurité d'être capable de récupérer de la compromission de toute ancre de confiance configurée pour une zone tant qu'au moins une autre clé, qui est connue pour n'avoir pas été compromise, est configurée comme ancre de confiance pour cette même zone à ce résolveur.

5.13 Non dégradation de la confiance

La solution de changement d'ancre de confiance DOIT fournir des moyens suffisants pour assurer l'authenticité et l'intégrité afin que la relation de confiance existante ne se dégrade pas en effectuant le changement.

6. Considérations sur la sécurité

Le présent document définit les exigences globales pour une solution automatisée du changement d'ancre de confiance fondée sur la spécification pour les résolveurs à capacité de sécurité mais ne définit pas spécifiquement les mécanismes de sécurité nécessaires pour satisfaire ces exigences.

7. Remerciements

Le présent document reflète l'opinion majoritaire des membres du groupe de travail DNSEXT sur le sujet des exigences relatives au changement d'ancre de confiance de DNSSEC. Les contributions faites par les divers membres du groupe de travail pour améliorer la lisibilité et le style de ce document ont été accueillies avec reconnaissance.

8. Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3979] S. Bradner, éd., "Droits de propriété intellectuelle dans les technologies de l'IETF", mars 2005. (*MàJ par* RFC4879) (BCP0079 ; *Remplacée par* RFC8179)

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005. (*MàJ par* RFC9077)

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005. *(P.S. ; MàJ par* RFC8198, 9077

Adresse des auteurs

Howard Eland
Afilias Limited
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
USA
mél : heland@afilias.info

Russ Mundy
SPARTA, Inc.
7110 Samuel Morse Dr.
Columbia, MD 21046
USA
mél : mundy@sparta.com

Steve Crocker
Shinkuro Inc.
1025 Vermont Ave, Suite 820
Washington, DC 20005
USA
mél : steve@shinkuro.com

Suresh Krishnaswamy
SPARTA, Inc.
7110 Samuel Morse Dr.
Columbia, MD 21046
USA
mél : suresh@sparta.com

Déclaration complète de droits de reproduction