Le programme MORECOWBELL de la NSA sonne le glas du DNS

Christian Grothoff, Matthias Wachs, Monika Ermert, Jacob Appelbaum, Ludovic Courtès

Le programme MORECOWBELL de la NSA sonne le glas du DNS

Christian Grothoff, Inria
Matthias Wachs, TU Munich
Monika Ermert, Heise Verlag
Jacob Appelbaum, Tor Project

Traduction : Ludovic Courtès

1 Introduction

Sur le net, presque tout commence par une requête au *Domain Name System* (DNS, pour « système de noms de domaine »), un protocole au cœur d'Internet qui permet aux usagers d'accéder à des services par un nom tel que `www.example.com`, plutôt que par une adresse IP numérique comme `2001 :DB8 :4145 : :4242`. Développé au « bon vieux temps », le DNS contemporain ressemble à un tableau de bord de l'activité du réseau pour malvoyants. Par conséquent, il attire non seulement toutes sortes de surveillances à des fins commerciales, mais aussi la *National Security Agency* (NSA), comme le montrent de nouveaux documents sur son programme MORECOWBELL. Étant données les faiblesses de conception du DNS, on peut se demander si le DNS peut être sécurisé et sauvé ou bien si il doit être remplacé—tout du moins pour certains cas d'utilisation.

Ces deux dernières années, il y a eu un florilège d'activités pour traiter les problèmes de sécurité et de respect de la vie privée à l'*Internet Engineering Task Force* (IETF), l'entité qui documente les standards relatifs au DNS. L'*Internet Architecture Board*, un pair de l'IETF, a fait appel aux ingénieurs pour utiliser du chiffrement partout, potentiellement y compris dans le DNS [4].

Un récent document de travail de l'IETF [6] sur les questions de vie privée pour le DNS commence par reconnaître le DNS

> « [...] comme un des plus importants composants de l'infrastructure d'Internet et un des plus souvent ignorés on incompris. Presque toute activité sur Internet commence par une requête DNS (et souvent plusieurs). Son utilisation a beaucoup d'implications sur le respect à la vie privée [...] »

Bien que cette affirmation fasse l'objet d'un consensus, l'IETF ne s'attend pas à ce que les solutions existantes puissent changer la situation dans un avenir proche :

> « Il semble aujourd'hui que l'éventualité d'un chiffrement massif du trafic DNS soit très éloignée. » [5]

Du point de vue de la surveillance, le DNS traite actuellement toutes les informations dans la base de données DNS comme des données publiques. Le contenu des requêtes et des réponses n'est typiquement pas chiffré. Cela permet à un attaquant passif d'observer toutes les requêtes d'un usager et de voir quels services elle ou il utilise et quels sites Web il ou elle visite. Pour un attaquant actif, le DNS permet de faciliter la localisation de services potentiellement vulnérables, un premier pas avant leur exploitation grâce à des attaques *0-day* (« jour 0 ») disponibles sur le marché.

Les discussions à l'IETF ont mené à des propositions comme la « réduction des requêtes », Confidential DNS, DNS sur TLS, et DNSCurve, ainsi qu'à des propositions plus radicales pour des systèmes de noms alternatifs conçus pour davantage respecter la vie privée. Tous ces travaux adoptent des approches différentes pour réduire le rôle du DNS en tant que source de méta-données ultime dans le panoptique numérique qu'est Internet.

2 MORECOWBELL : à l'écoute du DNS

Étant donné que le DNS aujourd'hui est comme un livre ouvert, il n'est pas étonnant de voir que de nouveaux documents *top secrets* auxquels Le Monde a eu accès révèlent que le programme MORECOWBELL (ou « MCB ») de l'agence d'espionnage américaine NSA se sert du DNS comme moyen de surveillance d'Internet (figure 1). Le programme MORECOWBELL utilise une infrastructure de surveillance dissimulée pour envoyer des requêtes aux serveurs DNS et des requêtes HTTP pour obtenir des informations sur les services et pour vérifier leur disponibilité (figure 4).

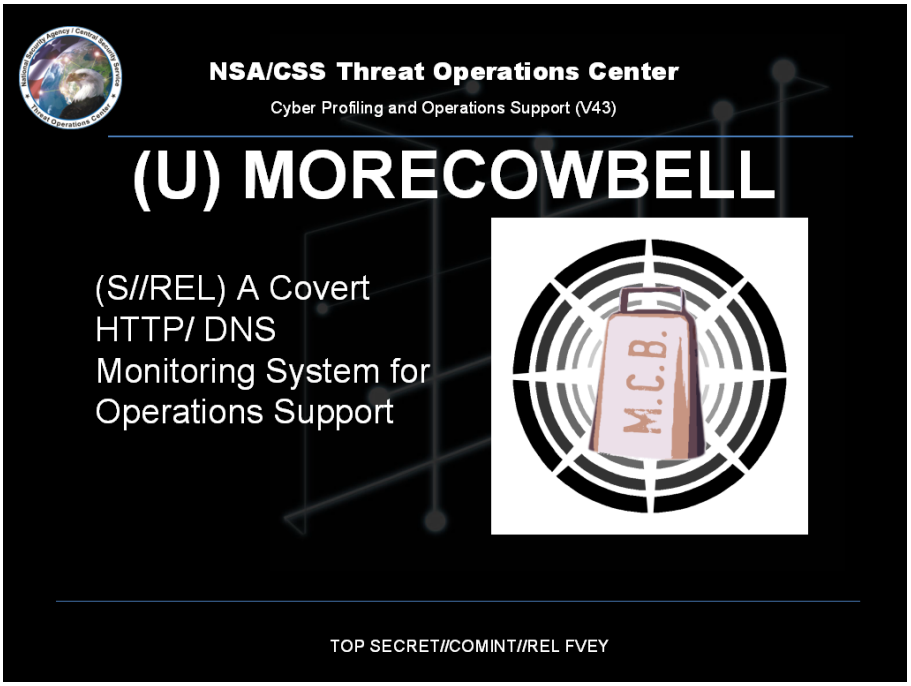


FIGURE 1 – Tiré de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html` : MORECOWBELL, un système de surveillance HTTP/DNS dissimulé.

Malgré la nature ouverte du DNS, la NSA procède en se dissimulant (figure 2) pour s'assurer que les milliers de requêtes DNS envoyées chaque heure ne sont pas imputées au gouvernement étasunien. Concrètement, les serveurs que la NSA a loués pour surveiller le DNS et sonder les serveurs Web avec HTTP sont localisés en Malaisie, en Allemagne et au Danemark (figure 3). Cela permet à la NSA d'effectuer cette surveillance en cachette et d'avoir une meilleure vue d'ensemble de la résolution DNS et de la disponibilité des services. Les transparents ne listent que ces trois pays, mais on sait que l'infrastructure PACKAGEDGOODS de surveillance non-imputable sur laquelle repose MORECOWBELL utilise des machines dans au moins 13 autres pays, comme l'a décrit Der Spiegel dans des transparents décrivant le programme TREASUREMAP de la NSA [12].

Ce qui est intéressant est qu'à l'époque, la NSA ne faisait guère attention au contenu des serveurs Web ou des entrées DNS—comme d'habitude la NSA se focalise sur les méta-données : elle veut savoir si les informations DNS ont changé et vérifier la disponibilité de services. Les transparents montrent que cette simple vérification a des utilisations bénignes, comme par exemple celle de surveiller les sites Web du gouvernement des États-Unis.

Selon toute vraisemblance, la principale raison pour laquelle ce sondage DNS est rendu non-imputable au gouvernement étasunien est son utilisation comme « indication des dommages de combat » (*battle damage indication* en anglais ; figure 5). En particulier, suite à des attaques contre une infrastructure réseau critique (*computer network attacks* ou « CNA »), les États-Unis pourraient utiliser ce genre de sonde pour confirmer que les attaques ont atteint leurs cibles, en observant que, par exemple, les systèmes d'un gouvernement étranger se retrouvent « débranchés » d'Internet. En surveillant les changements dans le DNS, l'attaque pourrait être répétée si la victime essaye de déplacer ses services vers un autre système ou réseau. En conservant l'infrastructure de surveillance dissimulée et répartie géographiquement, la NSA s'assure une vision globale de l'impact d'une attaque. De cette façon, l'identification des serveurs de surveillance est rendue encore plus difficile pour les victimes, qui sinon pourraient essayer d'échapper à une attaque en traitant les requêtes provenant des serveurs de surveillance différemment—c'est la technique de « vue fractionnée » (*split view*) couramment utilisée avec le DNS.

Bien que nous n'en ayons aucune preuve, l'« indication des dommages de combat » pourrait inclure des dommages causés par des sources autres que des cyber-attaques, telles que des bombardements ou

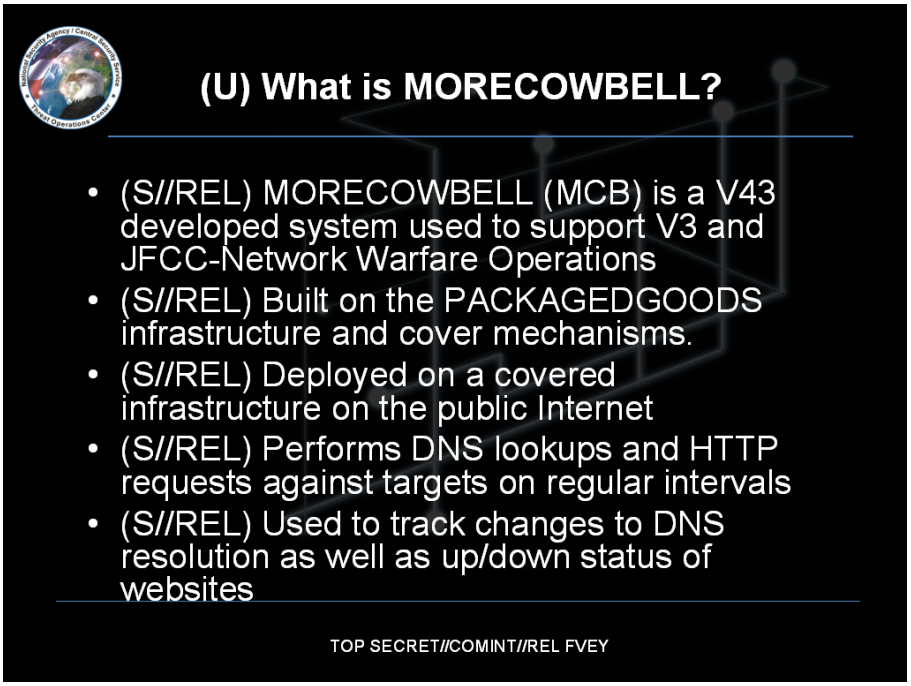


FIGURE 2 – Tiré de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html` : Qu'est-ce que MORECOWBELL ?

des câbles coupés. Le gouvernement des États-Unis utilise parfois ce terme d'« indication des dommages de combat » pour des attaques cinétiques :

> « INDICATION DES DOMMAGES DE COMBAT
> L'objectif de ce travail est de développer des méthodes novatrices bon marché pour rapidement déterminer l'effet qu'une munition aérienne a eu sur sa cible. Cette information est particulièrement importante dans le cas de cibles enfouies où, après attaque, il risque d'être difficile d'obtenir des indices visuels. Un lien réseau à bord de la munition pourrait permettre d'obtenir des indications sur les dommages causés à ce type de cible. Un tel lien pourrait soit reposer sur un câble tiré, soit être complètement sans-fil. En revanche, **l'indication des dommages de combat** pourrait être totalement indépendante de la munition qui est lancée. L'objectif de cette étude est de développer des moyens bon marché, efficaces et fiables pour rapidement donner aux combattants une indication précise, ou du moins une estimation fiable, des dégâts infligés à une cible—particulièrement pour une cible blindée ou enfouie.
> —Dr. Alex Cash AFRL/MNMI (850) 882-0391 cash@eglin.af.mil » [1]

Les différents documents de la NSA relatifs au DNS montrent que les attaques dissimulées existantes contre le DNS vont au-delà de la surveillance de masse jusqu'à être un support aux attaques actives [18]. Avec les révélations sur la famille de projets QUANTUMTHEORY de la NSA, et notamment des sous-projets comme QUANTUMDNS, nous savons que des attaquants puissants tels que des États peuvent non seulement écouter le trafic DNS, mais également injecter des réponses DNS pour modifier le résultat d'une résolution de nom ou faire carrément échouer des requêtes [13]. Étant donné que le DNS ne procure aucune confidentialité à ses usagers, il est facile de créer un profile des usagers et de leur comportement de *surf* sur le Web. Cette information peut ensuite être utilisée pour mener des attaques QUANTUMTHEORY contre la cible. Les programmes NSA tels que QUANTUMBOT ont pour but de surveiller des *botnets* IRC et de détecter les ordinateurs exploités comme robots dans un *botnet*, pour ensuite en détourner le canal de commande et de contrôle pour instrumenter les robots. Ces programmes sont considérés par la NSA comme *un grand succès* d'après leurs documents [11].

1. C'est nous qui soulignons. Cité d'après `http://www.darkgovernment.com/airforcedev.html`.

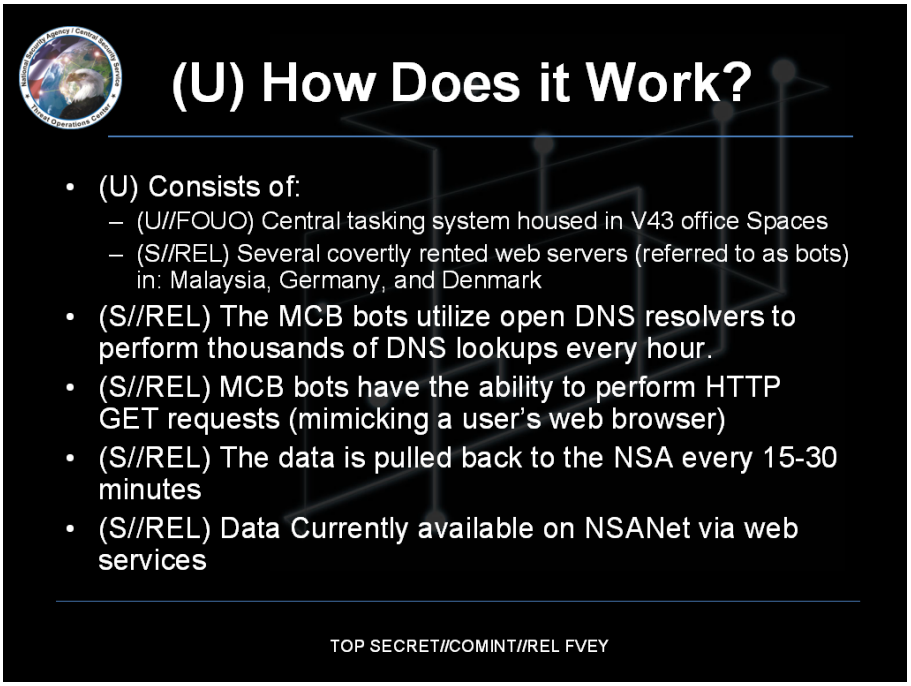


FIGURE 3 – Tiré de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html` : Comment MORECOWBELL fonctionne-t-il ?

Par conséquent, la communauté Internet doit travailler à la résolution des problèmes de respect de la vie privée et de sécurité relatifs à la résolution de noms et au système de noms de domaine (DNS) actuel. Dans la suite de cet article, nous passons en revue l'architecture DNS actuelle ainsi qu'un ensemble de propositions qui ont été faites pour améliorer la sécurité de ce service critique d'Internet.

3 Fonctionnement du DNS

Le système de noms de domaine ou *Domain Name System* (DNS) est un morceau essentiel d'Internet puisqu'il fournit la correspondance entre les noms de machines et leurs adresses IP, permettant aux usagers d'utiliser des noms faciles à mémoriser. Le DNS est hiérarchique ; il stocke des correspondances nom/valeur dans des « enregistrements » (*records*) dans un base de données répartie. Un enregistrement a un nom, un type, une valeur et une date d'expiration. Les noms sont des « étiquettes » (*labels*) délimitées par des points. Le sommet de la hiérarchie est l'étiquette vide, et l'étiquette la plus à droite dans un nom est appelée « domaine de plus haut niveau » (*top-level domain* ou TLD). Les noms ayant un suffixe commun sont dans le même *domaine*. Le *type d'enregistrement* spécifie le genre de valeur associé à un nom, et un nom peut avoir plusieurs enregistrements avec des types variés. Le type d'enregistrement le plus connu est le type « A » qui associe des noms à des adresses IPv4.

La base de données DNS est découpée en *zones*. Une zone est une partie de l'espace des noms dont la responsabilité administrative revient à une autorité précise. Une zone est autonome dans la gestion des enregistrements de un ou plusieurs domaines. Une autorité peut déléguer la responsabilité pour des *sous-domaines* à d'autres autorités. Cela se fait au moyen d'enregistrements « NS » dont la valeur est le nom d'un serveur DNS de l'autorité du sous-domaine. La *zone racine* (*root zone*) est la zone correspondant à l'étiquette vide. Elle est gérée par l'Autorité pour l'affectation des numéros sur Internet (la *Internet Assigned Numbers Authority* ou IANA) actuellement exploitée par la *Internet Corporation for Assigned Names and Numbers* (ICANN) sous contrat avec l'Administration nationale de l'information et des télécommunications (*National Telecommunications and Information Administration* ou NTIA). La NTIA est une agence du ministère du commerce étasunien. En tant que tel, elle joue un rôle mineur

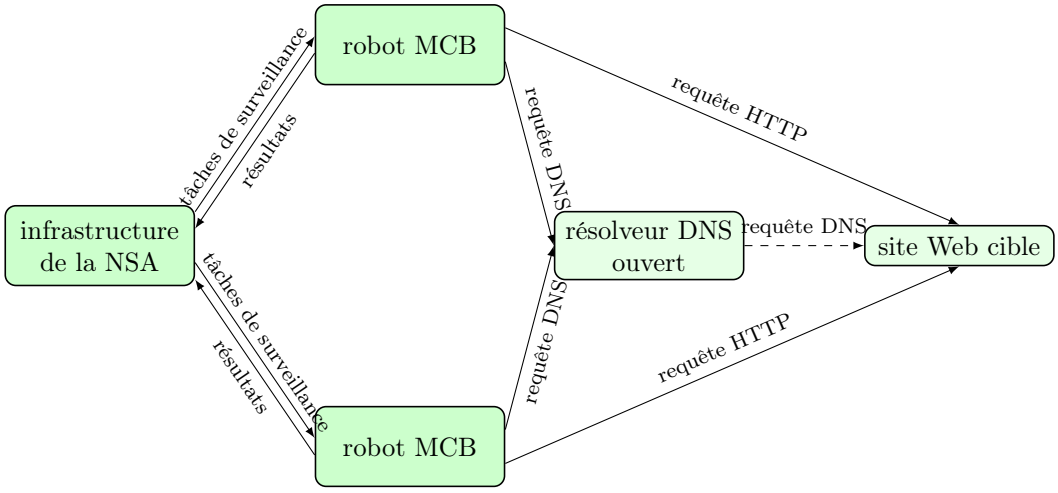


FIGURE 4 – L'infrastructure MORECOWBELL de la NSA : une liste de cibles à surveiller en envoyée à un ensemble de robots distribués géographiquement. Ces robots effectuent des requêtes DNS et HTTP contre les sites Web cibles pour collecter de l'information sur la disponibilité de services. Les résultats sont envoyés à la NSA à intervalles réguliers.

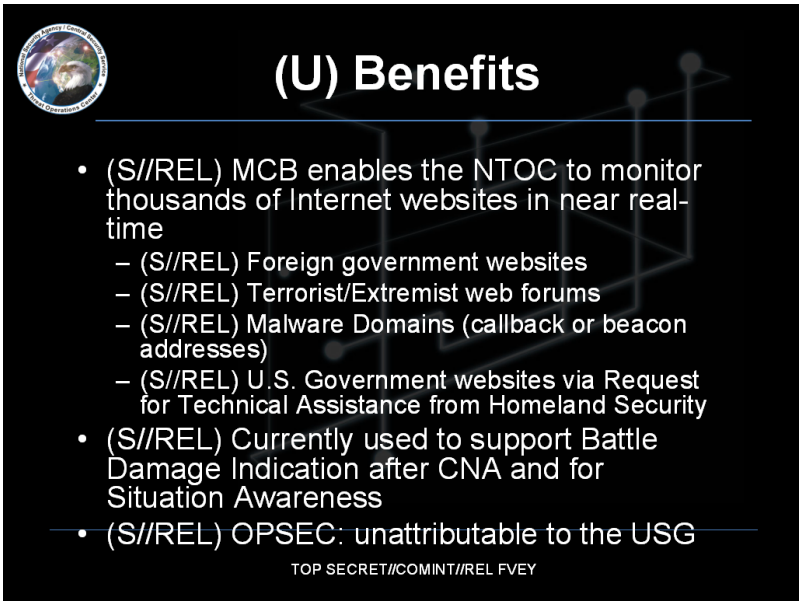


FIGURE 5 – Tiré de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html` : « Bénéfices » de MORECOWBELL.

mais significatif dans l'exploitation du DNS : elle vérifie chaque ajout et changement dans le fichier de la zone racine. Le contrat NTIA-IANA prend fin le 30 septembre 2015 et la NTIA a annoncé son intention d'amorcer une transition de son rôle actuel de contrôle vers une entité de supervision regroupant plusieurs intervenants (*multistakeholder oversight*). La zone racine contient des enregistrements « NS » spécifiant les noms des serveurs DNS ayant autorité pour tous les TLD, tels que « .fr » ou « .paris ».

Les noms DNS sont résolus par des *résolveurs* (*resolvers*). Beaucoup de systèmes d'exploitation modernes ne fournissent pas de résolveurs complets mais juste des « *résolveurs souche* » (*stub resolvers*). Ces souches ne résolvent pas les noms directement mais font suivre les requêtes à un *résolveur relais* (*forwarding resolver*), typiquement celui du fournisseur d'accès à Internet, comme le montre la figure 6.

Ces résolveurs résolvent les noms en interrogeant d'abord les serveurs racines. Si le serveur DNS interrogé ne peut pas fournir la réponse finale, il fournit au moins au résolveur un enregistrement « NS » qui renvoie le résolveur vers le serveur DNS suivant. Cette procédure *itérative* est répétée et ne se termine vraiment que quand le résolveur interroge *le serveur de noms ayant autorité* sur ce domaine précis. Le DNS bénéficie grandement de l'utilisation de caches : beaucoup de résolveurs (*caching resolvers*) stockent l'information précédemment demandée pour améliorer la performance des recherches de noms à venir. Ils utilisent les enregistrements gardés en cache pour se passer de tout ou partie des itérations, retournant ainsi l'information plus rapidement au demandeur.

Avec l'utilisation de résolveurs relais, l'adresse IP des demandeurs est cachée des serveurs de noms ayant autorité. Cela procure un certain degré de respect de la vie privée des utilisateurs puisque les exploitants des serveurs de noms autorisés sont dans l'incapacité de surveiller la source des requêtes DNS. Naturellement, les exploitants de résolveurs relais peuvent eux aisément surveiller et censurer les requêtes des utilisateurs. Les filets de surveillance passive tels que TURMOIL et XKEYSCORE peuvent également voir n'importe quelle partie d'une transaction disponible dans leur filtre d'entrée.

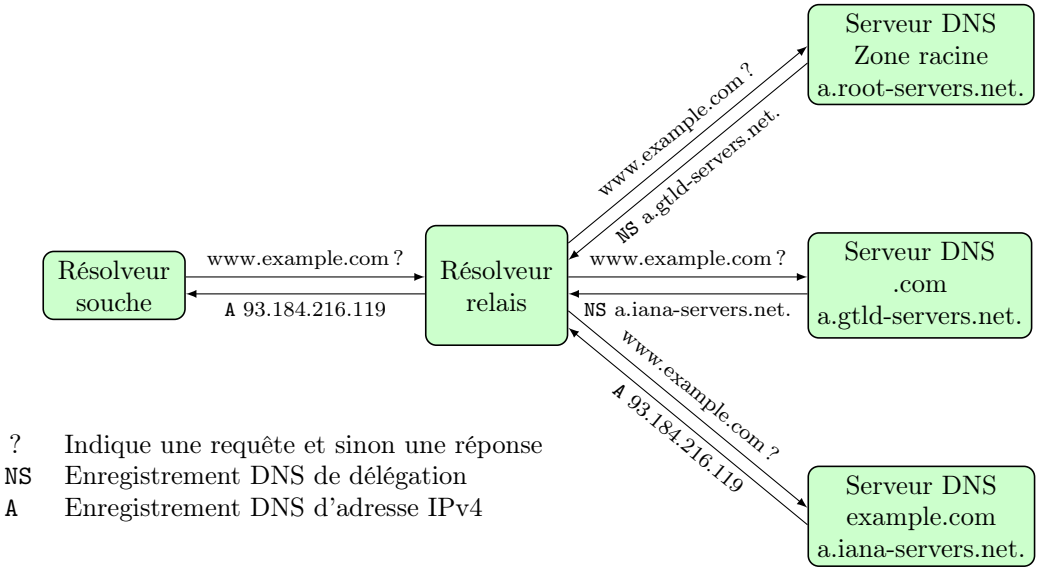


FIGURE 6 – Résolution DNS du nom `www.example.com`. Beaucoup de systèmes d'exploitation ne fournissent que des « résolveurs souche » qui font suivre les requêtes à des résolveurs complets. Pour résoudre un nom, ces résolveurs commencent par interroger les serveurs de noms de la zone racine. Si un serveur ne peut pas fournir l'information demandée, il renvoie le résolveur vers le serveur suivant à interroger jusqu'à ce qu'un serveur *autorisé* pour la zone concernée soit trouvé.

4 DNSSEC

Le DNS n'a pas été conçu pour apporter de la sécurité sur un réseau qui n'est pas sûr. Les Extensions de sécurité du DNS (*Domain Name System Security Extensions* ou DNSSEC) [1] étendent DNS avec une protection de l'intégrité des enregistrements DNS ainsi que l'authentification de leur origine. DNSSEC n'assure pas la confidentialité et ne protège pas contre le déni de service ; par conséquent DNSSEC n'apporte aucune protection contre la surveillance passive. Il ajoute des types d'enregistrements pour les clefs publiques (« DNSKEY »), la délégation de signature (« DS »), et pour les signatures sur les enregistrements de ressources (« RRSIG »). La figure 7 illustre les interactions entre résolveurs utilisant DNSSEC. DNSSEC créée une infrastructure de clefs publiques hiérarchique à laquelle doivent participer tous les exploitants de serveurs DNSSEC. Elle établit une chaîne de confiance entre le serveur de la zone autorisée et « l'ancre de confiance » (*trust anchor*) associée à la zone racine. Cette association se fait en distribuant la clef publique de la zone racine par des moyens hors bande, par exemple en la fournissant avec le système d'exploitation. La chaîne de confiance établie par DNSSEC reprend les délégations de zone du DNS. Les exploitants de TLD étant typiquement soumis à la même juridiction que les exploitants

de domaines dans leur zone, le risque existe que ces chaînes de confiance puissent être attaquées par des moyens techniques ou légaux.

Nous décrivons ci-après les plus grosses faiblesses qu'expose le DNS y compris avec ses extensions de sécurité (DNSSEC). DNSSEC échoue à garantir la confidentialité des requêtes : le contenu des requêtes et réponses DNS peut toujours être lu par n'importe quel adversaire ayant accès au canal de communication et, par conséquent, peut être corrélé aux utilisateurs, particulièrement si l'adversaire peut observer le lien entre le résolveur souche de l'utilisateur et le résolveur relais. Techniquement, le déploiement actuel de DNSSEC souffre de l'utilisation du système de cryptographie RSA (la zone racine utilise RSA-1024) ; tout résolveur compatible DNSSEC a obligation de prendre en charge RSA, ce qui mène à des clefs de grande taille, d'autant plus que les réponses incluent les signatures pour tout les schémas de signature pris en charge par le serveur ayant autorité. Cela donne lieu à des messages dont la taille excède les restrictions sur la taille des paquets DNS, créant ainsi de nouvelles vulnérabilités [7]. Enfin, DNSSEC n'est pas conçu pour résister aux attaques légales. Suivant leur influence, les gouvernements, entreprises ou leurs lobbies peuvent légalement obliger les exploitants d'autorités DNS à manipuler des entrées et faire valider les changements. Il s'agit là d'une préoccupation pertinente puisque DNSSEC maintient la structure hiérarchique du DNS et place donc une confiance étendue dans la zone racine et les exploitants de TLD.

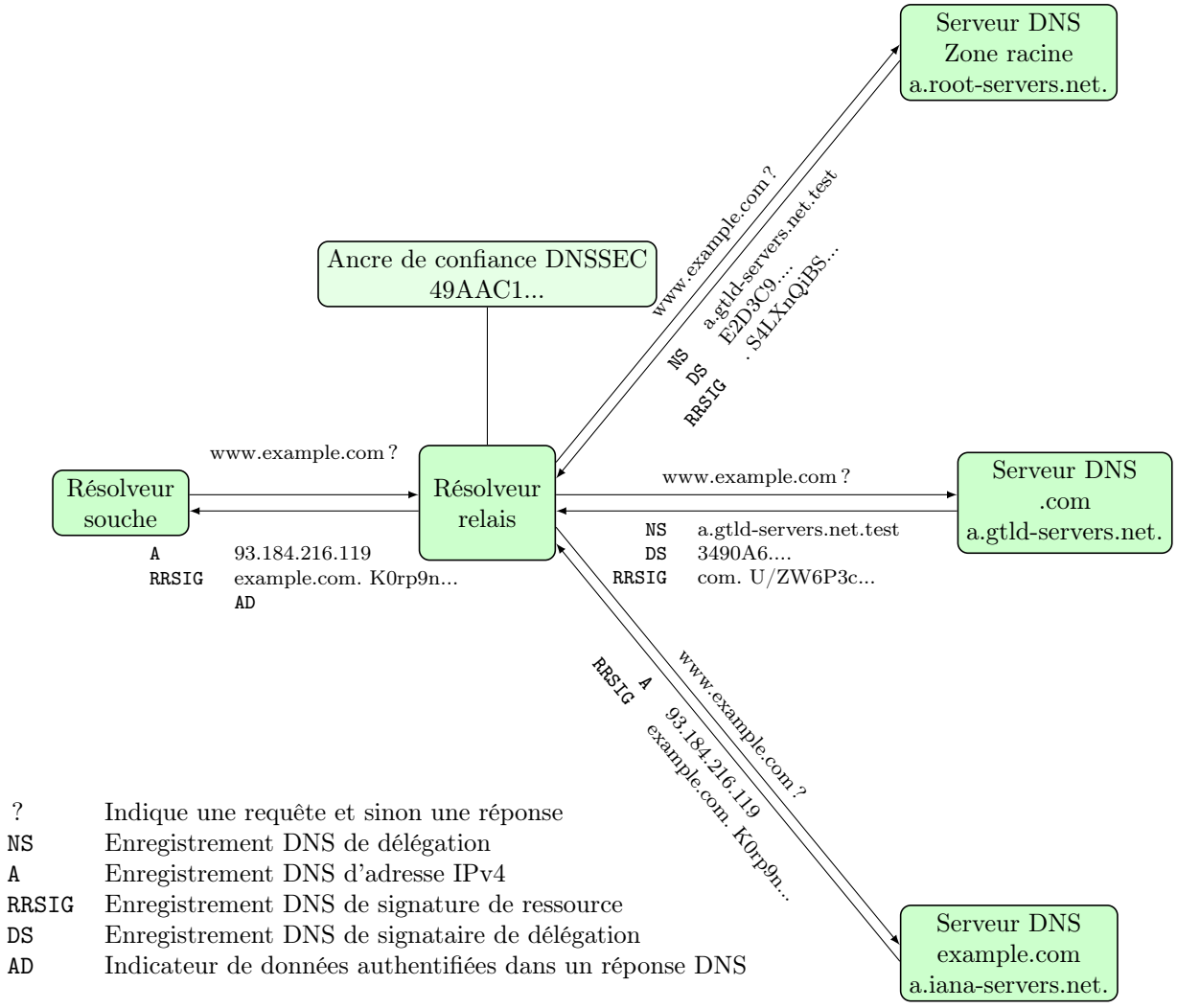
DNSSEC lève également quelques limites traditionnelles sur l'acquisition par lot des données de zone, telles que les restrictions sur les transferts de zones. Avant DNSSEC, les administrateurs de zones DNS pouvaient interdire le transfert de zone, rendant difficile pour un adversaire l'énumération systématique de tous les enregistrements DNS d'une zone. Cependant, comme le DNS autorise les réponses négatives (« NXDOMAIN »), il était nécessaire de trouver un moyen dans DNSSEC pour créer des déclarations signées de non-existence d'enregistrements. DNSSEC étant conçu pour garder les clef de signature hors-ligne, on a introduit les enregistrements « NSEC » pour certifier qu'une gamme entière de noms est inutilisée. En regardant les bornes de cette gamme, un adversaire peut rapidement énumérer tous les noms d'une zone qui sont utilisés. L'introduction des enregistrements « NSEC3 » a tenté de corriger ce problème, mais a été démontrée fichue avant même d'avoir été déployée de manière significative. Le résultat est que DNSSEC permet à un adversaire de découvrir encore plus facilement des services et systèmes vulnérables.

5 Réduction des requêtes

Les discussions récentes à l'IETF pour améliorer le respect de la vie privée dans le DNS incluent une proposition appelée *réduction des requêtes* (*query minimisation*) qui a de bonnes chances d'être adoptée rapidement car elle ne requiert aucun changement dans le protocole DNS. La réduction des requêtes améliorerait légèrement le respect de la vie privée en changeant les résolveurs relais de manière à ce qu'ils n'envoient plus la requête complète aux serveurs DNS contactés à chaque étape de la résolution. À la place, chaque serveur DNS ne recevrait que la fraction du nom DNS qui est strictement nécessaire pour faire progresser le processus de résolution (figure 8). Par conséquent, le nom complet qui est demandé ne sera typiquement montré qu'au serveur DNS final ayant autorité.

La réduction des requêtes peut être mise en œuvre simplement en changeant la manière dont les résolveurs relais construisent leurs requêtes itératives. La réduction des requêtes pourrait avoir un impact négatif sur le cache, au moins en théorie, puisque le fait d'avoir la requête complète peut permettre à un serveur DNS de renvoyer la réponse finale, par exemple parce que l'information a été mise en cache suite à des requêtes récursives, ou parce qu'il a déjà autorité sur le nom complet. Les résolveurs relais finissent toujours par apprendre la requête complète et la réponse de l'utilisateur, même avec la réduction des requêtes.

La réduction des requêtes a l'avantage que son déploiement ne requiert des changements qu'au niveau des résolveurs relais, et l'inconvénient que ce changement pour mieux respecter la vie privée des utilisateurs n'est pas du tout sous leur contrôle. La réduction des requêtes peut être combinée avec les différentes approches pour chiffrer le trafic DNS présentées dans les sections suivantes ; sans la réduction des requêtes, le simple chiffrement du trafic DNS continue de révéler la requête complète à beaucoup de serveurs DNS. Enfin, il se peut que Verisign Inc. cherche à empêcher l'adoption de la réduction de requêtes en tirant parti du racket au brevet [16].



?	Indique une requête et sinon une réponse
`NS`	Enregistrement DNS de délégation
`A`	Enregistrement DNS d'adresse IPv4
`RRSIG`	Enregistrement DNS de signature de ressource
`DS`	Enregistrement DNS de signataire de délégation
`AD`	Indicateur de données authentifiées dans un réponse DNS

FIGURE 7 – Résolution du nom `www.example.com` avec DNS et DNSSEC : l'information retournée par les serveurs de noms est signée cryptographiquement pour en assurer l'authenticité et l'intégrité. Cette information est stockée dans des enregistrements « RRSIG » et l'information sur la zone parent est stockée dans des enregistrements « DS ». Un résolveur peut vérifier la signature en suivant cette chaîne de confiance et en utilisant *l'ancre de confiance* livrée par des moyens hors bande. Les résolveurs souche ne peuvent pas vérifier cette chaîne et le résolveur indique donc au résolveur souche qu'il doit vérifier l'authenticité en activant le bit `AD` dans la réponse fournie au client.

6 T-DNS : DNS sur TLS

Auparavant, les propositions pour utiliser TLS (*Transport Layer Security*) pour chiffrer le trafic DNS étaient souvent rejetées en raison de la baisse de performance qu'engendrerait un tel changement. Dans un récent document de travail IETF à propos de DNS sur TLS, les auteurs expliquent que l'utilisation de TLS serait non seulement bénéfique pour le respect de la vie privée, mais aussi que le passage à TCP—c'est-à-dire le passage de l'UDP, sans connexion, au TCP, qui est orienté connexion—pourrait améliorer la protection contre les attaques par amplification sur (ou par) les serveurs DNS [8].

En réutilisant une connexion TCP pour plusieurs requêtes DNS avec des *timeouts* raisonnables, en permettant d'enchaîner plusieurs requêtes (*pipelining*) et de les traiter dans le désordre, la proposition T-DNS promet une performance raisonnable malgré le surcoût induit par TCP et TLS.

Cependant, même si TLS devait être déployé pour le DNS, les méta-données permettant à un attaquant

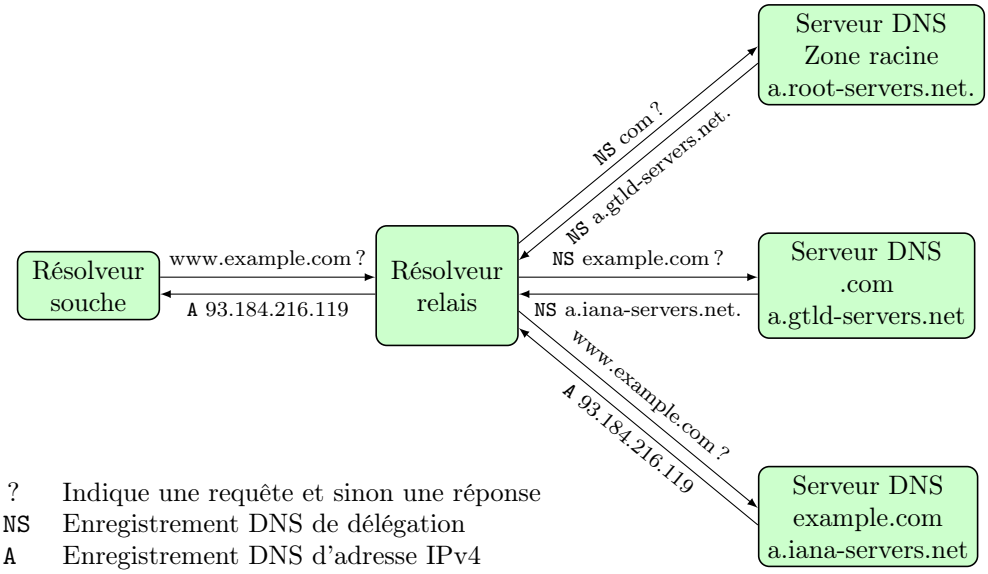


FIGURE 8 – Avec la réduction des requêtes, la résolution du nom `www.example.com` ne révèle plus le nom complet et le type de requête à la zone racine et à l'autorité `.com`. Naturellement, ce schéma livre encore des informations sensibles au serveur DNS du TLD. En outre, l'effet est encore plus faible en pratique puisque la zone racine est déjà rarement contactée du fait que l'information concernant les serveurs de noms des TLD est typiquement en cache au niveau des résolveurs relais.

de déterminer à quelles données DNS accède un usager seraient toujours révélées. Dans la proposition de l'IETF, TLS est combiné avec l'utilisation de résolveurs relais (*forward resolvers*) qui cachent l'adresse IP de l'usager aux serveurs DNS, mais auxquels on doit malgré tout faire confiance pour ne pas espionner l'usager. En outre, TLS lui-même n'a pas le meilleur bilan de sécurité, avec des dizaines de problèmes survenus ces dernières années allant de la compromission d'autorités de certification éminentes à des implémentations cassées ou encore des modes de chiffrement peu sûrs.

TLS n'est pas la seule méthode possible pour chiffrer les requêtes et réponses DNS quand elles parcourent le réseau. DNSCurve et Confidential DNS sont des propositions alternatives pour protéger le contenu des requêtes et réponses DNS de la surveillance au niveau réseau.

DNS sur TLS est disponible sur les serveurs DNS de Unbound.

7 DNSCurve

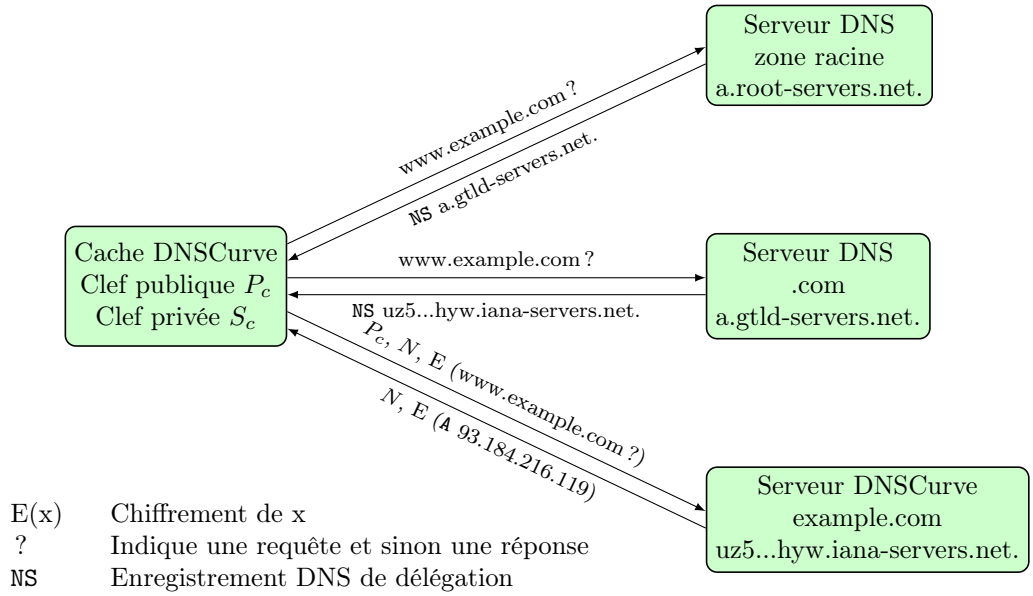
Le premier système à avoir amélioré la confidentialité des requêtes et réponses DNS est DNSCurve [3]. Dans DNSCurve, des clefs de session sont échangées en utilisant Curve25519 [2] puis utilisées pour l'authentification et le chiffrement entre les caches et les serveurs. DNSCurve ajoute au DNS actuel la confidentialité et l'intégrité sans avoir recours à des signatures coûteuses ni à des sessions (D)TLS. Concrètement, DNSCurve réussit à atteindre le même temps aller-retour (*round-trip time*, RTT) que DNS en intégrant la clef publique du serveur dans les enregistrements « NS ».

DNSCurve créée une association chiffrée et authentifiée entre un *serveur DNSCurve* et un *cache DNSCurve*, ce dernier étant, plutôt qu'un résolveur souche, un résolveur DNS récursif maintenant un cache et s'exécutant à l'extrémité (figure 9). Puisque DNSCurve n'utilise pas de signatures, un cache DNSCurve ne peut pas prouver l'authenticité des enregistrements gardés en cache aux autres usagers, ce qui fait que les caches ne sont utiles qu'aux extrémités.

D'un côté, avec DNSCurve l'usager n'a plus besoin de faire confiance à un résolveur relais, mais d'un autre côté, son adresse IP est maintenant directement révélée aux serveurs DNS ayant autorité : elle n'est plus cachée par les résolveurs relais des fournisseurs d'accès au réseau. DNSCurve peut donc améliorer les respect de la vie privée vis-à-vis d'un adversaire surveillant le trafic DNS sur des systèmes intermédiaires ou par des écoutes, mais réduit le respect de la vie privée vis-à-vis des serveurs DNS ayant

autorité, puisqu'ils apprennent à la fois la requête complète et l'identité (adresse IP) de l'usager. Une autre préoccupation largement partagée au sujet de DNSCurve est le besoin de garder les clefs privées en ligne. DNSCurve ne peut pas non plus protéger de la censure, puisque certains gouvernements continuent, en pratique, de contrôler la hiérarchie des *registrars* et peuvent donc faire disparaître des domaines. Par rapport aux attaques de la NSA, DNSCurve n'aide les usagers que contre la surveillance passive en protégeant au moins la confidentialité de la charge DNS.

Avec DNSCurve, les serveurs DNS restent une cible juteuse pour la surveillance de masse. De plus, comme avec DNS, les serveurs DNS connus et facilement localisables demeurent une cible et un moyen de confirmation des attaques sur l'infrastructure critique. Avec DNSCurve, la nécessité de faire de la cryptographie à clef publique en ligne peut théoriquement ouvrir la porte à de nouvelles vulnérabilités à des attaques en déni de service si un processeur peu puissant est utilisé pour traiter un lien à haut débit.



E(x)	Chiffrement de x
?	Indique une requête et sinon une réponse
`NS`	Enregistrement DNS de délégation
`A`	Enregistrement DNS d'adresse IPv4
N	nonce
S_c/P_c	Clef secrète/publique du cache

FIGURE 9 – Résolution du nom `www.example.com` avec DNSCurve. Avec DNSCurve, le cache de résolution et le serveur DNSCurve échangent un secret partagé pour chiffrer leurs communications. La clef publique du serveur DNSCurve est codée dans le nom du serveur de noms lui-même en base32. Quand un cache DNSCurve résout un nom et se rend compte que le serveur de noms prend en charge DNSCurve, il créée un secret partagé dérivé de la clef publique du serveur, de sa propre clef privée et d'un *nonce* à usage unique. Le cache envoie sa clef publique, le nonce et la requête chiffrée avec le secret partagé. Le serveur répond avec le résultat de la requête chiffré avec le secret partagé. Les consultations de la zone racine et du TLD « .com » n'utilisent pas DNSCurve sur ce schéma puisqu'il est actuellement impossible de le faire.

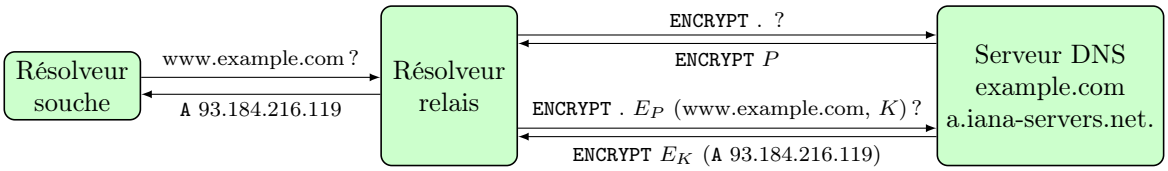
DNSCrypt

DNSCrypt est un protocole documenté mais non standardisé largement dérivé de DNSCurve. Il protège les requêtes du résolveur souche de l'usager final contre la surveillance réseau et les modifications. Étant basé sur DNSCurve, il ne résout aucun des autres problèmes majeurs de sécurité et respect de la vie privée présents dans DNS. Le plus gros résolveur connu prenant en charge DNSCrypt est OpenDNS. La communauté DNSCrypt fait fonctionner d'autres résolveurs DNSCrypt ouverts. Aujourd'hui, DNSCrypt est le protocole de chiffrement DNS conçu pour empêcher la surveillance réseau le plus largement déployé. Il ne résout toutefois que la moitié des problèmes liés au respect de la vie privée ; son utilisation demeure marginale et il n'est pas standardisé.

8 Confidential DNS

Un autre document de travail récent de l'IETF suggère une méthode différente pour ajouter du chiffrement au DNS, cette fois ci en utilisant le principal mécanisme d'extension de DNS : l'ajout de nouveaux types d'enregistrements pour chiffrer le trafic DNS [19]. Confidential DNS ajoute les enregistrements de types « ENCRYPT » pour fournir la clef publique nécessaire au résolveur récursif pour pouvoir chiffrer la connexion avec le serveur DNS. Ces enregistrements « ENCRYPT » contiennent la clef publique du serveur DNS à utiliser pour chiffrer les communications initiées par le résolveur. Cela permet d'éviter la bidouille à laquelle recourt DNSCurve consistant à ajouter la clef publique dans la réponse « NS » de la zone déléguée.

La version actuelle de ce document de travail décrit deux modes d'opération : le mode *opportuniste* qui est le plus simple à mettre en œuvre puisqu'il ne requiert aucun changement majeur à l'infrastructure DNS, et un mode *authentifié* où les clefs publiques d'un domaine sont également stockées dans la zone parente, ce qui demande une prise en charge de la part de l'infrastructure de cette zone parente.



?	Indique une requête et sinon une réponse
.	Requête pour la zone racine
P	Clef publique du serveur
K	Clef de chiffrement
E_P (x)	Chiffrement de x avec P
E_K (x)	Chiffrement de x avec K
`A`	Enregistrement DNS d'adresse IPv4
`ENCRYPT`	Enregistrement DNS « ENCRYPT »

FIGURE 10 – Résolution du nom `www.example.com` avec le mode opportuniste de Confidential DNS. Le résolveur récupère la clef publique des serveurs DNS en demandant l'enregistrement « ENCRYPT ». Cette clef publique est ensuite utilisée pour chiffrer la requête envoyée au serveur. Le résolveur envoie donc la requête chiffrée avec la clef publique du serveur, et cette requête contient également la clef avec laquelle la réponse doit être chiffrée.

Avec le mode opportuniste, la clef publique n'est plus associée à la zone parente ; au lieu de ça, elle est distribuée séparément, en clair et potentiellement sans authentification, comme un enregistrement de la zone cible. Par conséquent, en utilisant l'enregistrement « ENCRYPT », Confidential DNS ne permet de faire que du *chiffrement opportuniste*—du novlangue pour décrire du chiffrement pouvant être contourné de manière triviale par une attaque de type « une personne au milieu » (*man in the middle*) puisque le chiffrement utilise des clefs non authentifiées.

L'utilisation d'un nouveau type d'enregistrement est également l'occasion de produire la complexité nécessaire à une solution développée par un comité : Confidential DNS peut utiliser à la fois de la cryptographie symétrique ou asymétrique, et prend en charge AES et RSA 512 bits en mode CBC (qui a récemment été utilisé pour mettre un terme à SSL3 [9]). Ce document de travail ne définit pas de minimum requis ni de mécanisme pour s'assurer que ce minimum sera mis à jour pour prendre en compte de nouvelles considérations de sécurité.

Le document de travail sur Confidential DNS fournit une deuxième méthode pour assurer du « vrai » chiffrement authentifié en stockant la clef publique d'un domaine dans sa zone parente. Pour ce faire, Confidential DNS étend les enregistrements « DS » (*Delegation Signer*) de DNSSEC par une bidouille pour fournir la clef de chiffrement de la zone, dans le même esprit que la bidouille des enregistrements « NS » utilisée dans DNSCurve. Le document décrit un éventail de modes d'échec, incluant « se passer de sécurité » permettant aux clients de rechuter aux modes peu sûrs même après que des connexions

sûres aient été disponibles. Combiné avec la possibilité de « se passer de sécurité » également en cas d'algorithmes cryptographiques qui ne sont pas pris en charge, on peut dire que Confidential DNS fournit une sorte de sécurité imprévisible plutôt que des garanties strictes. Ne fournir aucune garantie et offrir plein d'options facilite le déploiement et la migration ; c'est un des maîtres mots pour le processus d'ingénierie de l'IETF dirigé par l'industrie.

9 Namecoin

Les systèmes de noms pair-à-pair fournissent des solutions plus radicales pour la résolution de noms. L'approche de Bitcoin [10] a été proposée pour créer des systèmes basés sur une chronologie et permettant d'utiliser des noms globaux, sûrs et mémorisables [14]. L'idée est de créer une chronologie globale et unique de tous les noms qui ont été enregistrés et à laquelle on ne peut que ajouter. Les systèmes reposant sur une chronologie utilisent un réseau pair-à-pair pour gérer les mises à jour et le stockage de cette chronologie. Dans Namecoin [15], les modifications à des associations clef/valeur sont liées à des transactions que l'on applique à la chronologie en faisant de « l'exploitation minière » (*mining*). Cette « exploitation » consiste en l'utilisation de méthodes « force brute » pour trouver des collisions partielles de condensés (*partial hash collisions*) avec une empreinte (*fingerprint*) de la chronologie—qui inclue tout l'historique.

Étant donné deux chronologies avec des associations clef/valeur différentes, le réseau reconnaîtra comme valide celle des deux ayant la plus longue chaîne puisqu'elle représente la plus grosse dépense en temps de calcul. Le coût en calcul rend pratiquement impossible la génération d'une chronologie alternative par un adversaire. Cela présuppose des capacités de calcul limitées, ce qui ne s'applique pas forcément à certains adversaires.

Pour résoudre un nom avec Namecoin, le client doit vérifier la chronologie pour voir si elle contient ledit nom et s'assurer que la chronologie est valide. Pour ce faire, l'usager doit disposer d'un exemplaire complet de la chronologie (figure 11). Elle faisait 2 Go en novembre 2014 [2]. Sinon, les usagers peuvent utiliser un serveur de noms de confiance participant au réseau Namecoin.

Namecoin améliore le respect à la vie privée des usagers quand toute la chronologie, ou chaîne de blocs (*block chain*), est dupliquée sur le système de l'utilisateur final. Quand c'est le cas, la résolution de nom est complètement privée. En revanche, dupliquer toute la chaîne sur les systèmes de chaque utilisateur pourrait s'avérer peu pratique pour certaines machines si Namecoin devenait un concurrent sérieux aux DNS. Par ailleurs, Namecoin ne protège pas l'information de zone contre la surveillance, et en particulier l'énumération des noms d'une zone est triviale. Toutefois, le fait que Namecoin soit décentralisé assure au moins que « l'indication des dommages de combat » contre un serveur n'a plus aucun sens.

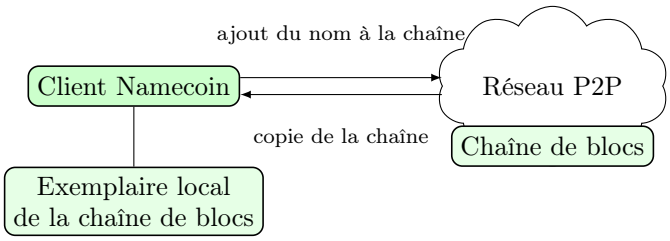


FIGURE 11 – Le système de noms Namecoin est décentralisé et utilise un réseau pair-à-pair. Pour parvenir à un consensus sur les noms qui sont enregistrés, Namecoin utilise une *chaîne de blocs* (*block chain*) stockée dans le réseau pair-à-pair. Pour enregistrer un nom, les clients doivent réaliser un travail de calcul qui leur permet d'ajouter le nom à la chaîne. Pour résoudre un nom, les clients doivent disposer d'un exemplaire complet de la chaîne et y chercher le nom à résoudre.

10 Le système de noms GNU

Les auteurs de cet article travaillent sur le système de noms GNU, ou *GNU name system* (GNS) [17]. Il s'agit d'une proposition radicale pour traiter les problèmes de respect de la vie privée et de sécurité

2. `https://bitinfocharts.com/de/namecoin/`

du DNS et qui, comme Namecoin, se démarque clairement du processus de résolution de noms DNS. Le processus de résolution de noms GNS ne repose pas sur des résolveurs interrogeant des autorités comme c'est le cas avec DNS. Au lieu de ça, GNS repose sur un réseau pair-à-pair et une table de hachage répartie (DHT, pour *distributed hash table*) utilisée par les résolveurs pour consulter les associations clef/valeur.

GNS assure la confidentialité des requêtes et réponses ; celles-ci sont chiffrées de telle sorte que même un adversaire participant activement peut, au mieux, faire une attaque par confirmation, et sinon n'apprend que la date d'expiration d'une réponse. Notons que ce sont les requêtes et réponses elles-mêmes qui sont chiffrées et non pas la connexion entre un résolveur et une autorité quelconque. Puisque les réponses ne sont pas seulement chiffrées mais aussi signées cryptographiquement, il est impossible pour un nœud de la DHT de modifier une réponse sans que cela soit immédiatement détecté.

Grâce à l'utilisation d'une DHT, GNS évite les complications du DNS telles que les enregistrements « glu » et les consultations d'enregistrements « hors zone » (*out-of-bailiwick*). Avec GNS, les étiquettes figurant dans un nom correspondent précisément à la séquence de résolution du nom, ce qui rend la chaîne de confiance immédiatement visible pour l'usager. Enfin, l'utilisation d'une DHT pour distribuer les enregistrements permet aux autorités GNS d'exploiter des zones sans qu'aucune infrastructure critique visible ou imputable à l'autorité ne puisse être utilisée pour indiquer des dommages de combat.

GNS peut associer des noms à n'importe quel type d'objet sécurisé de manière cryptographique. Par conséquent GNS peut être utilisé pour la résolution de noms mais aussi pour la gestion d'identités ou encore comme alternative à aux actuelles infrastructures à clef publique bien abîmées.

10.1 Noms, zones et délégation

Une zone GNS est une paire de clefs publique/privée associée à un ensemble d'enregistrements. Le processus de résolution de noms GNS résout donc une chaîne de clefs publiques. En l'absence de zone racine opérationnelle et largement reconnue, mais aussi parce qu'il est intrinsèquement une alternative aux noms hiérarchiques, GNS utilise le pseudo TLD « .gnu » pour faire référence à la zone de l'usager, que l'on appelle *zone maîtresse*. Chaque usager peut créer autant de zones que souhaité, mais l'une d'entre elles doit être désignée comme la zone maîtresse. Les usagers gèrent librement les correspondances clef/valeur pour les étiquettes au sein de leurs zones. De plus, ils ou elles peuvent déléguer le contrôle d'un sous-domaine à n'importe quelle autre zone (y compris les zones gérées par d'autres usagers) au moyen d'un enregistrement « PKEY » qui spécifie simplement la clef publique de la zone cible. Les enregistrements « PKEY » sont utilisés pour établir le chemin de délégation déjà mentionné. Grâce à l'utilisation d'une DHT, il n'est pas nécessaire de spécifier l'adresse d'un système qui serait responsable de l'exploitation de la zone cible. La validité des enregistrements dans la DHT est établie par leurs signatures et contrôlée par leur date d'expiration.

10.2 Cryptographie pour la confidentialité

Pour permettre aux autres usagers de consulter les enregistrements d'une zone, tous les enregistrements pour une étiquette donnée sont stockés dans un bloc signé cryptographiquement, dans la DHT. Pour maximiser la confidentialité lorsqu'un usager consulte des enregistrements dans la DHT, requêtes et réponses sont chiffrées, et les réponses sont signées avec une clef dérivée de la clef publique de la zone et de l'étiquette (figure 12). N'importe quel pair peut vérifier la signature mais est incapable de déchiffrer la réponse sans connaissance préalable de la clef publique et de l'étiquette de la zone. Par conséquent, les usagers peuvent utiliser des mots de passe en guise d'étiquettes, ou utiliser de clefs publiques qui ne sont pas connues publiquement, pour, concrètement, restreindre l'accès aux informations d'une zone aux seules personnes autorisées.

Grâce à l'utilisation d'une DHT, toutes les requêtes GNS sont envoyées à la même infrastructure globale, partagée et décentralisée plutôt que d'aller vers les serveurs d'un exploitant donné. Il devient donc impossible de cibler un serveur responsable spécifiquement d'une zone puisque toutes les machines participant à la DHT sont conjointement responsables de toutes les zones—en fait, les associations clef/valeur ne révèlent même pas à quelle zone elles appartiennent. Le chiffrement et l'authentification des enregistrements sont critiques puisqu'ils permettent de protéger les usagers contre la censure et la surveillance. Toutefois, à l'inverse des propositions moins radicales pour réformer DNS, déployer GNS sera un gros défi : GNS requiert beaucoup de changements logiciels significatifs ainsi qu'une implication de la communauté pour exploiter la DHT comme une nouvelle infrastructure publique.

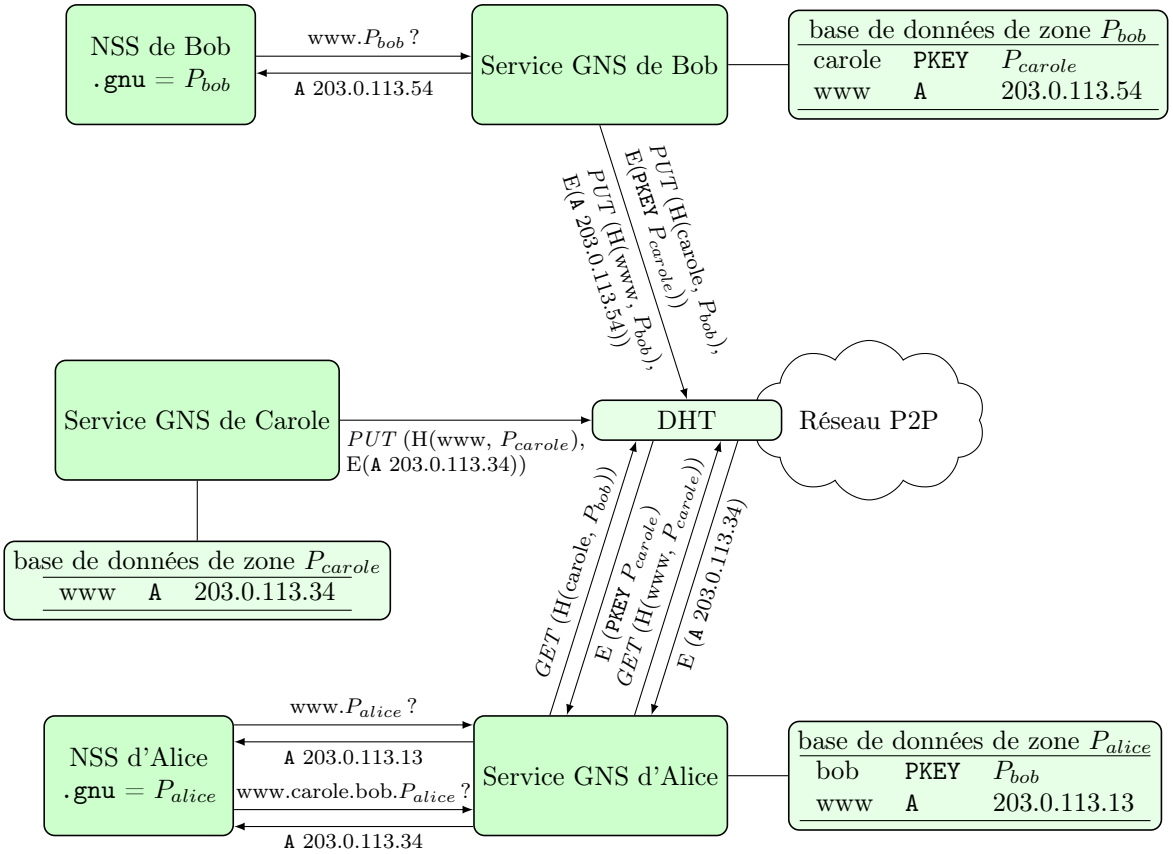


FIGURE 12 – Le système de noms GNU ou « GNS » : chaque usager maintient ses propres bases de données contenant des enregistrements organisés en zones. Ici, Alice, Bob et Carole ont chacun un serveur Web désigné par `www.gnu`. Pour Alice, `www.gnu` correspond à une adresse différente que pour Bob ou Carole car leur services de noms respectifs (*name service switches* ou NSS) associent leur propre clef publique à `.gnu`. Pour permettre aux autres usagers de résoudre le nom, la zone publique d'un usager est chiffrée et publiée dans une DHT sous une clef de requête obscurcie. Un usager peut *déléguer*, depuis son espace de noms, la résolution de noms externes à l'espace de noms d'un autre utilisateur. Par exemple, Alice peut accéder à l'espace de noms de Bob en déléguant le contrôle du nom `bob` à P_{bob} au sein de son propre espace de noms, en utilisant un enregistrement GNS de type « PKEY ». De cette façon, Alice peut accéder au serveur Web de Carole en utilisant le nom `www.carole.bob.gnu`.

11 Évolution politique

Le système de noms de domaine (DNS) et le registre d'adresses IP de l'IANA sont les deux bases de données clefs qui font tenir Internet. Étant donnée l'exploitation sans vergogne d'Internet comme une machine de surveillance par son actuel intendant, le gouvernement des États-Unis, on peut s'attendre à ce que la tendance des « internets nationaux » s'accélère.

Certains pays, particulièrement ceux qui, comme la Chine ou l'Iran, utilisent la manière forte pour censurer Internet, ont fermé leur internet national pour restreindre la circulation d'information pour un moment. Dans le même temps, et surtout depuis les révélations de Snowden, les débats autour de la construction d'infrastructure et de routage nationaux on fleuri, même dans des pays traditionnellement vus comme de solides alliés des États-Unis : le Brésil a parlé d'obliger les grosses entreprises d'Internet à être présentes au Brésil et à confiner les données brésiliennes sur le sol brésilien. En Allemagne, on a entendu des demandes pour un routage national ou Schengen. La cession de la fonction de l'IANA, demandée dès 2003 lors de la première conférence des Nations Unies sur la société de l'information (*World Summit of the Information Society*) a enfin été annoncée par le NTIA en avril 2014.

Comme toujours, les agences d'espionnage ont un tour d'avance quand il s'agit de se tenir à l'écart :

on sait que la NSA et le GCHQ exploitent en interne un système DNS privé avec leurs propres TLD non officiels, `.nsa` et `.gchq`. Toutefois, contrairement aux développeurs de Tor, les agences d'espionnage n'ont pas encore suivi la RFC 6761 pour essayer de réserver ces noms.

L'utilisation stratégique de TLD privés pour rendre les services Internet moins accessibles est logique, mais c'est un pas en avant vers une « Balkanisation » d'Internet. À l'échelle mondiale, cette tendance est mal vue par les États-Unis puisque cette décentralisation pourrait réduire la portée de la surveillance étasunienne. Pour se prémunir contre de tels développements, la procédure impliquant plusieurs intervenants (*multi-stakeholder*) est utilisée pour obscurcir la problématique de qui fait tourner le système et détourner de la question des responsabilités, tout en maintenant un contrôle indirect *via* ces intervenants.

Ces dernières années, l'ICANN a essayé, avec la prolifération des GTLD, d'accroître la concurrence entre les offres de noms de domaine. Malgré tout, le contrôle des procédés et des bénéfices du DNS reste aux mains d'une organisation étasunienne. Une question clef est donc de savoir si l'ICANN/IANA ou l'organisation qui leur succéderait—quel qu'en soit le modèle de gouvernance—continuerait à tenir la barre. Une autre possibilité est que l'on voit se développer des technologies permettant l'allocation de noms et adresses de manière complètement décentralisée, rendant caduques l'intendance mondiale et les batailles politiques pour le contrôle qui vont avec. Il semble qu'Internet soit tiré dans les deux directions en même temps.

12 Conclusion

Dans *Culture Is Our Business*, Marshall McLuhan écrit avec lucidité :

> « La troisième guerre mondiale est une guérilla de l'information à laquelle participent militaires et civils sans distinction. »

Cette prévision de 1970 reste pertinente quand on regarde l'architecture d'Internet à présent tissée dans notre vie quotidienne.

Le DNS n'a pas été conçu avec le respect de la vie privée ou la sécurité en tête. Dans la bataille des États pour la domination mondiale, n'importe quelle infrastructure d'Internet correspondant à un public particulier devient une cible pour des attaquants au service d'un État. L'infrastructure critique doit à présent être décentralisée et doit idéalement être partagée entre tous pour réduire l'intérêt de s'y attaquer. En se contentant de chiffrer le trafic DNS et Web, on risque de ne pas suffisamment réduire l'efficacité d'attaques visant des systèmes peu sûrs.

Alors que la communauté DNS prend conscience des problèmes liés au respect de la vie privée, les intérêts divers de ses membres rendent la progression vers un consensus pratiquement impossible. Les modifications d'un système déployé tel que le DNS, suivant la tendance générale d'Internet à s'ossifier, rencontrent l'inertie et bien souvent la mort par comité, tant n'importe quel changement significatif est susceptible non seulement d'entraîner des dysfonctionnements mais aussi de porter atteinte à un modèle commercial ou aux intérêts d'un État.

Dans un monde où la NSA est à la chasse aux administrateurs système [3] et où l'ICANN devient une victime de premier choix [4], les pansements proposés par l'IETF ne sont pas à la hauteur de l'ensemble des attaques sur le DNS : attaques sur l'authenticité, mais aussi censure, surveillance des usagers, et surveillance active des serveurs et de leur disponibilité.

Remerciements

Nous remercions Laura Poitras, Ludovic Courtès, Dan Bernstein, Luca Saiu et Hellekin O. Wolf pour leur aide et support dans la préparation de ce reportage.

Références

[1] R. Arends, R. Austein, M. Larson, D. Massey et S. Rose : DNS security introduction and requirements. *IETF RFC 4033*, mars 2005.

3. `http://cryptome.org/2014/03/nsa-hunt-sysadmins.pdf`
4. `http://www.heise.de/security/meldung/Erfolgreicher-Angriff-auf-Internet-Verwaltung-ICANN-2499609.html`

[2] Daniel J. Bernstein : Curve25519 : new Diffie-Hellman speed records. *In In Public Key Cryptography (PKC), Springer-Verlag LNCS 3958*, 2006.

[3] Daniel J. Bernstein : DNSCurve : Usable security for DNS. `http://dnscurve.org/`, 2008.

[4] Internet Architecture Board : IAB statement on Internet confidentiality. `https://mailarchive.ietf.org/arch/msg/ietf-announce/ObCNmWcsFPNTIdMX5fmbuJoKFR8`, 2014.

[5] S. Bortzmeyer : Possible solutions to DNS privacy issues. `http://tools.ietf.org/html/draft-bortzmeyer-dnsop-privacy-sol-00`, décembre 2013.

[6] S. Bortzmeyer : DNS privacy considerations. `https://datatracker.ietf.org/doc/draft-ietf-dprive-problem-statement/`, 2014.

[7] Amir Herzberg et Haya Shulman : Fragmentation considered poisonous : or one-domain-to-rule-them-all.org. *In CNS 2013. The Conference on Communications and Network Security*. IEEE, 2013.

[8] Allison Mankin, Duane Wessels, John Heidemann, Liang Zhu et Zi Hu : t-DNS : DNS over TCP/TLS. `http://www.isi.edu/ant/tdns/`, 2014.

[9] Bodo Möller, Thai Duong et Krzysztof Kotowicz : This POODLE bites : exploiting the SSL 3.0 fallback. `https://www.openssl.org/~bodo/ssl-poodle.pdf`, 2014.

[10] Satoshi Nakamoto : Bitcoin : A peer-to-peer electronic cash system. `http://bitcoin.org/bitcoin.pdf`, 2008.

[11] Anonymous (NSA) : There is more than one way to quantum. `https://www.documentcloud.org/documents/1076891-there-is-more-than-one-way-to-quantum.html#document/p1`, 2014.

[12] NSA/CSS Thread Operations Center (NTOC) : Bad guys are everywhere, good guys are somewhere ! `http://www.spiegel.de/media/media-34757.pdf`, 2014.

[13] Redacted (NSA, S32X) : QUANTUMTHEORY. `https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/`, 2014.

[14] Aaron Swartz : Squaring the triangle : Secure, decentralized, human-readable names. `http://www.aaronsw.com/weblog/squarezooko`, 2011.

[15] `http://dot-bit.org/` : The Dot-BIT project, a decentralized, open DNS system based on the Bitcoin technology. `http://dot-bit.org/`, 2013.

[16] Inc. Verisign : Verisign, Inc.'s statement about IPR related to draft-bortzmeyer-dns-qname-minimisation-02. `https://datatracker.ietf.org/ipr/2469/`, octobre 2014.

[17] Matthias Wachs, Martin Schanzenbach et Christian Grothoff : A censorship-resistant, privacy-enhancing and fully decentralized name system. *In 13th International Conference on Cryptology and Network Security (CANS 2014)*, pages 127–142, 2014.

[18] Nicholas Weaver : A close look at the NSA's most powerful Internet attack tool. *Wired*, 2014.

[19] W. Wijngaards : Confidential DNS. `http://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-02`, 2014.