Un caso de estudio en Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC). Resultados parciales

Ernesto Sánchez[1], Javier Díaz[2], Daniel Arias Figueroa[1], Sergio Rocabado[1],

[1] Centro de Investigación en Informática Aplicada (C.I.D.I.A.). Universidad Nacional de Salta. Argentina.
[2] Universidad Nacional de la Plata. Provincia de Buenos Aires. Argentina
{esanchez, daaf, srocabad}@cidia.unsa.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 presenta resultados parciales de la etapa inicial del proyecto de investigación Nº 1223/0: "Extensiones de Seguridad para el Sistema de Nombres de Dominio" del Consejo de Investigación de la Universidad Nacional de Salta, donde se exponen los aspectos teóricos de DNSSEC y una alternativa para la implementación, considerando que el dominio .ar, aún no se encuentra firmado. Se presenta también un análisis de los nuevos Registros de Recursos presentes en DNSSEC, considerando sus longitudes en bytes, lo que permitirá realizar futuras estimaciones de consumos de recursos tales como ancho de banda, uso de memoria y procesador.

Keywords: DNSSEC, Extensiones de Seguridad para DNS, Sistema de Nombres de Dominio, Universidad Nacional de Salta

1 Introducción

Desde su creación el Sistema de Nombres de Dominio, ha carecido de un diseño que asegure la comunicación entre las partes que intervienen en el proceso de resolución de nombres, lo que lo expuso a lo largo del tiempo, a constantes "ataques" de las más diversas formas, ataques que van desde la Denegación de Servicio, intercepción de los mensajes intercambiados entre clientes y servidores, suplantación de identidad mediante la técnica de Spoofing, hasta la técnica conocida como Envenenamiento de Cache.

Al igual que ha ocurrido con otros protocolos que se diseñaron en los primeros tiempos de Internet: IPv4, SMTP y FTP, por citar algunos, raramente se incluían medidas de seguridad como la integridad, autenticación y confidencialidad, las que tuvieron que ir añadiéndose a posteriori; en algunos casos, se rediseño el protocolo y en otros como es el caso de DNS, por medio de extensiones de seguridad.

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. [1].

Dada la condición de sistema jerárquico, es que el proceso de migración a tales extensiones de seguridad, no tiene una fácil solución y mucho menos rápida, ya que se hace necesaria una implementación a escala global. En [2], se muestra la situación actual de la implementación global de DNSSEC y cómo evoluciona la misma, donde se observa que a Marzo 2012, solo 81 países han adoptado estas extensiones, y el resto se encuentra en fase de prueba o bien aún no se han implementado.

En base a lo expuesto en el párrafo anterior, es que, desde el Centro de Investigaciones en Informática Aplicada (C.I.D.I.A.) y en el marco del proyecto de investigación Nº 1223/0: "Extensiones de Seguridad para el Sistema de Nombres de Dominio" del Consejo de Investigación de la Universidad Nacional de Salta, se desarrollan tareas de estudio del estado del arte de extensiones de seguridad para DNS, para una posterior implementación de un ambiente de pruebas para una arquitectura de DNS seguro.

El presente trabajo presenta resultados parciales de la etapa inicial del proyecto mencionado, donde se exponen los aspectos teóricos de DNSSEC y una alternativa para la implementación, considerando que el dominio .ar, aún no se encuentra firmado. Se presenta también un análisis de los nuevos Registros de Recursos presentes en DNSSEC, considerando sus longitudes en bytes, lo que permitirá realizar futuras estimaciones de consumos de recursos tales como ancho de banda, uso de memoria y procesador.

2 Aspectos generales 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.

El diseño de DNSSEC, se inicio a mediados de los 90, motivado por el creciente reconocimiento de los peligros de envenenamiento de caché DNS. La primera versión de éstas extensiones de seguridad fueron oficialmente publicadas en Enero de 1997 en el RFC 2065, seguida de una versión mejorada que fuera publicada en el RFC 2535

(Marzo de 1999). Luego de experiencias en pruebas piloto de implementación, la versión actual fue presentada en los RFC 4033, 4034 y 4035 (Marzo 2005).

A fin de lograr los propósitos antes descriptos, DNSSEC hace uso de cuatro nuevos Registros de Recursos y dos bits (CD = Comprobación Desactivada y AD = Dato Autenticado) presentes en el encabezado de un paquete DNS. Por otro lado, un Servidor Resolver que realiza una consulta, utiliza los mecanismos de extensión para DNS (EDNS0) y activa el bit DO (DNSSEC OK), presente en el Registro de Recurso Opcional (RR OPT). Por lo tanto, mediante la activación del bit anterior un Resolver esta indicando que tiene la capacidad de procesar información relacionada con DNSSEC. Es así que, un Servidor de Nombres que recibe solicitudes en las cuales el bit DO no estuviera presente, no responde con Registros de Recursos relacionados con DNSSEC, con lo que se contribuye a mejorar el rendimiento de DNS, ya que evita tener que retornar información que posteriormente no será procesada.

2.1 Nuevos Registros de Recursos

Los Registros de Recursos para DNSSEC son: [3].

- 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 Puntos de Entrada Seguros (SEPs)

En una estructura de DNS con soporte para las extensiones de seguridad, tanto el servidor con autoridad sobre una zona (Maestro o Esclavo), así como el servidor (Resolver) que realiza las consultas, ambos deben estar configurados con soporte para DNSSEC. La resolución DNSSEC comprueba si la consulta corresponde a una zona asegurada con estas extensiones. La respuesta es positiva cuando el destino se encuentra en zona segura, es decir que el archivo de zona esta criptográficamente firmado, lo que garantiza una respuesta genuina al Resolver que realizó la consulta. A

los nodos superiores de estas estructuras se los conoce como Puntos de Entrada Seguros (SEP), por lo tanto, la lista de SEPs es el equivalente en la práctica de los proveedores de certificados CA de los navegadores web [4].

En términos generales, DNSSEC se asegura de que tiene un solo SEP apuntando a la raíz de la zona DNS. Una cadena de confianza enlaza la clave de la firma con el resto de zonas que están por debajo en la jerarquía. Esto permite a los clientes de DNSSEC validar las firmas.

2.3 Cadena de Confianza

El proceso de construcción de una cadena confianza es fundamental para la rápida implementación de DNSSEC en una jerarquía DNS, ya que sin ésta característica, cada Servidor Resolver 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.

La siguiente ilustración permite observar los procesos involucrados en la creación de la cadena de confianza:

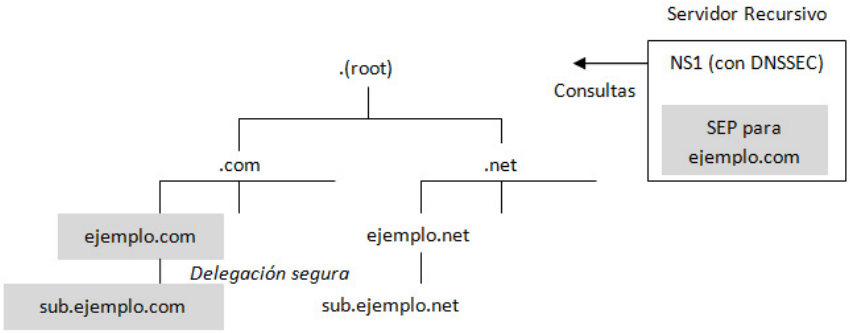

Fig. 1. Creación de cadena de confianza

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 97 los dominios de nivel superior que fueron firmados, de los cuales, 88 tienen puntos de anclaje seguros publicados como registros DS en la zona antes mencionada[5].

2.4 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 [9], 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.

Con respecto a lo citado en el párrafo anterior, cabe destacar que verdaderamente se cumple según estudios comparativos presentados en la última reunión de la IETF (Marzo 2012), donde se destacan las siguientes observaciones [10]:

- Todos los dominios de nivel superior (TLDs) que interactúan con los servidores raíz de la Internet Assigned Numbers Authority (IANA), emplean el modelo KSK/ZSK.

- La afirmación de que la clave KSK, puede ser distinguida de la clave ZSK, observando el bit SEP en el Registro de Recurso DNSKEY, es verdadera.

- Sobre 80 archivos de zonas firmados que fueron observados, solo 5 usan la misma longitud de clave, tanto para la KSK como para la ZSK, el resto tiene configurada la KSK con una longitud de clave mayor sobre la ZSK.

2.5 Un método de validación alternativo (DLV)

En situaciones en las que no sea posible delegar la confianza en un nivel superior de la jerarquía DNS, ya sea porque el nivel superior o niveles intermedios no estuvieran aún firmados, existe la posibilidad de implementar un proceso denominado "Domain Lookaside Validation" [6] [7], el cual proporciona un método alternativo mediante el cual se puede crear y verificar una cadena de confianza, sin la necesidad de delegar la confianza en una zona superior.

DLV provee un punto de entrada adicional (además de la zona raíz), del cual se puede obtener información de validación DNSSEC. Sin DLV, en ausencia de una ruta totalmente firmada desde la raíz a una zona en particular, los administradores que deseen habilitar DNSSEC en Servidores Resolvers tendrían que configurar y mantener múltiples claves de confianza, lo que claramente se convierte en una tarea inmanejable.

Organizaciones como Internet Systems Consortium [8], proveen un repositorio de puntos de entrada seguros (SEPs), a través del cual, las claves pueden ser obtenidas de manera segura. Mediante este tipo de servicio, se ha logrado montar un escenario de pruebas que permitirá la captura y análisis de tráfico de red DNSSEC, con lo que se espera evaluar impactos a nivel de consumo de recursos tales como: uso de procesador, memoria y ancho de banda.

Consideramos que el uso de DLV se presenta en la actualidad como una alternativa que sirve de punto de partida para aquellas organizaciones que necesitan asegurar sus redes privadas con las extensiones proporcionadas por DNSSEC, hasta tanto se logre un mayor despliegue de tales extensiones, en la arquitectura DNS.

3 Cálculo de longitud de nuevos Registros Recursos

El siguiente punto presenta un análisis de los nuevos Registros de Recursos, con respecto a la longitud en bytes de cada uno de ellos, lo que permitirá sentar las bases para posteriores estudios de consumo de recursos tales como ancho de banda, uso de memoria y procesador.

Sin lugar a dudas que las longitudes de los nuevos Registros de Recursos dependen de las longitudes de clave de encriptación y la función del propio Registro. Los cálculos que se presentan a continuación se realizaron a partir de la observación del formato del campo RDATA para cada uno de los Registros de Recursos descriptos en el RFC 4034 [4].

Para todos los casos se consideró el uso de los algoritmos RSA/SHA-1, ya que actualmente se presentan como de uso más frecuente (relación 2:1, frente a RSA/SHA-256), según mediciones realizadas a fines de Febrero 2012 [10]. Otra consideración que se debe hacer es con respecto al campo "Name" del Registro de Recurso, el cual se asume, es representado en formato comprimido [11]. Es decir que

todo nombre de dominio puede ser representado mediante un puntero almacenado en un campo de longitud igual a 2 bytes.

La siguiente tabla, resume los tamaños de paquetes de DNS utilizando los nuevos registros que agregan las extensiones de seguridad:

Tabla 1. Longitud de los nuevos registros DNSSEC.

Registro	Longitud en bytes
DNSKEY	16 + long. de clave
DS	36
RRSIG	46 + long. de clave + long. de zona
NSEC	23 + long. de nombre + long. de zona

Como se ha descripto al principio, los cálculos expresados en la tabla anterior, sirven de punto de partida para futuras estimaciones, pero fundamentalmente tiene como objetivo, familiarizar a los administradores con los aspectos fundamentales del protocolo, para una posterior implementación.

4 Conclusiones

A partir del año 2010, fecha en que fuera anunciado el firmado de la zona raíz, los avances que se observan en relación a la adopción y despliegue de DNSSEC ha tenido un importante avance, fundamentalmente por parte de los dominios de nivel superior.

Por el lado del software que permite la configuración de tales extensiones en los servidores de resolución de nombres, se ha observado un fuerte compromiso en los aspectos citados anteriormente. También desde el año 2010, DNSSEC es parte de la mayoría de las implementaciones tales como, Internet Systems Consortium (BIND9), NL-netLabs, Microsoft, Nominum, Secure64 y PowerDns, del mismo modo, herramientas administrativas tales como Opendnssec, han acompañado este crecimiento.

Aún así, DNSSEC se presenta en la práctica, como un conjunto de procedimientos complejos, que exige estar familiarizado con el protocolo, por lo que a partir de los resultados del proyecto antes mencionado, se espera proporcionar las herramientas necesarias que permitan acompañar el despliegue global de tales extensiones de seguridad en los entornos operacionales de DNS actuales.

Referencias

1. ARENDS, R., AUSTEIN, R., LARSON, M., MASSEY, D., AND ROSE, S. RFC 4033: DNS Security Introduction and Requirements, Marzo 2005.

2. Status map of DNSSEC deployment in ccTLD and gTLD. <http://www.ohmo.to/dnssec/maps/>. [Consulta: 27 jun. 2012].
3. ARENDS, R., AUSTEIN, R., LARSON, M., MASSEY, D., AND ROSE, S. RFC 4034: Resource Records for the DNS Security Extensions, Marzo 2005.
4. Amberg, Eric: Trusted name resolution with DNSSEC. In: Linux Magazine Issue 90, pp. 65. (2008).
5. TLD DNSSEC Report, Internet Corporation for Assigned Names and Numbers (ICANN). <http://stats.research.icann.org/dns/tld_report/>. [Consulta: 3 jul. 2012].
6. ANDREWS, M, WEILER, S. RFC 4431: The DNSSEC Lookaside Validation (DLV) DNS Resource Record, Febrero 2006.
7. WEILER, S. RFC 5074: DNSSEC Lookaside Validation (DLV), Noviembre 2007.
8. Internet Systems Consortium – DNSSEC Lookaside Validation Registry. <https://dlv.isc.org/>. [Consulta: 4 jul. 2012].
9. KOLKMAN, O, GIEBEN, R. RFC 4641: DNSSEC Operational Practices, Setiembre 2006.
10. Lewis, Edward: Comparing TLD DNSSEC Practices with RFCs. At the IEPG on the day before the 83rd IETF. Marzo 2012.
11. Mockapetris, P. RFC 1035: Domain Names - Implementation and Specification, pp. 30. (1987)