Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de Divulgación
Introducción a DNSSEC

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-3127-121128*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*28/11/2012*
N° de Páginas	*1 de 12*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal de la Junta de Andalucía y al público en general una idea general sobre el funcionamiento de la extensión de seguridad para el protocolo DNS: DNSSEC.

Se aborda en un principio la estructura general de la resolución de dominio y se exponen las amenazas más usuales que afectan a este protocolo mediante la exposición de los ataques más comunes. Finalmente se explica el funcionamiento general de DNSSEC y como su implementación puede ayudarnos a mitigar estas amenazas.

3 ALCANCE

El documento va destinado al personal de la Junta de Andalucía y público en general.

4 LA ESTRUCTURA DE RESOLUCIÓN DE NOMBRES DE DOMINIO

El sistema de nombres de dominio o Domain Name System (DNS) es un sistema jerárquico de nomenclatura de dominios usado para asignar nombres a equipos y servicios de red a cualquier recurso conectado a Internet o a una red privada. La función mas importante de este servicio es traducir (o resolver) nombres compresibles para las personas en identificadores asociados con los equipos conectados a la red con el propósito de poder localizarlos y direccionarlos correctamente.

4.1 Terminología básica

Para comprender el funcionamiento de la resolución de dominios, es necesario introducir algunos conceptos básicos:

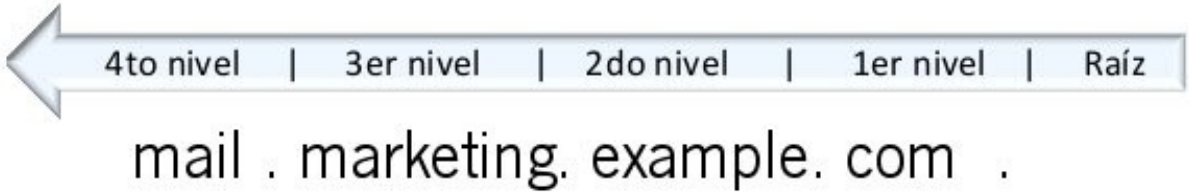
- **Host Name**: El nombre de un host es una sola "palabra" (formada por letras, números y guiones). Ejemplos de nombres de host son "*www*", "*ftp*" y "*blog*".
- **Fully Qualified Host Name (FQHN)**: Es el "nombre completo" de un host. Está formado por el hostname, seguido de un punto y su correspondiente nombre de dominio. Por ejemplo, "*www.juntadeandalucia.es*".
- **Domain Name**: El nombre de dominio es una sucesión de nombres concatenados por puntos. Algunos ejemplos son *"test.ejemplo.es"*, *"juntadeandalucia.es"* y "*es*".
- **Top Level Domains (TLD)**: Los dominios de nivel superior son aquellos que no pertenecen a otro dominio. Ejemplos de este tipo son "*com*", "*org*", "*uk*" y "*es*".

4.2 Partes de un nombre de dominio

Un nombre de dominio usualmente consiste en dos o más etiquetas separadas por puntos (por ejemplo: example.com), con respecto a las distintas partes de los nombres de dominios, se hacen las siguientes consideraciones:

- A la etiqueta ubicada más a la derecha se le llama **dominio de nivel superior** (en inglés top level domain o **TLD**). Como ".com" en "www.example.com".

- En la representación de nombres de dominio, el símbolo para el **dominio raiz** (".") es omitido de forma habitual, estando siempre presente de forma implícita.
- Cada etiqueta a la izquierda especifica una subdivisión o subdominio, llamados "**niveles**". Esta subdivisión puede ser de hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres.
- La parte más a la izquierda del dominio suele expresar el **nombre de la máquina** (en inglés hostname). El nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida. Por ejemplo, el dominio *mail.marketing.exaple.com* tendría el nombre de la máquina "*mail*", aunque pudiera no referirse a una máquina física en particular.
- La concatenación de todas las etiquetas desde el nivel actual hasta el TLD se denomina "**Fully qualified domain name**" (FQDN) o habitualmente "Nombre de Dominio" a secas.



4.3 Funcionamiento DNS

La infraestructura DNS está compuesta por multitud de entidades de computación y comunicación que se encuentran geográficamente dispersas en distintos puntos del mundo para el almacenamiento de la información asociada a nombres de domino, se dice, por tanto que DNS utiliza una base de datos distribuida y jerárquica.

La resolución de nombres se usa para distintos propósitos, pero lo más comunes son los siguientes:

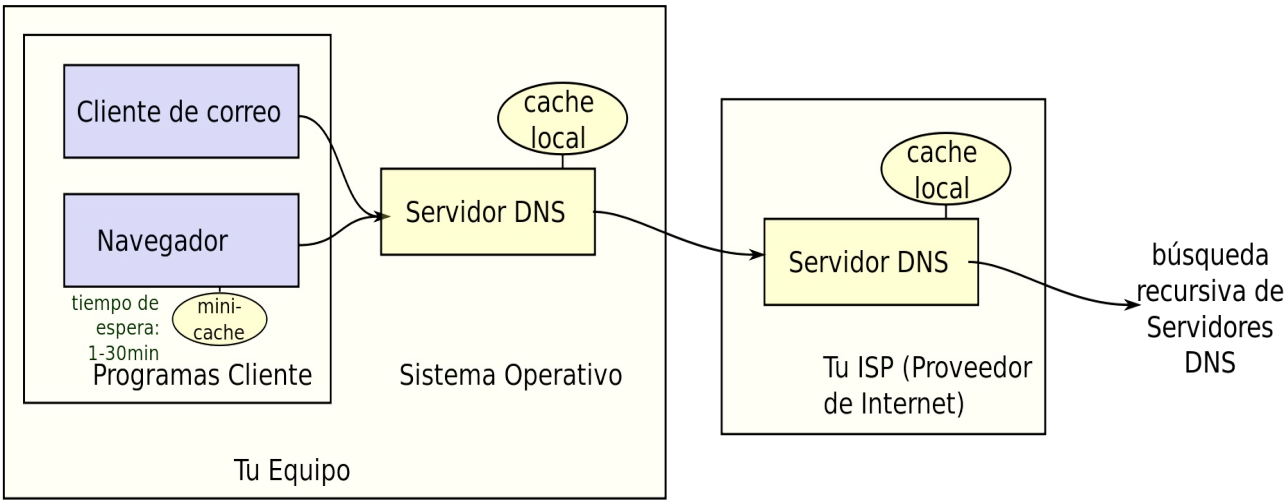
- **Resolución de nombres:** Dado el nombre completo de un host (www.google.com) obtener su dirección IP (173.194.41.209).
- **Resolución inversa de direcciones:** Es el mecanismo inverso al anterior, dada una dirección IP, obtener el nombre asociado a la misma.
- **Resolución de servicios del dominio**: Como por ejemplo el correo en el que dado un nombre de dominio (gmail.com) se obtiene el servidor a través del cual debe realizarse la entrega del correo (gmail-smtp-in.l.google.com).

Para el correcto funcionamiento del sistema de resolución se necesitan principalmente tres componentes:

- **Cliente DNS:** Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS.
- **Servidor DNS:** Resuelve la petición del cliente DNS y le envía la respuesta.
- **Zonas de autoridad**: Zona donde se le reconoce el derecho de organización o autoridad a un servidor de dominio determinado. Cada zona de autoridad abarca y define al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

Cada zona tiene que tener al menos un servidor de nombres que sea autoritativo para ella, es decir, que sea capaz de proporcionar una respuesta autoritativa a una cierta petición de resolución. Sólo un servidor autoritativo sobre un dominio es capaz de dar una respuesta autoritativa, denominándose respuestas no autoritativas a cualquier resolución que no provenga de este servidor de dominio, a este servidor de dominio se le llamará **servidor primario** de la zona.

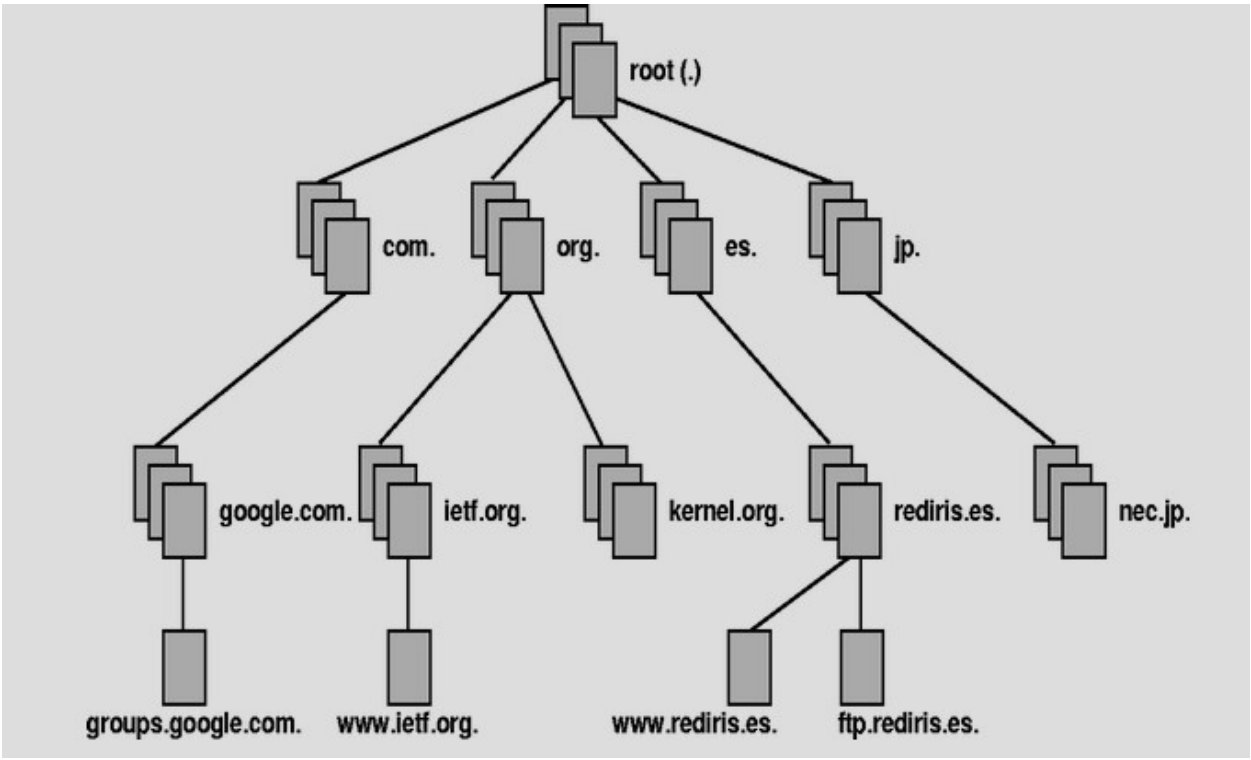
Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de no encontrarse, la petición se enviará a uno o más servidores DNS.



Los servidores DNS que reciben la petición, en primer lugar buscan en su propia memoria caché si disponen de la respuesta. En caso afirmativo, envía la petición al cliente; en caso contrario, se iniciaría la búsqueda de manera recursiva en otros servidores. Una vez encontrada la respuesta, el servidor DNS guardará el resultado en su memoria caché y devolverá el resultado al cliente.

4.4 Jerarquía DNS

El "espacio de nombres de dominio" (el conjunto de todos los nombres de domino) se encuentra organizado en forma de árbol. Cada nodo del árbol está compuesto por un grupo de servidores que se encargan de resolver un conjunto de dominios (zona de autoridad), así las hojas y los nodos del árbol se utilizan como etiquetas de los medios, siendo el nombre de dominio completo un objeto consiste en la concatenación de todas las etiquetas de un camino.



4.5 Registros DNS

Dentro de un dominio, es posible asignar direcciones a los sistemas asignados a distintos recursos. Los registros DNS conservan la dirección IP de los distintos servicios asociados a un nombre de dominio. Así, por ejemplo dentro del dominio *example.com* se podrían definir distintas entradas en los registros DNS para *www.example.com* o *mail.example.com.*

Existen varios tipos de registros DNS, los más comunes son los siguientes:

- **A (Address):** Son los registros principales del DNS. La función de estos registros es enlazar un dominio a una dirección IP.
- **PTR (Pointer)**: También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.
- **MX (Mail eXchanger).** Se usa para identificar servidores de correo, se pueden definir dos o más servidores de correo para un dominio, siendo que el orden implica su prioridad.

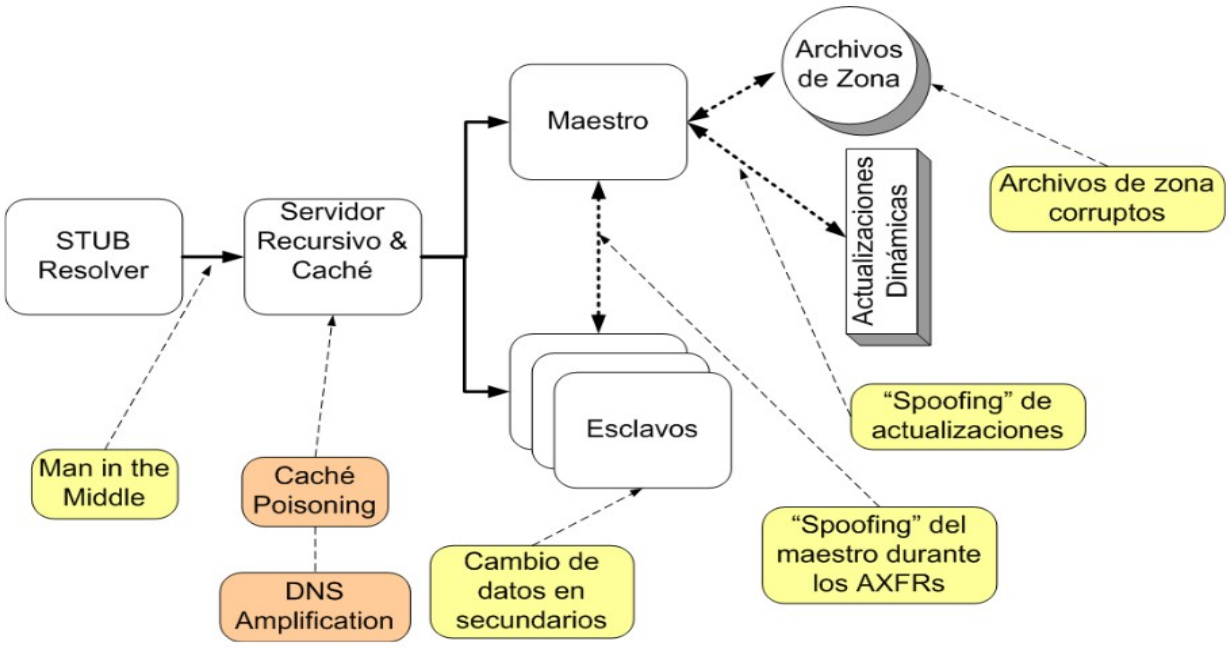
5 LA PROBLEMÁTICA DE DNS

La principal problemática del servicio DNS es que no fue concebido como un sistema seguro: no fue ideado para el uso que tiene actualmente, por lo que desde su diseño no se tuvieron en cuenta aspectos de seguridad. El sistema de resolución de dominios es considerado uno de los eslabones más débiles en la infraestructura actual de la red, y uno de los sistemas más explotados para intentar distintos ataques tanto a clientes finales como a servidores.

5.1 ¿Por qué atacar el sistema DNS?

El servicio DNS es considerado crítico para cualquier infraestructura de red, por el impacto que puede llegar a alcanzar la indisponibilidad de este servicio, y por la importancia de **asegurar la integridad de los datos devueltos por el servidor,** que estos sean correctos y que no hayan sido modificados por un tercero.

En la práctica, los atacantes aprovechan de distintos ataques a este sistema para suplantar la identidad, espiar o robar información. Los vectores de ataque más comunes al sistema DNS se resumen en el siguiente gráfico:



Sin entrar en todos los casos expuestos en el gráfico vamos a definir los ataques más comunes de los sistemas DNS.

5.2 Pharming

La mayoría de ataques relacionados con la resolución de dominios tienen por objetivo el robo de credenciales de usuario de bancos, redes sociales, juegos en línea, etc... Para conseguirlo, se redirecciona el tráfico dirigido a una Web legítima a otra falsa con una apariencia similar con el objetivo de suplantarla.

Esto a menudo se consigue mediante cierto tipo de malware que consigue modificar el archivo hosts del sistema (que se consulta antes de realizar la petición al servidor DNS) o la configuración de conexión a Internet, como realizaba el troyano **DNSChanger**.

5.3 Envenenamiento de la cache DNS: DNS caché poisoning

Para realizar un ataque de envenenamiento de caché, el atacante explota una debilidad en el sistema de DNS que puede hacer que éste acepte información incorrecta. Si el servidor no valida correctamente las respuestas DNS para asegurarse de que ellas provienen de una fuente autoritativa, el servidor puede terminar almacenando localmente información incorrecta y enviándola a los usuarios para que hagan la misma petición.

El DNS comprometido, desde ese momento hasta que borre los datos falsos de su caché, devolverá las IPs fraudulentas cuando reciba consultas asociadas a los dominios con los que contestó el DNS malicioso. Esto puede ser usado para reemplazar arbitrariamente contenido de una serie de víctimas con contenido elegido por un atacante.

En el verano de 2008 el investigador Dan Kaminsky publicó una serie de nuevos descubrimientos que mostraron cómo el problema del envenenamiento era serio y actual, pudiéndose incluso aplicar a escala global en Internet. Por ejemplo, se podría utilizar para comprometer la actualización de aplicaciones (spoofing de aplicaciones), lo que se conoce como *evilgrade*, de forma que un atacante podría hacerse pasar por el sitio del cual nos descargamos las actualizaciones del sistema operativo.

5.4 DNS Packet Forgery

Para realizar este tipo de ataque debe ser posible escuchar el tráfico que genera la máquina del usuario objetivo (*sniffing*). Si es posible capturar una petición realizada desde el sistema objetivo, antes de que el DNS consultado responda, el atacante tendrá que lanzar la respuesta a la petición que la originó, con el mismo identificador que la consulta al puerto, que también ha podido descubrir. Esta respuesta asociará el dominio consultado con una IP fraudulenta. Posteriormente, la máquina del usuario a engañar recibirá la respuesta no maliciosa; sin embargo, la desechará al haber ya recibido previamente otra con ese mismo identificador.

Para mitigar estos y otros riesgos asociados al mal diseño o configuración de DNS, Internet Engineering Task Force (IETF) diseña una serie de especificaciones que añaden una capa de seguridad a los sistemas de resolución de nombres de dominios denominado DNSSEC.

6 ¿QUÉ ES DNSSEC?

DNSSEC es el acrónimo para Domain Name System Security Extensions (Extensiones de seguridad para nombres de dominios), se trata de un conjunto de extensiones desarrolladas para asegurar cierto tipo de información del Sistema de Nombres de Dominio. Proporciona autenticación e integridad de los datos intercambiados vía DNS usando criptografía de clave pública, lo que dificulta ataques de suplantación.

Este conjunto de extensiones provee a los clientes DNS de la posibilidad de validar la autenticidad de quien genera la respuesta a una consulta DNS, indicación autenticada de la no existencia de información y de la integridad de los datos transferidos.

Es importante resaltar que DNSSEC no es un nuevo protocolo, si no un conjunto de extensiones añadidas. DNSSEC no incrementa la disponibilidad de los sistemas, ni confidencialidad en la información intercambiada ya que todas las respuestas de DNSSEC se autentican, pero no se cifran.

7 DNSSEC: ESTRUCTURA Y FUNCIONAMIENTO

DNSSEC proporciona:

- Un mecanismo para poder validar la autenticidad y la integridad de los datos contenidos en una zona DNS.
- Un mecanismo para delegar la confianza en ciertas claves públicas (cadena de confianza).
- Un mecanismo para autenticar las transferencias de zona entre primarios y secundarios .

7.1 Validación de autenticidad e integridad. Registros DNSSEC

Como vimos anteriormente, el sistema DNS se implementa mediante el uso de varios registros de recursos (A, MX, PTR, etc...). Para implementar DNSSEC, se han creado varios nuevos tipos de registros, entre ellos destacan:

- **RRSIG (Resource Record Signature)**: Guarda un hash cifrado del RRSET (uno o más registros DNS con el mismo nombre y tipo). Cifrado con la clave privada de la zona.
- **DNSKEY (DNS Public Key)**: Contiene una clave pública que los clientes pueden utilizar para verificar las firmas DNSSEC en los registros RRSIG.
- **DS (Delegation Signer)**: Contiene el hash de la clave pública de la zona hija firmado por la clave privada del padre.

- **NSEC (Next Secure)**: Es un enlace al siguiente nombre de registro (en el orden DNSSEC). Es utilizado para comprobar la inexistencia de un nombre y tipo de registro como parte de la validación de DNSSEC.

DNSSEC trabaja firmando digitalmente mediante criptografía de clave pública, lo cual le permite comprobar si la información es idéntica (correcta y completa) a la información en el servidor DNS autorizado, para ello se genera un par de claves (pública y privada) para cada **zona**, siendo siempre propio, este par de claves de dicha zona y no del servidor autoritativo. Por tanto:

- La clave privada se usa para firmar los datos RRSET de la zona (una clave para cada zona, como se ha indicado).
- Se debe publicar dichas firmas para cada RRSET en el archivo de zona correspondiente.
- La clave pública de la zona se debe divulgar en DNS mediante un registro DNSKEY, de modo que los validadores de la información pueden obtenerla.
- La clave pública se usa para validar las firmas y, por consiguiente, los datos DNS. Es importante destacar que un RRSET puede tener múltiples firmas generadas con diferentes claves.

7.2 Cadenas de confianza

Una vez que tenemos el mecanismo para comprobar que los datos enviados entre el servidor autoritativo y los validadores no han cambiado y son completos, ¿como podemos confiar en ellos?

Para ser capaz de comprobar que una respuesta DNS es confiable, es necesario saber que al menos una clave o registro DS es correcto a partir de fuentes distintas de la DNS. Estos puntos de partida son conocidos como **anclas de confianza** ("trust-anchor") y se obtienen normalmente con el sistema operativo o por alguna otra fuente confiable.

En DNSSEC para poder decir que una respuesta a una búsqueda DNS es autenticada de manera segura es necesaria una **cadena de autenticación completa**, desde el ancla de confianza, que comienza en un conjunto de claves públicas de la zona raíz del DNS, hasta el servidor de nombres autorizado. Para ello se deberá **tener la clave pública de cada zona firmada por la zona del nivel inmediatamente superior** (registro DS). De esta manera se asegura mantener la denominada cadena de confianza ("chain of trust").

En la práctica, ¿cómo puede un cliente verificar un RRSet de una cierta zona?:

- Se realiza una consulta por el DNSKEY correspondiente.
- Se realizan los cálculos correspondientes y son comparados con el RRSIG que nos indican la validez o no.

Llegado a este punto es lícito preguntarse quien firma la zona raiz (“.”), ya que es la única que no tiene entidad superior a la que pedirle un registro DS. El **ancla de confianza raiz** (“root trust anchor”) se encuentra firmada desde Julio del 2010 y es necesario obtenerla “fuera de banda” y cargarse manualmente, siendo necesario verificar su autenticidad mediante otros métodos.

8 CONCLUSIONES

El mayor problema del sistema DNS es no haber tenido en consideración, en su diseño, aspectos de seguridad. Uno de los retos más importantes en el desarrollo de las redes en general en los próximos años es asegurar este servicio básico. La existencia de nuevas extensiones de seguridad, como DNSSEC, ayudan a mitigar riesgos inherentes a este protocolo corrigiendo aspectos de seguridad que no fueron implementados en el servicio estándar y dificultando ciertos ataques de suplantación y corrupción de datos.

A pesar de su importancia, el despliegue de DNSSEC se ha visto obstaculizado por varias dificultades:

- La necesidad de diseñar un estándar compatible con versiones anteriores que puede escalarse al tamaño de la Internet.
- Debido a la naturaleza distribuida del servicio DNS, el despliegue de las implementaciones DNSSEC necesita ser realizado por una cantidad significativa de proveedores DNS antes de que pueda llegar a ser relevante.
- El desacuerdo entre los encargados de la ejecución sobre quién debe poseer las llaves de raíz de los dominios de nivel superior.
- La aparente complejidad de DNSSEC en su despliegue.

Es por ello que los administradores de la infraestructura DNS, TLD's y los sistemas raíz deben ser caldo de cultivo en el que DNSSEC puede despegar mientras los proveedores de servicios y los administradores de sistemas de las empresas preparan su infraestructura para validar datos firmados.

El despliegue completo de DNSSEC asegurará que el usuario final se encuentra conectado al sitio web o al servicio de un nombre de dominio verdadero. A pesar de que esto no resolverá todos los problemas de seguridad de Internet, si protege una parte critica del mismo. Las mejoras en la protección del sistema DNS en conjunción con otras tecnologías pueden constituir una base sólida para el desarrollo de futuras mejoras de seguridad en Internet.

9 REFERENCIAS

- ICANN: DNSSEC – What Is It and Why Is It Important?: http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm
- Wikipedia DNSSEC: http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- NIST - Secure Domain Name System (DNS) Deployment Guide - Recommendations of the National Institute of Standards and Technology

- LACNIC – Conceptos generales de DNS: http://www.labs.lacnic.net/site/sites/default/files/dnssec-citel-generalidades-ES-01.pdf