Despliegues DNSSEC

DNSSEC Implentations

Joao Damas, José. M Femenia, Antoni Santos Cutando, Silvia Onsurbe Martínez

Resumen

El DNS es una de las piezas fundamentales que permite el funcionamiento de Internet. Aunque el diseño original de DNS no proporciona mecanismos de seguridad a la altura de lo que se espera en la Internet actual, el protocolo se ha visto extendido en este aspecto con las extensiones DNSSEC. Aunque el protocolo conlleva una cierta complejidad en su definición su uso por parte de los administradores de DNS y usuarios finales no es complejo. En este artículo se analizan las características principales de las extensiones de seguridad del DNS, las herramientas disponibles para su uso en la vida real y se describe el estado del proyecto de despliegue en el dominio .es así como los de nuestro entorno más cercano.

Palabras clave: DNSSEC, dominios, DNS Security extensions, .es, .edu

El DNS es una de las piezas fundamentales que permite el funcionamiento de Internet

Summary

DNS is one of the key technologies that allows the operation of the Internet. Although the original design of DNS does not provide security mechanisms as expected on today's Internet, the protocol has been extended in this respect with DNSSEC extensions. Although the protocol involves a degree of complexity in its definition, its use by DNS administrators and end users is not so complex. This article analyses the main features of the DNS security extensions, what kind of tools are available for its use in real life, and describes the state of deployment in.es domains and in some others close to our environment.

Keywords: DNSSEC, domains, DNS Security extensions, .es, .edu

1. Introducción

Se diseñó hace más de 25 años, en una época en que las cuestiones de seguridad en las comunicaciones tenían una relevancia mucho menor

El DNS es una de las piezas fundamentales que permite el funcionamiento de la Internet. Su misión es traducir los nombres que los humanos utilizan para recordar como referirse a los servicios y máquinas en Internet a los identificadores que los ordenadores utilizan para establecer las comunicaciones.

El DNS se diseñó hace más de 25 años, en una época en que las cuestiones de seguridad en las comunicaciones tenían una relevancia mucho menor.

Esta evolución en las necesidades de integridad y fiabilidad del DNS llevaron al desarrollo de las extensiones de seguridad para el DNS, DNS Security extensions, o simplemente **DNSSEC**.

DNSSEC es un sistema que aumenta las capacidades del DNS sin romper la compatibilidad hacia atrás, proporcionando formas de permitir a los consumidores de información DNS la verificación de que la información que les está llegando es la que la fuente original de esa información publicó, tanto en el caso de que la respuesta a la pregunta de DNS contenga datos o no.

DNSSEC consigue esto haciendo uso de tecnologías de criptografía de clave pública (RSA, DSA, GOST), con las cuales se generan firmas para los distintos elementos de la respuesta de DNS. Estas firmas

pueden ser verificadas en los servidores de DNS de los proveedores de Internet o de las organizaciones, con el fin de comprobar que la información no se ha visto alterada respeto a lo que el administrador del dominio DNS hizo público.

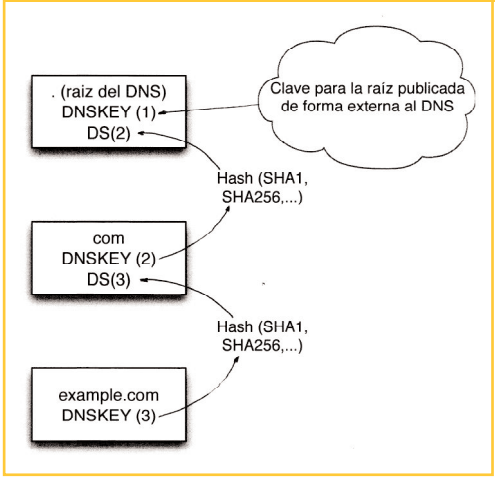
El servidor que lleva a cabo la verificación, puede obtener las claves públicas que se utilizan en el proceso de firma preguntando a la propia zona de DNS. Cada dominio debería estar enlazado a su zona superior (por ejemplo org para isc.org) utilizando un nuevo tipo de registro DNS denominado DS (Delegation signer, firmante de la delegación), mediante el cual el dominio superior identifica y firma la clave para una zona inmediatamente inferior. Enlazando dominios de esta forma y siguiendo la jerarquía del DNS, se construye una cadena de confianza.

Para poder asignar confianza a esa cadena, es necesario disponer de un punto inicial para el proceso que se pueda verificar por medios ajenos al sistema. En el caso ideal, este punto de entrada es la clave utilizada para firmar la raíz del DNS, que está disponible y en uso desde Julio de 2010.

Para facilitar el despliegue inicial, en ausencia de firmas para todo el árbol de DNS, lo que se puede encontrar son árboles parciales de firmas y claves DNSSEC que no empiecen en la raíz, por ejemplo si faltan dominios intermedios.

En el momento de escribir este artículo, por ejemplo, la zona .com no está aún firmada (aunque está previsto que lo esté el día 31 de Marzo de 2011) por lo cual es imposible realizar la verificación DNSSEC para un domino .com (por ejemplo, example.com) partiendo de la clave de la raíz.

FIGURA 1: Enlazando dominios a través de registros DS y DNSKEY



En este periodo inicial, se podría configurar manualmente en el servidor DNS la clave para el dominio example.com, de forma que permita la verificación de los datos para ese dominio. Esta clave insertada manualmente debería ser eliminada de la configuración del servidor DNS, que es el que realiza la verificación una vez que la zona .com esté firmada, permitiendo hacer uso de los mecanismos automáticos de renovación de claves previstos en el protocolo.

En la gráfico se muestra la relación entre los registros DS y las claves empleadas en los dominios que permiten establecer las cadenas de confianza. Una consecuencia de la implementación de DNSSEC es que la gestión del DNS por parte de los dueños de los dominios, que ahora es en la mayoría de los casos una tarea realizada con poca frecuencia, debe tomar un nuevo protagonismo como parte de la gestión de los servicios de Internet, ya que en caso contrario se producirán situaciones como la caducidad de las firmas DNSSEC, que harían desaparecer al dominio desde el punto de vista de los usuarios que lleven a cabo la verificación de las firmas.

También se debe de tener en cuenta que el despliegue de DNS conlleva un incremento en la necesidad de recursos en los servidores, tanto en los autoritativos ya que la zona firmada es mucho mayor y las respuestas consumen más ancho de banda, como en los recursivos/validadores ya que se ha de llevar a cabo la comprobación de las firmas.

Cada dominio debería estar enlazado a su zona superior utilizando un nuevo tipo de registro DNS denominado DS

Con DNSSEC la gestión del DNS por parte de los dueños de los dominios debe tomar un nuevo protagonismo como parte de la gestión de los servicios de Internet

En general, los beneficios de hacer uso de DNSSEC son importantes, con un gran aumento de la seguridad y confianza que se puede depositar en el DNS, pero su despliegue se ha de llevar a cabo de forma consciente y con un plan adecuado.

2. Herramientas de diagnóstico y pruebas para DNSSEC en .edu

Para la puesta en práctica de DNSSEC en un entorno de DNS basado en BIND de ISC, se pueden recomendar distinta documentación detallada, que puede servir de orientación a la hora de la realizar la instalación. En la Universitat de València hemos hecho uso de la siguiente lista. No es una relación exhaustiva, pero si la que nos ha permitido realizar la firma del dominio valencia.edu sin muchas dificultades.

En la Universitat de València, con esta documentación, hemos podido realizar la firma del dominio valencia.edu sin muchas dificultades

VeriSign Tool Guide Series on DNSSEC: http://www.educause.edu/Resources/ToolGuideSeriesonDNSSECVersion/210434	**Esta es una guía concisa dirigida a la configuración de DNSSEC en el entorno .edu, con ejemplos para BIND 9 y OpenDNSSEC.**
DNSSEC Operations: Setting the Parameters. http://www.dnssec-deployment.org/documents/SettingtheParameters.pdf	Un breve documento que define y aconseja los valores más para parámetros necesarios en DNSSEC, tales como tamaños y tiempos de expiración de claves.
DNSSEC HOWTO NLnet Labs. http://www.nlnetlabs.nl/dnssec_howto/dnssec_howto.pdf	
BIND 9 Administrator Reference. http://www.isc.org/files/arm97.pdf	Si se está usando este servidor de DNS, es muy conveniente consultar las últimas novedades que van a apareciendo que permiten una gestión más fácil y eficaz de las claves y la firma de zonas.
NIST Secure Domain Name System (DNS) Deployent Guide. http://csrc.nist.gov/publications/drafts/800-81-rev1/nist_draft_sp800-81r1-round2.pdf.	Un amplio compendio de sobre la seguridad en el servicio de resolución de nombres. Pese a su extensión es recomendable su lectura, ya que cubre otros aspectos más allá del DNSSEC.

Tabla 1

Una petición de resolución a un servidor asegurado presenta la marca ad

Una relación bastante completa de recursos adicionales y herramientas sobre DNSSEC puede encontrarse en los siguientes enlaces:

DNSSEC for .edu
http://net.educause.edu/edudomain/show_faq.asp?code=EDUDNSSEC

Herramientas y recursos:
https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources

De entre todas las herramientas, en la Universitat de València hemos encontrado particularmente útiles algunas de ellas.

Para la comprobar que el servidor está adecuadamente configurado para validar las firmas de DNSSEC y responder en a su cliente en consonancia, usamos el dig. Una petición de resolución a un servidor asegurado presenta la marca ad tal y como se aprecia en el ejemplo:

```
; <<>> DiG 9.7.1-P2 <<>> +dnssec SOA valencia.edu
;; global options: +cmd
```

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36257
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:

[borrado]

;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Nov 10 10:11:52 2010
;; MSG SIZE rcvd: 267

Un servidor de DNS sin la validación de DNSSEC activada, no presenta dicha marca:

; <<>> DiG 9.7.1-P2 <<>> @8.8.8.8 +dnssec SOA valencia.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45281
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

[borrado]

;; Query time: 252 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Nov 10 10:19:06 2010
;; MSG SIZE rcvd: 267

Un servidor de DNS sin la validación de DNSSEC activada no presenta la marca indicada

Por supuesto, la respuesta es diferente en cada caso al preguntar por un dominio con una firma de DNSSEC alterada. En el caso del servidor asegurado, no responde ninguna dirección válida, es decir, para el cliente como si no existiese el dominio, mientras que un servidor que no comprueba la validez DNSSEC resuelve en dominio.

DNS con comprobación de DNSSEC	; <<>> DiG 9.7.1-P2 <<>> +dnssec www.rhybar.cz +multiline ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 30554 ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: do; udp: 4096 ;; QUESTION SECTION: ;www.rhybar.cz. IN A ;; Query time: 130 msec ;; SERVER: 127.0.0.1#53(127.0.0.1) ;; WHEN: Wed Nov 10 11:39:14 2010 ;; MSG SIZE rcvd: 42
DNS sin comprobación de DNSSEC	; <<>> DiG 9.7.1-P2 <<>> @8.8.8.8 +dnssec www.rhybar.cz +multiline ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25341 ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: do; udp: 512 ;; QUESTION SECTION: ;www.rhybar.cz. IN A ;; ANSWER SECTION: www.rhybar.cz. 600 IN A 217.31.205.50 www.rhybar.cz. 600 IN RRSIG A 5 3 600 20081030080058 (20080930080058 5172 rhybar.cz. XVkut4l9mw2MhodZFIOD2L57AU2 cFC5NIe8ukw79jYdOCH3WwFgSMs XiU0ymFGFju9x/k10lv6SGS6Isl BnwTx7qK3j+bNzxKLvjpn7DY9f+) ;; Query time: 125 msec ;; SERVER: 8.8.8.8#53(8.8.8.8) ;; WHEN: Wed Nov 10 11:39:34 2010 ;; MSG SIZE rcvd: 227

Tabla 2

un servidor que no comprueba la validez DNSSEC resuelve en dominio

Otra utilidad recomendable que permite al usuario comprobar si un dominio está firmado con DNSSEC, y la su cadena de validación es correcta, es el complemento "DNSSEC Validator" para navegadores Firefox desarrollado y mantenido por CZ.NIC (http://www.dnssec-validator.cz). Mediante una codificación de colores sencilla, indica al usuario, de un modo semejante a cómo se le indica la validez de los certificados de servidor, si la dirección que se ha resuelto en el navegador está correctamente validada por DNSSEC.

También, Verisign ha desarrollado un interfaz web que permite chequear en detalle el estado de un dominio en lo que respecta a su firma DNSSEC, permitiendo trazar errores en el mismo y en la cadena de validación de las claves y firmas. Está disponible en http://dnssec-debugger.verisignlabs.com. Desde este interfaz se puede acceder a http://dnsviz.net que realiza un análisis similar pero con una presentación gráfica de la cadena de autenticación.

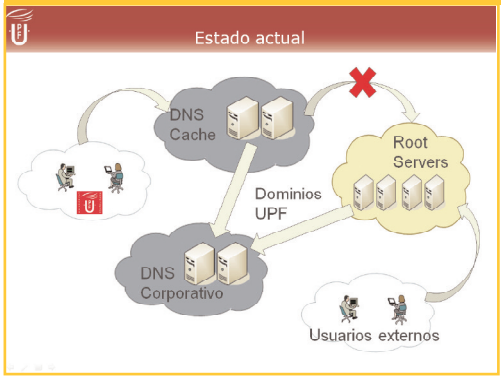
Verisign ha desarrollado un interfaz web que permite chequear en detalle el estado de un dominio en lo que respecta a su firma DNSSEC

3. Caso Universitat Pompeu Fabra

La **Universitat Pompeu Fabra** disponía de una arquitectura DNS obsoleta, tanto a nivel de Hardware como de Software. Se procedió a valorar la actualización de esta arquitectura y la posterior implementación de DNSSEC cuándo **Educause** publicó la intención de firmar el dominio .edu a principios de agosto del 2010.

En un estudio realizado por el grupo de Computer Science de la Universidad de los Angeles (UCLA) la implantación del DNSSEC ha visto un aumento considerable este ultimo año, que suponemos que ha sido a raíz de las firmas de los dominios org y edu.

FIGURA 1



El proceso de actualización de la arquitectura se realiza en dos fases, una primera fase en la que se actualizó el hardware, los servidores, y una segunda fase en la que se actualizó el software, en esta fase se aprovechó para implementar el sistema DNSSEC en los dominios upf.edu y upf.cat.

Para conseguir una mayor seguridad e integridad de los sistemas, los servidores autoritativos se configuraron para que no pudieran hacer consultas DNS recursivas

Se optó por servidores virtuales, creando dos servidores cachés, dónde se concentran todas las peticiones de los usuarios y dos servidores autoritativos, donde reside la información principal de los dominios gestionados desde la Universitat Pompeu Fabra.

Para conseguir una mayor seguridad e integridad de los sistemas, los servidores autoritativos se configuraron para que no pudieran hacer consultas DNS recursivas, es decir, si alguien hace una consulta a estos servidores de un dominio que no sea de la Universidad no dará ninguna respuesta.

Una vez se implantó la nueva arquitectura, se implementó DNSSEC para los dominios upf.edu y upf.cat. Se deben generar dos claves, una KSK (Key-signing key y una ZSK (Zone signing key) de la siguiente manera:

- dnssec-keygen –r/dev/random –f KSK –a RSASHA1 –b 2048 –n ZONE upf.edu
- dnssec-keygen –r/dev/random –a RSASHA1 –b 2048 –n ZONE upf.edu

Una vez tenemos las claves, se añaden al final del documento del fichero de la zona, de esta manera se propaga la clave a través de los root servers. Es necesario esperar a que se propague la información, este tiempo es el TTL configurado para cada zona.

Se firma la zona con ambas claves, esto genera un fichero con extensión *signed*

➢ dnssec-signzone -o upf.edu –k Kupf.edu.actual.key upf.edu.hosts Kupf.edu.actual.key

Cambiamos la configuración del servidor indicando que el fichero con la información de la zona es el fichero con extensión *signed*.

Se añaden los datos en el registrador de dominio y se verifica que resuelva correctamente.

En el caso de realizar una actualización de las claves, se añaden las nuevas claves en el fichero, además de las antiguas, y se espera a que se propague la información. Una vez haya pasado el TTL de la zona, se firma con la nueva clave y se hace la revocación de la antigua.

Es necesario esperar a que se propague la información, este tiempo es el TTL configurado para cada zona

FIGURA 2

Al actualizar las claves, hay que tener en cuenta que si nos equivocamos a la hora de publicar las claves y firmamos la zona con otra clave que no sea la que se ha publicado, la resolución de nombres dejará de funcionar al no poder validarla. Es importante habilitar que los paquetes DNS puedan tener un tamaño mayor a 512 bytes en los equipos de la red, sobre todo en los Firewalls.

Es importante habilitar que los paquetes DNS puedan tener un tamaño mayor a 512 bytes en los equipos de la red, sobre todo en los Firewalls

Con el plugin DNSSEC Validator instalado en Mozilla se puede comprobar que URLs están securizadas mediante DNSSEC. También se puede verificar con el comando dig o en diferentes web como dnscheck.iis.se

4. Despliegue de DNSSEC en los dominios .es

La infraestructura que compone el servicio de DNS está compuesta por sistemas distribuidos geográficamente por todo el mundo. La estructura y niveles que la conforman están directamente relacionados con la forma en la que se organizan los nombres de dominio. El nivel más alto de esta jerarquía lo constituyen los servidores raíz (13 a nivel mundial), y los siguientes se denominan top-level domain (TLD). En la actualidad, existen más de 250 TLDs, de los que forman parte:

• **Country-code TLDs (ccTLDs)**: es el denominativo que tienen los dominios territoriales: asociados a países, como por ejemplo: .es (España), .de (Alemania), .be (Bélgica), etc....
• **Sponsored generic TLDs (gTLDs)**: dominios que representan a una comunidad con ciertos intereses. Son por ejemplo: .edu, .gov, .int, .mil, .aero, .coop, y .museum.
• **Unsponsored generic TLDs (gTLDs)**: dominios genéricos que a diferencia de los gTLDs no cuentan con un sponsor. Son por ejemplo: .com, .net, .org, .biz, .info, .name, y .pro.

La estructura y niveles que la infraestructura conforman están directamente relacionados con la forma en la que se organizan los nombres de dominio

La información de los dominios se agrupa en lo que se denominan zonas. Éstas son entidades configurables dentro de un servidor DNS, de forma que administrativamente la gestión sea mucho más sencilla.

El registro .es es el responsable de la administración y gestión del fichero de zona de los dominios de segundo y tercer nivel de España: .es; .com.es; .nom.es; .gob.es; .edu.es; .org.es; y su propagación a los servidores raíz para su resolución a nivel mundial.

Para garantizar que el funcionamiento de DNSSEC sea correcto, hay que establecer varios pasos:

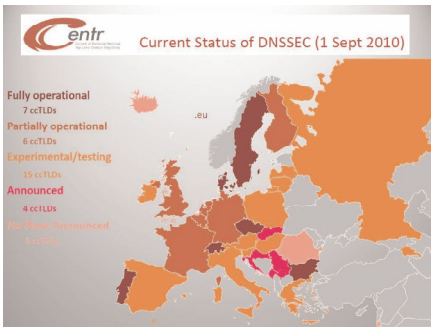
• En primer lugar deben tener implementada la firma del fichero de zona los servidores raíz, se espera que este proceso se cierre definitivamente a mediados de Julio de 2011.
• El resto de TLD deben contar con la infraestructura necesaria para que el fichero de zona vaya firmado, de forma que se siga garantizando la seguridad del proceso.
• Por extensión, y como parte importante de la cadena, son los proveedores de servicios de Internet y Agentes Registradores, los que también deben contar con esa capacidad.

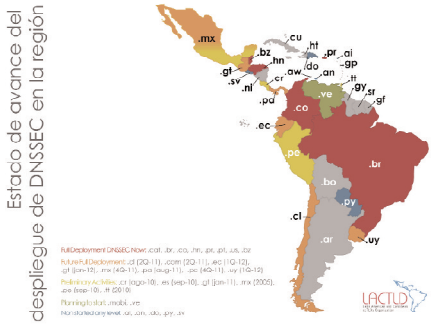
Respecto al panorama internacional son muchos los que ya disponen de DNSSEC o están en proceso de implantación en distinto grado

La responsabilidad por parte de los registros, tanto, cctld o gtlds queda clara para hacer que DNSSEC sea una realidad, ya que como gestores de los ficheros de zona de dominios, son un eslabón clave en el proceso de firma y certificación de los dominios, hasta su propagación en el servidor raíz.

Respecto al panorama internacional son muchos los que ya disponen de DNSSEC o están en proceso de implantación en distinto grado. En el caso de Europa ha sido el registro checo (.cz) es pionero en esta labor; si bien hay otros gtlds como el .info que ya lo tienen operativo. A continuación se muestran dos mapas que representan el estado de DNSSEC en Europa y Latinoamérica:

FIGURA 3: Mapa del estado DNSSEC en Europa. Documento CENTER septiembre 2010
FIGURA 4: Mapa del estado DNSSEC en Latinoamérica. Documento LACTLD 2010





En una primera fase, se ha definido un piloto en el que han intervenido **Agentes Registradores** acreditados del .es, entidades como el **Banco de España y RedIRIS**. En el mismo, se han determinado las necesidades técnicas para la puesta en marcha de un proyecto de este tipo y posibles riesgos o inconvenientes que son necesarios resolver, ya que si bien los cambios en infraestructura no son tan complejos, si lo es la posterior administración de los sistemas. La colaboración en diversos foros internacionales y el contacto con otros cctlds que ya tienen experiencia en la implantación de DNSSEC ha sido un refuerzo importante.

La colaboración en diversos foros internacionales y contacto con otros cctlds que ya tienen experiencia en la implantación de DNSSEC ha sido un refuerzo importante

En cualquier caso, DNSSEC sigue siendo un poco un desconocido en algunos foros, y en cierto modo es una amenaza que puede parar su impulso, ya que el éxito depende de la colaboración de todas las partes implicadas: servidores raíz, servidores de registros, operadores de comunicaciones, gestores de servicios de Internet, etc...

Es por ello, que independientemente de los aspectos relacionados con la infraestructura que da soporte a DNSSEC, desde el registro .es, se quiere establecer un plan difusión de DNSSEC, elaborando guías o manuales que puedan servir de referencia tanto a usuarios finales del servicio como a empresas involucradas en el sector o puesta en marcha de workshops técnicos más específicos.

Se quiere establecer un plan difusión de DNSSEC, elaborando guías o manuales que puedan servir de referencia

Referencias:

[1] http://www.dnssec.net/

Joao Damas
(joao@isc.org, joao@bondis.org)
ISC
José M.Femenia
(Jose.M.Femenia@uv.es)
Universitat de València
Antoni Santos Cutando
(antoni.santos@upf.edu)
Universitat Pompeu Fabra
Silvia Onsurbe Martínez
(silvia.onsurbe@red.es)
Dominio.es/Red.es