El programa MORECOWBELL de la NSA: Doblan las campanas para el DNS

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

Traducción: Hellekin O. Wolf

1 Introducción

En la red casi todo empieza con una petición al Sistema de Nombres de Dominios (en inglés: Domain Name System, o DNS), un protocolo central de Internet que permite a los usuarios acceder a los servicios mediante su nombre, como `www.example.com`, en vez de usar direcciones numéricas como 2001:DB8:4145::4242. Desarrollado en los "buenos tiempos de Internet" el DNS contemporáneo parece una gran mapa para miopes de la actividad de la red. Por lo que ahora no solamente atrae todo tipo de vigilancia motivada por razones mercantiles sino, como lo confirman nuevos documentos sobre el programa de la NSA MORECOWBELL, también atrae a la Agencia Nacional de Seguridad de los EE.UU. (National Security Agency, NSA). Considerando las fallas del diseño de DNS, se plantea la cuestión de saber si el DNS puede ser asegurado y salvado o si debe ser remplazado, por lo menos en algunos casos.

En los dos últimos años hubo mucha actividad para tratar de mejorar la seguridad y la privacidad del DNS en el grupo encargado de la ingeniería de Internet, el Internet Engineering Task Force (IETF), responsable de la documentación de los estandartes del DNS. El Internet Architecture Board (IAB), órgano semejante al IETF, justamente llamó a los ingenieros a usar cifrado en todos lados, incluso posiblemente en el DNS. [4]

Un borrador reciente [6] del IETF sobre la privacidad del DNS empieza por reconocer que el DNS

> "... es uno de los componentes más importantes de la infraestructura de Internet y uno de los más ignorados o mal conocidos. Casi cada actividad en Internet empieza con una petición al DNS (incluso más de una). Su uso tiene muchas implicaciones para la privacidad ..."

A pesar de un consenso aparentemente rápido sobre esta evaluación, el IETF no espera que las soluciones industriales existentes van a cambiar a corto plazo:

> "Parece que hoy en día la posibilidad de un cifrado masivo del tráfico DNS queda muy lejano." [5]

Desde una perspectiva de vigilancia, el DNS trata toda la información en su base de datos como datos públicos. El contenido de las peticiones y de las respuestas no es generalmente cifrado. Eso permite a atacantes pasivos vigilar las peticiones de los usuarios y ver cuáles servicios están usando y cuáles sitios están visitando. Para un atacante activo, el DNS facilita la localización de servicios potencialmente vulnerables, lo qué constituye un primer paso hacia su explotación consiguiente con ataques disponibles en el mercado de los llamados *0-day*[1].

Las discusiones en el IETF ahora incluyen propuestas para "la minimización de peticiones", el DNS confidencial, DNS sobre TLS, DNSCurve y otras propuestas radicales para diseños alternativos de sistemas de nombres con el fin de mejorar la privacidad. Todos estos diseños toman distintos turnos para reducir el rol del DNS como última fuente de meta-datos en el panóptico digital conocido como Internet.

2 MORECOWBELL: Escuchando en el DNS

Aprovechando qué el DNS de hoy es un libro abierto, no es sorprendente que en una nueva serie de documentos de alto secreto vistos por Le Monde y Heise, se revela que el programa MORECOWBELL (MCB) de la agencia de espionaje estadounidense vigila el DNS cómo una fuente de información sobre Internet (figura 2). El

[1] de día cero, es decir: vulnerabilidades exclusivas

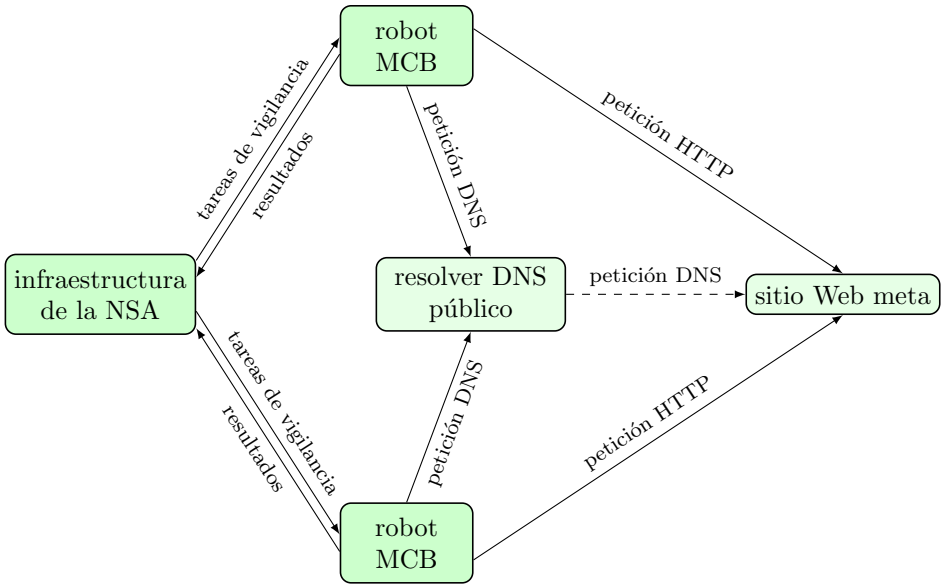


Figure 1: La infraestructura del programa MORECOWBELL de la NSA: una lista de metas para vigilar está desplegada geográficamente con robots interrogando al DNS y HTTP encuentra de sitios elegidos para colectar información sobre la disponibilidad de sus servicios. Los datos resultando de esta operación vuelven a la NSA a intervalos regulares.

programa MORECOWBELL de la NSA usa una infraestructura de monitoreo encubierto dedicada para mandar activamente solicitudes a los servidores DNS y satisfacer peticiones HTTP para obtener meta-información sobre servicios y conocer su disponibilidad.

A pesar de la naturaleza abierta del DNS, la NSA lo hace encubierto (figura 3) para asegurar que las miles de peticiones por hora no sean atribuidas al gobierno estadounidense (USG). Por eso la NSA alquila servidores dedicados a la vigilancia del DNS en Malasia, Alemania y Dinamarca (figura 4), de manera que hagan su investigación encubierta y que obtengan una visión más global de la resolución del DNS y de la disponibilidad de los servicios. Aunque las diapositivas sólo mencionan tres países, la infraestructura no-atribuible PACKAGEGOODS sobre la cual se basa MORECOWBELL es conocida para usar máquinas en otros 13 países por lo menos, como descrito previamente por Der Spiegel en una serie de diapositivas sobre el programa TREASUREMAP de la NSA. [13]

Lo interesante es que en este momento a la NSA lo le importaba mucho los contenidos específicos de los servicios Web o de las entradas de registros del DNS - habitualmente la NSA busca meta-datos: aquí la NSA quiere saber si la información en el DNS ha cambiado, y averiguar la disponibilidad del servicio. Las diapositivas muestran que esta simple revisión tiene usos benignos como por ejemplo vigilar algunos de los sitios del propio gobierno.

Una justificación para hacer las pruebas activas del DNS de manera in-atribuible al gobierno estadounidense es muy probablemente su uso para la "Indicación de Daños en Batalla (Battle Damage Indication, BDI)" (figura 5). Específicamente, después de que "Ataques de Red de Computadoras (Computer Network Attacks, CNA)" fuesen conductas contra una infraestructura crítica de la red, los EE.UU. podrían usar esas pruebas para confirmar que los ataques encontraron su blanco cuando se apagan los sistemas en Internet, digamos, de algún gobierno. Vigilando los cambios en el DNS, el ataque podría ser repetido si la víctima trata de esquivarlo cambiando la dirección de sus servicios a otro sistema de la red. Con tal infraestructura encubierta y distribuida, la NSA mantiene una vista global sobre el impacto de un ataque. También hace más difícil para las victimas identificar a los servidores de vigilancia, lo que permitiría a las víctimas evadir los ataques tratando las respuestas a estos servidores identificados de manera diferente, una táctica comuna con el DNS y conocida como *vista dividida* (*split view*).

Aunque no tenemos la prueba de esto, la "Indicación de Daños en Batalla" podría incluir daños de otras fuentes que ciberataques como los ataques aéreos o los cortos de cables. El gobierno estadounidense usa el término "Indicación de Daños en Batalla" para ataques cinéticas:

> "INDICACIÓN DE DAÑOS EN BATALLA
>
> El objetivo de este trabajo es desarrollar métodos innovadores de bajo costo para determinar rápidamente el efecto que la munición entregada por aire hubo sobre su blanco planeado. Eso es especialmente importante considerando blancos enterrados profundamente adonde los índices visuales pos-ataque podrían ser difíciles de percibir. Un enlace de datos embarcado en la munición misma podría ser adecuada para obtener indicación del daño contra este tipo de blanco. Tal enlace de datos podría depender de un cable en cola o ser completamente inalámbrico. De otro manera el **indicador de daño en batalla** podría ser totalmente independiente de la munición penetrante. El objetivo de este estudio es desarrollar medios de bajo costo, eficientes y fiable para proveer al avión de combate (*warfighter*) una determinación precisa o por lo menos una estimación fiable del daño infligido al blanco - en particular una blindada y/o profundamente enterrada.
>
> —Dr. Alex Cash AFRL/MNMI (850) 882-0391 cash@eglin.af.mil"[2]

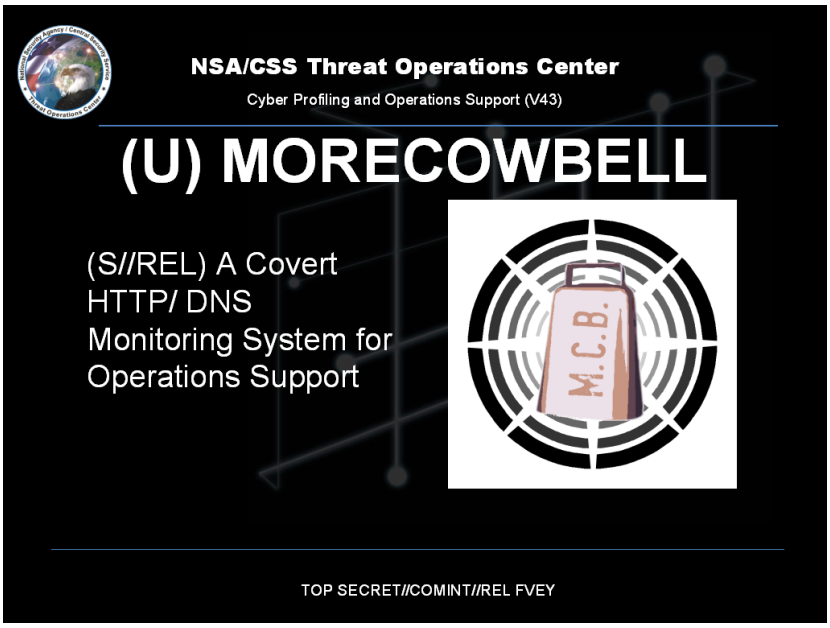


Figure 2: Obtenido de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html`: MORECOWBELL: un sistema de vigilancia encubierta de HTTP/DNS

Varios documentos de la NSA relativos al DNS muestran ataques encubiertos contra el DNS más allá de la vigilancia masiva y su rol en soporte de ataques activas. [19] Con la revelación de la familia de proyectos QUANTUMTHEORY de la NSA con subproyecto como QUANTUMDNS, sabemos que atacantes poderosos como estados-naciones no solamente escuchan al tráfico DNS sino que además inyectan respuestas DNS para modificar el resultado de la resolución de nombres o hacerlo fallar completamente. [14] Con un DNS que no provee confidencialidad para proteger la privacidad del usuario, es fácil crear perfiles de usuarios y sus comportamientos de navegación en la Web. Tal información puede ser usada entonces para lanzar ataques de

[2] nuestra énfasis. Citado según `http://www.darkgovernment.com/airforcedev.html`.

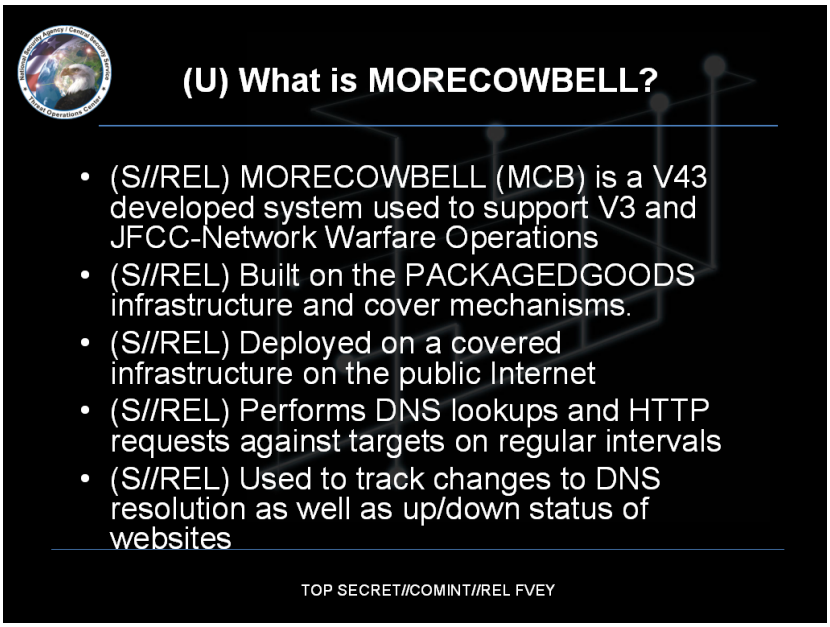


Figure 3: Obtenido de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html`: Lo que es MORECOWBELL.

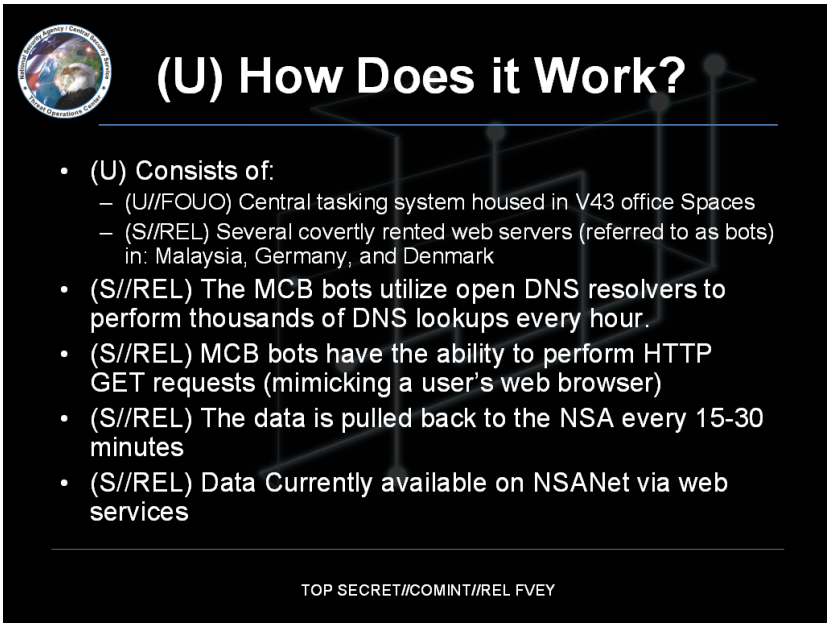


Figure 4: Obtenido de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html`: ¿Cómo funciona MORECOWBELL?

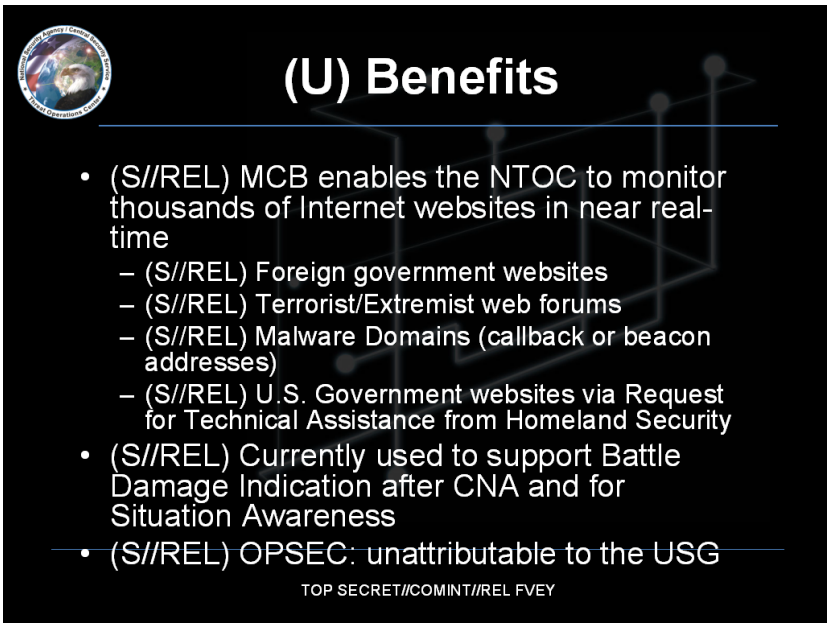


Figure 5: Obtenido de `http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html`: "Beneficios" de MORECOWBELL.

QUANTUMTHEORY contra la meta. Los programas de la NSA como QUANTUMBOT tienen el objetivo de vigilar redes de robots en IRC, detectar computadoras operando como robots para estas redes y tomar control del canal de comando para instrumentalizar estos robots. Estos programas están evaluados por la NSA como *muy exitosos* en sus propios documentos. [12]

Entonces, la comunidad de Internet necesita trabajar en la resolución de los problemas de seguridad y privacidad con la resolución de nombres y el corriente Sistema de Nombres de Dominios (DNS). En el resto de este artículo vamos a revisar la arquitectura existente del DNS y el rango de propuestas actuales que fueron hechas para mejorar la seguridad de este servicio crítico del Internet.

3 Trasfondo: el DNS

El Sistema de Nombres de Dominios (DNS) es una parte esencial de Internet cómo proporciona la correspondencia entre los nombres de sistemas y las direcciones IP, ofreciendo nombres memorables por los usuarios. El DNS es jerárquico y guarda mapeos de nombres-valores en llamados *registros* en una base de datos distribuida. Un registro consiste en un nombre, un tipo, un valor y una fecha de expiración. Los nombres consisten en *etiquetas* delimitadas por puntos. La raíz de la hierarquía es la etiqueta vacía y la etiqueta la más a la derecha es conocida como dominio de nivel superior (Top Level Domain, TLD). Se dice de nombres con un sufijo común que son parte del mismo *dominio*. El *tipo de registro* (Record Type) específica que tipo de valor está asociada con el nombre y un nombre puede tener muchos registros de varios tipos. El tipo de registro más conocido es el tipo de registro "A" que hacer corresponder un nombre con una dirección IPv4.

La base de datos del DNS es partida en *zonas*. Una *zona* es una porción del espacio de nombres cuya responsabilidad administrativa corresponde a una autoridad particular. Una zona tiene autonomía sin restricción para manejar los registros en uno o más dominios. Más importante, una autoridad puede delegar esta responsabilidad para *subdominios* a otras autoridades. Esto se hace con un registro "NS" cuya valor apunta al nombre del servidor DNS de la autoridad para este subdominio. La *zona raíz* (Root Zone) es

la zona correspondiente a la etiqueta vacía y es mantenida por la autoridad de asignación de números en Internet (Internet Assigned Numbers Authority, IANA), que ahora está operada por la corporación de Internet para los nombres y números asignados (Internet Corporation for Assigned Names and Numbers, ICANN) bajo un contrato con la administración nacional de la telecomunicaciones y la información (National Telecommunications and Information Administration, NTIA). La NTIA es una agencia del ministerio estadounidense del comercio, así como tiene un papel operacional pequeño pero significativo: averigua cada adición y cada cambio en el archivo de la zona raíz. El contrato NTIA-IANA caduca al fin de setiembre 2015 y la NTIA ya anunció su intención de salir de su papel en un esfuerzo de pasar el control a una supervisión global multi-actores. La zona raíz contiene registros "NS" que especifican los nombres de los servidores que detienen la autoridad sobre todos los TLDs, como ".ar" o ".com".

Los nombres en el DNS son resueltos usando *resolvedores*. La mayoría de los sistemas operativos modernos no proveen una implementación completa de resolución de DNS sino una parcial llamada *resolvedor matriz* (*stub resolver*). Estos resolvedores matrices no resuelven los nombres directamente sino que pasan la pregunta a un *resolvedor DNS repetidor* (*forward resolver*) que típicamente es dado por el proveedor de Internet, tal mostrado en la figura6. Estos repetidores resuelven el nombre primero preguntando a los servidores raíces para el nombre requerido. Si el servidor DNS interrogado no sabe dar una respuesta definitiva, por lo menos indica un dirección en un registro "NS" que refiere el resolvedor al servidor DNS siguiente. Este proceso *iterativo* se repite y termina por supuesto cuando el resolvedor pregunta al *servidor autoritativo* que es responsable para este dominio particular. El DNS beneficia enormemente de cachear la información del DNS: muchos *cachés de resolución* (*caching resolvers*) guardan la información ya conocida para acelerar el rendimiento de la búsqueda. Usan datos de registros guardados para evitar parte o todas las iteraciones para responder mucho más rápido al cliente.

Con el uso de servidores de nombres repetidores, la dirección IP del cliente está escondida de los servidores autoritativos. Esto da al usuario algún grado de privacidad cómo impide a los operadores de servidores autoritativos de nombres vigilar la fuente de las peticiones DNS. Naturalmente los operadores de resolvedores repetidores pueden vigilar fácilmente estos datos y censurar las peticiones de sus usuarios. Sistemas de vigilancia pasivo global como TURMOIL o XKEYSCORE también pueden ver cualquier parte de la transacción dado que esta sea disponible para su filtro de ingestión.

4 DNSSEC

DNS fue originalmente no diseñado par proveer cualquier seguridad cuando está usado en una red insegura. Las extensiones de seguridad del DNS (DNS Security Extensions, DNSSEC) [1] agrega protección de la integridad y autenticación del origen de los datos de registros DNS. DNSSEC no agrega la confidencialidad ni la protección contra deniego-de-servicio y entonces no protege para nada contra la vigilancia pasiva. Añade tipos de registro para claves públicas ("DNSKEY"), delegación de firmante ("DS"), y para fimas de registros ("RRSIG"). La figura 7 ilustra las interacciones entre resolvedores usando DNSSEC. DNSSEC crea una infraestructura hierárquica de claves públicas en la cual todos los operadores de DNSSEC deben participar. Esta establece una cadena de confianza desde la zona de autoridad hacia el ancla de confianza asociado a la zona raíz. Esta asociación es lograda distribuyendo la clave pública de la zona raíz fuera-del-canal, por ejemplo con el sistema operativo. La cadena de confianza establecida por DNSSEC refleja las delegaciones de zona de DNS. Dado que los operadores de TLDs generalmente dependen de la misma jurisdicción que los operadores de dominios en dicha zona, estas cadenas de confianza corren el riesgo de ataques usando medios tantos técnicos como jurídicos.

Lo siguiente muestra las debilidades más graves del DNS incluso en presencia de la extensiones de seguridad (DNSSEC). DNSSEC falla al proporcionar cualquier nivel de privacidad de petición: los contenidos de la peticiones DNS como de las respuestas siguen leibles por cualquier adversario con acceso al canal de comunicación y puede ser correlacionado con los usuarios después, especialmente si el atacante puede observar el enlace entre el resolvedor matriz del usuario y el servidor de nombres del proveedor de acceso a Internet. Al nivel técnico, el despliego actual de DNSSEC sufre del uso del sistema de encriptación RSA (la zona raíz usa RSA-1024), el soporte de lo cual es requerido para cada resolvedor usando DNSSEC y conduce

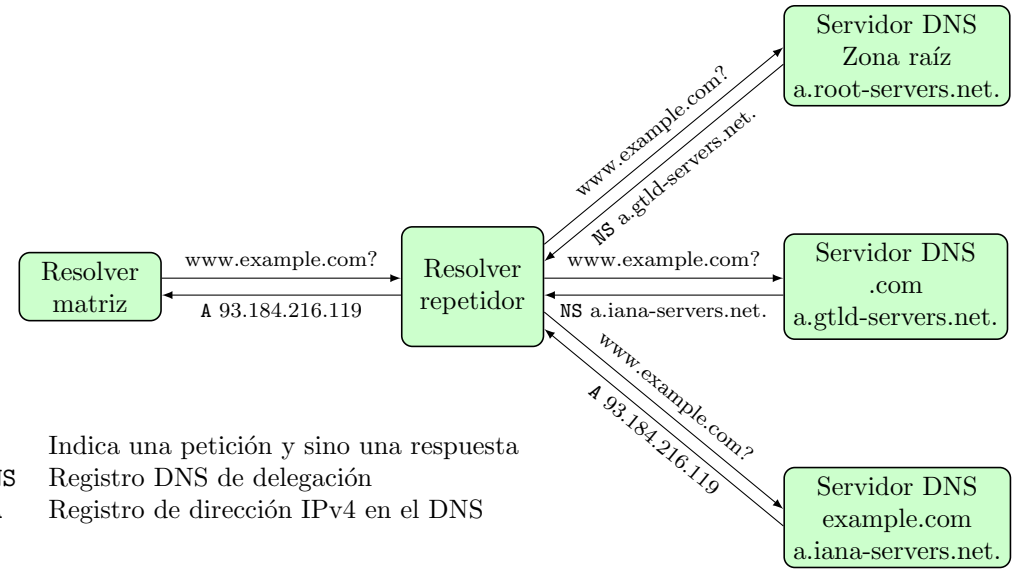


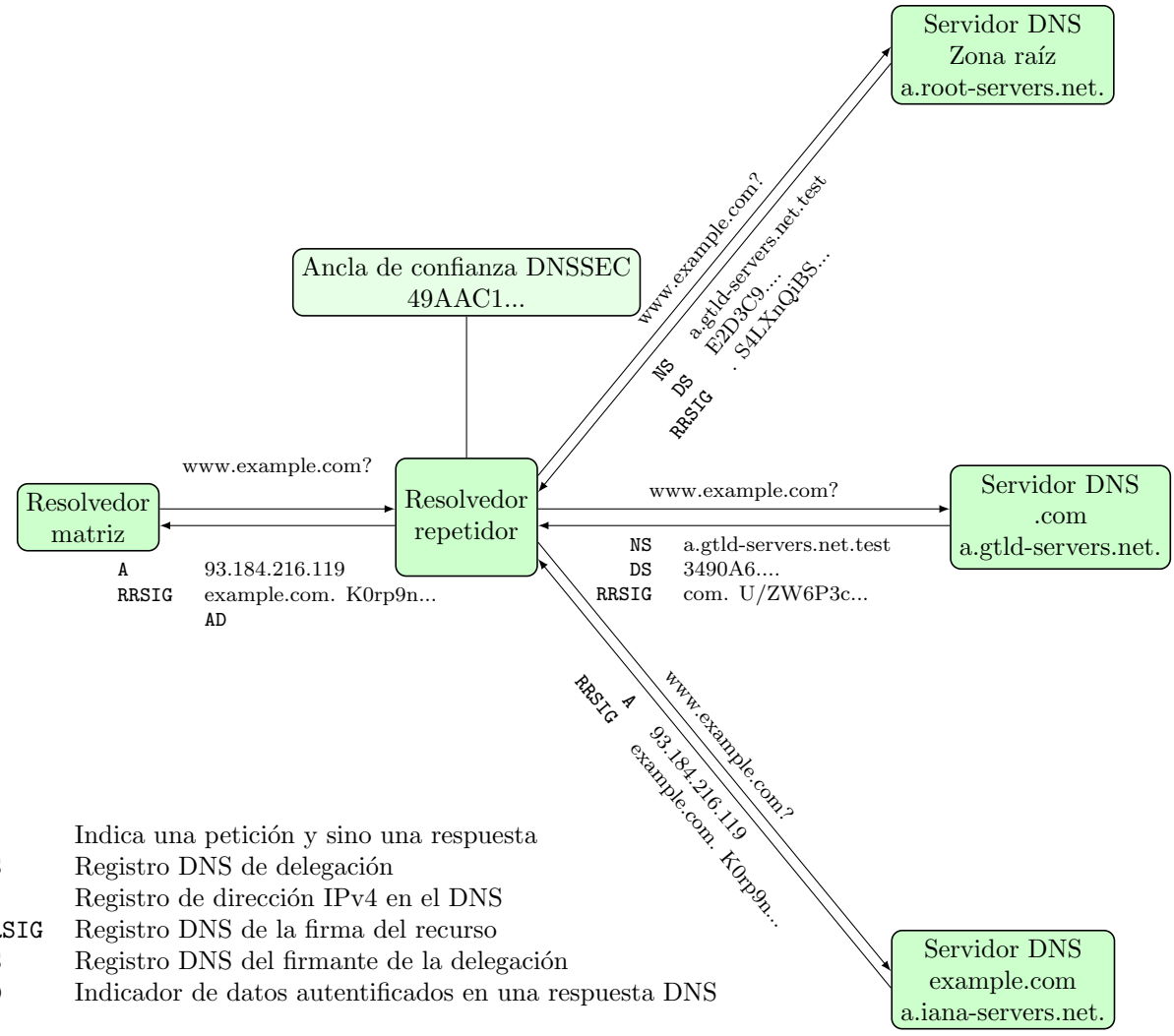
Figure 6: Resolviendo el nombre `www.example.com` con el DNS. Muchos sistemas operativos proporcionan un *resolvedor matriz* (*stub resolver*) mínimo pasando las peticiones a servidores repetidores. Para resolver un nombre estos servidores empiezan por preguntar a los servidores de la zona raíz. Si el servidor no puede proveer la información requerida, refiere el resolvedor al servidor siguiente hacia que el servidor *autoritativo* sea encontrado para la zona respectiva.

al uso de claves criptográficas largas, especialmente considerando que las respuestas incluyen firmas para todos los esquemas de firmas que soporta el servidor de autoridad. Esto puede llegar a mensajes de un tamaño que excede las restricciones de tamaño para los paquetes DNS, abriendo oportunidades para nuevas vulnerabilidades [8]. Finalmente, DNSSEC no está diseñado para defenderse de ataques legales. Dependiendo de su alcance, los gobiernos, las corporaciones y su lobbies pueden legalmente forzar operadores o autoridades del DNS en manipular los registros y certificar estos cambios. Esto es particularmente relevante ya que DNSSEC mantiene la estructura jerárquica del DNS y entonces da una confianza extensiva en la zona raíz y los operadores de TLDs.

DNSSEC también elimina las pocas limitaciones tradicionales en la adquisición masiva de datos de la zona, como las restricciones sobre transferencias de zona. Antes de DNSSEC, los administradores de zona de DNS podían prohibir la transferencia de su zona, lo que hacía difícil para un adversario enumerar sistemáticamente todos los registros de una zona. Sin embargo como DNS permite respuestas negativas (NXDOMAIN), DNSSEC necesitaba una manera de crear una declaración firmada que algunos registros no existían. Cómo DNSSEC fue diseñado para mantener la clave de firma fuera de la red, los registros "NSEC" fueron introducidos para certificar que un rango entero de nombres no estaba en uso. Mirando hacia los límites de estos rangos, un adversario puede rápidamente enumerar todos los nombres en uso en esta zona. Un intento de arreglar esto con la introducción de registros "NSEC3" fue demostrado ineficaz antes de llegar a un despliego significativo. En definitiva, DNSSEC facilita aún más el descubrimiento por parte de un adversario de vulnerabilidades en los servicios y sistemas.

5 Minimización de petición

La recientes discusiones en el IETF para mejorar la privacidad en el DNS incluyen una propuesta para dicha *minimización de petición* (*query minimization*) [7] que buenas probabilidades de adopción rápida porque no requiere ningún cambio en el protocolo DNS. La minimización de petición mejoraría ligeramente la privacidad cambiando cómo los servidores repetidores resuelven los nombres: en vez de preguntar para el



?	Indica una petición y sino una respuesta
`NS`	Registro DNS de delegación
`A`	Registro de dirección IPv4 en el DNS
`RRSIG`	Registro DNS de la firma del recurso
`DS`	Registro DNS del firmante de la delegación
`AD`	Indicador de datos autentificados en una respuesta DNS

Figure 7: Resolviendo el nombre `www.example.com` con DNS y DNSSEC: la información devuelta por servidores de nombres es firmada criptográficamente para asegurar su autenticidad y su integridad. Esta información es almacenada en registros "RRSIG" y la información sobre la zona madre en registros "DS". Un resolvedor puede averiguar una firma siguiendo la cadena de confianza y usando el *ancla de confianza* recibido fuera-de-banda. Los resolvedores matrices no pueden averiguar esta cadena y el resolvedor entonces indica al resolvedor matriz que hizo la verificación de autenticidad con el bit `AD` en la respuesta al cliente.

nombre completo a todos los servidores en cada paso de la búsqueda del servidor de autoridad, cada servidor recibiría solamente la parte necesaria del nombre para hacer un paso en la resolución del nombre (figura 8). En consecuencia, el nombre completo sería expuesto solamente al servidor de nombres DNS autoritativo final.

Tal minimización de petición puede ser implementada simplemente cambiando cómo los resolvedores construyen sus peticiones iterativas. La minimización de petición puede impactar negativamente los cachés, por lo menos en teoría la petición completa podría permitir a los servidores de nombres responder con la última respuesta, por ejemplo aprovechando la información cacheada de las peticiones recursivas, o porque ya son la autoridad para el nombre completo. Aún con minimización de petición, los resolvedores repetidores siguen aprendiendo la petición completa y la respuesta válida para un usuario.

La minimización de petición tiene la ventaja de que su despliego sólo requiere cambios en el resolvedor intermediario y el inconveniente que este posible cambio para mejorar su privacidad queda enteramente fuera de su control. La minimización de petición puede ser combinada con varios métodos para cifrar el tráfico DNS presentadas en las próximas secciones; sin minimización de petición, simplemente cifrar el tráfico DNS sigue exponiendo el contenido completo de la petición hacia muchos servidores del DNS. Finalmente, Verisign Inc. podría impedir la adopción de esta propuesta con la explotación del chantaje de las patentes de software [17].

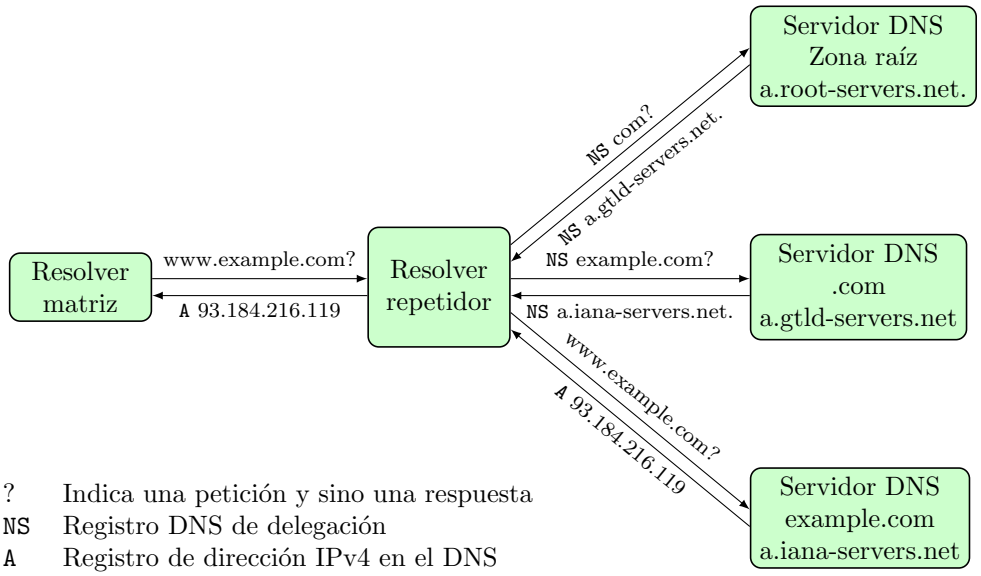


Figure 8: Con la minimización de petición, resolver el nombre `www.example.com` no expone más el nombre completo ni tampoco el tipo de registro a la zona raíz ni a la autoridad del `.com`. Naturalmente, este esquema todavía filtra algo de información sencilla al servidor DNS del TLD. Además el efecto es aún más débil en práctica ya que la zona raíz no está tan solicitada porque la información sobre los servidores de TLD está típicamente disponible en un servidor más cercano del usuario.

6 T-DNS: DNS sobre TLS

Previas discusiones sobre el uso de la capa de transporte seguro (Transport Layer Security, TLS) para cifrar el tráfico del DNS fue bastante rechazado por el hecho de la perdida de rendimiento involucrada. En el contexto de un reciente borrador del IETF sobre empezar DNS sobre TLS, los autores apuntaron en que usar TLS no sería solamente beneficioso para la privacidad sino también porque pasar a TCP - y de repente del UDP sin conexión al TCP orientado a las conexiones - podría ayudar en la mitigación de ataques de amplificación sobre (o por) los servidores de DNS. [9]

Re-utilizando una misma conexión TCP para múltiples peticiones DNS con una expiración moderada, entubando peticiones y habilitando el procesamiento no secuencial, la propuesta de T-DNS promete un rendimiento razonable a pesar de los gastos generales introducidos por TCP y TLS.

Sin embargo, aún si TLS fuese desplegado para DNS, esto seguiría filtrando meta-datos, permitiendo a terceros de fácilmente determinar a cuales datos del DNS un usuario accede: en la propuesta del IETF, TLS está combinado con el uso de resolvedores repetidores, y por lo tanto de que esconden la dirección IP del usuario de los servidores DNS, necesita ser confiado en que no espía a los usuarios. Además TLS mismo no beneficio de lo mejor historial de seguridad con docenas de problemas en los últimos años desde la compromisión de autoridades de certificación de alto perfil hasta fallos de implementación y modos inseguros de cifrado.

TLS no es la única posibilidad para cifrar las peticiones del DNS y sus respuestas cuando atraviesan la red. DNSCurve y DNS Confidencial son propuestas alternativas para proteger de la vigilancia al nivel de la red, los contenidos de las peticiones DNS y sus respuestas.

DNS-sobre-TLS ya es disponible en el servidor DNS libre Unbound.

7 DNSCurve

El primer sistema práctico que mejora la confidencialidad al respeto de las peticiones de DNS y las respuestas fue DNSCurve [3]. En DNSCurve la claves de sesión son intercambiados usando Curve25519 [2] y después usadas para proveer identificación y cifrado entre cachés y servidores. DNSCurve mejora el sistema de nombres de dominios existente con confidencialidad y integridad sin necesidades de crear firmas costosas o sesiones (D)TLS. Específicamente, DNSCurve logra lo mismo tiempo de ida y vuelta (Round Time Trip, RTT) que DNS por encapsular la clave pública del servidor en el registro "NS".

DNSCurve crea una asociación cifrada y autenticada entre un *servidor DNSCurve* y un *caché DNSCurve*, lo último siendo un resolvedor repetidor con caché corriendo al punto final en lugar de un resolvedor matriz (figura 9). Cómo DNSCurve no usa firmas, el caché de DNSCurve no puede probar la autenticidad de los registros a otros usuarios, lo que limita la utilidad de cada caché a los puntos respectivos.

Mientras en DNSCurve el usuario no tiene más que dar confianza al resolvedor intermediario, la dirección IP del punto final ahora está directamente expuesta a los servidores DNS autoritativos: no está más ofuscada por los resolvedores intermediarios operados por los proveedores de Internet. Entonces, DNSCurve puede mejorar la privacidad contra un adversario que vigila el tráfico DNS en sistemas intermediarios o con otro método de pinchar cables, pero reduce la privacidad con respeto a los servidores DNS autoritativos ya que ellos se dan cuenta y de la petición completa y de la identidad (dirección IP) del usuario. Otra preocupación expresada con respeto a DNSCurve es la necesidad de mantener las claves secretas en la red. DNSCurve tampoco puede proteger de la censura ya que algunos gobiernos siguen controlando efectivamente la jerarquía de los registros públicos (*registrars*) y entonces pueden hacer desaparecer dominios. Con respeto a los ataques de la NSA, DNSCurve solamente ayuda a los usuarios contra la vigilancia pasiva durante la transmisión gracias a la protección de la confidencialidad por lo menos del contenido de la petición DNS.

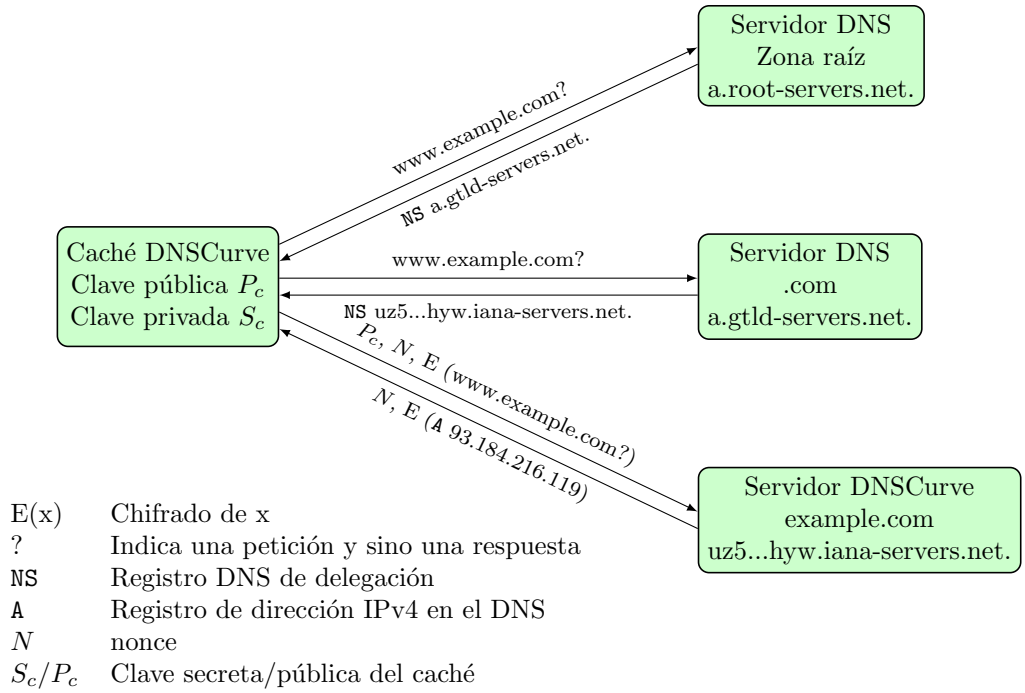
Aún con DNSCurve, los servidores del DNS siguen estando metas jugosas para la vigilancia global. Más allá, como en el caso de DNS, los servidores conocidos y bien localizados son metas y vectores de confirmación para ataques contra la infraestructura crítica. Con DNSCurve, la necesidad de usar criptografía de claves públicas en linea por parte de las autoridades del DNS puede abrir nuevas oportunidades de vulnerabilidades a ataques por denegación de servicio si un pequeño CPU es usado para servir un enlace rápido.

DNSCrypt

DNSCrypt es un protocolo no estandardizado pero bien documentado en gran parte basado en DNSCurve. Protege las peticiones del resolvedor matriz del usuario contra la vigilancia en la red y las interferencias. Cómo está basado en DNSCurve no resuelve ningún otro problema mayor de privacidad o de seguridad presentes en el DNS. El resolvedor más importante conocido para soportar DNSCrypt es OpenDNS. Existen varios resolvedores de DNSCrypt operados por la comunidad de DNSCrypt. Hoy en día DNSCrypt es el protocolo de cifrado de DNS lo más desplegado que sea diseñado para impedir la vigilancia de los usuarios finales en la red. Sin embargo sólo ayuda en resolver la mitad del problema de la privacidad y no es muy conocido ni estandardizado.

8 DNS Confidencial

Otro borrador reciente del IETF sugiere un método alternativo para agregar cifrado al DNS que usa el modo principal y los mecanismos de extensión del DNS con la introducción de tipos de registro adicionales para cifrar el tráfico DNS. [20]. Con el DNS Confidencial, un nuevo tipo de registro "ENCRYPT" está presentado



E(x)	Chifrado de x
?	Indica una petición y sino una respuesta
`NS`	Registro DNS de delegación
`A`	Registro de dirección IPv4 en el DNS
N	nonce
S_c/P_c	Clave secreta/pública del caché

Figure 9: Resolviendo el nombre `www.example.com` con DNSCurve. Con DNSCurve, el caché de resolución y el servidor DNSCurve intercambian un secreto compartido para cifrar sus comunicaciones. La clave pública del servidor DNSCurve es codificada en el nombre mismo del servidor de nombres usando Base32. Cuando un caché DNSCurve resuelve un nombre y descubre que el servidor soporta DNSCurve, el caché crea una clave compartida basada en la clave pública del servidor, la clave privada del caché, un nonce y la petición cifrada con un secreto compartido. El servidor va a responder con el resultado de la petición cifrado con el secreto compartido. Las dos primeras búsquedas hacia la zona raíz y el TLD ".com" no usan DNSCurve en la ilustración porque todavía no lo soportan.

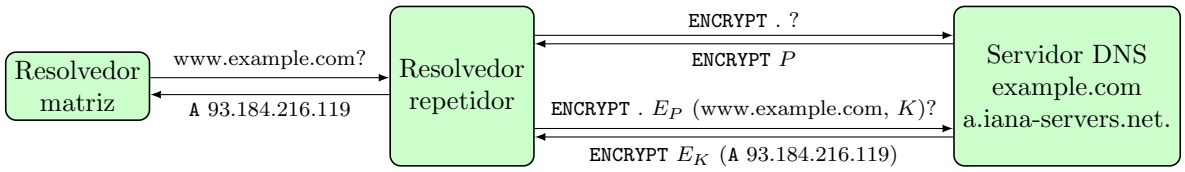
para proveer la necesaria clave pública que permite al resolvedor repetidor cifrar la comunicación con el servidor DNS. Este tipo de registro "ENCRYPT" contiene la clave pública del servidor de nombres par cifrar la comunicación iniciada por el resolvedor. Esto es para evitar el hack usado en DNSCurve adonde la clave pública se encuentra en la respuesta "NS" de la zona de delegación.

El borrador corriente soporta dos modos diferentes de operación: un modo *oportunístico* que es más fácil para implementar como no necesita cambios mayores en la infraestructura del DNS y un modo *identificado* adonde las claves públicas del dominio también están en la zona madre correspondiente, de modo que necesita el soporte de la infraestructura de DNS de la zona madre.

Con el modo oportunístico la clave pública no está más asociada con la zona madre sino servida por separado en texto claro y posiblemente sin identificación cómo un registro en la zona meta. Con resultado de que el DNS Confidencial usa el registro "ENCRYPT" solamente con soporte a dicho *cifrado oportunístico* - lo que significa en novlang un cifrado trivialmente trastornable por un ataque man-in-the-middle cómo usa claves no identificadas para cifrar.

El uso de un nuevo tipo de registro también crea la oportunidad para lograr la complejidad necesaria digna de una solución diseñada por comité: el DNS Confidencial puede usar criptografía simétrica o asimétrica y lleva soporte para RSA 512-bit y AES en modo CBC (lo cual fue usado recién para definitivamente enterrar SSL3 [10]). El borrador falla establecer un mínimo suficiente y asegurar que este mínimo será actualizado para reflejar nuevas consideraciones de seguridad cuando corresponda.

El borrador sobre DNS Confidencial proporciona un segundo método para lograr un cifrado identificado



?	Indica una petición y sino una respuesta
.	Petición para la zona raíz
P	Clave pública del servidor
K	Clave de encriptación
E_P (x)	Cifrado de x con P
E_K (x)	Cifrado de x con K
`A`	Registro de dirección IPv4 en el DNS
`ENCRYPT`	Registro DNS de tipo "ENCRYPT"

Figure 10: Resolviendo el nombre `www.example.com` con DNS Confidencial en modo oportunístico. El resolvedor recibe la clave pública del servidor de nombres mediante el nuevo registro de tipo "ENCRYPT". La clave pública puede ser usada para cifrar la petición al servidor. El resolvedor envía la petición cifrada con la clave pública del servidor que contiene la pregunta y una clave con la cual cifrar la respuesta.

"real" poniendo la clave pública de un dominio en la zona madre respectiva. Para hacer esto, DNS Confidencial extiende el registro de firmante delegado de DNSSEC ("DS") con un hack para lograr una clave de cifrado para la zona similar al hack del registro "NS" usado por DNSCurve. El borrador proporciona varios tipos de modos de error como "vuelva a lo inseguro" permitiendo a los clientes recaer en modos inseguros con "saltos de fe" aún después de la desaparición de conexiones previamente seguras. En combinación con "vuelva a lo inseguro", por el hecho de algoritmos de cifrado no soportados, DNS Confidencial proporciona una seguridad imprescindible en lugar de cualquier seguro estricto y sin hacer ninguna garantía y ofreciendo muchas opciones para facilitar el despliego y la migración, lo que forma el hilo principal del proceso de ingeniería conducto por la industria en el IETF.

9 Namecoin

Los sistemas alternativos de nombres entre pares proveen soluciones aún más radicales para la resolución segura de nombres. Sistemas basados en el tiempo en el estilo de Bitcoin [11] fueron propuestos para crear un sistema global, seguro y memorable [15]. Aquí la idea es crear una linea-de-tiempo única globalmente accesible para grabar nombres en la cual sólo se pueden adjuntar registros. Los sistemas basados en una linea-de-tiempo requieren una red de pares-a-pares para administrar actualizaciones y mantener la linea-de-tiempo. En el sistema Namecoin [16] las modificaciones de pares (clave, valor) son adjuntadas a transacciones cuales son agregadas a la linea-de-tiempo por extracción. La extracción es el uso de métodos de fuerza bruta para encontrar colisiones parciales de hash con un resumen de estado (huella digital o fingerprint) que representa el estado global completo - incluyendo todo el historial - de la linea-de-tiempo.

Dados dos lineas-de-tiempo con correspondencias posiblemente en conflicto, la red elige la linea-de-tiempo con la cadena más larga porque representa el mayor gasto de potencia computacional. Esto es para impedir que un adversario pueda producir una cadena alternativa válida a tiempo. Esto presupone un poder computacional limitado y quizás no se puede aplicar para algunos adversarios.

Para realizar la búsqueda de un nombre con Namecoin, el cliente debe recorrer la linea-de-tiempo para encontrar el nombre en cuestión y también averiguar la integridad de la linea-de-tiempo con la red para asegurar su validez. Para eso, el usuario debe poseer una copia completa de la linea-de-tiempo (figura 11),

cual tamaño es de 2 GB en Noviembre 2014.[3]

Alternativamente los usuarios pueden usar un servidor de nombres de confianza participando en la red de Namecoin.

Namecoin puede mejorar la privacidad del usuario si la cadena de bloques completa está replicada en el sistema del usuario. En este caso, la resolución de los nombres no involucra ninguna búsqueda fuera del sistema y entonces queda perfectamente privado. Sin embargo replicar la cadena completa para cada usuario puede ser impracticable para algunos aparatos si Namecoin debe crecer para volverse una competencia seria para DNS. Tampoco Namecoin protege la información de la zona de la vigilancia y particularmente la enumeración de zonas es trivial. Pero la naturaleza descentralizada de Namecoin asegura por lo menos que la indicación de daños en batalla contra un servidor de nombres no tiene más sentido.

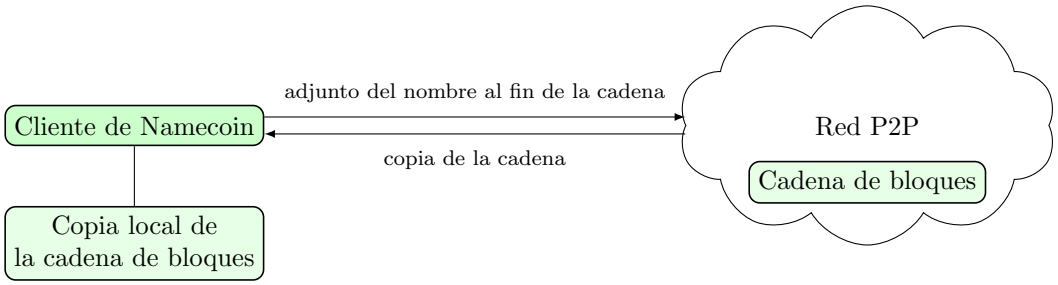


Figure 11: El sistema de nombres de Namecoin es descentralizado y usa una red de pares. Para lograr un consenso con respeto al registro de los nombres, Namcoin usa una *cadena de bloques* compartida en la red P2P. Para registrar un nombre, clientes deben hacer algún trabajo computacional que les va permitir adjuntar sur nombre a la cadena. Para resolver un nombre, los clientes deben poseer una copia completa de la cadena de bloques y buscar adentro de ella el nombre requerido.

10 El sistema de nombres de GNU

Los autores de este artículo trabajan en el Sistema de Nombres de GNU (GNU Name System, o GNS) [18] lo cual es una propuesta más radical ante los problemas de privacidad y de seguridad del DNS y tal como Namecoin se aleja bastante del proceso de resolución de nombres del DNS. El proceso de resolución de GNS no usa resolvedores preguntando a autoridades del DNS. Mejor, el proceso de GNS usa una red de pares-a-pares y una tabla de hash distribuidas (en inglés, Distributed Hash Table, DHT) para habilitar resolvedores buscar pares (clave, valor).

GNS preserva la privacidad ya que las peticiones como las respuestas son cifradas de tal manera que aún un adversario activo y participante puede a lo mejor alcanzar un ataque de confirmación y sino aprender la fecha de caducidad de la respuesta. Es importante notar que la peticiones y las respuestas mismas son cifradas y no las conexiones entre el resolvedor y alguna autoridad. Cómo todas las respuestas no solamente son cifrados sino también firmadas criptográficamente, los pares en la DHT no pueden interferir con los resultados sin detección inmediata.

Porque usa una DHT, GNS evita las complicaciones del DNS como los registros de IP de los servidores de nombre del propio dominio (*glue records*) y las peticiones hacia registros de nombres de servidor DNS de un dominio fuera del propio dominio (*out-of-bailiwick lookups*), haciendo obvio para el usuario el camino de confianza completo. Finalmente, el uso de una DHT para distribuir los registros también hace posible que las autoridades de GNS operen zonas sin infraestructura crítica visible o atribuible que podría ser usada para indicación de daño en batalla.

El GNS resuelve los nombres de manera segura hacia cualquier identificador criptográfico. Entonces puede ser usado para la s direcciones o la gestión de identidad y como alternativa a las maltrechas infraestructuras

[3] `https://bitinfocharts.com/de/namecoin/`

de claves públicas de hoy.

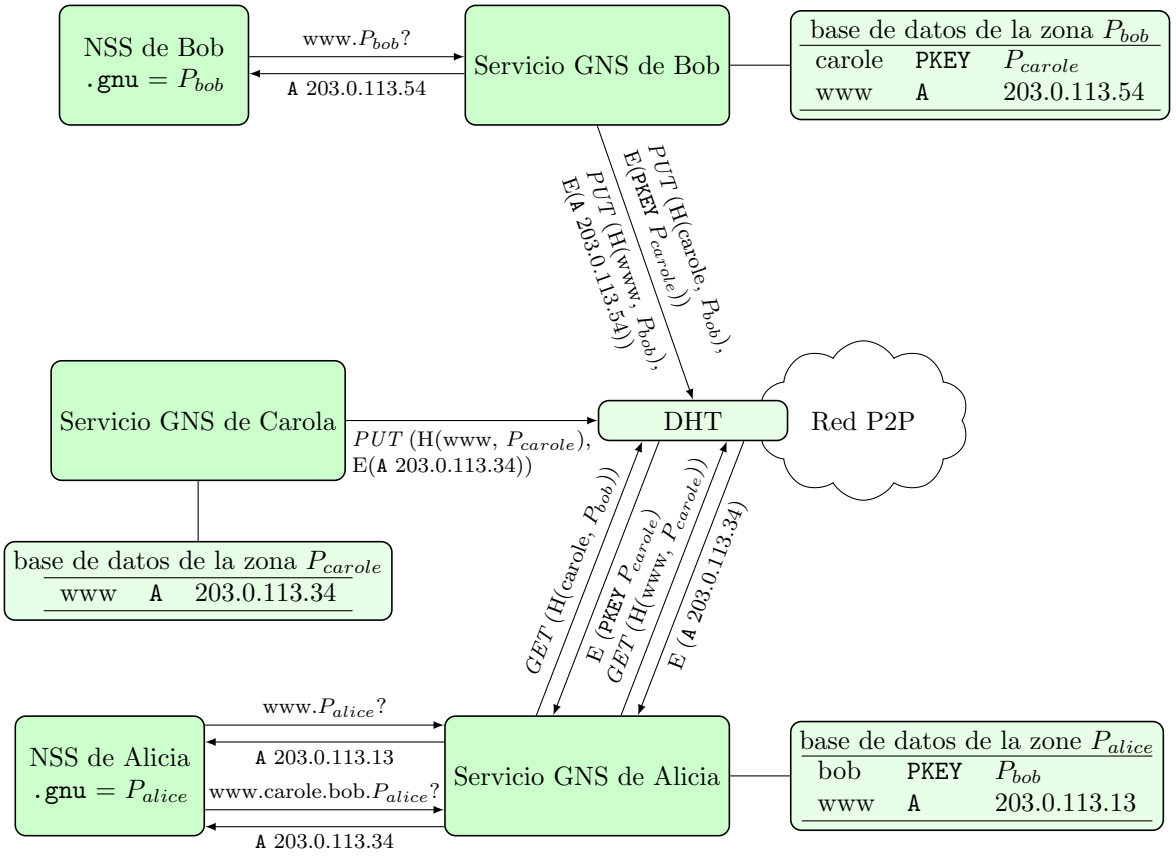


Figure 12: El Sistema de Nombres de GNU: con GNS, cada usuario mantiene sus propias bases de datos conteniendo conjuntos de registros bajo etiquetas organizadas en zonas. Una zona es referida por un par de clave-pública. Aquí Alicia, Bob y Carola tienen servidores de Web todos accesibles por `www.gnu`. Para Alicia, `www.gnu` resuelve a una dirección diferente de Bob o Carola, como su conmutador local respectivo de servicio de nombres (Name Service Swicth, NSS) asocia a un usuario específico una clave pública con `www.gnu`. Para permitir a otros usuarios resolver los nombres, la información de la zona pública del usuario es cifrada y publicada en la DHT bajo una clave de petición ofuscada. Un usuario puede *delegar* al espacio de nombres de otro usuario desde su propio espacio de nombres para resolver nombres ajenos. Por ejemplo Alicia puede acceder al espacio de Bob delegando el nombre `bob` a P_{bob} en su espacio de nombres usando el registro específico "PKEY" del GNS. Así Alicia puede acceder al servidor Web de Carola por el nombre `www.carol.bob.gnu`

10.1 Nombres, zonas y delegaciones

Una zona de GNS es un par de claves pública-privada y un conjunto de registros asociados. El proceso de resolución de un nombre en el GNS básicamente resuelve una cadena de claves públicas. En la ausencia de una *zona raíz* ampliamente reconocida y operacional así como una alternativa inherente al direccionamiento jerárquico, GNS usa el pseudo-TLD ".gnu" para referirse a la zona propia del usuario, también llamada *zona maestra*. Cada usuario puede administrar libremente las correspondencias para las etiquetas de sus propias zonas. Más importante, los usuarios pueden delegar el control de un subdominio a cualquier otra zona (incluso aquellas operadas por otros usuarios) gracias a un registro de tipo "PKEY" que simplemente

especifica la clave pública de la zona meta. Los registros "PKEY" son usados para establecer el camino de delegación mencionado antes. Debido al uso de una DHT, no es necesario especificar la dirección de algún sistema que sería responsable para operar cierta zona. La validez del registro en la DHT es establecida usando firmas y controlada con valores de caducidad.

10.2 Criptografía para la privacidad

Para habilitar a otros usuarios a que busquen los registros de una zona, todos los registros de una etiqueta dada son guardados en un bloque firmado criptográficamente en la DHT. Para maximizar la privacidad del usuario cuando usé la DHT para encontrar registros, ambos las peticiones como las respuestas son cifradas y las respuestas además son firmadas usando una clave pública derivada de la clave pública de la zona y de la etiqueta (figura 12). Cualquier par puede fácilmente validar la firma pero no descifrar la respuesta sin conocimiento previo de la clave pública y la etiqueta de la zona. En consecuencia los usuarios pueden usar contraseñas como etiquetas o claves públicas que no son conocidas públicamente para restringir el acceso no autorizado a la información de la zona.

Debido al uso de la DHT, todas las peticiones en GNS van a la misma infraestructura global descentralizada y compartida y no a servidores específicos de unos operadores. Eso hace imposible dirigirse a un servidor especial para una zona dicha porque todas las máquinas que participan en la DHT son responsables en conjunto de todas las zonas - de hecho, los pares de clave-valor nunca revelan su zona de pertenencia. Al mismo tiempo, el cifrado y la identificación de los registros es crítica por lo tanto que ayuda en proteger los usuarios contra la censura efectiva o la vigilancia. Sin embargo, a contrario de otras propuestas menos radicales para revisar DNS, desplegar GNS será un desafío significativo: GNS requiere más cambios significativos al software así como un esfuerzo de la comunidad para operar la DHT como una nueva infraestructura pública.

11 Situación política

El DNS y el registro de direcciones IP de IANA son dos bases de datos claves que enlazan el Internet global. Dado la explotación temeraria del Internet como máquina de vigilancia por su supervisor actual, el gobierno de los EE.UU., la tendencia hacia las "redes intra-nacionales" puede ganar velocidad.

Algunos paises, especialmente los que usan métodos más pesados para la censura de Internet como China y Iran, cerrarón sus Internet nacionales cómo medio para restringir el flujo de información para un tiempo. Pero desde las revelaciones de Snowden, debates a propósito de routing nacional y construcción de infraestructura lluvieron incluso en paises normalmente considerados fuertes aliados de los EE.UU.: Brasil habló de obligar a plataformas de Internet una presencia física en el país y confinar los datos brasileños adentro de Brasil. En Alemania hubó propuestas de routing nacional o limitado al espacio de Schengen. La disvestidura de la función de IANA, demandada desde la primera Cumbre Mundial sobre la Sociedad de la Información (CMSI, 2003) fue finalmente anunciada por la NTIA en abril 2014.

Como siempre las agencias de espionaje van con ventaja cuánto a aislarse de los otros: tanto la NSA como el CGHQ operan sistemas de DNS internos no públicos con sus propios TLDs no oficiales, `.nsa` y `.cghq`. Pero al contrario de los desarrolladores de Tor, estas agencias todavía no siguieron el RFC 6761 para tratar de reservar estos nombres.

El uso estratégico de TLDs no públicos para hacer que los servicios Internet menos accesible es lógico y un paso claro para la "Balkanización" de Internet. En la escala global, esta tendencia no está apreciada por el gobierno estadounidense cómo la descentralización puede limitar el alcance de su vigilancia. Para repeler este desarrollo un proceso "multi-actores" está usado para obscurecer el tema de quién está manejando el sistema y para evitar la cuestión de la responsabilidad aunque manteniendo un control indirecto mediante los "actores".

En los años recientes, ICANN trató de aumentar la competición en la oferta de nombres de dominio con la proliferación de gTLDs. Por lo tanto, sigue siendo una organización incorporada en los Estados Unidos quienes controlan los procesos y las ganancias. Entonces, una cuestión llave es saber si la pareja ICANN/IANA o cualquier organización que le sucede va seguir - bajo cualquier estructura de gobernanza -

estando al cabo. Alternativamente podríamos ver tecnologías desarrolladas y desplegadas que plenamente descentralizan la asignación de direcciones y nombres, haciendo que un administrador global y los conflictos políticos asociados para el control se vuelvan innecesarios. Parece que Internet está dirigiéndose en las dos direcciones al mismo tiempo.

12 Conclusion

En el libro "Culture is Our Business" Marshall McLuhan enunciaba proféticamente:

> "La Tercera Guerra Mundial es una guerrilla de información sin división entre la participación civil y militar."

Parece que sigue estando relevante esta predicción de 1970 cuando consideramos cómo la arquitectura de Internet está tejida con nuestras vidas diarias.

El DNS nunca fue diseñado para mejorar la privacidad o la seguridad. En la batalla de los estados-naciones para la dominación global, cualquier infraestructura de Internet que sirve a una audiencia específica es el blanco de atacantes estatales. La infraestructura crítica necesita lógicamente ser descentralizada y debería en lo ideal ser compartida globalmente para reducir el valor de dañar la. Solamente cifrar el tráfico DNS y Web puede no reducir suficientemente la efectividad de los ataques contra diseños inseguros.

Si bien hay una conciencia en la comunidad del DNS de que la privacidad es un tema, los varios intereses en la comunidad misma hacen virtualmente imposible progresar de manera significativa con consenso. Modificaciones en un sistema desplegado como el DNS, siguiendo la tendencia de Internet a la osificación, son recibidas por inercia y se terminan generalmente en "muerte por comisión" cómo cualquier cambio significativo no solamente podría resultar en fallos serios sino también impactar el modelo de negocio de alguien o el interés de alguna nación.

En un mundo en el cual la NSA caza a los administradores de sistemas[4] y el ICANN se vuelve una víctima fácil[5], los parches propuestos por el IETF fallan comprender la amplitud del problema: la vigilancia de los usuarios, la censura comercial y el peligro de un nuevo reino del terror adonde los operadores de DNS son metas legítimas deben ser abordados de mejor manera en futuros diseños.

Agradecimientos

Gracias a Laura Poitras, Ludovic Courtès, Dan Bernstein, Luca Saiu y Hellekin O. Wolf para su ayuda y soporte en la preparación de este artículo.

References

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

[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`, December 2013.

[4] `http://cryptome.org/2014/03/nsa-hunt-sysadmins.pdf`

[5] `http://www.heise.de/security/meldung/Erfolgreicher-Angriff-auf-Internet-Verwaltung-ICANN-2499609.html`

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

[7] S. Bortzmeyer. DNS query name minimisation to improve privacy. https://tools.ietf.org/html/draft-bortzmeyer-dns-qname-minimisation-02, May 2014.

[8] Amir Herzberg and 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.

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

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

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

[12] 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.

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

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

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

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

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

[18] Matthias Wachs, Martin Schanzenbach, and 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.

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

[20] W. Wijngaards. Confidential DNS. http://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-00, 2013.