Groupe de travail Réseau
Request for Comments : 4955
Catégorie : sur la voie de la normalisation

D. Blacka, VeriSign, Inc.
juillet 2007
Traduction Claude Brière de L'Isle

Expériences de la sécurité du DNS (DNSSEC)

Résumé
Le présent document décrit une méthodologie pour déployer des méthodologies de remplacement, non rétro compatibles, de la sécurité du DNS (DNSSEC, *DNS Security*) d'une façon expérimentale sans perturber le déploiement du DNSSEC standard.

Table des Matières

1. Généralités

Historiquement, les expériences de solution de remplacement de DNSSEC ont été des entreprises problématiques. Il y a eu normalement le désir à la fois d'introduire des changements non rétro compatibles à DNSSEC et d'essayer ces changements sur les zones réelles dans le DNS public. Cela crée un problème quand le changement au DNSSEC ferait apparaître tout ou partie de la zone qui utilise ces changements comme boguée (mauvaise) ou perturber autrement les résolveurs à capacité de sécurité existants.

Le présent document décrit une méthodologie standard pour effectuer des expériences sur DNSSEC. Cette méthodologie vise le problème de la coexistence entre le DNSSEC standard et le DNS en utilisant des identifiants d'algorithme inconnus pour cacher les modifications expérimentales du protocole DNSSEC aux résolveurs à capacité de sécurité standard.

2. Définitions et terminologie

Dans le présent document, la familiarité avec le système DNS ([RFC1035]) et les extensions de sécurité du DNS ([RFC4033], [RFC4034] et [RFC4035]) est supposée.

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].

3. Expériences

Quand on discute des expériences sur DNSSEC, il est nécessaire de classer ces expériences en deux grandes catégories :

Rétro compatibles : elles décrivent des changements expérimentaux qui, bien qu'ils ne respectent pas strictement le DNSSEC standard, sont néanmoins interopérables avec les clients et serveurs qui mettent en œuvre le DNSSEC standard.

Non rétro compatibles : elles décrivent des expériences qui causeraient une détermination (incorrecte) par un résolveur standard à capacité de sécurité que tout ou partie d'une zone est bogué, ou autrement de ne plus interopérer avec les clients et servers DNSSEC standard.

Ne sont pas incluses dans ces termes les expériences sur le cœur du protocole DNS lui-même.

La méthodologie décrite dans le présent document n'est pas nécessaire pour les expériences rétro compatibles, bien qu'elle puisse certainement être utilisée si on le désire.

4. Méthode

Le cœur de la méthodologie est l'utilisation d'identifiants d'algorithme strictement inconnus lors de la signature de la zone expérimentale, et plus important, d'avoir seulement des identifiants d'algorithme inconnus dans les enregistrements du signataire par délégation (DS, *Delegation Signer*) pour la délégation de la zone par la parente.

Cette technique fonctionne à cause de la façon dont les valideurs conformes à DNSSEC sont supposés fonctionner en présence d'un ensemble de DS avec seulement des identifiants d'algorithme inconnus. D'après le paragraphe 5.2 de la [RFC4035] : "Si le valideur ne prend en charge aucun des algorithmes mentionnés dans un RRset DS authentifié, alors le résolveur n'a pas de chemin d'authentification pris en charge qui conduise de la zone parente à la fille. Le résolveur devrait traiter ce cas comme il le ferait du cas d'un RRset NSEC authentifié prouvant qu'aucun RRset DS n'existe, comme décrit ci-dessus."
Et plus loin : "Si le résolveur ne prend en charge aucun des algorithmes mentionnés dans un RRset DS authentifié, alors le résolveur ne sera pas capable de vérifier le chemin d'authentification vers la zone fille. Dans ce cas, le résolveur DEVRAIT traiter la zone fille comme si elle n'était pas signée."

Bien que ce comportement ne soit pas strictement obligatoire (comme marqué par DOIT) il est peu probable qu'un valideur mette en œuvre un comportement substantiellement différent. En gros, si le valideur n'a pas de chaîne de confiance utilisable pour une zone fille, alors il ne peut faire qu'une des deux choses suivantes : traiter les réponses provenant de la zone comme non sûres (comportement recommandé) ou traiter les réponses comme boguées. Si le valideur choisit la première, cela va à la fois violer les attentes du propriétaire de la zone et être contraire à l'objet de la règle ci-dessus. Cependant, avec une politique locale, un valideur est en droit de refuser de faire confiance à certaines zones sur la base de tout critère, incluant l'utilisation d'algorithmes de signature inconnus.

Parce qu'on parle d'expériences, il est RECOMMANDÉ que soient utilisés des numéros d'algorithme privés (voir l'Appendice A.1.1 de la [RFC4034]. Noter que le traitement sûr des algorithmes privés exige un traitement spécial de la part de la logique du valideur. Voir les détails dans "Précision et notes de mise en œuvre pour la sécurité du DNS (DNSSEC)" [RFC6840]). Normalement, au lieu d'inventer de nouveaux algorithmes de signature, la voie recommandée est de créer des identifiants d'algorithme de remplacement qui soient des alias des algorithmes connus existants. Bien que, strictement parlant, il soit seulement nécessaire de créer un identifiant de remplacement pour les algorithmes obligatoires, il est suggéré que tous les algorithmes définis comme facultatifs soient aussi sous un nom de remplacement.

Il est RECOMMANDÉ que pour une expérience de DNSSEC particulière, un nom de domaine particulier soit choisi pour tous les nouveaux algorithmes, puis que le numéro (ou nom) de l'algorithme lui soit ajouté devant. Par exemple, pour l'expérience A, le nom de base de "dnssec-experiment-a.exemple.com" est choisi. Alors, les alias pour les algorithmes 3 (DSA) et 5 (RSASHA1) sont définis comme étant "3.dnssec-experiment-a.exemple.com" et "5.dnssec-experiment-a.exemple.com". Cependant, tout identifiant univoque devrait suffire.

En utilisant cette méthode, les résolveurs (ou, plus précisément, les valideurs de DNSSEC) indiquent essentiellement leur

capacité à comprendre la sémantique de l'expérience DNSSEC en comprenant ce que les nouveaux identifiants d'algorithme signifient.

Cette méthode crée deux classes de serveurs et résolveurs à capacité de sécurité : les serveurs et résolveurs qui comprennent l'expérience (et donc reconnaissent les identifiants d'algorithme expérimentaux et la signification de l'expérience) et les serveurs et résolveurs qui ne comprennent pas l'expérience.

Cette méthode empêche aussi toute zone d'être à la fois une expérience et dans un îlot de sécurité du DNSSEC classique. C'est-à-dire qu'une zone est soit dans une expérience et il est seulement possible de la valider expérimentalement, soit elle n'y est pas.

5. Définir une expérience

L'expérience de DNSSEC DOIT définir l'ensemble particulier des identifiants (précédemment inconnus) d'algorithme qui identifient l'expérience et définir ce que chaque identifiant d'algorithme inconnu signifie. Normalement, sauf si l'expérience est en fait une expérience d'un nouvel algorithme DNSSEC, cela va être une transposition d'identifiants d'algorithme privés en des algorithmes existants connus.

Normalement, l'expérience va choisir un nom DNS comme base de l'identifiant d'algorithme. Ce nom DNS DEVRAIT être sous le contrôle des auteurs de l'expérience. Ensuite, l'expérience va définir une transposition entre les algorithmes obligatoires connus et les algorithmes facultatifs dans cet espace d'identifiants d'algorithmes privé. Autrement, l'expérience PEUT à la place utiliser l'espace d'identifiant d'objet (OID, *Object Identifier*) d'algorithme privé (en utilisant le numéro d'algorithme 254) ou PEUT choisir des numéros d'algorithme non privés, mais cela exige une allocation par l'IANA.

Par exemple, une expérience pourrait spécifier dans sa description le nom DNS "dnssec-experiment-a.exemple.com" comme nom de base, et déclarer que "3.dnssec-experiment-a.exemple.com" est un alias de l'algorithme DNSSEC 3 (DSA) et que "5.dnssec-experiment-a.exemple.com" est un alias de l'algorithme DNSSEC 5 (RSASHA1).

Les résolveurs DOIVENT seulement reconnaître la sémantique de l'expérience quand elle est présente dans une zone signée par un ou plusieurs de ces identifiants d'algorithme. Ceci est nécessaire pour isoler la sémantique d'une expérience de toute autre que le résolveur pourrait comprendre.

En général, les résolveurs impliqués dans l'expérience sont supposés comprendre à la fois le protocole DNSSEC standard et le protocole DNSSEC défini comme expérimental, bien que ce ne soit pas exigé.

6. Considérations

Un certain nombre de considérations doivent être faites sur l'utilisation de cette méthodologie.

1. Si un valideur non averti ne suit pas correctement les règles posées dans la RFC 4035 (par exemple, le valideur interprète un enregistrement DNSSEC avant de le valider) ou si l'expérience est d'une portée plus large que de juste modifier la sémantique de DNSSEC, l'expérience peut n'être pas suffisamment masquée par cette technique. Cela peut causer des échecs de résolution inattendus.

2. Il ne sera pas possible aux résolveurs à capacité de sécurité qui n'ont pas la capacité de prendre en charge l'expérimentation de construire une chaîne de confiance à travers une zone expérimentale.

7. Utilisation non expérimentale

Cette méthodologie générale PEUT être utilisée pour des changements de protocole non rétro compatibles avec le DNSSEC qui commencent à être ou deviennent des normes. Dans ce cas :

- Le changement de protocole DEVRAIT utiliser des identifiants d'algorithme publics alloués par l'IANA au lieu d'identifiants d'algorithme privés. Cela va aider à identifier le changement de protocole comme une norme, plutôt que comme expérience.

o Les résolveurs PEUVENT reconnaître le changement de protocole dans les zones non signées (ou non entièrement signées) en utilisant les nouveaux identifiants d'algorithme.

8. Considérations sur la sécurité

Les zones qui utilisent cette méthodologie vont être considérées comme non sûres par tous les résolveurs sauf ceux qui ont la capacité de l'expérience. Il n'est généralement pas possible de créer une délégation sûre à partir d'une zone expérimentale qui va être suivie par les résolveurs qui n'ont pas la capacité de l'expérience.

Les mises en œuvre devraient tenir compte de toutes les questions de sécurité qui peuvent résulter d'environnements configurés à faire confiance aux zones à la fois expérimentales et non expérimentales. Si la zone expérimentale est plus vulnérable aux attaques, elle pourrait, par exemple, être utilisée pour promouvoir la confiance dans des zones qui ne font pas partie de l'expérience, éventuellement sous le contrôle d'un attaquant.

9. Références

9.1 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

9.2 Références pour information

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC6840] S. Weiler et D. Blacka, éd., "Précision et notes de mise en œuvre pour la sécurité du DNS (DNSSEC)", février 2013. *(MàJ par* RFC8749*)*

Adresse de l'auteur

David Blacka
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166
US

téléphone : +1 703 948 3200
mél : davidb@verisign.com
URI : http://www.verisignlabs.com

Déclaration complète de droits de reproduction

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