Groupe de travail Réseau
Request for Comments : 4470
RFC mises à jour : 4035, 4034
Catégorie : Sur la voie de la normalisation

S. Weiler, SPARTA, Inc.
J. Ihren, Autonomica AB
avril 2006
Traduction Claude Brière de L'Isle

Traitement minimal des enregistrements NSEC et de la signature en ligne DNSSEC

Résumé
Le présent document décrit comment construire des enregistrements de ressource NSEC du DNSSEC qui couvrent une plus petite gamme de noms que selon la RFC 4034. En générant et signant ces enregistrements à la demande, les serveurs de noms d'autorité peuvent effectivement arrêter la divulgation des contenus de zone rendue autrement possible en parcourant la chaîne des enregistrements NSEC dans une zone signée.

Table des matières

1. Introduction

Dans DNSSEC [RFC4033], un enregistrement NSEC fait la liste des prochains noms instanciés dans sa zone, prouvant qu'aucun nom n'existe dans "l'intervalle" entre le nom du propriétaire NSEC et le nom dans le champ "prochain nom". Dans le présent document, un enregistrement NSEC est dit "couvrir" les noms entre son nom de propriétaire et le prochain nom.

Par des interrogations répétées qui retournent des enregistrements NSEC, il est possible de restituer tous les noms dans la zone, un processus couramment appelé "parcourir" la zone. Certains propriétaires de zone ont des politiques qui interdisent les transferts de zone par des clients arbitraires ; cet effet collatéral de l'architecture NSEC subvertit ces politiques.

Le présent document présente un moyen d'empêcher le parcours de zone en construisant des enregistrements NSEC qui couvent moins de noms. Ces enregistrements peuvent faire que le parcours de zone prenne approximativement autant d'interrogations que de simplement demander tous les noms possibles dans une zone, rendant le parcours de zone impraticable. Certains de ces enregistrements doivent être créés et signés sur demande, ce qui exige des clés privées en ligne. Tous ceux qui envisagent d'utiliser cette technique sont fortement encouragés à voir la discussion des risques de la signature en ligne à la Section 5.

1.2 Mots clés

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].

2. Applicabilité de cette technique

La technique présentée ici peut être utile à un propriétaire de zone qui veut utiliser DNSSEC, qui est concerné par l'exposition du contenu de sa zone via le parcours de zone, et veut bloquer les risques de la signature en ligne.

Comme discuté dans la Section 5, la signature en ligne présente plusieurs risques pour la sécurité, incluant une probabilité accrue que des clés privées soient divulguées et un risque accru d'attaque de déni de service. Quiconque envisage l'utilisation de cette technique est fortement encouragé à lire la discussion sur les risques de la signature en ligne à la Section 5.

De plus, au moment de la publication du présent document, le groupe de travail DNSEXT travaillait activement sur un mécanisme pour empêcher le parcours de zone qui n'exige pas de signature en ligne (sous le nom proposé de NSEC3). Le nouveau mécanisme va probablement exposer un petit peu plus d'informations sur la zone que cette technique (par exemple, le nombre de noms instanciés) mais cela peut être préférable à cette technique.

3. Couverture minimale des enregistrements NSEC

Ce mécanisme implique des changements aux enregistrements NSEC pour les noms instanciés, qui peuvent toujours être générés et signés à l'avance, tout comme la génération et signature à la demande de nouveaux enregistrements NSEC chaque fois qu'il doit être prouvé qu'un nom n'existe pas.

Dans le champ "prochain nom" de l'enregistrement NSEC des noms instanciés, plutôt que de mentionner le prochain nom instancié dans la zone, mentionner tout nom qui suit dans l'ordre lexical le nom du propriétaire du NSEC et avant le prochain nom instancié dans la zone, conformément à la fonction de rangement du paragraphe 6.1 de la [RFC4034]. Cela relâche l'exigence du paragraphe 4.1.1 de la RFC 4034 que le champ "prochain nom" contienne le prochain nom de propriétaire dans la zone. Ce changement est supposé pleinement compatible avec tous les validateurs DNSSEC existants. Ces enregistrements NSEC sont retournés chaque fois qu'il se révèle quelque chose de spécifique sur le nom du propriétaire (par exemple, qu'aucun enregistrement de ressource d'un certain type n'apparaît à ce nom).

Chaque fois qu'un enregistrement NSEC est nécessaire pour prouver la non existence d'un nom, un nouvel enregistrement NSEC est produit dynamiquement et signé. Le nouvel enregistrement NSEC a un nom de propriétaire lexiquement avant le QNAME mais suivant lexicalement tout nom existant et un "prochain nom" suivant lexicalement le QNAME mais avant tout nom existant.

La correspondance binaire du type d'enregistrement NSEC généré DOIT avoir les bits RRSIG et NSEC établis et NE DEVRAIT PAS avoir d'autre bit établi. Cela relâche l'exigence du paragraphe 2.3 de la RFC4035 que les enregistrements de ressource (RR, *Resource Record*) NSEC n'apparaissent pas aux noms qui n'existaient pas avant que la zone ait été signée.

Les fonctions pour générer les noms qui suivent et précèdent lexicalement les noms n'ont pas besoin d'être parfaitement cohérentes, mais les enregistrements NSEC générés ne doivent pas couvrir de noms existants. De plus, cette technique fonctionne mieux quand les enregistrements NSEC générés couvrent aussi peu de noms que possible. Dans le présent document, les fonctions qui génèrent les noms du voisinage sont appelées fonctions "epsilon", référence à la convention mathématique d'utiliser la lettre grecque epsilon pour représenter les très petites différences.

Un enregistrement NSEC qui dénie l'existence d'un caractère générique peut être généré de la même façon. Comme l'enregistrement NSEC qui couvre un caractère générique non existant va probablement être utilisé en réponse à de nombreuses interrogations, les serveurs de noms d'autorité qui utilisent les techniques décrites ici peuvent vouloir pré générer ou mettre en antémémoire cet enregistrement et son RRSIOG correspondant.

Par exemple, une interrogation pour un enregistrement A au nom non instancié exemple.com pourrait produire les deux enregistrements NSEC suivants, le premier niant l'existence du nom exemple.com et le second niant l'existence d'un

caractère générique :

exempld.com 3600 IN NSEC exemple-.com (RRSIG NSEC)

\).com 3600 IN NSEC +.com (RRSIG NSEC)

Avant de répondre à une interrogation avec ces enregistrements, un serveur d'autorité doit vérifier l'existence de noms entre ces points d'extrémité. Si le NSEC généré couvrait des noms existants (par exemple, exemplde.com ou *bizarre.exemple.com) une meilleure fonction epsilon peut être utilisée ou le plus proche nom couvert du QNAME pourrait être utilisé comme nom de propriétaire du NSEC ou comme prochain nom, comme approprié. Si un nom existant est utilisé comme nom de propriétaire du NSEC, l'enregistrement NSEC réel de ce nom DOIT être retourné. En utilisant le même exemple, et en supposant qu'il existe une délégation exemplde.com, cet enregistrement pourrait être retourné du parent :

exemplde.com 3600 IN NSEC exemple-.com (NS DS RRSIG NSEC)

Comme chaque enregistrement d'autorité dans la zone, chaque enregistrement NSEC généré DOIT avoir des RRSIG correspondants générés en utilisant chaque algorithme (mais pas nécessairement chaque DNSKEY) dans l'ensemble des enregistrements de ressource *(RRset)* DNSKEY de la zone, comme décrit dans la [RFC4035] paragraphe 2.2. Pour minimiser le nombre de signatures à générer, une zone peut souhaiter limiter le nombre d'algorithmes dans son RRset DNSKEY.

4. Meilleures fonctions epsilon

Le paragraphe 6.1 de la RFC 4034 définit un ordre strict des noms du DNS. En prenant cette définition en sens inverse, il devrait être possible de définir des fonctions epsilon qui génèrent respectivement les noms suivant et précédant immédiatement. Le présent document ne définit pas de telles fonctions. Cette section présente plutôt les fonctions qui sont raisonnablement proche des fonctions parfaites. Comme décrit ci-dessus, un serveur d'autorité devrait toujours s'assurer qu'aucun NSEC généré ne couvre un nom existant.

Pour incrémenter un nom, ajouter une étiquette devant avec un seul octet nul (de valeur zéro).

Pour décrémenter un nom, décrémenter le dernier caractère de l'étiquette la plus à gauche, puis remplir cette étiquette jusqu'à une longueur de 63 octets avec des octets de valeur 255. Pour décrémenter un octet nul (de valeur zéro) on supprime l'octet -- si il reste une étiquette vide, supprimer l'étiquette. Pour définir cette fonction numériquement : remplir cette étiquette la plus à gauche jusqu'à sa longueur maximale de zéros (numériques, pas des zéros ASCII) et soustraire un.

En réponse à une interrogation sur la non existence du nom foo.exemple.com, ces fonctions produisent les enregistrements NSEC suivants :

fon\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255.exemple.com 3600 IN NSEC \000.foo.exemple.com (NSEC RRSIG)

\)\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255\255\255\255\255\255\255\255\255\255\255\255\255\255
\255\255.exemple.com 3600 IN NSEC \000.*.exemple.com (NSEC RRSIG)

Le premier de ces RR NSEC prouve qu'aucune correspondance exacte n'existe pour foo.exemple.com, et le second prouve qu'il n'y a pas de caractère générique dans exemple.com.

Ces deux fonctions sont imparfaites : elles ne prennent pas en compte les contraintes sur le nombre d'étiquettes dans un nom ni sur la longueur totale d'un nom. Comme on l'a noté au paragraphe précédent, cette technique ne dépend cependant pas de l'utilisation des fonctions parfaites d'epsilon : il est suffisant de vérifier si un des noms instanciés tombe dans la portée couverte par le NSEC généré, et si il en est ainsi, substituer ces noms de propriétaire instancié au nom de propriétaire du NSEC ou au prochain nom, comme approprié.

5. Considérations sur la sécurité

Cette approche exige la génération à la demande des enregistrements RRSIG. Cela crée plusieurs nouvelles vulnérabilités.

D'abord, la signature à la demande exige que les serveur d'autorité d'une zone aient accès à ses clés privées. Mémoriser des clés privées sur des serveurs bien connus accessibles sur l'Internet peut les rendre plus vulnérables à une divulgation involontaire.

Ensuite, comme la génération de signatures numériques tend à être lourde en matière de calcul, les exigences de signature à la demande rendent les serveurs d'autorité vulnérables à des attaques de déni de service.

Enfin, si les fonctions epsilon sont prévisibles, la signature à la demande peut permettre une attaque de texte en clair choisi sur les clés privées d'une zone. Les zones qui utilisent cette approche devraient tenter d'utiliser des algorithmes de chiffrement qui sont résistants aux attaques de texte en clair choisi. On notera que bien que DNSSEC ait un algorithme de "mise en œuvre obligatoire", c'est une exigence pour les résolveurs et les valideurs -- il n'y a pas d'exigence qu'une zone soit signée avec un algorithme particulier.

Le succès de l'utilisation d'enregistrements NSEC à couverture minimale pour empêcher le parcours de zone dépend largement de la qualité des fonctions epsilon choisies. Une fonction d'incrément qui choisit un nom visiblement déduit du prochain nom instancié peut facilement être trouvée par ingénierie inverse, détruisant la valeur de cette technique. Une fonction d'incrément qui retourne toujours un nom proche du prochain nom instancié est de même un mauvais choix. Les bons choix de fonction epsilon sont ceux qui produisent les noms qui suivent et précédent immédiatement, respectivement, bien que les administrateurs de zone puisent souhaiter utiliser des fonctions moins parfaites qui retournent des noms plus faciles à lire par l'homme que les fonctions décrites à la Section 4.

Un autre souci évident mais peu envisagé est le danger que des enregistrements NSEC synthétisés soient répétés. Il est possible à un attaquant de répéter un vieil enregistrement NSEC dont la signature est encore valide après qu'un nouveau nom a été ajouté dans la portée couverte par ce NSEC, prouvant incorrectement qu'il n'y a pas d'enregistrement à ce nom. Ce danger existe avec le DNSSEC comme défini dans la [RFC4035]. Les techniques décrites ici diminuent en fait ce danger, car la portée couverte par tout enregistrement NSEC est plus petite qu'avant. Choisir une meilleure fonction epsilon va encore réduire ce danger.

6. Remerciements

De nombreuses personnes ont contribué à ce concept. Cela inclut, en plus des auteurs de ce document, Olaf Kolkman, Ed Lewis, Peter Koch, Matt Larson, David Blacka, Suzanne Woolf, Jaap Akkerhuis, Jakob Schlyter, Bill Manning, et Joao Damas.

De plus, les éditeurs tiennent à remercier Ed Lewis, Scott Rose, et David Blacka de leur relecture attentive du document.

7. 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)

[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.

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

Adresse des auteurs

Samuel Weiler
SPARTA, Inc.
7075 Samuel Morse Drive
Columbia, Maryland 21046
US
mél : weiler@tislabs.com

Johan Ihren
Autonomica AB
Bellmansgatan 30
Stockholm SE-118 47
Sweden
mél : johani@autonomica.se

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.