Una experiencia en la implementación de Extensiones de Seguridad para el Sistema de Nombres de Dominio.

Ernesto Sánchez
C.I.D.I.A.
Universidad Nacional de Salta
Salta, Argentina, 4400
esanchez@cidia.unsa.edu.ar

Daniel Arias Figueroa
C.I.D.I.A.
Universidad Nacional de Salta
Salta, Argentina, 4400
daaf@cidia.unsa.edu.ar

Sergio Rocabado
C.I.D.I.A.
Universidad Nacional de Salta
Salta, Argentina, 4400
srocabad@cidia.unsa.edu.ar

Álvaro Gamarra
Universidad Católica de Salta
Salta, Argentina, 4400
alvaroig@yahoo.com

Javier Díaz
Universidad Nacional de la Plata
La Plata, Argentina, 1900
jdiaz@unlp.edu.ar

Abstract

Las extensiones de Seguridad para DNS (DNSSEC) proveen autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS. Las mejoras que ofrece DNSSEC radican principalmente en el uso de una jerarquía de "firmas criptográficas" que permite proteger el flujo de información intercambiado entre Servidores Autoritativos, Servidores DNS Recursivos y Clientes DNS. El presente trabajo tiene por objetivo mostrar una experiencia en la implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio en una estructura basada en servidor raíz, servidor de nivel superior, servidor autoritativo y servidor recursivo. Para cada etapa del proceso de implementación se describirán las tareas asociadas y las observaciones que surgieron a partir de las mismas, de manera tal que puedan ser utilizadas para futuros trabajos, con la finalidad de una pronta adopción en el ámbito de las universidades, considerando que desde Junio 2015, el dominio de nivel superior .ar ya adoptó tales aspectos de seguridad.

1. Introducción

El despliegue a nivel mundial de las extensiones de seguridad para el Sistema de Nombres de Dominio (DNSSEC) ha alcanzado a la fecha el 88%, considerando que son 1405 los dominios de nivel superior en la zona raíz [1]. La implementación de tales extensiones ha sido relativamente lenta en términos de tiempo, si se tiene en cuenta que en el año 2010 se anunció el firmado de la zona raíz. Esto se debe principalmente a la naturaleza jerárquica del sistema DNS, donde cada eslabón de la cadena es administrado de forma independiente por entidades privadas, públicas, ISPs, etc. Otro aspecto crítico, que influye en la migración a DNSSEC, es la naturaleza del servicio de resolución de nombres, fundamental para el funcionamiento de Internet.

Otros aspectos no menos importantes, son los relacionados directamente con las nuevas características de DNSSEC, tales como, nuevos registros de recursos, criptografía de clave pública, proceso de validación de confianza entre zona padre y zona hijo, entre otros.

Son justamente estas nuevas características, las que implican un costo en término de tiempo, asociado a configuración, mantenimiento y coordinación de tareas, entre las partes involucradas en la jerarquía antes mencionada.

El presente trabajo tiene por objetivo mostrar una experiencia en la implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio en una estructura basada en servidor raíz, servidor de nivel superior, servidor autoritativo y servidor recursivo. Para

cada etapa del proceso de implementación se describirán las tareas asociadas y las observaciones que surgieron a partir de las mismas, de manera tal que puedan ser utilizadas para futuros trabajos, con la finalidad de una pronta adopción en el ámbito de las universidades, considerando que desde Junio 2015, el dominio de nivel superior .ar ya adoptó tales aspectos de seguridad.

2. Características de DNSSEC

En términos generales y según se describe en el *RFC 4033: DNS Security Introduction and Requirements*, las Extensiones de Seguridad para DNS (DNSSEC) proveen autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS. Las mejoras que ofrece DNSSEC radican principalmente en el uso de una jerarquía de "firmas criptográficas" que permite proteger el flujo de información intercambiado entre Servidores Autoritativos, Servidores DNS Recursivos y Clientes DNS.

Para poder proveer los aspectos de seguridad anteriormente citados, DNSSEC hace uso de nuevos Registros de Recursos y una particular infraestructura de clave pública, basada en la construcción de una "cadena de confianza", necesaria para la validación de los datos en el proceso de consulta/respuesta DNS.

2.1. Nuevos Registros de Recursos

Los Registros de Recursos para DNSSEC son: [2].

- DNSKEY: Registro de Recurso habilitado para almacenar claves públicas, que posteriormente serán usadas por DNSSEC en procesos de autenticación.

- RRSIG: Contiene la firma para un conjunto de Registros de Recursos (RRset) con un nombre particular, clase y tipo. El registro RRSIG se genera en el proceso de firmado de una zona utilizando la clave privada y cuyo par (clave pública) es almacenada en el registro DNSKEY.

- NSEC: Permite validar la estructura de una zona y los Registros de Recurso que esta contiene.

- DS: Permite crear una cadena de confianza o de autoridad de una zona padre firmada, hacia una zona hija firmada. DS está relacionado con el Registro DNSKEY, ya que contiene un resumen (hash o digesto) de la clave (KSK) almacenada en éste último.

2.2. Cadena de confianza

El proceso de construcción de una cadena confianza es fundamental para la implementación de DNSSEC en una jerarquía DNS, ya que sin ésta característica, cada Servidor Recursivo configurado con DNSSEC, debería tener un punto de entrada seguro (SEP) por cada dominio seguro en Internet, lo que claramente haría imposible un despliegue a escala global de tales extensiones de seguridad. [4].
La siguiente ilustración permite observar los procesos involucrados en la creación de la cadena de confianza:

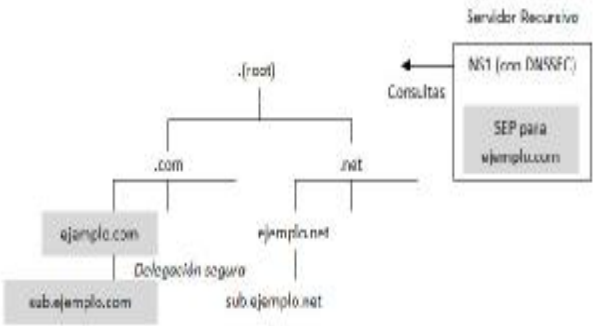

Fig. 1. Creación de cadena de confianza

Tanto el dominio ejemplo.com como sub.ejemplo.com se encuentran asegurados, es decir que para que pueda ocurrir una delegación segura es requisito previo haber asegurado la zona hija (sub.ejemplo.com). El punto de entrada seguro para ejemplo.com cubre las zonas seguras que son delegadas a partir de él, a través de una delegación segura creando una cadena de confianza provista por el uso del Registro de Recurso DS.

Una cadena de confianza puede ser construida tanto hacia arriba como hacia abajo en una jerarquía DNS, por lo que si el dominio de nivel superior .com fue asegurado, el dominio ejemplo.com puede unirse a la cadena.

Continuando con el ejemplo de la figura, el servidor NS1 (configurado con DNSSEC), podría ahora requerir un nuevo SEP para el dominio .com, y este único SEP cubriría ahora los dominios .com, ejemplo.com, así como sub.ejemplo.com.

Desde Julio 2010 la zona raíz se encuentra firmada y a la fecha, son 1257 los dominios de nivel superior que fueron firmados, de los cuales, 1245 tienen puntos de anclaje seguros publicados como registros DS en la zona antes mencionada [1]. Es importante resaltar que en Junio del año 2015, el dominio .ar, se encuentra asegurado y publicado en la zona raíz. [3].

2.3. Clave de Zona (ZSK) y Clave de Claves (KSK)

En los procesos de delegación y posterior validación de claves criptográficas de firmado, la siguiente clasificación de claves se hace necesaria a fin de facilitar las tareas operacionales llevadas a cabo por DNSSEC. Según se describe en el RFC 4641 [5], las claves usadas para el firmado de registros asociados a un dominio pueden ser de dos tipos, ZSK (Zone Signing Key) o KSK (Key Signing Key), donde la primera tiene por función la de proteger los Registros de Recursos individuales de una Zona dada, mientras que la KSK se encarga de proteger la ZSK. Operacionalmente se almacenan en un registro DNSKEY y se distinguen mediante el bit llamado SEP, presente en la porción RDATA del Registro de Recurso DNSKEY.

Algunas de las motivaciones para un uso separado de claves son: La KSK puede configurarse con longitudes de clave mayores, lo que la convierte en una clave de mayor fortaleza. Operacionalmente tiene poco impacto en consumo de recursos, ya que solo se usa para el firmado de una pequeña porción de datos de una zona dada. Por otro lado, dado que la KSK sólo se utiliza para firmar un conjunto de claves, ésta puede actualizarse con menos frecuencia que otros datos en la Zona y ser almacenada en una localización diferente de la ZSK

3. Escenario de prueba utilizado

Según se expuso en 2.2, para poder garantizar la autenticidad e integridad de una respuesta DNS, en un momento determinado, se debe verificar la cadena de confianza desde el último eslabón de la cadena, hasta llegar al nodo raíz, es por esto que se configuró una jerarquía DNS, utilizando la herramienta de virtualización VMWare Player, según se muestra en la siguiente figura.

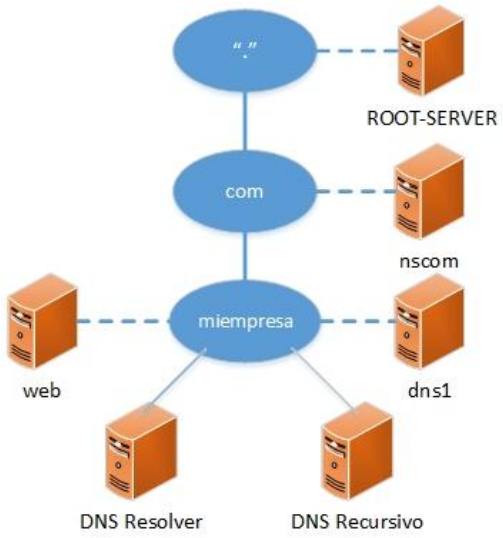

Fig. 2. Escenario de prueba

La siguiente tabla muestra detalles de la configuración utilizada, tales como direccionamiento IP y funcionalidad.

Tabla 1. Configuración escenario de prueba.

Nombre servidor	Dirección IP	Observaciones
ROOT-SERVER	10.0.0.254	Servidor DNS Raíz
nscom	10.0.0.253	Servidor TLD .com
dns1	10.0.0.2	Servidor Autoritativo miempresa.com
web	10.0.0.100	Servidor web miempresa.com
recursivo	10.0.0.11	Servidor Recursivo Cache
resolver	10.0.0.12	Cliente DNS

Todos los servidores están basados en Debian Linux con software DNS BIND versión 9.8.4

3.1. Configuración de escenario DNSSEC

El proceso de configuración de DNSSEC, y tareas relacionadas, tales como generación de claves, firmado de zonas, delegación segura, etc., requiere la ejecución de una secuencia de pasos siguiendo un determinado orden. Cabe resaltar que son varias las alternativas de software que permiten la puesta en marcha de las extensiones de seguridad, entre las que se destacan, DNSSEC-Tools [7], OpenDNSSEC [8] y las provistas por el mismo software BIND. Para llevar adelante las pruebas, se eligieron éstas últimas, ya que si bien todo el proceso debe realizarse de manera manual, esto permitió una mejor comprensión de

cuál es el aporte de los aspectos de seguridad (integridad y autenticación) y de qué manera lo hacen.

Tomando como base el escenario presentado en la figura 2, se implementó DNSSEC en todos los servidores involucrados en la jerarquía DNS, es decir que, se configuró el servidor recursivo para validación DNSSEC, se firmaron zona raíz, zona .com y zona miempresa.com. El proceso se completó creando la cadena de confianza a partir de la publicación del registro DS desde zona hija a zona padre.

La implementación de DNSSEC para el escenario propuesto, se resume en los siguientes pasos:

- Generación de claves de firmado pública/privada ZSK y KSK.
- Publicación de claves pública ZSK y KSK en archivo de zona.
- Firmado de archivo de zona con clave privada ZSK.
- Publicación de archive DS en zona padre. Esto se realizó de zona .com a zona raíz y de zona miempresa.com a zona .com
- Refirmado de zona padre.
- Configuración de clave pública de validación inicial (KSK), para todos los servidores de la jerarquía, incluidos recursivo y resolver. Esta clave se obtuvo de lo generado en zona raíz (ROOT-SERVER).

A modo de ejemplo se presenta la siguiente figura, la cual describe el recorrido de la cadena de confianza, la cual resulta de la configuración antes descripta.

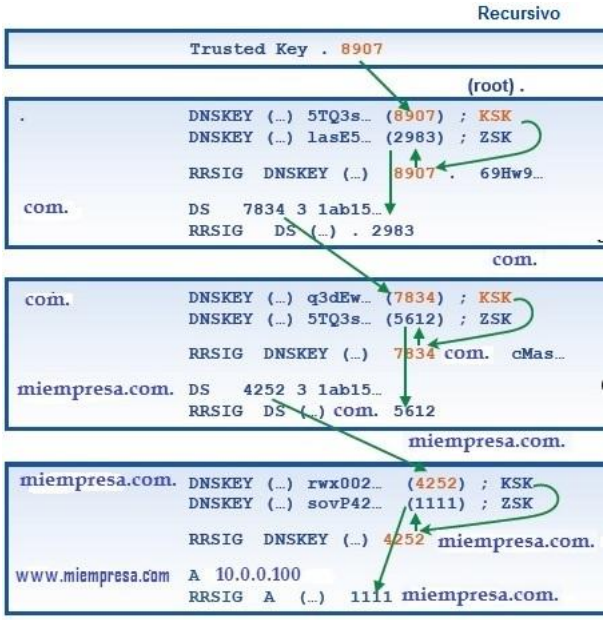

Fig. 3. Recorrido de cadena de confianza DNSSEC [6]

3.2. Observaciones finales

A modo de observaciones finales con respecto al proceso de configuración DNSSEC y posterior análisis de tráfico en procesos de resolución de nombre para la arquitectura propuesta, se tiene que:

- El proceso de generación de claves, publicación de las mismas y firmado de zonas, es un proceso que no demanda tiempo de ejecución ni de procesamiento, si trata de zonas almacenadas en servidores autoritativos; sin embargo para casos de zonas en niveles superiores como ccTLDs, se recomienda el uso de hardware HSM [9], tal como se describe en "*Guidelines for Deploying* DNSSEC", [10]. En otro orden, se requiere prestar especial atención a la ubicación de los archivos de claves y la edición de los archivos de zona, ya que un error de sintaxis o de inconsistencia en nombres provocaría que no se lograra el firmado de la misma. Se sugiere al finalizar el proceso de firmado, la verificación mediante comandos de comprobación de configuración *(ej: named-checkconf).*

- La creación de la "cadena de confianza" mediante la publicación del registro DS en zona

padre, es un proceso que en situaciones reales, requiere la distribución por medios seguros, tales como vía email o soportes de almacenamiento.

- Con respecto a la configuración de clave pública de validación inicial (KSK root), requiere especial atención al momento del agregado de la misma a los archivos de configuración de los servidores que posteriormente realizaran el proceso de validación de firmas, ya que de existir alguna inconsistencia, provocaría una falla en toda la verificación de la cadena de confianza.

- Es necesario la configuración de registros de eventos mediante archivos logs, ya que brindan información importante al momento de realizar comprobación de errores tanto en configuración generales como en procesos de validación de firmas.

- Un aspecto importante a tener en cuenta, es con respecto al tiempo de validez de las zonas firmadas, el cual, por defecto caduca a los treinta días del firmado de las mismas. En caso de expirar dichas firmas, el proceso de validación devuelve un error general y por lo tanto no es posible la resolución de nombres. El proceso de refirmado se realiza simplemente mediante el comando correspondiente.

- Otra observación relevante, se obtuvo al analizar el proceso de validación de firmas, donde se pudo comprobar que un servidor autoritativo con características DNSSEC, ahora debe responder a dos consultas adicionales, un registro DNSKEY y un registro DS, ya que el mismo es responsable de las zonas firmadas que contiene y de las claves KSK que le fueron delegadas mediante registros DS.

- Con respecto al servidor recursivo configurado con DNSSEC, se observa que, en una primera instancia en donde al nombre de dominio consultado no se encuentra almacenado en cache, se requieren tres veces más de tiempo de respuesta y la carga de tráfico (consulta/respuesta), se incrementa en 8 veces más, si se lo compara con un escenario DNS no seguro. Pero, una vez que la consulta se almacena en cache, una próxima solicitud se responde en un solo paso, por lo que la función de almacenamiento en cache se transforma en una herramienta de gran utilidad, al mejorar considerablemente la perfomance de DNSSEC.

4. Conclusiones

Considerando las tareas de configuración, pruebas y análisis de tráfico de red, la puesta en marcha de tales aspectos de seguridad no se alcanza de manera inmediata, ya que requiere estar altamente familiarizado con el protocolo y el funcionamiento del mismo.

Desde la perspectiva de un cliente DNS recursivo, se destaca la funcionalidad de almacenamiento en cache, ya que la misma “absorbe” de manera eficiente, el impacto en los procesos de validación de firmas, necesarias para una resolución de nombres segura.

A la fecha, siguen surgiendo casos de implementación y documentación al respecto, lo que sumado a la adopción para el dominio .ar, permitirán continuar con las pruebas de implementación y análisis de perfomance sobre tráfico de consulta/respuesta sobre un entorno real como lo es Internet.

5. Referencias

[1] ICANN Research, TLD DNSSEC Report, http://stats.research.icann.org/dns/tld_report/

[2] ARENDS, R., AUSTEIN, R., LARSON, M., MASSEY, D., AND ROSE, S. RFC 4034: Resource Records for the DNS Security Extensions, Marzo 2005.

[3] NIC Ar. https://nic.ar/Enterate/Noticias/primera-ceremonia-de-dnssec-para-la-zona-ar

[4] Ron Aitchison: Pro DNS and BIND. APRESS, New York (2011), pp. 320-322.

[5] KOLKMAN, O, GIEBEN, R. RFC 4641: DNSSEC Operational Practices, Setiembre 2006.

[6] RIPE Network Cordination Centre. DNSSEC Training Course. https://www.ripe.net/support/training/material/dnssec-training-course/DNSSEC-Slides-Single.pdf.

[7] DNSSEC Tools Project. http://www.dnssec-tools.org/

[8] Open DNSSEC Project. https://www.opendnssec.org/.

[9] DNSSEC Practice Statement for the Root Zone KSK Operator. ICANN. https://www.iana.org/dnssec/icann-dps.txt. pp 44.

[10] Guidelines for Deploying DNSSEC. Antti Ristimäki (CSC/Funet), Tuukka Vainio (University of Turku), Kaisa Haapala (CSC/Funet). http://services.geant.net/cbp/Knowledge_Base/Campus_Networking/Documents/CBP-07_guidelines-for-deploying-DNSSEC.pdf. pp 9.