DNSSEC: Protección del DNS

Oficina del Director de Tecnologías de la ICANN

David Conrad
OCTO-006v3
24 de julio de 2020

ICANN

ÍNDICE

El presente documento forma parte de la serie de documentos de la OCTO. Consulte la página de publicaciones de la OCTO
para obtener una lista de documentos en las series. Si tiene preguntas o sugerencias sobre cualquiera de estos documentos, envíelas a octo@icann.org.

Esta revisión contiene actualizaciones de muchas personas que leyeron la versión OCTO-006v2. La ICANN valora en gran medida los comentarios que nos han enviado.

Introducción

Las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) ayudan a proteger la forma en que la información se mueve por Internet.

El Sistema de Nombres de Dominio (*DNS*) es utilizado por todos los que se conectan a Internet y por casi todos los dispositivos de Internet todos los días. Mediante un proceso automatizado conocido como *búsqueda* o *resolución*, una de las principales funciones del DNS es asignar nombres fáciles de recordar (como ejemplo.com) a los números únicos conocidos como *direcciones de Protocolo de Internet* (IP) (como 192.0.2.189 o 2001:DB8:107A:61F7). Los dispositivos luego utilizan estas direcciones IP para identificarse y comunicarse entre sí. De esta manera, el DNS se compara a menudo con una guía telefónica o una lista de contactos, que traduce los nombres en números.

¿Qué son las DNSSEC?

Cuando se creó el DNS a principios de la década de 1980, la seguridad no era parte del enfoque del diseño. Debido a una decisión de diseño que tenía sentido en ese momento, en casos excepcionales, era posible que los atacantes proporcionaran sus propias respuestas a las búsquedas de nombres de dominio en lugar de lo que pretendía el propietario del dominio (el registratario). Por ejemplo, en lugar de ir al sitio web que usted solicitaba en su navegador, un atacante podría comprometer los mensajes del DNS para redirigirlo a otro sitio web que se parece al sitio web que deseaba ir, pero que, en cambio, estaba controlado por el atacante. En la década de 1990, la comunidad técnica del DNS llegó a la solución definitiva para este problema, conocida como las Extensiones de Seguridad del DNS o *DNSSEC*.

¿Cómo funcionan las DNSSEC?

Un registratario es la persona u organización que controla la información asociada a un nombre de dominio, es decir, el relacionamiento entre nombres y direcciones y otros datos. Las DNSSEC permiten a los registratarios firmar digitalmente la información que ponen en el DNS; esto permite a los clientes (por ejemplo, su navegador web) verificar que las respuestas del DNS que reciben como contestación a las solicitudes de búsqueda no han sido modificadas dado que fueron firmadas.

En 2010, la ICANN permitió que el nivel más alto del DNS, conocido como la raíz, fuera firmado por las DNSSEC, facilitando así en gran medida la implementación mundial de las DNSSEC. Sin embargo, incluso una década más tarde, la implementación de las DNSSEC sigue retrasada.

¿Cuáles son los beneficios de desplegar DNSSEC?

- **Las DNSSEC protegen Internet**: Dado que el DNS es esencial para el funcionamiento de Internet, la protección de los datos proporcionados por el DNS es fundamental. Por

analogía, el DNS puede verse como señales de tránsito en Internet, que permiten que la comunicación se dirija al contenido o servicio correcto. Al igual que con las señales de tránsito en las carreteras reales, si los atacantes cambian hacia donde apuntan esas señales, podría resultar en un tránsito mal dirigido, tal vez redirigiéndolo hacia una parte mala de la ciudad.

- **Las DNSSEC protegen a los usuarios finales**: Las DNSSEC pueden garantizar que los datos de los nombres de dominio que reciben los usuarios finales son los mismos datos que el registratario pretendía que recibiera el usuario final. Las DNSSEC ayudan a garantizar que cuando un usuario final o un dispositivo intente obtener el contenido o servicio al que apunta un nombre de dominio, el sitio con el que se está comunicando es el sitio que el registratario tenía previsto.

- **Las DNSSEC protegen a las empresas, organizaciones y gobiernos**: Las DNSSEC reducen la probabilidad de que los usuarios finales que deseen hacer uso de sus servicios o ver su contenido sean mal dirigidos a un sitio en el que posiblemente puedan ser defraudados por un atacante. Los proveedores de servicios de Internet (ISP) pueden agregar valor al servicio que prestan a sus clientes mediante la habilitación de la validación de DNSSEC en sus resolutores. Las organizaciones que firman sus nombres de dominio con DNSSEC reducen el riesgo de que las personas que los buscan en Internet sufran un redireccionamiento no autorizado.

- **Las DNSSEC fomentan la innovación**: Las DNSSEC ofrece una forma de verificar y proteger los datos del DNS y permite así que esos datos sean confiables. Esto a su vez permite aprovechar el DNS a escala global para crear una base de datos segura de nombre/valor (por ejemplo, usted envía un nombre y el DNS devuelve valores asociados con ese nombre) que se distribuye globalmente y es accesible públicamente por cualquier persona en Internet. Como resultado, esta base de datos segura puede generar oportunidades para la innovación y permitir nuevas tecnologías, servicios e instalaciones. Por ejemplo, una de esas tecnologías, la Autenticación Basada en el DNS de Entidades Nominadas (DANE), crea una nueva forma de asegurar las conexiones a través de Internet. La DANE aprovecha los datos protegidos por las DNSSEC en el DNS y aborda algunas de las vulnerabilidades de la forma actual en que se realizan las conexiones seguras en Internet. Esto hace que el comercio y las comunicaciones por Internet sean más seguros.

¿Cómo pongo en práctica las DNSSEC?

En términos generales, el DNS tiene dos lados: la publicación, que la realizan los registratarios o sus agentes, y la búsqueda (también conocida como resolución), que la suelen realizar los operadores de red como los proveedores de servicios de Internet. Para beneficiarse de las DNSSEC, ambos lados deben usarlas.

- **Registratarios:** Las personas responsables de publicar la información del DNS deben asegurarse de que sus datos del DNS estén firmados por las DNSSEC. Históricamente, este proceso tendía a ser complicado y propenso a errores. Sin embargo, hoy en día, la mayoría de los paquetes de software y sistemas de registración del DNS modernos tienen herramientas que automatizan la firma mediante DNSSEC de los datos que los registratarios desean publicar. En consecuencia, los registratarios o sus agentes solo

tienen que habilitar la firma de las DNSSEC en sus servidores del DNS (o en sus registradores) y proporcionar información a su registrador, conocida como *registro de firmante de delegación*, para ayudar a establecer la confianza en la información que acaban de firmar.

- **Operadores de redes:** En la parte de búsqueda, es aún más fácil: los operadores de red solo necesitan habilitar la validación de DNSSEC en los resolutores que manejan las búsquedas del DNS para los usuarios. El software de resolutores habilita cada vez más la validación de DNSSEC de forma predeterminada.

- **Usuarios finales de Internet:** Por lo general, los usuarios finales no necesitan hacer nada más que alentar a sus operadores de red a habilitar la firma y validación de DNSSEC de los nombres de dominio que utilizan.

¿Cuáles son los costos asociados a las DNSSEC?

Los servidores del DNS, tanto en el lado de la publicación como en el de la búsqueda, deben admitir las DNSSEC, por lo que puede ser necesario que las organizaciones actualicen sus paquetes de software del DNS (una mejor práctica, independientemente de si se implementan las DNSSEC).

- Por el lado de la publicación, también puede ser necesario que los registratarios o sus agentes modifiquen sus procesos para admitir los registros de los "firmantes de delegación" que se enviarán a su registrador. El costo de dichas modificaciones puede ser considerable, sin embargo esto sería un cambio y un costo que se debe realizar una única vez.

- Por el lado de la búsqueda, asumiendo que el software del servidor del DNS es razonablemente moderno, los costos deberían ser insignificantes dado que todo lo que podría exigirse sería un cambio de configuración que se debe realizar una única vez para habilitar la validación de DNSSEC.

¿Qué sucede si no despliego DNSSEC?

- **Los usuarios podrían ser vulnerables a los ataques:** Si una organización decide no implementar o habilitar las DNSSEC, sus usuarios son susceptibles de sufrir un tipo de ataque en particular conocido como "envenenamiento de la memoria caché". Cuando un usuario final realiza una búsqueda, los atacantes podrían insertar de forma transparente las respuestas a las consultas del DNS, redirigiendo potencialmente los intentos de comunicación a los dispositivos controlados por los atacantes. Los atacantes podrían entonces imitar sitios web u otros servicios, robar nombres de usuario y contraseñas, etc. Las respuestas incorrectas también se mantendrían en el servidor que realiza la búsqueda durante algún período de tiempo, para provocar así que la redirección continúe hasta que las respuestas caduquen o se eliminen. Si bien estos tipos de ataques son poco frecuentes, dado que las DNSSEC existen para hacer frente a estos ataques y están disponibles desde hace ya un tiempo, las organizaciones que son

víctimas de esta explotación pueden tener que mantener difíciles debates con sus usuarios sobre por qué no desplegaron las DNSSEC. A medida que se evitan otras formas de ataque, es probable que los atacantes se aprovechen de los sitios que no han desplegado las DNSSEC dado que la implementación de ataques a través del DNS se hace más común.

- **La innovación podría verse frenada:** La falta de implementación de las DNSSEC obstaculiza la innovación y retrasa el despliegue de nuevas tecnologías que utilizan el DNS como una base de datos de confianza a nivel mundial. Algunas de esas tecnologías prometen ofrecer mejores formas de confiar en las conexiones de los servicios de Internet, como el correo electrónico o la web.

Aunque las vulnerabilidades que abordan las DNSSEC han existido desde que se creó el DNS, todavía no ha habido muchos ataques de alto perfil que se aprovechen de esas vulnerabilidades. Debido a esto, algunos pueden creer que los costos de la implementación de las DNSSEC superan los beneficios que éstas proporcionan. No obstante, cabe señalar que los costos y riesgos de la implementación de las DNSSEC han disminuido considerablemente. De hecho, los beneficios de las DNSSEC aumentan a medida que más redes las implementan.

Otra forma de ver la cuestión de la implementación de las DNSSEC: "Si vale la pena el esfuerzo de poner datos en el DNS, ¿no vale la pena el esfuerzo de asegurarse de que esos datos no sean falsificados?"

Un poco de historia sobre las DNSSEC

En 1983, Paul Mockapetris, del Instituto de Ciencias de la Información de la Universidad de California del Sur, publicó una serie de documentos que introdujeron el concepto del sistema de nombres de dominio. En su formato original, en la década de 1980, el DNS no tenía incorporado ningún tipo de seguridad, confidencialidad o autenticación; no existía ningún mecanismo que garantizara que una respuesta recibida fuera legítima y correspondiera realmente a la consulta realizada.

Hacia 1990, Steve Bellovin de AT&T Bell Laboratories redactó un artículo que describía cómo los atacantes podían aprovechar una decisión de diseño particular en el DNS para entrar en los sistemas a la fuerza. En su trabajo, Bellovin recomendó utilizar la autenticación criptográfica para proteger mejor el DNS. Tras la publicación del documento de Bellovin, se inició un proceso formal para convertir su propuesta en una norma de protocolo del Grupo de Trabajo en Ingeniería de Internet (IETF) denominada "Extensiones de Seguridad del DNS" (*DNSSEC*).

El software del DNS que implementó las DNSSEC se desarrolló inicialmente a fines de la década de 1990, y algunas implementaciones tempranas de las DNSSEC comenzaron hacia el año 2000, incluso por el ccTLD famoso .SE (el código de país de Suecia). Sin embargo, esas implementaciones tempranas revelaron numerosos desafíos técnicos para operar las DNSSEC a escala de producción, lo que llevó al IETF a seguir trabajando en la mejora del protocolo durante los ocho años siguientes.

No ocurrió nada importante en términos de implementación hasta 2008, cuando un investigador de seguridad llamado Dan Kaminsky descubrió una grave deficiencia de diseño en el propio protocolo del DNS que permitía a los atacantes lanzar ataques de envenenamiento de la

memoria caché contra el lado de búsqueda del DNS. Este hallazgo impulsó los renovados intentos de la comunidad técnica del DNS para conseguir una mayor implementación de las DNSSEC y, en particular, para conseguir que se firmara la raíz del DNS.

En julio de 2010, la zona raíz fue firmada por primera vez por la ICANN, lo que proporcionó un anclaje de confianza global para toda la validación de DNSSEC. En octubre de 2018, la clave para la firma de la llave de la zona raíz se actualizó con éxito por primera vez, lo que representa un hito importante para las DNSSEC.

Una serie de campañas internacionales de secuestro del DNS en 2018 y 2019 dieron lugar a la primera Directiva de Emergencia de la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (US-CERT), e impulsaron a la ICANN a renovar su convocatoria a todas las partes interesadas del DNS para que implementaran plenamente las DNSSEC.

Rol de la ICANN en las DNSSEC

La ICANN, como parte de su misión de promover un ecosistema del DNS más estable, seguro y resiliente, ha sido durante mucho tiempo uno de los principales defensores de la implementación de las DNSSEC. Los acuerdos operativos formales de la ICANN con los Registros y Registradores requieren que se admitan las DNSSEC. La organización de la ICANN participa de forma periódica con partes interesadas del DNS en todo el mundo para ayudarles a comprender la importancia de las DNSSEC y para capacitar a los ingenieros en la forma de implementar y operar las DNSSEC en sus redes. Además de la concientización y el desarrollo de capacidades, los tecnólogos de la ICANN trabajan con la comunidad del IETF en las mejoras de las DNSSEC.

Desde el punto de vista operativo, la ICANN sigue desempeñando un rol fundamental. La ICANN es responsable de generar, almacenar y actualizar periódicamente la clave para la firma de la llave de la zona raíz, una clave criptográfica en la que confían todos los resolutores de validación en Internet, que se utiliza en el proceso de firma de la raíz del DNS global.

Más información

Existen muchos recursos y grupos técnicos que participan en las DNSSEC y su implementación. Una pequeña muestra:

- Las DNSSEC y todos los demás esfuerzos relacionados con el protocolo del DNS se debaten dentro del IETF, en particular en el Grupo de Trabajo de Operaciones del DNS (DNSOP).

- Los talleres sobre las DNSSEC se realizan tres veces al año en las Reuniones Públicas de la ICANN. Estos talleres, que organiza la Sociedad de Internet, proporcionan conocimientos operativos, asesoramiento y análisis sobre la implementación de las DNSSEC. Un sitio asociado, patrocinado por la Sociedad de Internet, ofrece un archivo de dichas reuniones.

- Para obtener más información, la ICANN proporciona una descripción general de las DNSSEC y por qué son importantes.