Groupe de travail Réseau
Request for Comments : 3833
Catégorie : Information
Traduction Claude Brière de L'Isle

D. Atkins, IHTFP Consulting
R. Austein, ISC
août 2004

Analyse des menaces pour le système des noms de domaine (DNS)

Résumé
Bien que les extensions de sécurité du DNS (DNSSEC, *DNS Security Extensions*) aient été développées pendant la plus grande partie de la dernière décade, l'IETF n'a jamais mis par écrit l'ensemble spécifique de menaces contre lequel le DNSSEC est censé protéger. Entre autres inconvénients, cette situation de "charrette avant les bœufs" a rendu difficile de déterminer si le DNSSEC atteint les objectifs pour lesquels il a été conçu, car ceux-ci ne sont pas très bien spécifiés. La présente note tente de documenter certaines des menaces connues contre le DNS, et, ce faisant, tente de savoir dans quelle mesure (s'il en est) le DNSSEC est un outil utile pour se défendre contre ces menaces.

1. Introduction

Le premier travail organisé sur le DNSSEC au sein de l'IETF était la réunion d'une équipe de conception ouverte organisée par les membres du groupe de travail DNS en novembre 1993 à la 28ème réunion de l'IETF à Houston. Les grandes lignes du DNSSEC comme nous le connaissons aujourd'hui sont déjà claires dans le résumé de Jim Galvin des résultats de cette réunion [Galvin93]:

- Bien que certains participants à la réunion aient été intéressés par la protection contre la divulgation des données du DNS aux personnes non autorisées, l'équipe de conception a pris la décision explicite que "les données du DNS sont `publiques'", et a exclu explicitement toutes les menaces de divulgation des données hors du domaine d'application de DNSSEC.

- Bien que certains participants à la réunion aient été intéressés par l'authentification des clients et serveurs du DNS comme base du contrôle d'accès, cette tâche a aussi été exclue du champ d'application de DNSSEC en soi.

- La rétro compatibilité et la coexistence avec "le DNS non sûr" a été citée comme exigence explicite.

- La liste résultante des service de sécurité désirés était
  1) l'intégrité des données,
  2) l'authentification. de l'origine des données.

- L'équipe de conception a noté qu'un mécanisme de signature numérique prendrait en charge les services désirés.

Bien qu'un certain nombre de décisions de détail restent encore à prendre (et dans certains cas à reprendre après l'expérience de leur mise en œuvre) pendant la décade suivante, le modèle de base et les objectifs conceptuels sont restés fixes.

Nulle part, cependant, un travail sur le DNSSEC n'a tenté de spécifier en détail les sortes d'attaques contre lesquelles DNSSEC est destiné à protéger, ni les raisons qui sous-tendent la liste des services de sécurité désirés qui est sortie de la réunion de Houston. Pour cela, on doit se reporter à l'article écrit à l'origine par Steve Bellovin en 1990 mais non publié jusqu'en 1995, pour des raisons que Bellovin a expliquées dans la conclusion de son article [Bellovin95].

Bien qu'il puisse sembler un peu étrange de publier l'analyse des menaces dix ans après avoir commencé le travail sur le protocole destiné à défendre contre elles, c'est néanmoins ce que la présente note tente de faire. Mieux vaut tard que jamais.

Cette note suppose que le lecteur est familier avec le DNS et avec DNSSEC, et ne cherche pas à fournir un guide sur l'un ou l'autre. Les documents du DNS les plus pertinents sur le sujet de cette note sont : [RFC1034], [RFC1035], le paragraphe 6.1 de la [RFC1123], [RFC2181], [RFC2308], [RFC2671], [RFC2845], [RFC2930], [RFC3007], et la [RFC2535].

Pour les besoins de la discussion, la présente note utilise le terme de "DNSSEC" pour se référer au mécanisme de clé publique hiérarchique et de signature spécifié dans les documents DNSSEC, et se réfère à TKEY et TSIG comme à des mécanismes séparés, bien que les mécanismes de sécurité du canal comme TKEY et TSIG fassent aussi partie du problème plus large de la "sécurisation du DNS" et soient donc souvent considérés comme parties de l'ensemble global des "extensions de sécurité du DNS". Cette distinction est arbitraire et reflète en partie la façon dont le protocole a évolué (introduction d'un modèle de sécurité du canal potentiellement plus simple pour certaines opérations comme les transferts de zone et les demandes de mise à jour dynamiques) et devrait peut-être être changée dans une future révision de cette note.

2. Menaces connues

Il y a plusieurs classes distinctes de menaces contre le DNS, dont la plupart sont des instances en relation avec le DNS de problèmes plus généraux, mais dont quelques unes sont spécifiques des particularités du protocole du DNS.

2.1 Interception de paquet

Certaines des plus simples menaces contre le DNS sont des formes diverses de l'interception de paquet : des attaques par interposition, de l'espionnage des demandes combiné avec des réponses falsifiées qui refoulent la réponse réelle au résolveur, et ainsi de suite. Dans beaucoup de ces scénarios, l'attaquant peut simplement dire à l'une ou l'autre partie (usuellement le résolveur) ce qu'il veut que cette partie croie. Bien que les attaques d'interception de paquet soient loin d'être uniques au DNS, le comportement habituel du DNS d'envoyer une interrogation ou une réponse entière dans un seul paquet UDP non signé et non chiffré rend ces attaques particulièrement faciles pour tout mauvais garçon qui est capable d'intercepter des paquets sur un réseau partagé ou de transit.

Pour compliquer un peu plus les choses, l'interrogation au DNS que l'attaquant intercepte peut être juste un moyen détourné pour les objectifs de l'attaquant : il peut même choisir de retourner le résultat correct dans la section réponse d'un message en retour tout en utilisant d'autres parties du message pour mettre en scène quelque chose de plus compliqué, par exemple, une attaque de chaînage de nom (voir au paragraphe 2.3). Bien qu'il soit certainement possible de signer les messages du DNS en utilisant un mécanisme de sécurité du canal comme TSIG ou IPsec, ou même de les chiffrer en utilisant IPsec, ce ne serait pas une très bonne solution aux attaques par interception. D'abord, cette approche imposerait un coût de traitement très élevé par message DNS, ainsi qu'un très fort coût associé à l'établissement et à la gestion de relations de confiance bilatérales entre toutes les parties qui pourraient être impliquées dans la résolution de toute interrogation. Pour des serveurs de noms très utilisés (comme les serveurs pour la zone racine) ce coût serait très certainement prohibitif. Encore plus important, cependant, est que le modèle de confiance sous-jacent dans une telle conception serait faux, car au mieux, il fournirait seulement une vérification d'intégrité bond par bond sur les messages du DNS et ne fournirait aucune sorte de vérification d'intégrité de bout en bout entre le producteur des données du DNS (l'administrateur de zone) et le consommateur des données du DNS (l'application qui a déclanché l'interrogation).

À l'opposé, DNSSEC (lorsque utilisé de façon appropriée) fournit bien une vérification d'intégrité des données de bout en bout, et est donc une bien meilleure solution pour cette classe de problèmes durant les opérations de base d'une recherche dans le DNS.

TSIG a sa place dans les coins du protocole DNS où il y a une relation de confiance spécifique entre un certain client et un certain serveur, comme un transfert de zone, une mise à jour dynamique, ou un résolveur (de bout ou autre) qui ne va pas vérifier lui-même toutes les signatures DNSSEC.

Noter que DNSSEC ne fournit aucune protection contre la modification de l'en-tête de message DNS, aussi tout résolveur raisonnablement paranoïaque doit :
- effectuer de lui-même toutes les vérifications de signature DNSSEC,
- utiliser TSIG (ou quelque mécanisme équivalent) pour s'assurer de l'intégrité de ses communications avec tout serveur de noms auquel il choisit de faire confiance, ou
- se résigner à la possibilité d'être attaqué via une interception de paquet (et via d'autres techniques exposées plus loin).

2.2 Deviner l'identité et prédire l'interrogation

Comme le DNS est pour la plus grande partie utilisé sur UDP/IP, il est relativement facile à un attaquant de générer des paquets qui vont correspondre aux paramètres du protocole de transport. Le champ ID dans l'en-tête DNS est seulement un champ de 16 bits et l'accès de serveur UDP associé au DNS est une valeur bien connue, de sorte qu'il y a seulement 2**32 combinaisons possibles d'ID et d'accès de client pour un certain client et serveur. Ceci n'est pas une gamme particulièrement large, et n'est pas suffisante pour protéger contre une attaque en force brute ; de plus, en pratique l'accès de client UDP et l'identifiant peuvent souvent être tous deux prédits à partir du trafic précédent, et il n'est rare que l'accès client soit une valeur fixe connue elle aussi (à cause des pare-feu ou autres restrictions) ce qui réduit souvent l'espace de recherche à une gamme plus petite que 2**16.

En soi, deviner l'identifiant n'est pas suffisant pour permettre à un attaquant d'injecter des données boguées, mais combiné avec la connaissance (ou la conjecture) des QNAME et des QTYPE pour lesquels un résolveur pourrait être interrogé, cela laisse le résolveur seulement faiblement défendu contre l'injection de réponses boguées.

Comme cette attaque s'appuie sur la prédiction du comportement d'un résolveur, elle a des chances de réussir lorsque la victime est dans un état connu, soit parce que la victime a réamorcé récemment, soit parce que le comportement de la victime a été influencé par quelque autre action de l'attaquant, soit parce que la victime répond (d'une façon prévisible) à une action d'un tiers connue de l'attaquant.

Cette attaque est à la fois plus difficile et moins difficile pour l'attaquant que la simple attaque d'interception décrite plus haut : plus difficile, parce que l'attaque ne fonctionne que lorsque l'attaquant réussit à deviner correctement ; moins difficile, parce que l'attaquant n'a pas besoin d'être sur un réseau de transit ou partagé.

À beaucoup d'égards, cette attaque est similaire à une attaque d'interception de paquet. Un résolveur qui vérifie les signatures DNSSEC va être capable de détecter la réponse falsifiée ; les résolveurs qui n'effectuent pas la vérification de signature DNSSEC eux-mêmes devraient utiliser TSIG ou un mécanisme équivalent pour s'assurer de l'intégrité de leur communication avec un serveur de noms récurrent qui n'effectue pas la vérification des signatures DNSSEC.

2.3 Chaînage de noms

Peut-être la classe la plus intéressante de menaces spécifiques du DNS est l'attaque de chaînage de noms. C'est un sous ensemble d'une classe plus large d'attaques fondées sur le nom, parfois appelées attaques "d'empoisonnement d'antémémoire". La plupart des attaques fondées sur le nom peuvent être partiellement atténuées par la vieille défense consistant à vérifier les RR dans les messages de réponse pour voir leur pertinence par rapport à l'interrogation d'origine, mais une telle défense n'a pas de prise sur les attaques de chaînage de noms. Il y a plusieurs variantes de l'attaque de base, mais ce que toutes ont en commun est qu'elles impliquent les enregistrements de ressource du DNS dont la portion RDATA (côté droit) inclut un nom du DNS (ou, dans quelques cas, quelque chose qui n'est pas un nom DNS mais qui se transpose directement en un nom DNS). Tout RR de ce genre est, au moins en principe, un hameçon qui permet à un attaquant de s'alimenter des données dans une antémémoire de sa victime, subvertissant potentiellement les décisions suivantes fondées sur des noms du DNS.

Les pires exemples de cette classe de RR sont les RR CNAME, NS, et DNAME parce qu'ils peuvent rediriger l'interrogation d'une victime sur une localisation du choix de l'attaquant . Les RR comme MX et SRV sont un peu moins dangereux, mais en principe ils peuvent aussi être utilisés pour déclancher d'autres recherches sur des localisations du choix de l'attaquant. Les types de RR d'adresse comme les A ou AAAA n'ont pas de noms DNS dans leur RDATA, mais comme les arborescences IN-ADDR.ARPA et IP6.ARPA sont indexées en utilisant un codage DNS d'adresses IPv4 et IPv6, ces types d'enregistrement peuvent aussi être utilisés dans une attaque de chaînage de noms.

La forme générale d'une attaque de chaînage de nom ressemble à ceci :

- La victime fait une interrogation, peut-être à l'instigation de l'attaquant ou d'un tiers ; dans certains cas, l'interrogation elle-même peut être sans relation avec le nom attaqué (c'est-à-dire que l'attaquant utilise juste cette interrogation comme moyen pour injecter de fausses informations sur un autre nom).
- L'attaquant injecte une réponse, via l'interception de paquet, la conjecture d'interrogation, ou en étant un serveur de noms légitime qui est impliqué à un certain point du processus de réponse aux interrogations que produit la victime.
- La réponse de l'attaquant inclut un ou plusieurs RR avec des noms du DNS dans leurs RDATA ; selon la forme particulière de cette attaque, l'objet peut être d'injecter de fausses données associées à ces noms dans l'antémémoire de la victime via la section Additionnelle de cette réponse, ou peut être de rediriger la prochaine étape de l'interrogation vers un serveur du choix de l'attaquant (afin d'injecter plus de mensonges complexes dans l'antémémoire de la victime qu'il n'en tient aisément dans une seule réponse, ou afin de placer les mensonges dans la section Autorité ou Réponse d'une réponse où ils auront une meilleure chance de se faufiler derrière les défenses d'un résolveur).

Tout attaquant qui peut insérer des enregistrements de ressource dans l'antémémoire d'une victime peut presque certainement commettre certaines sortes de dommages, de sorte qu'il y a des attaques d'empoisonnement d'antémémoire qui ne sont pas des attaques de chaînage de noms au sens exposé ici. Cependant, dans le cas des attaques de chaînage de noms, les relations de

cause et d'effet entre l'attaque initiale et le résultat éventuel peuvent être significativement plus complexes que les autres formes d'empoisonnement d'antémémoire, de sorte que les attaques de chaînage de noms méritent une attention particulière.

Le fil commun de toutes les attaques de chaînage de noms est que les messages de réponse permettent à l'attaquant d'introduire des noms DNS arbitraires du choix de l'attaquant et de fournir d'autres informations que l'attaquant va prétendre associées à ces noms ; sauf si la victime a une meilleure connaissance des données associées à ces noms, la victime va avoir du mal à se défendre contre cette classe d'attaques.

Cette classe d'attaques est particulièrement insidieuse étant donné qu'il est assez facile à l'attaquant de provoquer l'interrogation par la victime d'un nom particulier du choix de l'attaquant, par exemple, en incorporant un lien à un graphique de "punaise de la toile" de 1x1 pixel dans un morceau de message de Text/HTML à la victime. Si le programme de lecture de message de la victime tente de suivre un tel lien, le résultat sera une interrogation au DNS pour un nom choisi par l'attaquant.

DNSSEC devrait fournir une bonne défense contre la plupart (toutes ?) des variantes de cette classe d'attaques. En vérifiant les signatures, un résolveur peut déterminer si les données associées à un nom ont été réellement insérées par l'autorité déléguée pour cette portion de l'espace de noms du DNS. Plus précisément, un résolveur peut déterminer si l'entité qui a injecté les données avait accès à une clé prétendument secrète dont la clé publique correspondante apparaît à une localisation attendue dans l'espace de noms du DNS avec une chaîne attendue de signatures parentes qui commence par une clé publique dont le résolveur a la connaissance préalable

Les signatures DNSSEC ne couvrent pas les enregistrements colle, de sorte qu'il y a quand même une possibilité d'une attaque de chaînage de noms impliquant une colle, mais avec DNSSEC il est possible de détecter l'attaque en acceptant temporairement la colle afin d'aller chercher la version signée d'autorité des mêmes données, puis de vérifier les signatures sur la version d'autorité.

2.4 Trahison d'un serveur de confiance

Une autre variante de l'attaque d'interception de paquet est le serveur de confiance qui se révèle n'être pas de confiance du tout, que ce soit par accident ou intentionnellement. De nombreuses machines de client sont seulement configurées avec des résolveurs de bout, et utilisent des serveurs de confiance pour effectuer leurs interrogations du DNS en leur nom. Dans de nombreux cas, le serveur de confiance est fourni par le FAI de l'usager et annoncé au client via DHCP ou des options PPP. À côté de la trahison accidentelle de cette relation de confiance (via une faute de configuration du serveur, une intrusion réussie dans le serveur, etc.) le serveur lui-même peut être configuré à renvoyer des réponses qui ne sont pas celle attendues, que ce soit dans une tentative honnête d'aide de l'usager, ou pour promouvoir quelque autre objectif comme celui de relayer un partenariat commercial entre le FAI et un tiers.

Ce problème est particulièrement aigu pour les voyageurs fréquents qui emportent leur propre équipement et s'attendent à le voir fonctionner de la même façon quel que soit l'endroit où ils vont. Ces voyageurs ont besoin d'un service DNS de confiance sans considération de l'exploitant du réseau sur lequel leur équipement est actuellement raccordé ou de la marque du boîtier de médiation qu'utilise l'infrastructure locale.

Bien que la solution évidente à ce problème serait que le client choisisse un serveur qui soit plus digne de confiance, en pratique, ceci n'est peut être pas une option pour le client. Dans de nombreux environnements de réseau, la machine cliente a seulement un ensemble limité de serveurs de noms récurrents à partir desquels faire son choix, et aucun d'eux n'est peut-être particulièrement digne de confiance. Dans des cas extrêmes, le filtrage d'accès ou d'autres formes d'interception de paquet peuvent empêcher l'hôte client d'être capable de faire fonctionner un résolveur itératif même si le propriétaire de la machine cliente est d'accord et capable de le faire. Donc, bien que la source initiale de ce problème ne soit pas une attaque du protocole DNS en soi, cette sorte de trahison est une menace pour les clients du DNS, et la simple commutation sur un serveur de nom récurrent différent n'est pas une défense adéquate.

Du strict point de vue du protocole DNS, la seule différence entre cette sorte de trahison et une attaque d'interception de paquet est que dans ce cas le client a volontairement envoyé sa demande à l'attaquant. La défense contre cela est la même qu'avec une attaque d'interception de paquet : le résolveur doit soit vérifier lui-même les signatures DNSSEC, soit utiliser TSIG (ou un équivalent) pour authentifier le serveur auquel il a choisi de faire confiance. Noter que l'utilisation de TSIG ne garantit pas par elle-même qu'un serveur de noms est digne de confiance : tout ce que TSIG peut faire est d'aider un résolveur à protéger ses communication avec un serveur de noms dont il a déjà décidé pour d'autres raison qu'il était digne de confiance. Protéger les communications d'un résolveur avec un serveur qui donne des réponses boguées n'est pas particulièrement utile.

On notera aussi que si le résolveur de bout ne fait pas confiance au serveur de noms qui travaille en son nom et veut faire lui-même la vérification des signatures DNSSEC, le résolveur a réellement besoin d'avoir une connaissance indépendante de la ou des clés publiques du DNSSEC dont il a besoin pour effectuer la vérification. D'habitude, la clé publique pour la zone racine est suffisante, mais dans certains cas, la connaissance des clés supplémentaires peut être aussi appropriée.

Il est difficile d'échapper à la conclusion qu'un résolveur raisonnablement paranoïaque doit toujours effectuer sa propre vérification de signatures, et que cette règle s'applique même aux résolveurs.

2.5 Déni de service

Comme avec tout service réseau (ou, bien sûr, presque tout service de toute sorte dans tous les domaines) le DNS est vulnérable aux attaques de déni de service. DNSSEC n'y peut rien, et peut en fait rendre le problème pire pour les résolveurs qui vérifient les signatures, car cela augmente le coût de traitement pour chaque message du DNS et dans certains cas peut aussi augmenter le nombre de messages nécessaires pour répondre à une interrogation. TSIG (et les mécanismes similaires) pose un problème équivalent.

Les serveurs DNS courent aussi le risque d'être utilisés comme amplificateurs du déni de service car les paquets de réponse du DNS tendent à être significativement plus longs que les paquets d'interrogation du DNS. On ne sera pas surpris que DNSSEC n'aide dans aucun des deux cas.

2.6 Négation de nom de domaine authentifiée

Beaucoup de discussions ont eu lieu autour de la question de la négation authentifiée de nom de domaine. La question particulière porte sur l'exigence d'une authentification de la non existence d'un nom. Le problème est de savoir si le résolveur devrait être capable de détecter quand l'attaquant retire des RR d'une réponse.

Toute paranoïa mise à part, l'existence de types de RR dont l'absence cause une action autre qu'un échec immédiat (comme des RR MX et SRV manquants, qui retombent sur des RR A) constitue une menace réelle. On peut se demander si dans certains cas, même l'absence d'un RR pourrait être considérée comme un problème. La question reste posée : quel est le sérieux de cette menace ? Il est clair que la menace existe ; la paranoïa générale dit qu'un de ces jours cela sera en première page des journaux, même si on ne peut pas concevoir de scénario plausible qui implique cette attaque aujourd'hui. Cela implique que certaines atténuations de ce risque sont exigées.

Noter qu'il est nécessaire de prouver la non existence des RR génériques applicables au titre du mécanisme de négation authentifiée, et que, dans une zone qui a plus d'une étiquette de profondeur, une telle preuve pourrait exiger de prouver la non existence de plusieurs ensembles discrets de RR génériques.

DNSSEC comporte bien des mécanismes qui rendent possible de déterminer quels noms d'autorité existent dans une zone, et quels types d'enregistrement de ressource d'autorité existent à ces noms. Les protections de DNSSEC ne couvrent pas les données non d'autorité comme les enregistrements colles.

2.7 Caractères génériques

Beaucoup de discussions ont eu lieu sur la question de si et comment assurer l'intégrité des données et l'authentification de l'origine des données pour les noms du DNS avec des "caractères génériques" *(wildcard)*. Conceptuellement, les RR avec des noms comportant des caractères génériques sont des schémas pour synthétiser des RR au vol selon les règles de correspondance décrites au paragraphe 4.3.2 de la RFC 1034. Bien que les règles qui contrôlent le comportement des noms à caractères génériques aient quelques bizarreries qui peuvent en faire des chausse-trappes pour un administrateur de zone distrait, il est clair qu'un certain nombre de sites font un gros usage des RR à caractères génériques, en particulier les RR MX à caractères génériques.

Afin de fournir les services désirés pour les RR à caractères génériques, on doit faire deux choses :
- on doit avoir un moyen d'attester de l'existence du RR à caractères générique lui-même (c'est-à-dire, on a besoin de montrer que la règle de synthèse existe) et
- on a besoin d'un moyen d'attester de la non existence de tous RR qui, si ils existaient, rendraient le RR à caractères génériques non pertinent selon les règles de synthèse qui gouvernent la façon dont les RR à caractères génériques sont utilisés (c'est-à-dire, on a besoin de montrer que la règle de synthèse est applicable).

Noter que cela rend les mécanismes de caractères génériques dépendants du mécanisme de négation authentifiée décrit au paragraphe précédent.

DNSSEC comporte des mécanismes conformes aux lignes décrites ci-dessus, qui rendent possible à un résolveur de vérifier qu'un serveur de noms a appliqué correctement les règles d'expansion des caractères génériques lorsque il a généré une réponse.

3. Faiblesses de DNSSEC

DNSSEC a ses propres problèmes :

- DNSSEC est d'une mise en œuvre complexe et comporte des cas bordures difficiles aux coupures de zone qui exigent un codage très soigneux. Les expérience de ban d'essais d'aujourd'hui suggèrent que des erreurs de configuration de zone triviales ou de clés expirées peuvent causer de sérieux problèmes à un résolveur à capacité DNSSEC, et que les capacités de rapport d'erreur du protocole actuel peuvent laisser à désirer.

- DNSSEC augmente de façon significative la taille des paquets de réponse du DNS, entre autres problèmes, cela rend les serveurs à capacité DNSSEC encore plus efficaces comme amplificateurs de déni de service.

- La validation de réponses DNSSEC augmente la charge de travail du résolveur, car un résolveur à capacité DNSSEC va avoir besoin d'effectuer la validation de signature et dans certains cas, il va devoir aussi produire de nouvelles interrogations. Cette charge de travail accrue va aussi augmenter le temps nécessaire pour le retour d'une réponse au client DNS d'origine, qui va vraisemblablement déclancher à la fois des fins de temporisation et de nouvelles interrogations dans certains cas. On peut se demander si de nombreux clients DNS actuels ne sont pas déjà trop impatients même avant de prendre en compte les retards supplémentaires que DNSSEC va imposer, mais cette question sort du domaine d'application de la présente note.

- Comme celui du DNS lui-même, le modèle de confiance de DNSSEC est presque totalement hiérarchique. Bien que DNSSEC permette bien aux résolveurs d'avoir une connaissance particulière supplémentaire des clés publiques au delà de celles pour la racine, dans le cas général, la clé racine est celle qui importe. Donc, tout compromis dans une des zones entre la racine et un nom cible particulier peut endommager la capacité de DNSSEC à protéger l'intégrité des données possédées par ce nom cible. Ce n'a pas changé, car le DNS non sécurisé a le même modèle.

- Le retournement de clé à la racine est vraiment dur. Les travaux à ce jour ne sont pas encore arrivés à s'approcher d'une spécification adéquate de la façon dont la clé racine peut se retourner, ou même de la façon dont elle est configurée en premier lieu.

- DNSSEC crée une exigence de synchronisation lâche entre le résolveur valideur et l'entité qui crée les signatures DNSSEC. Avant DNSSEC, toutes les actions en rapport avec le temps dans le DNS pouvaient être effectuées par une machine qui savait seulement le temps "écoulé" ou le temps "relatif". Parce que la période de validité d'une signature DNSSEC se fonde sur le temps "absolu", un résolveur valideur doit avoir le même concept de temps absolu que le signataire de la zone afin de déterminer si la signature est dans sa période de validité ou a expiré. Un attaquant qui peut changer l'opinion d'un résolveur sur le temps absolu actuel peut tromper le résolveur en utilisant des signatures expirées. Un attaquant qui peut changer l'opinion du signataire de zone sur le temps absolu actuel peut tromper le signataire de zone et l'amener à générer des signatures dont la période de validité ne correspond pas à ce que voulait le signataire.

- L'existence possible d'enregistrements de ressource qui comportent des caractères génériques dans une zone complique considérablement le mécanisme de négation authentifiée. Pendant la plus grande partie de la décade pendant laquelle DNSSEC a été développé, ces questions n'ont pas été très bien comprises. Il y a eu à plusieurs reprises la question de savoir si le mécanisme de négation authentifiée est complètement étanche et si il vaudrait la peine de l'optimiser pour le cas courant dans lequel il n'y a pas de présence de caractères génériques dans une zone. Cependant, le problème principal est juste la complexité inhérente du mécanisme de caractère générique lui-même. Cette complexité rend probablement le code pour générer et vérifier les attestations de négation authentifiée un peu fragile, mais comme la solution de remplacement d'abandonner complètement les caractères génériques n'est pas praticable à cause de leur large utilisation, on va devoir vivre avec les caractères génériques. La question devient alors juste de savoir si les optimisations proposées rendraient les mécanismes de DNSSEC plus ou moins fragiles.

- Même avec DNSSEC, la classe des attaques discutées au paragraphe 2.4 n'est pas facile à vaincre. Pour que DNSSEC soit efficace dans ce cas, il doit être possible de configurer le résolveur à attendre que certaines catégories d'enregistrements DNS soient signées. Cela peut exiger une configuration manuelle du résolveur, en particulier durant la période de retournement initial de DNSSEC lorsque le résolveur ne peut pas raisonnablement s'attendre à ce que la racine et les zones TLD soient signées.

4. Sujets de travaux futurs

La présent section énumère quelques sujets non couverts ci-dessus qui nécessiteraient probablement des études complémentaires, des mécanismes supplémentaires, ou les deux.

4.1 Interactions avec les autres protocoles

La discussion ci-dessus s'est concentrée exclusivement sur les attaques dans les frontières du protocole DNS lui-même, car elles sont (un des) les problèmes contre lesquels DNSSEC était destiné à protéger. Il y a cependant d'autres problèmes potentiels aux frontières où le DNS interagit avec les autres protocoles.

4.2 Sécurisation des mises à jour dynamiques de DNS

La mise à jour dynamique du DNS soulève un certain nombre de problèmes potentiels lorsque elle est combinée avec DNSSEC. La mise à jour dynamique d'une zone non sécurisée peut utiliser TSIG pour authentifier auprès du serveur le client qui met à jour. Bien que TSIG ne s'adapte pas très bien (il exige une configuration manuelle de clés partagées entre le serveur de noms DNS et chaque client TSIG), il fonctionne bien dans un environnement limité ou clos comme celui d'un serveur DHCP qui met à jour un serveur local de noms du DNS.

Des questions majeures surviennent lorsque on essaye d'utiliser la mise à jour dynamique sur une zone sûre. TSIG peut de même être utilisé de façon limitée pour authentifier le client auprès du serveur, mais TSIG ne protège que les transactions DNS, et non les données réelles, et le mécanisme TSIG n'est pas inséré dans la zone DNS, de sorte que les résolveurs ne peuvent pas utiliser le TSIG comme moyen de vérifier les changements apportés à la zone. Cela signifie que soit :

a) le client qui met à jour doit avoir accès à une clé de signature de zone afin de signer la mise à jour avant son envoi, ou
b) le serveur de noms DNS doit avoir accès à une clé de signature de zone en ligne afin de signer la mise à jour.

Dans l'un et l'autre cas, une clé de signature de zone doit être disponible pour créer des ensembles d'enregistrements de ressource signés à placer dans la zone mise à jour. Le fait que cette clé doive être en ligne (ou au moins disponible en ligne) est un risque de sécurité potentiel.

La mise à jour dynamique exige aussi une mise à jour du champ SERIAL du RR SOA de la zone. En théorie, cela pourrait aussi être traité par l'une ou l'autre des options ci-dessus, mais en pratique (a) serait très certainement extrêmement fragile, de sorte que (b) est le seul mécanisme envisageable.

Il y a d'autres menaces en termes de description de la politique de qui peut faire quels changements à quels ensembles d'enregistrements de ressource dans la zone. Le schéma actuel de contrôle d'accès dans la mise à jour dynamique sécurisée est très limité. Il n'y a aucun moyen de donner une fine granularité d'accès aux mises à jour des informations de zone du DNS à plusieurs entités, dont chacune peut requérir des sortes d'accès différentes. Par exemple, Alice peut avoir besoin d'être capable d'ajouter de nouveaux nœuds à la zone ou de changer les nœuds existants, mais pas de les retirer ; Bob peut avoir besoin d'être capable de supprimer des zones mais pas d'en ajouter ; Carol peut avoir besoin d'être capable d'ajouter, retirer, ou modifier les nœuds, mais seulement les enregistrements A.

Le problème des propriétés d'adaptation de la gestion de clé est ici d'une importance particulière qui requiert des études complémentaires.

4.3 Sécurisation des duplications de zones DNS

Comme on l'a exposé dans les sections précédentes, par lui-même, DNSSEC tente de fournir des services d'intégrité des données et d'authentification de l'origine des données par dessus le protocole normal d'interrogation du DNS. En utilisant la terminologie exposée dans la [RFC3552], DNSSEC fournit la "sécurité des objets" pour le protocole normal d'interrogation du DNS. Pour les besoins de la duplication de zones entières du DNS, DNSSEC ne fournit cependant pas la sécurité des objets, parce que les zones incluent des RR NS non signés et des RR colles aux points de délégation. L'utilisation de TSIG pour protéger les opérations de transfert de zone (AXFR ou IXFR) fournit la "sécurité du canal", mais ne fournit quand même pas la sécurité des objets pour des zones complètes. Les relations de confiance impliquées dans le transfert de zone est surtout une affaire bond par bond pour les opérateurs de serveurs de noms qui font confiance à un autre opérateur de serveur de nom plutôt qu'une affaire de bout en bout d'opérateurs de serveur de noms qui font confiance aux administrateurs de zone.

La sécurité des objets de zone n'était pas un objectif de conception explicite de DNSSEC, de sorte que l'échec de la fourniture de ce service ne devrait pas être une surprise. Néanmoins, il y a des scénarios de duplication de zone pour lesquels ce serait un service supplémentaire très utile, de sorte que ce semble être un domaine où des travaux futurs seraient utiles. En théorie, il ne devrait pas être difficile d'ajouter la sécurité des objets de zone comme amélioration rétro compatible au modèle existant de DNSSEC, mais le groupe de travail DNSEXT n'a encore discuté ni si cela est souhaitable ni les exigences pour une telle amélioration.

5. Conclusion

Sur la base de l'analyse ci-dessus, les extensions à DNSSEC apparaissent bien résoudre un ensemble de problèmes qui avaient besoin de l'être, et qu'il vaut la peine de les déployer.

Considérations sur la sécurité

Le présent document est tout entier consacré aux considérations sur la sécurité du DNS. Les auteurs pensent que le déploiement de DNSSEC aidera à résoudre certaines, mais pas toutes, les menaces connues qui pèsent sur le DNS.

Remerciements

La présente note se fonde à la fois sur les travaux antérieurs publiés par d'autres et sur un certain nombre de discussions publiques et privés sur plusieurs années, mais des remerciements particuliers sont adressés à Jaap Akkerhuis, Steve Bellovin, Dan Bernstein, Randy Bush, Steve Crocker, Olafur Gudmundsson, Russ Housley, Rip Loomis, Allison Mankin, Paul Mockapetris, Thomas Narten, Mans Nilsson, Pekka Savola, Paul Vixie, Xunhua Wang, et à tous les autres membres des groupes de travail DNS, DNSSEC, DNSIND, et DNSEXT dont les auteurs ont oublié les noms et les contributions, dont aucun n'est responsable de ce que les auteurs ont fait de leurs idées.

Comme pour tout travail de cette nature, les auteurs de la présente note reconnaissent qu'ils marchent sur les traces de ceux qui ont ouvert la voie. Les lecteurs intéressés par le sujet pourront aussi souhaiter lire [Bellovin95], [Schuba93], et [Vixie95].

Références

[Bellovin95] Bellovin, S., "Using the Domain Name System for System Break-Ins", Proceedings of the Fifth Usenix Unix Security Symposium, juin 1995.

[Galvin93] Message de résumé de la réunion de l'équipe de conception envoyé à la liste de diffusion dns-security@tis.com par Jim Galvin le 19 novembre 1993.

[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)

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(Information)*

[RFC2308] M. Andrews, "Mise en antémémoire négative des interrogations du DNS (DNS NCACHE)", mars 1998. (*MàJ par* RFC4035, RFC4033, RFC4034, RFC6604) *(P.S.)*

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC2671] P. Vixie, "Mécanismes d'extension pour le DNS (EDNS0)", août 1999. *(P.S.) (Remplacée par* RFC6891)

[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.)*

[RFC3007] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", novembre 2000.

[RFC3552] E. Rescorla, B. Korver, "Lignes directrices pour la rédaction d'une section de considérations sur la sécurité dans les RFC", juillet 2003. (BCP0072)

[Schuba93] Schuba, C., "Addressing Weaknesses in the Domain Name System Protocol", Master's thesis, Purdue University Department of Computer Sciences, août 1993.

[Vixie95] Vixie, P, "DNS and BIND Security Issues", Proceedings of the Fifth Usenix Unix Security Symposium, juin 1995.

Adresse des auteurs

Derek Atkins
IHTFP Consulting, Inc.
6 Farragut Ave
Somerville, MA 02144
USA
mél : derek@ihtfp.com

Rob Austein
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
USA
mél : sra@isc.org

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

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