Groupe de travail Réseau
Request for Comments : 5452
RFC mise à jour : 2181
Catégorie : Sur la voie de la normalisation

A. Hubert, Netherlabs Computer Consulting BV.
R. van Mook, Equinix
janvier 2009
Traduction Claude Brière de L'Isle

Mesures pour rendre le DNS plus résiliant aux réponses falsifiées

Résumé
Le climat actuel de l'Internet fait peser des menaces sérieuses sur le système des noms de domaines. Dans la période intérimaire avant que le protocole DNS puisse être plus complètement sécurisé, des mesures peuvent déjà être prises pour renforcer le DNS pour rendre plus difficile de plusieurs ordres de grandeur d'usurper un serveur de noms.

Même un DNS cryptographiquement sécurisé bénéficie d'avoir la capacité d'éliminer rapidement les réponses boguées, car cela épargne potentiellement de grandes quantités de calcul.

En décrivant certains comportements qui n'ont pas été précédemment standardisés, le présent document établit comment rendre le DNS plus résiliant contre l'acceptation de réponses incorrectes. Le présent document met à jour la RFC 2181.

Table des matières

1. Introduction

Le présent document décrit plusieurs problèmes courants dans les mises en œuvre du DNS, qui, bien que reconnues précédemment, restent largement non résolus. À côté d'une brève récapitulation de ces problèmes, le présent document contient des règles qui, si elles sont mises en œuvre, rendent les résolveurs conformes largement plus résistants aux attaques décrites. Le but est de rendre le DNS existant aussi sûr que possible dans les limites actuelles du protocole.

Le texte ci-dessous est destiné aux auteurs de résolveurs : il appartient aux opérateurs de décider quelles mise en œuvre de serveur de noms utiliser, ou quelles options activer. Les contraintes de fonctionnement peuvent outrepasser les soucis de sécurité décrits ci-dessous. Cependant, il est attendu des mises en œuvre qu'elles permettent à un opérateur d'activer la fonction décrite dans ce document.

Presque toutes les transactions de l'Internet impliquent le système des noms de domaines, qui est décrit dans les [RFC1034], [RFC1035], et au delà.

De plus, il est devenu récemment possible d'acquérir des certificats de couche de connexion sécurisée/sécurité de la couche transport (SSL/TLS, *Secure Socket Layer/Transport Layer Security*) sans autre confirmation d'identité que la capacité de répondre à un message de vérification envoyé via SMTP ([RFC5321]) -- qui utilise généralement le DNS pour son acheminement.

En d'autres termes, toute entité qui contrôle (temporairement) le système des noms de domaines est en position de réacheminer la plupart des transactions de l'Internet, y compris les étapes de vérification de l'acquisition d'un certificat SSL/TLS pour un domaine. Cela à son tour signifie que même les transactions protégées par SSL/TLS pourraient être détournées.

Il est parfaitement concevable qu'un tel trafic réacheminé puisse être utilisé au détriment des utilisateurs de l'Internet.

Ces développements et d'autres ont renouvelé l'importance de la sécurité et de la fiabilite du DNS. Bien que la communauté du DNS travaille dur à la finalisation et la mise en œuvre d'un protocole DNS cryptographiquement amélioré, des mesures devraient être prises pour s'assurer que l'utilisation existante du DNS est aussi sûre que possible dans les limites des normes pertinentes.

On devrait noter que les résolveurs les plus couramment utilisés actuellement ne fonctionnent pas aussi bien que possible à cet égard, rendant le présent document d'une urgente importance.

Une analyse approfondie des risques auxquels fait face le DNS se trouve dans la [RFC3833].

Le présent document s'étend sur certains des risques mentionnés dans la RFC 3833, en particulier ceux soulignés dans les paragraphes sur "Deviner l'identifiant et prédiction d'interrogation" et "Chaînage de noms". De plus, il souligne un certain nombre de règles et lignes directrices existantes incorporées dans les spécifications pertinentes du protocole du DNS. On spécifie aussi de nouvelles exigences pour s'assurer que le système des noms de domaines peut être fiable jusqu'à ce qu'un protocole plus sûr ait été normalisé et déployé.

On devrait noter que même quand toutes les mesures suggérées ci-dessous sont mises en œuvre, les utilisateurs du protocole ne sont pas protégés contre des tiers qui ont la capacité d'observer, modifier, ou injecter des paquets dans le trafic d'un résolveur.

Pour les extensions de protocole qui offrent une protection contre ces scénarios, voir la [RFC4033] et au delà.

2. Exigences et définitions

2.1 Définitions

Le présent document utilise les définitions suivantes :

Client : normalement un "résolveur de bout" sur un ordinateur d'un utilisateur d'extrémité.

Résolveur : serveur de noms qui effectue un service de restitution pour les clients, aussi appelé un serveur de mise en antémémoire, ou un résolveur de plein exercice ([RFC1123], paragraphe 6.1.3.1).

Résolveur de bout : résolveur très limité sur un ordinateur client, qui laisse le travail récurrent à un résolveur de plein exercice.

Interrogation : question envoyée par un résolveur, normalement dans un paquet UDP.

Réponse : message renvoyé par un serveur de noms d'autorité, normalement dans un paquet UDP.

Tiers : toute entité autre que le résolveur ou le receveur prévu d'une question. Le tiers peut avoir accès à un serveur de noms d'autorité arbitraire, mais n'a pas accès aux paquets transmis par le résolveur ou le serveur d'autorité.

Attaquant : tiers malveillant.

Usurpation : activité de tenter de subvertir le processus du DNS en faisant qu'une réponse choisie soit acceptée.

Réponse authentique : réponse correcte qui vient du bon serveur d'autorité.

Nom de domaine cible : domaine pour lequel l'attaquant souhaite s'infiltrer dans une réponse.

Fausses données : réponse choisie par l'attaquant.

2.2 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].

3. Description de l'usurpation du DNS

Quand certaines mesures sont prises, il est faisable "d'usurper" la majorité des résolveurs couramment déployés avec des paquets DNS soigneusement préparés envoyés en temps utile. Une fois usurpé, un serveur de mise en antémémoire va répéter les données qu'il a accepté à tort, et faire que ses clients contactent le mauvais serveur, potentiellement malveillant.

Pour comprendre comment ce processus fonctionne, il est important de savoir ce qui fait qu'un résolveur accepte une réponse.

La phrase suivante du paragraphe 5.3.3 de la [RFC1034] laissait présager le présent problème :

"Le résolveur devra faire preuve d'une grande paranoïa dans l'analyse de ces réponses. Il devra en outre vérifier que la réponse correspond bien à la requête émise grâce à la lecture du champ ID dans la réponse."

Les données du DNS sont à accepter par un résolveur si et seulement si :
1. La section question du paquet de réponse est équivalente à celle du paquet de question qui attend actuellement une réponse.
2. Le champ ID du paquet de réponse correspond à celui du paquet de question.
3. La réponse vient de la même adresse réseau que celle d'où la question a été envoyée.
4. La réponse vient sur la même adresse réseau, incluant le numéro d'accès, d'où la question a été envoyée.

En général, les premières réponses correspondant à ces quatre conditions sont acceptées.

Si un tiers réussit à satisfaire les quatre conditions avant que la réponse provenant du serveur de noms authentique le fasse, il est en position de fournir au résolveur des données fabriquées. Quand il le fait, on l'appelle un "attaquant", tentant de fournir de fausses données.

Toutes les conditions mentionnées ci-dessus peuvent théoriquement être satisfaites par un tiers, avec une difficulté qui est fonction de la mise en œuvre de résolveur et la configuration de la zone.

4. Description détaillée de scénarios d'usurpation

Le paragraphe précédent discutait un certain nombre d'exigences qu'un attaquant doit satisfaire afin de tromper avec des données manipulées (ou fausses). Cette section discute les difficultés relatives et comment les choix définis par la mise en œuvre impactent la quantité de travail qu'un attaquant doit effectuer pour surmonter les dites difficultés.

Plus de détails se trouvent au paragraphe 2.2 de la [RFC3833].

4.1 Forçage d'une interrogation

Formellement, un serveur de noms n'a besoin d'effectuer de service que pour son opérateur, ses clients, ou plus généralement ses utilisateurs. Récemment, des serveurs de noms récurrents ouverts ont été utilisés pour amplifier des attaques de déni de service.

Fournir un service complet permet au tiers d'envoyer au résolveur cible une interrogation sur le nom de domaine qu'il a l'intention de tromper. En recevant cette interrogation, et en ne trouvant pas la réponse dans son antémémoire, le résolveur va transmettre des interrogations aux serveurs de noms d'autorité pertinents. Cela ouvre une fenêtre d'opportunité pour faire accepter des données de réponse falsifiées.

Les interrogations peuvent cependant être forcées indirectement, par exemple, en amenant un serveur de messagerie à effectuer des recherches dans le DNS.

Certains opérateurs restreignent l'accès en ne faisant pas de récurrence pour les adresses IP non autorisées, mais répondent seulement avec les données en antémémoire. Cela rend l'usurpation plus difficile pour un tiers car il ne peut pas alors forcer le moment exact où une question va être posée. Il est cependant encore possible de déterminer une plage de temps où cela va se produire, parce que les serveurs de noms publient la durée de vie (TTL, *time to live*) décroissante des entrées dans l'antémémoire, qui indique jusqu'à quel instant absolu une nouvelle interrogation pourrait être envoyée pour rafraîchir l'entrée expirée.

La durée de vie des RRSet du nom de domaine cible détermine la fréquence d'ouverture d'une fenêtre d'opportunité, ce qui implique qu'un TTL court rend l'usurpation bien plus viable.

Noter que l'attaquant pourrait très bien avoir un accès autorisé au résolveur cible comme étant un consommateur ou un employé de son opérateur. De plus, l'accès peut être activé par l'utilisation de réflecteurs, comme souligné dans la [RFC5358].

4.2 Confrontation de la section Question

Les paquets du DNS, questions et réponses, contiennent une section question. Il devrait être vérifié que les réponses entrantes ont une section question équivalente à celle de l'interrogation sortante.

4.3 Confrontation du champ ID

Le champ Identifiant DNS fait 16 bits, ce qui signifie que si tous ces bits sont utilisés, et si leur contenu est vraiment aléatoire, il faudra une moyenne de 32768 tentatives pour le deviner. L'évidence montre que sur les mises en œuvre qui utilisent seulement 14 bits, en moyenne 8192 tentatives vont suffire.

De plus, si le serveur de noms cible peut être forcé d'avoir plusieurs interrogations identiques en cours, le phénomène de l'attaque de l'anniversaire signifie que toutes fausses données envoyées par l'attaquant seront confrontées à plusieurs interrogations en instance, augmentant significativement les chances de succès. Plus de détails figurent à la Section 5.

4.4 Confrontation de l'adresse de source de la réponse authentique

Il devrait être noté que satisfaire cette condition englobe d'être capable de transmettre des paquets au nom de l'adresse du

serveur de noms d'autorité. Bien que deux documents de bonnes pratiques actuelles (à savoir les [RFC2827] et [RFC3013]) demandent aux fournisseurs d'accès Internet d'empêcher leurs consommateurs de s'attribuer des adresses qui ne leur sont pas allouées, ces recommandations ne sont pas universellement (ni même largement) mises en œuvre.

De nombreuses zones ont deux ou trois serveurs de noms d'autorité, ce qui rend les chances que la confrontation de l'adresse de source de la réponse authentique même avec un choix simple ait un taux de succès à deux chiffres.

La plupart des serveurs de noms récurrents mémorisent les indications de performances relatives des serveurs de noms d'autorité, ce qui peut rendre plus facile de prédire quel serveur de noms va d'abord être interrogé -- celui qui a le plus de chances de répondre le plus vite.

Généralement, cette condition exige tout au plus deux ou trois tentatives avant d'avoir la correspondance.

4.5 Confrontation de l'adresse de destination de la réponse authentique

Noter que l'adresse de destination de la réponse authentique est l'adresse de source de l'interrogation originale.

L'adresse réelle d'un serveur de noms récurrent est généralement connue ; l'accès utilisé pour poser les questions est plus difficile à déterminer. La plupart des résolveurs actuels prennent un accès arbitraire au démarrage (éventuellement au hasard) et l'utilisent pour toutes les interrogations sortantes. Dans un certain nombre de cas, l'accès de source des questions sortantes est fixé au numéro d'accès traditionnel de serveur DNS de 53.

Si l'accès de source de l'interrogation originale est aléatoire, mais statique, tout serveur de noms d'autorité observé par l'attaquant peut être utilisé pour déterminer cet accès. Cela signifie que satisfaire à ces conditions n'exige souvent pas d'effort d'imagination.

Si plusieurs accès sont utilisés pour envoyer des interrogations, cela élargit l'espace effectif d'identifiants d'un facteur égal au nombre d'accès utilisé.

Des serveurs de résolution moins courants choisissent un accès aléatoire par interrogation sortante. Si cette stratégie est suivie, ce numéro d'accès peut être vu comme un champ d'identifiant supplémentaire, contenant là aussi jusqu'à 16 bits.

Si la gamme maximum d'accès est utilisée, en moyenne, environ 32256 accès de source vont être essayés avant de trouver l'accès de source de l'interrogation originale, car des accès en dessous de 1024 peuvent être indisponibles à l'utilisation, laissant 64512 options.

Il est en général sûr pour le DNS d'utiliser des accès dans la gamme de 1024 à 49152 même si certains de ces accès sont alloués à d'autres protocoles. Les résolveurs du DNS ne vont pas être capables d'utiliser d'accès qui sont déjà utilisés. Si un résolveur DNS utilise un accès, il va libérer cet accès après un court délai et migrer sur un accès différent. C'est seulement dans le cas d'un résolveur de haut volume qu'il est possible qu'une application qui veut un accès UDP particulier subisse un blocage à long terme.

On devrait noter qu'un pare-feu ne va pas empêcher la correspondance de cette adresse, car il va accepter des réponses qui (apparaissent comme) viennent de l'adresse correcte, n'offrant pas de sécurité supplémentaire.

4.6 Faire que la réponse arrive avant la réponse authentique

Une fois qu'un paquet a satisfait les quatre conditions précédentes (plus d'éventuelles conditions supplémentaires) aucune autre réponse n'est généralement acceptée.

Cela signifie que le tiers a un délai limité dans lequel injecter sa réponse falsifiée. Pour les calculs, on va supposer une fenêtre de l'ordre d'au plus 100 ms (selon la distance du réseau au serveur de noms d'autorité authentique).

Ce délai peut être beaucoup plus long si les serveurs de noms d'autorité authentiques sont (brièvement) surchargés par des interrogations, peut-être par l'attaquant.

5. Attaques de l'anniversaire

Ce qu'on appelle le "paradoxe de l'anniversaire" implique qu'un groupe de 23 personnes suffit pour avoir plus d'une chance sur deux d'avoir deux membres ou plus du groupe qui ont la même date d'anniversaire.

Un attaquant peut tirer parti de ce phénomène exact si il peut forcer le résolveur cible à avoir plusieurs interrogations équivalentes (QNAME, QTYPE, et QCLASS identiques) en instance à un instant donné dans le même serveur d'autorité.

Tout paquet que l'attaquant envoie alors a beaucoup plus de chances d'être accepté parce que il doit seulement correspondre à une des interrogations en instance pour ce seul domaine. Comparé à l'analogie de l'anniversaire ci-dessus, du groupe composé d'interrogations et de réponses, les chances d'avoir une d'elles partager un identifiant augmentent rapidement.

Tant qu'un petit nombre d'interrogations est envoyé, les chance de réussir à usurper une réponse augmentent linéairement avec le nombre d'interrogations en instance pour le domaine et serveur de noms exacts.

Pour les plus grands nombres, cet effet est moins prononcé.

Plus de détails sont fournis dans US-CERT [vu-457875].

6. Accepter seulement les enregistrements dans le domaine

Les réponses provenant de serveurs de noms d'autorité contiennent souvent des informations qui ne font pas partie de la zone pour laquelle on les tient pour d'autorité. Par exemple, une interrogation pour l'enregistrement MX d'un domaine pourrait obtenir comme réponses un échangeur de messagerie dans un autre domaine, et l'adresse IP de cet échangeur de messagerie.

Si c'est accepté aveuglément, le résolveur court le risque d'accepter des données provenant une source non fiable. Il faut veiller à n'accepter des données que si il est connu que l'origine est d'autorité pour le QNAME ou un parent du QNAME.

Une façon très simple de réaliser cela est de n'accepter de données que si elles font partie du domaine pour lequel l'interrogation était destinée.

7. Difficultés combinées

Étant donné un accès de destination connu ou statique, un champ d'identifiant correspondant, l'adresse de source et de destination exige en moyenne de l'ordre de 2 * 2^15 = 65000 paquets, en supposant qu'une zone a deux serveurs de noms d'autorité.

Si la fenêtre d'opportunité disponible est d'environ 100 ms, comme supposé ci-dessus, un attaquant devra être capable de transmettre brièvement 650000 paquets/s pour avoir 50 % de chances d'avoir des données falsifiées acceptées sur les premières tentatives.

Un réponse réaliste minimale du DNS consiste en environ 80 octets, incluant les en-têtes IP, faisant le taux de paquets ci-dessus correspondre à une salve respectable de 416 Mbit/s.

À la mi 2006, cette sorte de bande passante n'était pas courante mais pas rare non plus, en particulier parmi ceux en position de contrôler de nombreux serveurs.

Ces nombres changent quand une fenêtre d'une pleine seconde est supposée, éventuellement parce que l'arrivée de la réponse authentique peut être empêchée en surchargeant les hôtes d'autorité de bonne foi avec des interrogations factices. Cela réduit la bande passante nécessaire à 42 Mbit/s.

Si, de plus, l'attaquant se donne plus d'une seule chance et a la possibilité de jusqu'à 60 minutes de travail sur un domaine avec une durée de vie de 300 secondes, un simple 4 Mbit/s suffit pour avoir 50 % de chances de faire accepter ses données falsifiées. Une fois qu'il dispose d'un temps plus long, satisfaire la condition 1 mentionnée ci-dessus est aisé -- tout domaine populaire aura été interrogé un certain nombre de fois pendant cette heure, et étant donné le court TTL, cela va conduire à

des interrogations aux serveurs de noms d'autorité, ouvrant des fenêtres d'opportunité.

7.1 Symboles utilisés dans les calculs

On suppose l'utilisation des symboles suivants :

I : Nombre d'identifiants distincts disponibles (maximum 65536).

P : Nombre d'accès utilisés (maximum autour de 64000 car les accès en dessous de 1024 ne sont pas toujours disponibles, mais souvent 1).

N : Nombre de serveurs de noms d'autorité pour un domaine (en moyenne autour de 2,5).

F : Nombre de "faux" paquets envoyés par l'attaquant.

R : Nombre de paquets envoyés par seconde par l'attaquant.

W : Fenêtre d'opportunité, en secondes. Bordé par le temps de réponse des serveurs d'autorité (souvent 0,1 s).

D : Nombre moyen d'interrogations identiques en instance d'un résolveur (normalement 1, voir la Section 5).

A : Nombre de tentatives, une pour chaque fenêtre d'opportunité.

7.2 Calcul

La probabilité de tromper un résolveur est égale à la quantité de faux paquets qui arrivent dans la fenêtre d'opportunité, divisée par la taille de l'espace de problème.

Quand le résolveur a "D" multiples interrogations identiques en instance, chaque faux paquet a une chance proportionnellement supérieure de correspondre à une de ces interrogations. Cette hypothèse ne tient que pour de petites valeurs de "D".

En symboles, si la probabilité d'être trompé est notée par P_s :

$$P\_s = \frac{D * F}{N * P * I}$$

Il est plus utile de raisonner non en termes de paquets agrégés mais de convertir en taux de paquets, qui peut facilement être converti en bande passante si nécessaire.

Si la longueur de la fenêtre d'opportunité est "W" et si l'attaquant peut envoyer "R" paquets par seconde, le nombre de faux paquets "F" qui sont candidats à être acceptés est :

$$F = R * W \rightarrow P\_s = \frac{D * R * W}{N * P * I}$$

Finalement, pour calculer les chances combinées "P_cs" de tromper sur une période choisie "T", on devrait réaliser que l'attaquant a une nouvelle fenêtre d'opportunité chaque fois que le TTL "TTL" du domaine cible expire. Cela signifie que le nombre de tentatives "A" est égal à "T / TTL".

Pour calculer les chances combinées d'au moins un succès, la formule suivante donne :

$$P\_cs = 1 - (1 - P\_s)^A = 1 - \left(1 - \frac{D * R * W}{N * P * I}\right)^{(T / TTL)}$$

Quand des nombres communs (comme donnés ci-dessus) pour D, W, N, P, et I sont insérés, cette formule se réduit à :

$$P\_cs = 1 - \left(1 - \frac{R}{1\,638\,400}\right)^{(T / TTL)}$$

D'après cette formule, on peut voir que, si la mise en œuvre de serveur de noms est inchangée, seule l'augmentation du TTL offre une protection. Augmenter N, le nombre de serveurs d'autorité, n'est pas faisable au delà d'un petit nombre.

Pour le cas limite d'un TTL de zéro seconde, une fenêtre d'opportunité s'ouvre à chaque interrogation envoyée, rendant le TTL effectif égal à "W" ci-dessus, le temps de réponse du serveur d'autorité.

Ce dernier cas tient aussi pour les techniques d'usurpation qui ne s'appuient pas sur l'expiration du TTL, mais utilisent des interrogations répétées et changeantes.

8. Discussion

Les calculs ci-dessus indiquent la relative facilité avec laquelle les données du DNS peuvent être usurpées. Par exemple, en utilisant la formule déduite précédemment sur un RRSet avec un TTL de 3600 secondes, un attaquant qui envoie 7000 faux paquets de réponse par seconde (un taux de 4,5 Mbit/s) tient 10 % de chances de falsifier un enregistrement dans les premières 24 heures, qui montent à 50 % après une semaine.

Pour un RRSet avec un TTL de 60 secondes, le niveau de 10 % est atteint après 24 minutes, 50 % après moins de 3 heures, 90 % après environ 9 heures.

Pour certaines classes d'attaques, le TTL effectif est proche de zéro, comme on l'a noté ci-dessus.

Noter que les attaques mentionnées ci-dessus peuvent être détectée s par les opérateurs de serveur attentifs - un flux entrant inattendu de 4,5 Mbit/s de paquets pourrait être remarqué.

Une hypothèse importante dans ce calcul est un accès de destination connu ou statique de la réponse authentique.

Si ce numéro d'accès est inconnu et doit aussi être deviné, l'espace de problème s'étend d'un facteur de 64000, conduisant l'attaquant à avoir besoin de 285 Gbit/s de plus pour réaliser des taux de succès similaires.

Une telle bande passante n'est généralement pas disponible, et ne le sera pas dans un avenir prévisible.

Noter que certains pare-feu peuvent devoir être reconfigurés si ils sont actuellement réglés à ne permettre que des interrogations sortantes à partir d'un seul accès de source du DNS.

8.1 Tentatives répétitives d'usurpation pour un seul nom de domaine

Des techniques sont disponibles pour utiliser un nombre effectivement infini d'interrogations pour réaliser un but d'usurpation désiré. Dans le calcul ci-dessus, cela réduit le TTL effectif à 0.

Si de telles techniques sont employées, en utilisant le même taux de 7000 paquets/s mentionné ci-dessus, et en utilisant un seul accès de source, les chances d'usurpation montent à 50 % en 7 secondes.

Si 64000 accès sont utilisés, comme recommandé dans le présent document, en utilisant le même taux d'interrogations, le niveau de 50 % est atteint après environ 116 heures.

9. Contre mesures à la falsification

9.1 Règles de confrontation d'interrogation

Une mise en œuvre de résolveur DOIT confronter les réponses à tous les attributs suivants de l'interrogation :

- o l'adresse de source à l'adresse de destination de l'interrogation,
- o l'adresse de destination à l'adresse de source de l'interrogation,
- o l'accès de destination à l'accès de source de l'interrogation,
- o l'identifiant de l'interrogation
- o le nom de l'interrogation,
- o la classe et le type de l'interrogation,

avant d'appliquer les règles de fiabilité du DNS (voir le paragraphe 5.4.1 de la [RFC2181]).

En cas de discordance, la réponse DOIT être considérée comme invalide.

9.2 Extension de l'espace de Q-ID en utilisant les accès et adresses

Les mises en œuvre de résolveur DOIVENT :

- o utiliser un accès de source imprévisible pour les interrogations sortantes dans la gamme des accès disponibles (53, ou 1024 et au-dessus) qui est aussi grande que possible et praticable ;
- o utiliser plusieurs accès de source différents simultanément en cas d'interrogations multiples en instance ;
- o utiliser un identifiant d'interrogation imprévisible pour les interrogations sortantes, en utilisant toute la gamme disponible (0 à 65535).

Les résolveurs qui ont plusieurs adresses IP DEVRAIENT les utiliser de façon imprévisible pour les interrogations sortantes.

Les mises en œuvre de résolveur DEVRAIENT fournir des moyens d'éviter l'usage de certains accès.

Les résolveurs DEVRAIENT favoriser les serveurs de noms d'autorité avec lesquels une relation de confiance a été établie ; les résolveurs de bout DEVRAIENT être capables d'utiliser une signature de transaction (TSIG, *Transaction Signature*) ([RFC2845]) ou IPsec ([RFC4301]) quand ils communiquent avec leur résolveur récurrent.

Dans le cas où une vérification cryptographique de la validité d'une réponse est disponible (TSIG, SIG(0)) les mises en œuvre de résolveur PEUVENT ignorer les règles ci-dessus, et s'appuyer plutôt sur cette garantie.

Une imprévisibilité appropriée peut être réalisée en employant un générateur de nombre (pseudo-)aléatoires de grande qualité, comme décrit dans la [RFC4086].

9.2.1 Justification et discussion

Comme un attaquant peut forcer un résolveur DNS plein à envoyer des interrogations aux propres serveurs de noms de l'attaquant, tout état constant ou séquentiel conservé par un tel résolveur peut être mesuré, et il ne doit pas être trivialement facile d'inverser l'ingénierie de l'état interne du résolveur d'une façon qui permette une prévision à bas coût de haute précision de l'état futur.

Un résolveur DNS plein avec seulement un ou un petit nombre de points d'extrémité vers l'aval utilise effectivement des constantes pour l'adresse IP de source et le numéro d'accès UDP, et elles sont très prévisibles par de potentiels attaquants, et doivent donc être évitées.

Un résolveur DNS plein qui utilise un simple incrément pour obtenir son prochain identifiant d'interrogation DNS est de même très prévisible et donc très facile à tromper.

Finalement, il a été montré que des générateurs de nombres aléatoires faibles exposent leur état interne, de sorte qu'un attaquant qui est témoin de plusieurs valeurs "aléatoires" à la suite peut facilement prédire les suivantes. Un générateur de nombres aléatoires de force cryptographique est tel qu'on ne peut pas prédire le résultat quel que soit le nombre de valeurs successives sont vues.

9.3 Détection d'usurpation et contre mesures

Si un résolveur détecte qu'une tentative d'usurpation est faite, peut-être en découvrant que de nombreux paquets échouent aux critères mentionnés plus haut, il PEUT abandonner l'interrogation UDP et la refaire sur TCP. TCP est, grâce à son utilisation de numéros de séquence, bien plus résiliant à la falsification par des tiers.

10. Considérations sur la sécurité

Le présent document donne des éclaircissements sur la spécification du DNS pour diminuer la probabilité que les réponses du DNS puissent réussir à être falsifiées. Les recommandations qui se trouvent ci-dessus devraient être considérées comme complémentaires aux éventuelles améliorations cryptographique du système des noms de domaine, qui protègent contre une plus large classe d'attaques.

Le présent document recommande l'utilisation de numéros d'accès de source UDP aléatoires pour étendre l'identifiant de transaction DNS effectif au delà des 16 bits disponibles.

Un résolveur qui ne met pas en œuvre les recommandations mentionnées ci-dessus peut facilement être forcé d'accepter des réponses falsifiées, qui sont à leur tour passées aux ordinateurs clients -- redirigeant le trafic (d'utilisateur) sur des entités potentiellement malveillantes.

Le présent document impacte directement la sécurité du système des noms de domaines, et les mises en œuvre sont invitées à suivre ses recommandations.

La plupart des considérations sur la sécurité se trouvent dans les Sections 4 et 5, tandis que les contre-mesures proposées sont décrites à la Section 9. Pour faire court, au lieu de répéter les références des considérations de sécurité, le lecteur se reportera à ces sections.

Rien dans ce document ne spécifie des algorithmes spécifiques à utiliser par les opérateurs ; il spécifie des algorithmes que les mises en œuvre DEVRAIENT ou DOIVENT prendre en charge.

On devrait noter que les effets de l'accès de source aléatoire peuvent être considérablement réduits par des appareils de traduction d'adresse réseau (NAT) qui mettent en série ou limitent en volume les accès de source UDP utilisés par le résolveur interrogateur.

Les serveurs récurrents du DNS qui se tiennent derrière un NAT ou un pare-feu à états pleins peuvent consommer toutes les entrées/accès de traduction de NAT disponibles quand ils opèrent dans un contexte de lourde charge d'interrogation. L'allocation aléatoire d'accès va causer la consommation plus rapide des entrées de traduction qu'avec un accès fixe d'interrogation.

Pour éviter cela, les boîtiers de NAT et les pare-feu à états pleins peuvent/devraient purger les entrées de traduction d'interrogations sortantes du DNS 10 à 17 secondes après l'envoi de la dernière interrogation sortante sur cette transposition. Les appareils conformes à la [RFC4787] doivent traiter les messages UDP sur l'accès 53 différemment de la plupart des autres protocoles UDP.

Pour minimiser le potentiel que des attaques d'épuisement d'accès/état puissent être organisées de l'extérieur, il est recommandé que les services qui génèrent un certain nombre d'interrogations du DNS pour chaque connexion soient limitées en débit. Cela s'applique en particulier aux serveurs de messagerie électronique.

11. Remerciements

L'accès de source aléatoire dans le DNS a été mis en œuvre pour la première fois et peut-être inventé par Dan J. Bernstein.

Bien que toutes les fautes soient de notre fait, les auteurs remercient chaleureusement de leur aide et de leurs contributions Stephane Bortzmeyer, Alfred Hoenes, Peter Koch, Sean Leach, Norbert Sendetzky, Paul Vixie, Florian Weimer, Wouter Wijngaards et Dan Wing

12. Références

12.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[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)

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

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(P.S., MàJ par* RFC4035, RFC2535, RFC4343, RFC4033, RFC4034, RFC5452, RFC8767)

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 2000, DOI 10.17487/RFC2845, (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

[RFC3013] T. Killalea, "Services et procédures de sécurité recommandés pour les fournisseurs de service Internet", novembre 2000. (BCP0046)

[RFC4043] D. Pinkas, T. Gindin, "Identifiant permanent d'infrastructure de clé publique X.509 pour l'Internet", mai 2005.

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005, DOI 10.17487/RFC4086, (*Remplace* RFC1750) (BCP0106)

[RFC5321] J. Klensin, "Protocole simple de transfert de messagerie(SMTP)", octobre 2008. (*Remplace* RFC2821) (*MàJ* RFC1123) *(D.S.)*

12.2 Références pour information

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, DOI 10.17487/RFC1123, octobre 1989. *(MàJ par* RFC7766, RFC9210)

[RFC3833] D. Atkins, R. Austein, "Analyse des menaces contre le système des noms de domaines (DNS)", août 2004.

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", DOI 10.17487/RFC4301, décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4787] F. Audet, éd., C. Jennings, "Exigences sur le comportement des traducteurs d'adresse réseau (NAT) pour UDP en envoi individuel", janvier 2007. (BCP0127) *(MàJ par* RFC7857)

[RFC5358] J. Damas, F. Nves, "Empêcher l'utilisation de noms de serveurs récurrents dans les attaques par réflecteur", octobre 2008. (BCP0140)

[vu-457875] United States CERT, "Various DNS service implementations generate multiple simultaneous queries for the same resource record", VU 457875, novembre 2002.

Adresse des auteurs

Bert Hubert
Netherlabs Computer Consulting BV.
Braillelaan 10
Rijswijk (ZH) 2289 CM
The Netherlands
mél : bert.hubert@netherlabs.nl

Remco van Mook
Equinix
Auke Vleerstraat 1
Enschede 7521 PE
The Netherlands
mél : remco@eu.equinix.com