INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS MONTERREY
PROGRAMA DE GRADUADOS EN TECNOLOGIAS DE INFORMACION Y ELECTRONICA

TECNOLÓGICO DE MONTERREY.

IMPACTO EN EL DESEMPEÑO DE SERVIDORES RECURSIVOS QUE IMPLEMENTAN DNSSEC

T E S I S

PRESENTADA COMO REQUISITO PARCIAL
PARA OBTENER EL GRADO ACADEMICO DE:
MAESTRO EN ADMINISTRACION
DE LAS TELECOMUNICACIONES

POR
JOSE IVAN RAMIREZ CARREÑO

Monterrey, N. L. Marzo 2007

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS DE LA DIVISIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA

TECNOLÓGICO DE MONTERREY®

IMPACTO EN EL DESEMPEÑO DE SERVIDORES RECURSIVOS QUE IMPLEMENTAN DNSSEC

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN DE TELECOMUNICACIONES

POR:

JOSÉ IVÁN RAMÍREZ CARREÑO

Monterrey, NL. Marzo 2007

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS DE LA DIVISIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA

IMPACTO EN EL DESEMPEÑO DE SERVIDORES RECURSIVOS QUE IMPLEMENTAN DNSSEC

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN DE TELECOMUNICACIONES

POR:

JOSÉ IVÁN RAMÍREZ CARREÑO

Monterrey, NL. Marzo 2007

IMPACTO EN EL DESEMPEÑO DE SERVIDORES RECURSIVOS QUE IMPLEMENTAN DNSSEC

POR:

JOSÉ IVÁN RAMÍREZ CARREÑO

TESIS

Presentada al Programa de Graduados en Tecnologías de Información y Electrónica

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de Telecomunicaciones

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

MARZO 2007

Dedicatoria

A mis padres, Araceli y José Luís por apoyarme incondicionalmente y mostrarme con su cariño y ejemplo a dar siempre lo mejor.

A mi hermana Arely, por apoyarme en la distancia.

A Sel, por apoyarme incondicionalmente en mis decisiones.

A mis amigos, por sus muestras de apoyo y solidaridad.

A Dios, por acompañarme en todos los proyectos y retos que he emprendido

Agradecimientos

Agradezco enormemente a mi asesor Dr. Carlos Mex por su paciencia y disciplina para poder conseguir los objetivos planteados en este trabajo de investigación.

Agradezco también a mis sinodales Dr. Campuzano y M.C. Parra que compartieron conmigo sus experiencias y valiosa retroalimentación para enriquecer los resultados que aquí se han presentado.

Agradezco especialmente a Gustavo Lozano del NIC MX por las facilidades otorgadas para la realización de las investigaciones y pruebas de simulación, además de compartir su experiencia y conocimiento en esta disciplina.

Resumen

Internet es el medio de comunicación más importante de nuestros días. Sin embargo la demanda exponencial y la creciente explotación de vulnerabilidades de este servicio ha generado que la comunidad científica ponga especial atención en el estudio de nuevas y mejoradas versiones de seguridad de los diversos protocolos que permiten la operación actual de Internet.

DNSSEC es una de las extensiones de seguridad más importantes desarrolladas en los últimos años, que permite robustecer el *servicio de nombres de dominio* DNS considerado como uno de los elementos críticos dentro de la arquitectura de Internet.

En el presente trabajo se analiza el impacto en el desempeño que producirá la implementación de estas nuevas extensiones de seguridad en los servidores recursivos de DNS, caracterizando principalmente las afectaciones en recursos como *CPU, Memoria Caché, Ancho de Banda y Tiempos de Repuesta* necesarios para la correcta operación de este nuevo protocolo denominado DNSSEC.

Índice

Lista de Figuras

Lista de Gráficas

Lista de Tablas

Capítulo 1. Introducción

ANTECEDENTES

A principios de los años 70 surge un proyecto experimental de la milicia norteamericana denominado ARPANET, mejor conocido como el antecesor de lo que es hoy es la red de Internet.

La función principal de este proyecto era el intercomunicar y compartir información a través de una red de computadoras localizadas a lo largo de los Estados Unidos de Norteamérica. Conjuntamente con este proyecto se comenzó el desarrollo de nuevos y diversos *protocolos de comunicación* con la finalidad de coordinar las operaciones de comunicación entre los diferentes participantes que deseaban intercambiar su información a través de la red.

Desafortunadamente la alta penetración y comercialización que ha tenido Internet en nuestra actividad diaria, ha llevado a que muchos de esos protocolos diseñados hace más de 30 años sean susceptibles a la explotación de vulnerabilidades y que permiten realizar ataques hacia la infraestructura y servicios de Internet.

Uno de los protocolos que más ampliamente ha sido utilizado y que permite una operación amigable con Internet es el servicio de nombres de dominio (*Domain Name Service* por sus siglas en inglés). Este servicio permite la traducción entre direcciones de IP y los nombres de domino, las cuales son mucho más fáciles de recordar y utilizar para el ser humano.

DNS es uno de los principales servicios utilizados por las diversas aplicaciones que se desarrollan en Internet, sin embargo a partir de los años 90, se han publicado un gran número de documentos enfatizando las diferentes *vulnerabilidades y ataques* a los que esta expuesto este protocolo definido originalmente por *Paul Mockapetris* en el año 1987.

La creciente aparición de problemas relacionados con la seguridad en Internet y en general de cualquier tipo de redes de comunicaciones ha llevado a la búsqueda constante de fortalecer con nuevas extensiones de seguridad gran parte de los protocolos que se han desarrollado desde los inicios de Internet, *DNS* no es la excepción.

Acorde con un estudio realizado por Gartner en el 2006, se puede identificar que los ataques hacía la infraestructura de DNS ocurren se materializan con mayor frecuencia gracias a la utilización de técnicas conocidas como "pharming" que consiste básicamente en explotar vulnerabilidades de envenenamiento del servidor recursivo con la intención de redireccionar el tráfico hacía otro servidor destino sin que el usuario final pueda notar el direccionamiento.

Este tipo de ataques a través del DNS ha dado permitido la existencia de fraudes electrónicos, robos de identidad bancaria e incluso negaciones de servicio importantes hacía sitios de Internet. Por mencionar algunos casos podemos enumerar los siguientes ejemplos:

- En enero de 2005, el nombre de dominio de Panix, un ISP de Nueva York, fue redireccionado a un sitio web en Australia.
- Hushmail, un proveedor de Secure e-mail, fue atacado mediante pharming el 24 de Abril de 2005.

El pharming es considerado en la actualidad un ataque robusto y que aplica prácticamente a cualquier servicio de Internet que haga uso de DNS.

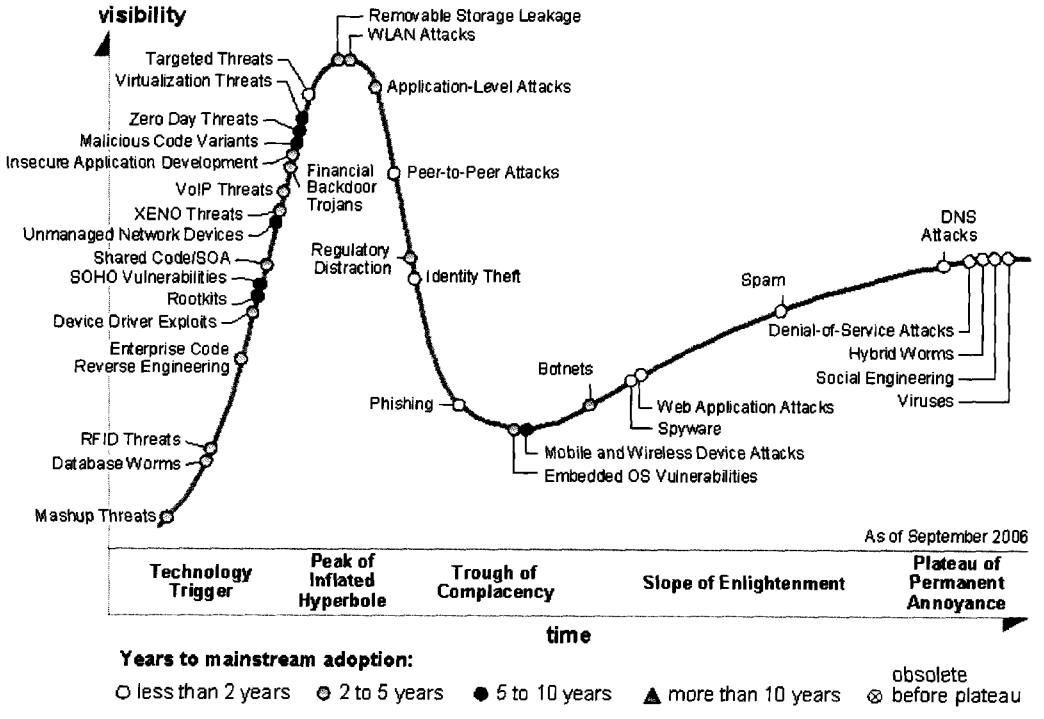


Figura 1: Estudio de Gartner de los principales ataques cibernéticos 2006

La principal propuesta que se ha desarrollado a lo largo de 10 años por el *IETF* (Internet Engineering Task Force) para robustecer la seguridad del DNS, es utilizar un esquema de *llaves públicas y privadas* que permitan garantizar a través del uso de firmas digitales, la autenticidad e integridad de la información que se transmite durante cada una de las peticiones que son realizadas hacia los servidores de DNS. Esta nueva variante al protocolo fue definida por la comunidad científica como *DNSSEC*.

1.1 Descripción del Problema

Aunque esta nueva versión de DNS ofrece un mejor esquema de seguridad comparado con el actual, es importante reconocer que DNSSEC agregará nuevos retos y requerimientos operativos.

El intentar robustecer la infraestructura de DNS a través de criptografía de llave pública y de firmas digitales generará un costo e impacto adicional en los recursos con los que cuentan actualmente los servidores de DNS.

El proceso de intercambio y validación de firmas digitales bajo este nuevo esquema de servicio de nombres de dominio, ha generado principalmente las siguientes expectativas:

¿En qué medida se impactará el desempeño de los servidores y de la red al hacer uso de este nuevo protocolo?

¿Estará la infraestructura actual de DNS preparada para soportar estas nuevas extensiones de seguridad?

Uno de los elementos de la arquitectura de DNS que demanda especial atención bajo este esquema de seguridad es el *servidor recursivo o de caché*, cuya función principal es la de almacenar de manera temporal las peticiones realizadas hacia otros servidores autoritativos de DNS, permitiendo con esta función el poder simplificar los tiempos de respuesta y el ancho de banda requeridos para traducir un nombre de dominio a su dirección IP o vicerversa, sin embargo, bajo esta nueva solución este tipo de servidores recursivos deberá de ser capaz de procesar un gran contenido criptográfico derivado de la validación entre llaves y firmas digitales para de esta manera cumplir con su función dentro de la solución propuesta por DNSSEC.

1.2 Objetivo

El objetivo principal de este documento es analizar e identificar a través de simulaciones, el impacto en el desempeño en variables como CPU, Memoria Caché, Ancho de Banda y Tiempo de Respuesta que demandarán estas nuevas extensiones de seguridad cuando sean implementadas en los servidores DNS recursivos.

La realización de simulaciones en un ambiente de prueba permitirá ofrecer a los administradores de este servicio la posibilidad de conocer y dimensionar los recursos necesarios que deberán de ser considerados durante la implementación de este nuevo protocolo.

1.3 Justificación

La función del servidor recursivo dentro de la arquitectura de DNS lo hace que sea uno de los elementos que mayor cantidad de operaciones y validaciones criptográficas tenga que realizar ante este nuevo esquema de seguridad.

Por tal motivo es importante identificar los requerimientos necesarios para el correcto funcionamiento de este tipo de servidores con la intención de garantizar el éxito y viabilidad de implementación de este nuevo protocolo en los ambientes de producción de las empresas, universidades o proveedores de servicio.

1.4 Contribución

Para realizar dichas simulaciones se ha recolectado tráfico real de los servidores de caché del ITESM Campus Monterrey con la finalidad de caracterizar primeramente el comportamiento en producción del protocolo DNS tradicional, esto permitirá posteriormente analizar y comparar el impacto que tendrá el agregar las nuevas extensiones de seguridad a ese mismo tráfico al replicarlo en un ambiente simulado.

Las simulaciones presentadas en este documento intentan reproducir en lo posible la cantidad de peticiones recursivas e iterativas que el servidor del ITESM Campus Monterrey tiene que realizar hacia los diferentes servidores autoritativos de dominio necesarias para resolver una petición de DNS, con ello se garantiza que el procesamiento criptográfico al que estará sometido este servidor será lo más semejante a la realidad o de un ambiente en producción.

Capítulo 2. Marco Teórico

2. Servicio de Nombres de Dominio (DNS)

Internet es la red computacional más grande del mundo en la cual interactúan millones de usuarios. Desde la perspectiva de un entorno de infraestructura de red cada nodo o recurso con el que se desea establecer una comunicación debe tener asignada una dirección IP, por ejemplo *220.120.200.4*.

Para tener acceso a cualquiera de estos nodos o recursos de la red de una manera más accesible o amigable para el usuario, es decir que no se tenga que recordar cada una de las direcciones IP de cada destino con los que se desee comunicar, se diseñó originalmente un archivo denominado *hosts.txt*.

El archivo *hosts.txt* fue la primera solución que permitió el mapeo de cada una de las direcciones IP con un nombre de host o nodo, de tal manera que fuera más fácil de recordar cuando los usuarios deseaban establecer una conexión con algún dispositivo de la red (Albitz, 2006).

Este esquema fue utilizado inicialmente por ARPANET a principios de los años 70's cuando el archivo *hosts.txt* era mantenido de manera centralizada y disponible para descarga de cada uno de los nodos participantes en la infraestructura de red. Esta solución funcionó muy bien mientras la cantidad de dispositivos era relativamente baja (Aproximadamente 100 equipos).

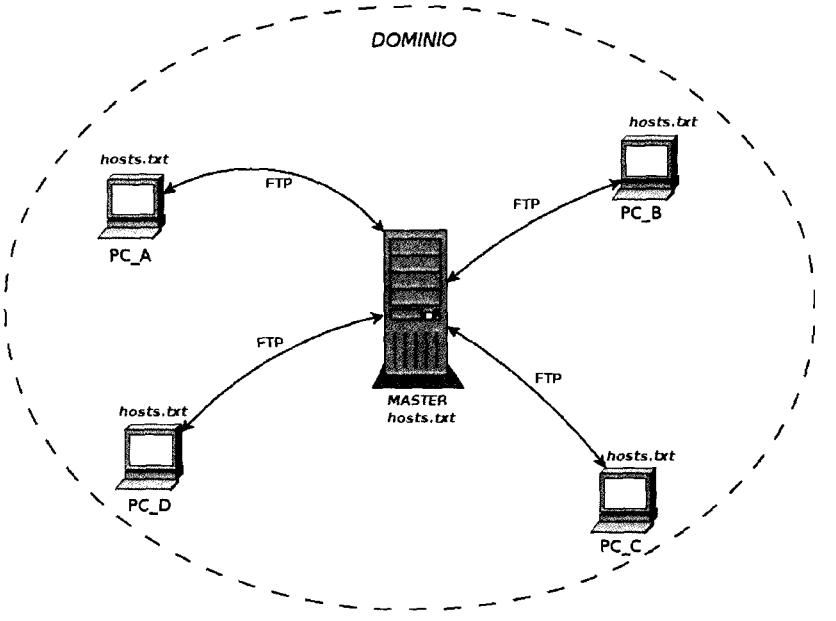


Figura 2: Esquema inicial de Nombres de Dominio (hosts.txt)

La fuerte penetración y comercialización del Internet en los años 80's, llevó a un incremento exponencial en la cantidad de nodos que actualmente forman parte de la red más grande del mundo, considerando impráctico el esquema de centralización de nombres que proponía el archivo *hosts.txt* debido a lo extenuante que era para los administradores el tener actualizado el contenido de dicho archivo y a la poca escalabilidad que representaba dicha solución (Albitz, 2006).

El esquema anterior presenta principalmente las siguientes problemáticas:

- Posibilidad de existir nombres duplicados dentro de dominio.
- Falta de consistencia y actualización dinámica de los nombres del dominio.
- Tráfico y sobrecarga hacia un solo punto de la red.

En el año de 1987, Paul Mockapetris diseñó una propuesta para resolver la problemática de escalabilidad y de administración de los nombres de los diferentes nodos de la red. Propuso un esquema que permitía la descentralización de las operaciones de gestión de los nombres de dominio entre diferentes entidades que forman parte de la infraestructura de Internet. Este enfoque permite generar una *base de datos distribuida jerárquicamente* que ayuda a la administración y el balanceo de carga para la traducción de los nombres de los dispositivos hacia sus respectivas direcciones de IP y viceversa. A este esquema se le conoce hoy en día como servicio de nombres de dominio DNS (Mockapetris, 1987).

Las características principales de este esquema son:

- Arquitectura Cliente-Servidor.
- Base de Datos Distribuida
- Estructura Jerárquica

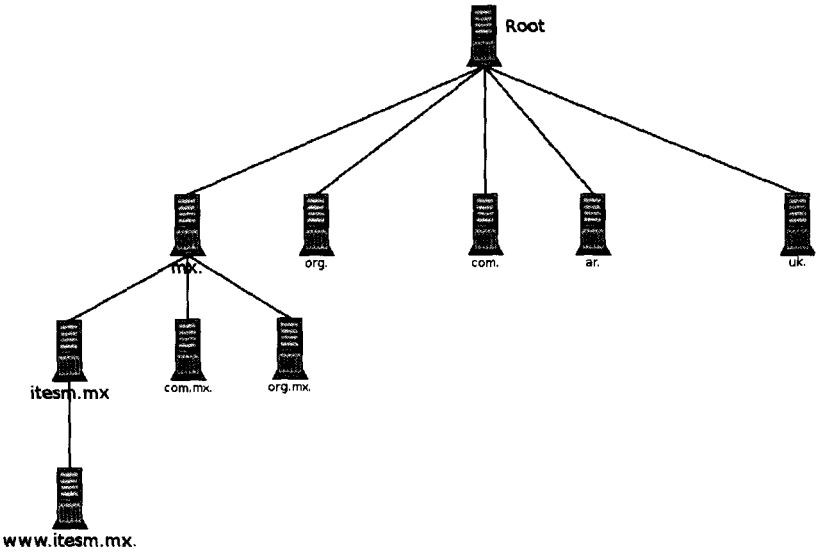


Figura 3: Esquema Actual de Nombres de Dominio (DNS)

2.1 Conceptos básicos

Acorde con Mockapetris, dentro de la operación del esquema de DNS participan tres componentes principales:

- Los *Clientes DNS (resolvers)*, un programa cliente DNS que se ejecuta en la computadora del usuario y genera peticiones hacia un servidor de nombres de dominio. *(Por ejemplo: ¿Qué dirección IP corresponde a* www.itesm.mx*?).*
- Los *Servidores DNS (name servers)*, son los encargados de responder a las peticiones realizadas por los clientes. Existen principalmente 2 tipos de servidores de nombres:
    - Servidor de nombres autoritativo
    - Servidor de nombres recursivo o de caché.
- Las *Zonas de autoridad*, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y en ocasiones a sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

Un nombre de dominio usualmente consiste en dos o más partes (técnicamente denominadas *etiquetas*) las cuales se encuentran separadas por puntos. Por ejemplo, www.itesm.mx.

- Cada nombre de dominio inicia por la derecha con un punto ("."), explícito regularmente y que hace referencia al nodo raíz (root).
- A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior <*Top Level Domain*>, por ejemplo la etiqueta ".mx" es el TLD de www.itesm.mx . Este tipo de etiquetas a su vez se clasifican en:
    - *Código de país - TLDs (ccTLDs).* Dominios asociados con países o territorios. Existen más de 240 ccTLDs como por ejemplo mx (Mexico), us (USA) o jp (Japón).
    - *Genéricos TLDs (gTLDs).* Dominios especializados que representan grupos o asociaciones con los mismos intereses u ocupación, por ejemplo .edu, .gob, .mil.
- Cada etiqueta a la izquierda especifica una *subdivisión o subdominio*. En teoría, esta subdivisión puede tener hasta 127 niveles, en donde cada etiqueta puede contener hasta 63 caracteres, pero restringido a que la longitud total del nombre del dominio no exceda los 255 caracteres.
- Finalmente, la parte más a la izquierda del dominio representa el nodo hoja mejor conocido como el nombre del equipo al que se desea establecer una conexión (*hostname*).

Existen dos tipos de consultas que un cliente (resolver) puede hacer a un servidor DNS:

- Iterativa
- Recursiva

En las consultas recursivas el servidor repite el mismo proceso básico (consultar a un servidor remoto y seguir cualquier referencia) hasta que obtiene la respuesta a la petición realizada.

Las consultas iterativas, o resolución iterativa, consisten en ofrecer la mejor respuesta o referencia que el servidor de nombres pueda ofrecer a una petición de DNS. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados.

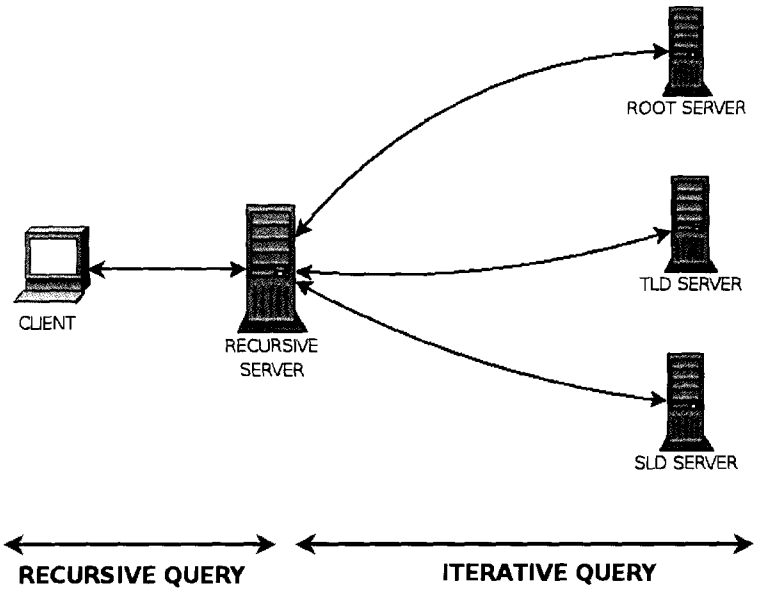


Figura: 4 Tipos de peticiones de DNS.

DNS es un protocolo que se implementa a través de UDP y por razones de desempeño la longitud del paquete se encuentra limitada a 512 bytes. El utilizar conexiones basadas en TCP generaría un alto costo en procesamiento debido a que se debe reservar un puerto para cada conexión que es establecida, de igual manera existiría una sobrecarga en el tráfico de la red debido a que el protocolo de TCP debe realizar un negociación de 3 vías (handshake) previo al establecimiento de la comunicación de datos entre origen y destino (Albitz, 2006).

2.1.1 Resource Record

Albitz define "resource record" (RR), como la unidad más pequeña de información que un servidor de nombres puede entregar durante una petición. Este registro está formado principalmente por los siguientes campos:

Nombre (Name)	*TTL*	*Clase (Class)*	*Tipo (Type)*	*Dato (RDATA)*

- Nombre (Name): contiene el nombre del registro conocido como nombre del equipo (hostname).
- Tipo (Type): contiene un entero de 8 bits que se refiere a alguno de los siguientes tipos de registro:
    - A – Conversión de un hostname a una dirección IP
    - CNAME – Alias para hacer referencia a otro registro.

- MX – Mail Exchange, contiene el nombre del servidor de correo de la zona.
- NS - Servidor de nombres utilizado para delegar una zona.
- PTR – Apuntador utilizado para la conversión de una dirección IP a un hostname.
- SOA – Inicio de la zona de autoridad. (Start of Authority)
- A6 – Conversión de un hostname a una dirección de IPv6.

- *Clase (Class)*: es un campo de 8 bits que describe el contexto del registro. El mayormente utilizado es la clase de Internet (IN).
- *Tiempo de vida (TTL):* es un campo de 32 bits que describe la cantidad en segundos que permite almacenar de manera temporal un registro determinado en la memoria caché de los servidores de DNS.
- *RDATA:* contiene la información del RR que es válida para el campo tipo que ha sido definido previamente.
- *Longitud del campo de datos (RDLength):* almacena la longitud del campo de RDATA.

La estructura del resource record es la siguiente:

Nombre (Name)	*TTL*	*Clase (Class)*	*Tipo (Type)*	*Dato (RDATA)*

Un ejemplo de resource record es:

www.itesm.mx	3600	IN	A	131.178.53.76

De igual manera es importante definir que los *RRset* son un conjunto de resource records RRs caracterizados por tener la misma información en los campos de nombre, clase y tipo, sin embargo el contenido del campo *RDATA* es diferente. Si el campo de RDATA es el mismo, entonces se dice que existen RRs repetidos y uno de ellos deberá ser eliminado para evitar duplicidad.

A continuación se presenta un ejemplo de *RRset* válido:

itesm.mx	*3600*	*IN*	*NS*	*dns1.itesm.mx*
itesm.mx	*3600*	*IN*	*NS*	*dns2.itesm.mx*
itesm.mx	*3600*	*IN*	*NS*	*dns3.itesm.mx*

2.1.2 Name Servers

Como se mencionó anteriormente existen dos tipos de servidores de nombres de dominio: *Autoritativo y Recursivo* conocido este último también como *servidor de caché* (Albitiz, 2006).

Servidores de Nombres Autoritativos

Estos servidores se pueden clasificar en 2 tipos principales de servidores de nombres autoritativos: *maestro (primario) y esclavo (secundario).*

El servidor de nombres maestro contiene los archivos de zona que son creados y editados manualmente por el administrador de dicha zona. Los *servidores de nombres maestro - primario* tienen la capacidad de transmitir los archivos de zona de manera dinámica hacia los *servidores autoritativos secundarios* mejor conocidos como *esclavos.*

Este tipo de comunicación entre servidor maestro y esclavo es conocida como transferencia de zona y consiste principalmente en el envío de una notificación por parte del maestro (DNS Notify) hacia los servidores esclavos indicándoles que el contenido del archivo de zona ha cambiado y que deben proceder a iniciar un proceso de replica del nuevo archivo de zona.

Servidor de Nombres de Caché

Este tipo de servidor es llamado comúnmente servidor de nombres recursivo o de caché y se encarga principalmente de atender las peticiones enviadas por un *stub resolver (cliente)*, para ello realiza búsquedas primeramente en su propia memoria temporal (caché) y de no encontrar respuestas comienza una serie de peticiones iterativas a los diferentes servidores de nombres autoritativos con la finalidad de ofrecer una respuesta al stub resolver que le hizo la petición.

Podemos definir como "caché" al área de memoria del proceso servidor de DNS en el que se va acumulando todos los registros que se obtiene de otros servidores durante el proceso de resolución de nombres de dominio.

2.1.3 Resolvers

Herramientas como los navegadores de red o los clientes de correo utilizan un cliente de DNS conocido como stub resolver. Su función principal es la de codificar las peticiones que son generadas por los usuarios y enviarlas hacia un servidor de nombres recursivo en formato de DNS.

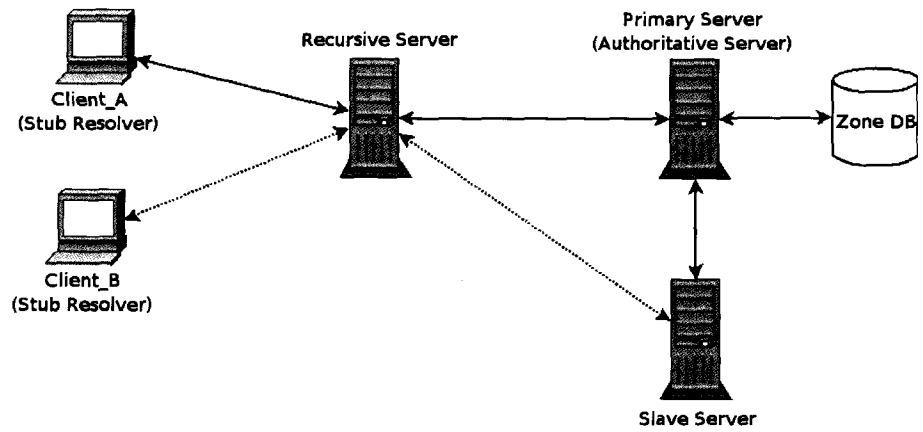


Figura 5: Elementos principales de la arquitectura de DNS

2.2 Cómo funciona el DNS

Con ayuda de los conceptos anteriormente definidos se procede a describir en mayor detalle el proceso de resolución de nombres efectuado por la infraestructura de DNS definida por Paul Mockapetris.

Una de las aplicaciones que realiza una gran cantidad de peticiones al DNS y que resulta familiar para la mayoría de los usuarios es el navegador de páginas web. Cuando un usuario introduce un URL en su navegador como por ejemplo www.itesm.mx, el programa (Explorer, Firefox) contacta al primer componente del DNS denominado stub resolver.

Este primer elemento es el encargado de traducir la petición que ha realizado el usuario y la envía en formato DNS al servidor local comúnmente llamado recursivo o de caché.

El servidor local de nombres revisará primeramente si existe algún resource record en su memoria temporal o de caché que sea válida para la petición que acaba de recibir.

En caso de no existir respuesta dentro del caché del servidor recursivo, comenzará una búsqueda iterativa con cada uno de los servidores autoritativos que forman parte del nombre de dominio de la petición.

Imaginemos que el usuario ha realizado la petición www.itesm.mx del tipo A (address) indicando que desea conocer la dirección IPv4 del servidor que contenga dicha página web.

Los pasos simplificados de la resolución de la petición "www.itesm.mx" son los siguientes:

1.- El navegador envía al stub resolver la petición www.itesm.mx para que sea codificada en formato DNS y sea enviada al servidor de nombres local.

2.- El servidor de nombres local verifica primeramente en su caché si existe algún RR (Resource Record) que corresponda a la petición realizada. En caso afirmativo se regresa al usuario la dirección IPv4 131.178.53.76 finalizando el proceso de resolución de nombres.

3.- Si el servidor de nombres local no contiene ningún RR en su caché para dicha petición, entonces se inicia un proceso de búsqueda recursiva iniciando desde lo más general a lo más particular, por lo que el nombre de dominio debe ser segmentado en cada una de sus etiquetas separadas por puntos. Recordemos que existe un punto explícito al final del nombre de dominio que indica la zona raíz. Para el caso de nuestro ejemplo la segmentación sería la siguiente:

www	**Itesm**	**mx**	**.**
Nombre del equipo (hostname)	Dominio de segundo nivel	Dominio de nivel superior (Country Code TLD)	Zona raíz

4.- La primer búsqueda se realiza preguntando al *servidor raíz* por el dominio *"mx"* este responderá al servidor local con un referencia (referral) indicándole quién es el servidor autoritativo para dicho dominio.

5.- El servidor de nombres preguntará posteriormente al servidor autoritativo del dominio *"mx"* por el servidor *"itesm.mx."*, de igual manera le será devuelto un referral indicándole cual es el servidor autoritativo para dicha zona.

6.- El servidor de nombres local enviará posteriormente una petición al servidor autoritativo para la zona *"itesm.mx."* preguntando si conoce la dirección del equipo "www". Dado que dicho servidor es autoritativo para "itesm.mx" y existe el registro "www" en su archivo de zona, entonces el servidor autoritativo responde al servidor de nombres local con la dirección IPv4 que responde a la petición enviada por la pregunta www.itesm.mx

7.- Finalmente el servidor de nombres local envía al stub resolver del usuario, un RR indicándole la dirección IPv4 obtenida a partir del proceso de resolución. Esta respuesta es almacenada temporalmente en el caché del servidor de nombres de local durante X segundos que indique el campo TTL del RR de la petición encontrada.

A continuación se presenta un diagrama que sintentiza el proceso de resolución para la petición www.itesm.mx.

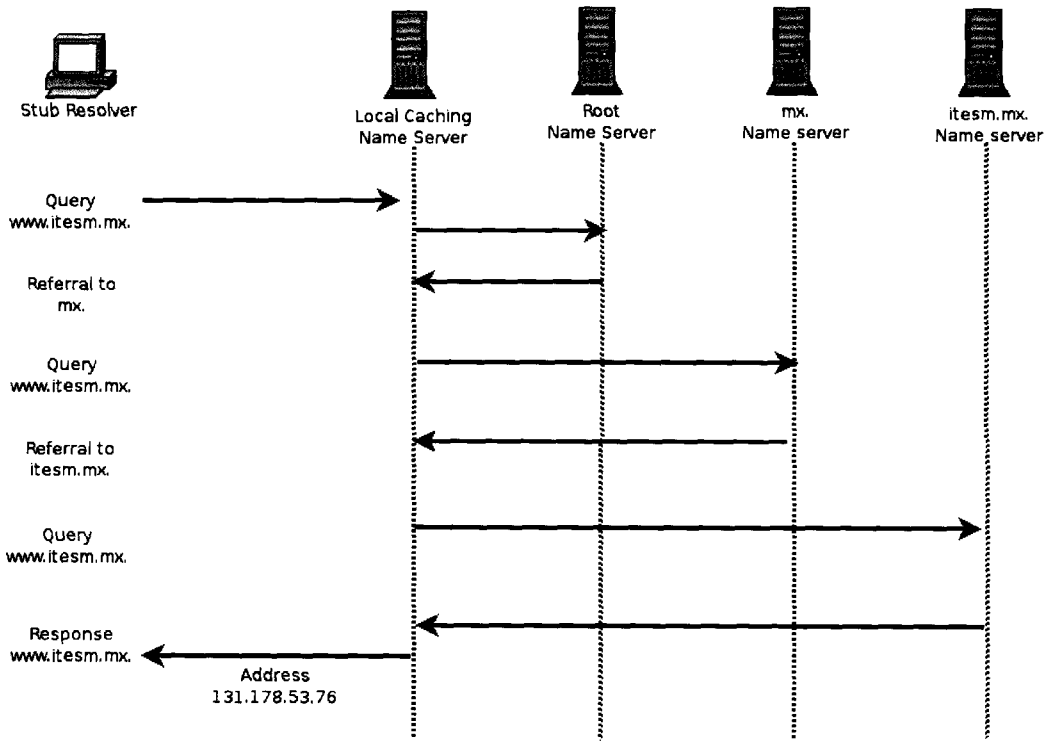


Figura 6: Proceso de resolución de Nombres de Dominio

2.3 Problemas de seguridad del DNS

Dado la naturaleza de DNS de utilizar UDP como protocolo de transporte, existen vulnerabilidades importantes que han sido documentadas y ampliamente difundidas mencionando la manera como pueden ser explotadas por un atacante. Acorde al RFC 3833 podemos mencionar que existen principalmente las siguientes amenazas y vulnerabilidades para el protocolo actual de DNS.

2.3.1 Intercepción de Paquetes

UDP es un protocolo no orientado a conexión que hace un mejor uso de los recursos de la red pero que en contraparte no verifica si la información realmente está siendo enviada por el origen de quien se espera recibir dicha información. Esta característica es diferente en el protocolo TCP, ya que establece un conexión de 3 vías previo a cualquier intercambio de información entre origen y destino, lo cual representa un alto costo para servicios como el DNS.

Para el caso de DNS, los mensajes de intercambio durante el proceso de resolución de una petición, pueden ser fácilmente interceptados por un atacante y descifrados debido a que carecen de mecanismos de encriptación o cifrado.

Esta vulnerabilidad permite ataques del tipo *Impersonalización de Servidor (Caché Impersonation)*.

2.3.2 Predicción del ID

En la actualidad la mayoría de las peticiones de DNS viajan por un medio que carece de encriptación y que además no se verifica la autenticidad entre el origen y el destino de la comunicación. Este aspecto facilita en gran medida la capacidad que un atacante puede tener para suplantar la información que es intercambiada entre los diferentes participantes de la arquitectura de DNS.

El campo que identifica y valida la comunicación cliente-servidor en el DNS es un campo de 16 bits conocido como ID y el cual puede tomar valores que van del 0 al 65536.

Actualmente el atacante cuenta con un gran capacidad en el procesamiento y grandes anchos de banda disponibles, lo cual le permite generar un ataque de fuerza bruta para poder adivinar el ID que viaja en la cabecera de un paquete de DNS.

Si el atacante es capaz de construir una respuesta antes que el servidor de nombres autorizado forme un paquete con el mismo ID que genera un usuario durante su petición, entonces se dice que tiene la capacidad para redireccionar el flujo hacia cualquier destino que el atacante desee, sin que el usuario pueda identificarlo.

Esta vulnerabilidad permite ataques del tipo *Impersonalización de Servidor (Caché Impersonation).*

2.3.3. Caché poisoning

Este tipo de ataques son más robustos y complejos que los anteriormente mencionados.

La característica que tienen en común los ataques de caché poisoning consiste en la inserción de RR en el caché de los servidores de nombres por parte de los atacantes, de tal manera que son "envenedados" durante el periodo que indique el campo de TTL del RR insertado con información incorrecta o maliciosa, generando de esta manera una negación de servicio o bien redirección el tráfico hacia otros servidores con la intención de impersonalizar al destino que el cliente desea contactar durante la petición del DNS.

Los RR más susceptibles a estos ataques son CNAME, NS y DNAME debido a que su función es la de redireccionar el tráfico o la petición hacia otro servidor de nombres, por lo que si el atacante es capaz de introducir información maliciosa en dichos registros tiene la posibilidad de controlar el flujo de las peticiones realizadas.

El procedimiento para realizar el caché poisoning es el siguiente:

1. La víctima genera una petición hacia el servidor de nombres.

2. El atacante captura y responde la petición antes que el servidor de nombres autorizado por medio de la explotación de vulnerabilidades como la predicción de ID y la intercepción de paquetes previamente explicadas.

3. En su respuesta el atacante incluye en el campo de sección adicional del RR información maliciosa que se almacenará de manera temporal (Duración del TTL) en el caché del servidor de nombres de la víctima.

4. Al realizar la inserción de RR el atacante tiene la capacidad de redireccionar las peticiones hacia sus propios servidores o bien producir una negación de servicio en el servidor de nombres de la victima mientras no expire el TTL.

2.4 Extensiones de seguridad al DNS

Como se ha mencionado anteriormente, DNS es vulnerable a ataques de intercepción de paquetes que pueden producir amenazas importantes como el corromper con información maliciosa el caché de los servidores de dominio o bien impersonalizar al servidor de nombres al que se le realiza una petición.

DNSSEC es una versión mejorada que agrega nuevos registros y conserva los previamente definidos por el protocolo tradicional de DNS, por lo que se dice que esta nueva solución es totalmente compatible con el esquema actual de resolución de nombres.

La finalidad de este nuevo esquema de seguridad no es precisamente erradicar los ataques al DNS, si no de mitigar las vulnerabilidades existentes y ofrecer la capacidad a los usuarios de poder detectar cuando un ataque se esta produciendo.

DNSSEC resuelve principalmente dos problemas importantes:

- *Autenticación* de los participantes que intercambian información de DNS.
- Ofrecer *integridad* de la información que es intercambiada a través del protocolo DNS.

Las mejoras que ofrece DNSSEC radican principalmente en la utilización de criptografía para proteger el flujo de información que es trasferido durante las peticiones que son realizadas a los servidores DNS autoritativos y a los servidores recursivos o de caché.

2.4.1 Conceptos básicos de Criptografía

Desde el punto de vista criptográfico, podemos mencionar que existen dos esquemas para cifrar la información que se transmite a través de un medio inseguro y que es vulnerable ante posibles atacantes.

Los esquemas de encriptación son:

- Criptografía simétrica
- Criptografía asimétrica.

Criptografía de llave privada

La *criptografía simétrica* o mejor conocida como *llave secreta*, ha sido utilizada desde hace mucho años y consiste en la utilización de una misma llave para los procesos de encriptación / desencriptación del mensaje que se desea transmitir. Esta característica obliga a que la llave secreta deba ser compartida previamente entre todos aquellos participantes que deseen intercambiar información de manera segura.

El compartir la llave secreta origina un serio problema de administración, ya que de caer en manos de un atacante, el contenido del mensaje se puede ver seriamente comprometido cuando es transmitido.

Actualmente el poder de cómputo y los algoritmos matemáticos utilizados para los procesos de encripción / desencripción son bastante robustos, lo cual permite que este esquema de cifrado sea poco vulnerable a ataques de fuerza bruta en periodos cortos de tiempo.

El esquema de *criptografía de llave privada o simétrica* es mucho más rápido de procesar en los equipos de computo, por lo que se recomienda sea utilizado cuando se requiere transmitir una cantidad considerable de información, sin embargo la complejidad de la administración de la llave secreta limita a que sea utilizado en ambientes de grandes grupos de participantes, en los cuales resulta imposible anunciar un cambio rápido de la llave secreta en caso de que ésta se encuentre comprometida.

La *criptografía de llave simétrica* utiliza principalmente cifradores de bloque y cifradores de flujo. Se recomienda que la longitud mínima de la llave simétrica generada por estos cifradores sea de al menos 128 bits aunque es preferible el utilizar 256 bits en aquellas transmisiones de información crítica.

Los *cifradores de bloque* operan sobre bloques de texto plano y encriptado. El mismo bloque de texto plano siempre se encriptará como el mismo bloque cifrado si se utiliza la misma llave secreta.

Los *cifradores de flujo* operan sobre bloques de texto plano y encriptado ya sea por bit, byte o incluso 32 bits. Cada bit de texto plano podrá cifrarse a un bit diferente incluso si se utiliza la misma llave secreta.

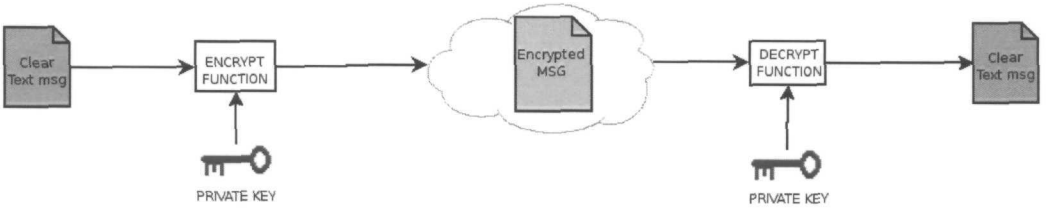


Figura 7: Esquema de encriptación de llave privada

Algunos ejemplos de algoritmos que utilizan criptografía de llave simétrica son:

1. DES (56 bits)
2. IDEA (128 bits)
3. Blowfish (Hasta 448 bits)
4. AES (Hasta 256 bits)
5. RC4
6. RC5
7. RC6
8. SEAL

Criptografía de llave pública

La complejidad de la administración de la llave secreta del esquema simétrico es disminuida considerablemente con la utilización de *criptografía asimétrica*.

La *criptografía de llave asimétrica o pública* utiliza dos llaves matemáticamente ligadas, con las cuales una de ellas es utilizada para codificar la información y la otra para decodificarla en el otro extremo. Bajo este esquema de algoritmos matemáticos es prácticamente imposible generar una llave a partir de la otra debido a que se requiere una alta capacidad de cómputo para la realización de dicho proceso.

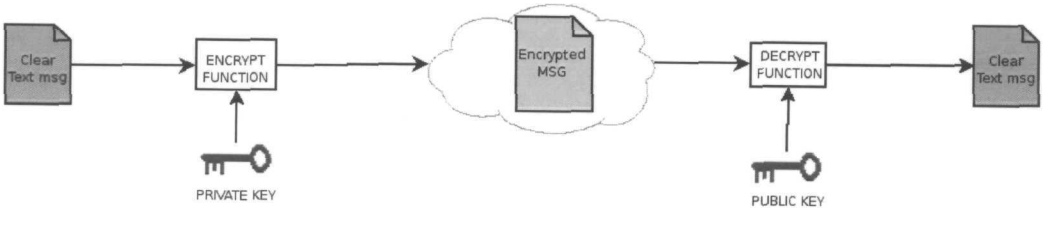


Figura 8: Esquema de encriptación de llave pública

Los algoritmos de llave asimétrica generan un mayor impacto en el procesamiento de los equipos de cómputo debido a la necesidad de validar dos llaves de encriptación / descencriptación, razón por la que se dice son más lentos que los propuestos por el esquema de llave simétrica.

Los algoritmos matemáticos utilizando por la criptografía de llave asimétrica son menos robustos que los de llave simétrica, motivo por el cual se recomienda que la longitud de las llaves sea de al menos 1024 bits. Algunos ejemplos de algoritmos de llave asimétrica son:

1. RSA
2. ECC
3. Rabin
4. ElGamal

La característica *escalabilidad y de mayor flexibilidad* para la administración de las llaves bajo el esquema de criptografía asimétrica es clave para que este enfoque sea utilizado como mecanismo de codificación de información en DNSSEC. Como se ha mencionado con anterioridad, el servicio de DNS opera en un ambiente complejo donde interactúan una gran cantidad de participantes durante el proceso de intercambio de información, razón por la cual esquemas de criptografía de llave simétrica resultan poco escalables para la dimensión de esta infraestructura.

Funciones Hash

Otra herramienta importante para robustecer la seguridad son las funciones de hash o resumen.

Las funciones de hash toman como entrada una cadena de bits o texto de longitud variable llamada pre-imagen y la convierten a una cadena de salida de longitud fija llamada resumen.

Una de las funciones hash más importantes es la denominada *one-way hash* debido a que dada la pre-imagen es muy fácil obtener su resumen, pero es muy difícil el proceso inverso, es decir a partir de la función hash es dificil encontrar la pre-imagen que lo generó a menos que sea especificada. Bajo este esquema es prácticamente imposible encontrar dos o más pre-imágenes que generen la misma función resumen.

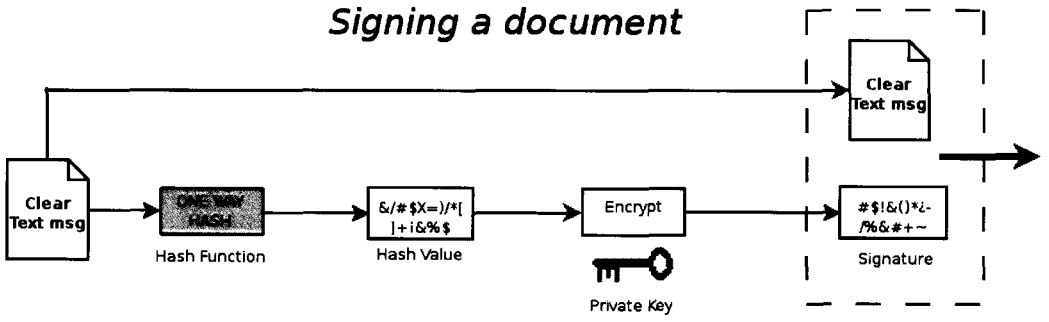


Figura 9: Esquema de función One Way Hash para la generación de firmas digitales

La longitud del resumen se recomienda que sea de al menos 128 bits aunque lo más usado en la actualidad son longitudes de 160 bits. Algunos ejemplos de algoritmos para funciones hash son los siguientes:

- Haval (128 Bits)
- MD2 (128 Bits)
- MD4 (128 Bits)
- MD5 (128 Bits)
- RIPE-MD (128 Bits)
- SHA-1 (160 bits)
- Snefru (128 o 256 Bits)

Las funciones hash son utilizadas para generar firmas digitales de un documento o información que se desea transmitir por la red para con ello garantizar la integridad y no repudiación por parte del remitente.

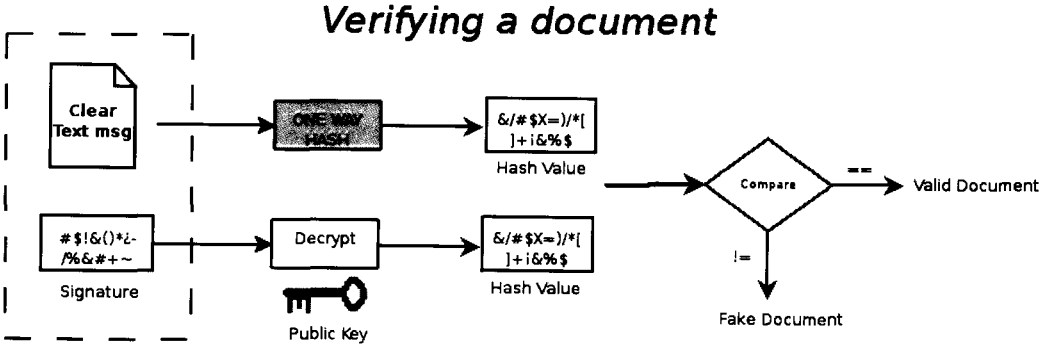


Figura 10: Esquema de verificación de firmas digitales

A continuación se presenta la manera de cómo DNSSEC hace uso del esquema de criptografía para implementar las extensiones de seguridad durante las transacciones realizadas por el servicio de resolución de nombres.

2.4.2 Introducción a DNSSEC

Como se ha mencionado anteriormente, DNSSEC utiliza criptografía de *llave pública o asimétrica* que le permite a través de firmas digitales proveer las características de *autenticación del origen y de integridad* de información anteriormente mencionadas.

La criptografía de llave pública es un esquema en el cual una llave es dividida en 2 componentes principales:

- Llave privada: debe ser protegida y almacenada en algún sitio seguro.
- Llave pública: es publicada y compartida con todos aquellos elementos que participan en el intercambio de información de DNS.

Si el mensaje es transmitido por un canal o medio inseguro pero se codifica utilizando la llave pública, solo podrá ser descifrado por aquel participante que conoce la llave privada. Este procedimiento es conocido como encriptación y permite que sólo el poseedor de la llave privada pueda leer el contenido del mensaje que ha sido transmitido a través de un medio inseguro.

Por otra parte, si el mensaje que se desea transmitir por el medio se codifica utilizando la llave privada, cualquiera que posea la llave pública tiene la posibilidad de descifrar el mensaje que ha sido codificado. Este procedimiento se conoce como *firmado digital del mensaje* y permite que los usuarios que conocen la llave pública *autentiquen el origen de la información,* ya que este mensaje sólo pudo ser generado por aquel participante que conoce exclusivamente la llave privada, razón por la cual esta llave debe permanecer almacenada en un sitio seguro. Este mecanismo de cifrado es el que utiliza actualmente el protocolo DNSSEC.

Otra característica importante de utilizar mecanismos criptográficos es la capacidad poder garantizar que *la integridad de la información* que viaja en un medio o canal inseguro no ha sido alterado o modificado por algún posible atacante.

Por razones de desempeño, el firmado digital para el esquema que plantea DNSSEC, solo se efectúa sobre la función resumen (hash) del mensaje DNS que será transmitido.

DNSSEC utiliza el esquema de criptografía de llave pública para firmar los contenidos de la zona y definirla como segura. Los administradores del servicio de DNS deberán ser los responsables de generar las llaves tanto pública como privada y utilizarlas para el proceso de aseguramiento de dicha zona.

La *llave privada* desde luego deberá permanecer en un sitio seguro ya que su función principal es la de generar las firmas digitales para los RRset que se encuentran definidos en el archivo de zona que se esta administrando.

Bajo el planteamiento de estas nuevas extensiones de seguridad, la *llave pública* deberá de ser introducida en un nuevo registro denominado *DNSKEY* el cual se encargará de anunciar a todos los involucrados en la arquitectura de DNS que esta llave es la que debe de ser utilizada para validar las firmas digitales localizadas en los registros *RRSIG*.

Los registros RRSIG son transmitidos adicionalmente junto con el mensaje de DNS que son intercambiados durante el proceso de resolución de nombres. (Los registros *DNSKEY y RRSIG* son nuevos registros que agregan las extensiones de seguridad y que son detallados posteriormente).

Finalmente, el *resolver* es el encargado de validar con la llave pública de la zona consultada a todas aquellas firmas digitales de los RRset que ha recibido, por lo tanto si la validación es incorrecta, se dice que la información es maliciosa o ha sufrido alguna alteración durante su paso por el medio de transporte.

Este modelo de extensiones de seguridad que plantea DNSSEC fue introducido por el RFC2535, sin embargo el esquema para el manejo de las llaves criptográficas resultó impráctico y poco escalable, por lo que nuevos modelos han sido propuestos.

Actualmente el esquema que mayor importancia tiene dentro del grupo de IETF es la delegación por firma (*Delegation Signer – DS*) el cual corresponde al RFC 3658 y que su vez ha permitido definir los tres documentos más importantes que explican el esquema DNSSEC en la actualidad. Los documentos son los siguientes:

1. *dnssec-intro* (RFC 4033): introducción a los conceptos y requerimientos de las extensiones de seguridad al DNS.

2. *dnssec-records* (RFC 4034): introducción a los nuevos registros que agrega DNSSEC.

3. *dnssec-protocol* (RFC 4035): detalle del mecanismo y la operación de las nuevas extensiones de seguridad.

Nuevos registros

Los cuatro nuevos registros que agrega DNSSEC a la estructura tradicional de DNS y que son descritos en el RFC 4034 son:

1. DNSKEY
2. RRSIG
3. DS
4. NSEC

Es importante mencionar que el hecho de utilizar firmas criptográficas y añadirlas en la estructura del paquete de DNS, genera mayor sobrecarga en la información que se desea transmitir, por lo que los servidores de nombres y los resolvers que implementen DNSSEC deben ser capaces de soportar los mecanismos de extensión propuestos por *EDNS0* en el RFC2671, ya que estos permiten aumentar la capacidad de información (hasta 4096 bytes) que puede transportarse a través de UDP utilizando el protocolo de DNS.

Registro DNSKEY

DNSSEC utiliza criptografía de llave pública para firmar y autenticar los RRset de las zonas definidas como seguras. Las llaves públicas son almacenadas en los RR llamados DNSKEY.

Acorde al RFC 4034, este tipo de registro no debe ser utilizado para el almacenamiento arbitrario de llaves públicas o certificados que no estén directamente relacionados con la infraestructura de DNS.

El valor asignado para el campo de tipo de este RR es 48, además el tipo y la clase están clasificados como independientes. Este nuevo registro no tiene requerimientos especiales para el valor del TTL.

El formato del nuevo registro DNSKEY es el siguiente:

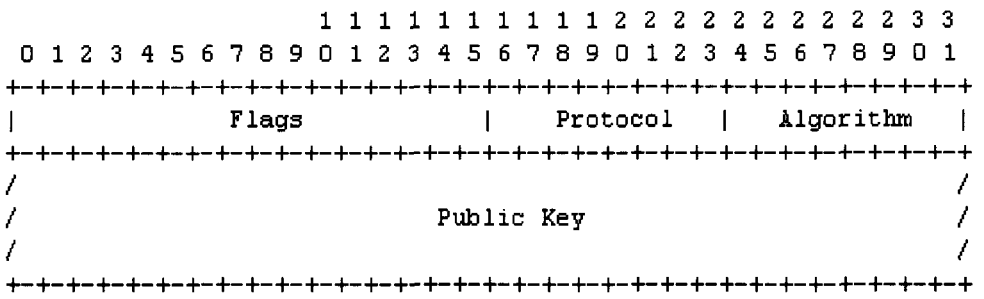


Figura 11: Formato de Registro DNSKEY (RFC 4034)

Un ejemplo del nuevo registro es el siguiente:

```
itesm.mx.       59944 IN DNSKEY 257 3 5 (
                AQOslQdVBrjAehjz/5zRwPh/ii9X3Lw8a/GJmC+HhmPu
                mWehKhqVYn4aPlA4ZdKzp4v+jVjydXqN9VSZwXCT7yIp
                Ninfbw7l59gwCXa1H+dnlqT5KcMljZ4gm3Q82tJjd6Np
                zwQMHe3wct2zf2D8k1ws/CvE8rRCVuzBpiSw+UAfDT37
                RekKTi3GVwbQSTn+zOllVF0QcUyr53far+gXhihGrugD
                jW2RUySbbBPP5lFeyNi/zBfD9UsuR9JJbGLmf7mCqOYT
                SXf3uwMiYg0jZqZos3kU97GAwGD6tdAqLR7E6F0JExbY
                ubekHNYMJB8lx5rT+DFiztBf4wU6gpdUinmV
                ) ; key id = 28551

itesm.mx.       59944 IN DNSKEY 256 3 5 (
                AQPYazZqH/TCEeg7om2C+KRVwXygzFG5RXOxbpzXcet7
                9HApdp2AGadcj197HZKrODZlbhhotvZZnXybGtVVBAEo
                iqtPnkvNJ1KJbw3bTg7quo+BCR6z2UXGn0UCfRR/OtIE
                URvTHwfd8lXLyvEZu5k1/XDRLVmFQ/NGpRpaUGdJ3Q==
                ) ; key id = 26129
```

- Los primeros cuatro campos de textos especifican el ownername, TTL, clase y el tipo de RR (DNSSKEY) respectivamente.
- El siguiente valor indica el tipo de llave criptográfica que está siendo utilizada: 256 para ZSK y 257 para KSK.
- El siguiente campo (valor 3 - DNSSEC) indica el protocolo predeterminado que esta siendo utilizado, si no tiene este valor, el proceso de verificación de firmas será descartado.

Los valores soportados para este campo son los siguientes:

Valor	Protocolo
0	Reservado
1	TLS
2	Email
3	DNSSEC
4	IPSEC
5-254	Disponible para asignación IANA
255	Todos

Tabla 1: Protocolos soportados por DNSSEC

- El siguiente valor definido como 5 especifica que está siendo utilizado RSA/SHA1 como algoritmo de llave pública.

Los valores soportados por el campo de algoritmo son los siguientes:

Valor	Algoritmo
0	Reserved
1	RSA/MD5
2	Diffie-Hellman
3	DSA/SHA-1
4	Elliptic Curve
5	RSA/SHA-1
255	Reserved

Tabla 2: Algoritmos soportados por el protocolo DNSSEC

- El último campo de texto define la codificación en base64 de la llave pública que se esta utilizando.

Registro RRSIG

Las firmas digitales utilizadas por DNSSEC para autenticar los RRset son almacenadas en los registros RRSIG y son utilizados por los resolvers para validar junto con las llaves públicas de los registros DNSKEY, que las firmas digitales son legítimas y que la transacción de información se ha realizado de manera segura.

Acorde al RFC 4034, el valor definido para el tipo RRSIG es 46, además su clase y el TTL debe tener el mismo valor que el del RRset a los cuales representa.

El formato del nuevo registro es el siguiente:

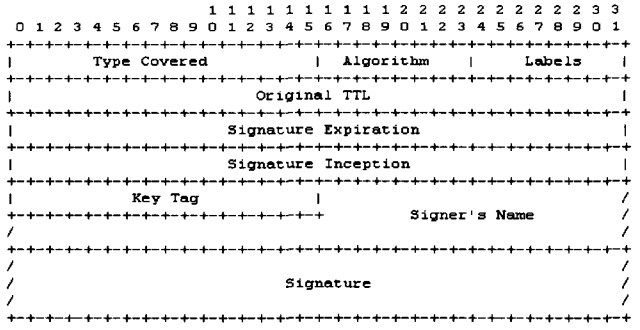


Figura 12: Formato de Registro RRSIG (RFC 4034)

Un ejemplo es el siguiente:

```
www.itesm.mx.    56371 IN RRSIG A 5 3 60000 20070304043507 (
                         20070202043507 26129 itesm.mx.
                         qyELZljCIVtXdvyshTfDo4F+0s7oX1JrXUWAe51br8tG
                         x5RFlvdc4ZxAn41aGsHHtKMNEke+OAXKcZqTjnxVU4nk
                         FrblyWCb4r20WjK89mQF7hxKjcYqXYmbSKDlK9OUuQdN
                         NxoG6LQRF2i3543xQmnrYnKR0f+iq/CqdOi8jYI= )
```

- Los primeros 4 campos corresponden al ownername, TTL, clase y tipo del RR, para el ejemplo en cuestión corresponde a RRSIG.
- El siguiente valor "A" representa el tipo del RR para el cual se está generando la firma digital.
- El valor de 5 corresponde al algoritmo RSA/SHA1 utilizado para la generación de la firma digital. Para ver más detalles de este campo refiérase a la Tabla 2.
- El valor de 3 es el número de etiquetas por las que esta formado el valor del owner namer (www.itesm.mx).
- El valor 56371 corresponde al TTL del RRset del cual se está generando la firma digital.
- 20070304043507 y 20070202043507 representan las fechas de alta y baja del registro RRSIG.

- El valor 26129 representa el identificador de la llave (key tag) con la que se está realizando la firma digital.
- itesm.mx. es el nombre de la zona que realiza la firma digital.
- El texto restante corresponde a la firma digital codificada en base 64.

Nota: El algoritmo, el nombre del firmante y el identificador de la llave indican que la firma digital en base 64 puede ser autenticada utilizando la llave pública contenida en el registro DNSKEY de la zona itesm.mx.

Registro DS

El registro DS es uno de lo más importantes ya que es utilizado para generar la cadena de confianza establecida entre padres e hijos a través de la estructura de DNS y el cual es definido en el RFC 3568.

Este registro hace referencia a un RR del tipo DNSKEY localizado en la zona hijo, por lo que debe almacenar el identificador de la llave, el número del algoritmo de llave pública utilizado y una función resumen de la llave utilizada.

El registro DS y su correspondiente registro DNSKEY tienen el mismo owner name, sin embargo son almacenadas en diferentes localidades. Por ejemplo, el registro DS para "itesm.mx" es almacenado en la zona zona padre ("mx"), mientras que el registro DNSKEY con la llave pública es almacenado en la zona hija ("itesm.mx").

El valor asociado para este tipo de registro es el 43, su clase es independiente y no tiene requerimientos importantes para la asignación del TTL.

El formato del nuevo registro DS es el siguiente:

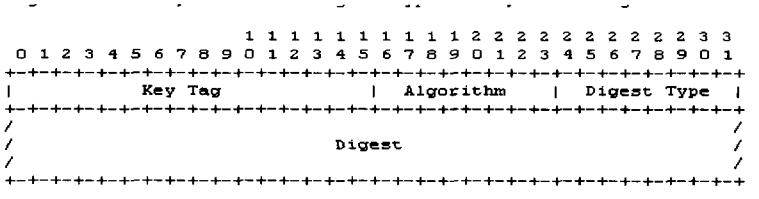


Figura 13 Formato de Registro DS (RFC 4034)

Para el campo "algoritmo" los valores soportados corresponden a los mencionados en la tabla 2 de esta sección.

Los valores de "Digest Type" soportados son los siguientes:

Valor	Algoritmo
0	Reserved
1	SHA-1
2-255	Unsigned

Tabla 3: Algoritmos soportados en la sección Digest Type

A continuación se presenta un ejemplo del registro DS y su correspondiente llave pública.

```
itesm.mx.        55744 IN DS 28551 5 1
                 (23796622E406297082F769D9E0477B1921EF128D )
```

- Los primeros 4 campos del registro DS corresponden al ownername, TTL, Clase y el tipo de RR utilizado (DS).
- El valor 28551 corresponde al valor del identificador (key tag) de la llave pública utilizada por el registro DNSKEY de "itesm.mx.".
- El valor 5 corresponde al número de algoritmo de llave pública utilizado por el registro DNSKEY de "itesm.mx.".
- El valor de 1 representa el algoritmo utilizado para la construcción del resumen de la llave publicada por el registro DNSKEY.
- El texto restante corresponde al valor en hexadecimal de la función resumen (hash) de la llave pública.

Registro NSEC

Es importante indicar que los registros anteriormente mencionados son firmados fuera de línea, por lo que cuando un servidor de nombres recibe una petición, éste regresa la respuesta al "resolver" agregando la firma digital que se encuentra en su archivo de zona previamente almacenado (RRSIG + RRset) .

Sin embargo, ¿Qué sucede cuando la petición que recibe el servidor de nombres, no existe en su archivo de zona (NXDOMAIN)?. La única manera de responder utilizando firmado fuera de línea, es firmando todo aquello que no se conoce o no se tiene registrado en el archivo de zona.

En DNSSEC existe un nuevo registro denominado Next SECure (NSEC), el cual se encarga de almacenar información referente al siguiente registro seguro configurado en la zona.

Para ejemplificar la utilización de registros NSEC se presenta la siguiente zona ordenada de manera canónica.

zone file {
a.mx

g.mx

o.mx

}

Al realizar el proceso de firmado de la zona se tiene (sólo se muestran los registros NSEC para el caso de este ejemplo):

```
zone file{
        a.mx
        a.mx NSEC g.mx (Desde "a.mx" hasta "g.mx" no existe ningún otro registro)

        g.mx
        g.mx NSEC o.mx (Desde "g.mx" hasta "o.mx" no existe ningún otro registro)

        o.mx
        o.mx NSEC a.mx (Desde o.mx hasta  a.mx no existe ningún otro registro)

}
```

Si el resolver realiza una petición preguntando por el registro "x.mx", el servidor de nombres no encontrará nada referente a esa petición en su archivo de zona, por lo que regresará un registro NSEC con su firma digital indicando que no existe ningún registro entre *o.mx y a.mx*. Esta respuesta debe servir para que el "resolver" que envió la petición concluya que "x.mx" no existe y que además es una respuesta de negación de existencia segura dado a que se incluyó la firma digital correspondiente la cual podrá validarse (como en los otros registros anteriormente presentados) con la llave pública de la zona.

Acorde con el RFC 4034, el valor de tipo para el nuevo registro NSEC es de 47, su clase es independiente y el valor de TTL debe ser el mismo que el asignado al valor del registro SOA.

El registro NSEC tiene el siguiente formato:

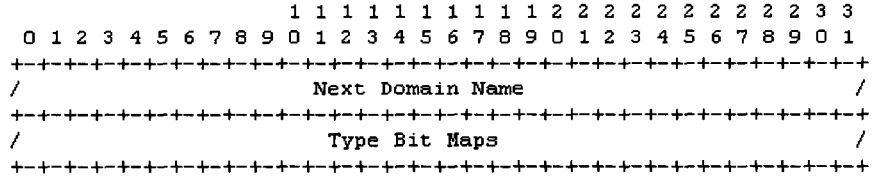


Figura 14: Formato de Registro DS (RFC 4034)

Un ejemplo del registro NSEC para la petición ftp.itesm.mx., el cual no se encuentra configurado en el archivo de zona de itesm.mx. es el siguiente:

```
exatec1.itesm.mx.    50 IN NSEC libreria.itesm.mx. NS DS RRSIG NSEC
exatec1.itesm.mx.    50 IN RRSIG NSEC 5 3 50 20070304043507 (
                         20070202043507 26129 itesm.mx.
                         dkb8y1XWo0ZMbz/w/hPUbX6CFBO4JikLszkuAD3deZWL
                         irAMTpdW8s+GlA5qSvw30B109McFSFzgZ7esfJ/ahTcc
                         prCbnEch8x9eDwqM1NB2Q6DJpVRil8bKWPgQKBYcVPWt
                         al9LlOaWE00eeJSt3QUkTJBmiQ6CFok8s5hHpeY= )
```

- Los primeros cuatro campos de texto corresponden al ownername, TTL, clase y el tipo de registro (NSEC).
- Para el caso de NSEC, el owner name exatec1.itesm.mx representa el valor del nombre autoritativo ordenado canónicamente anterior a ftp.itesm.mx
- El valor de libreria.itesm.mx corresponde al valor del siguiente nombre autoritativo ordenado canónicamente después de ftp.itesm.mx.
- Los valores de NS, DS, RRSIG y NSEC indican que son los RRset asociados con el nombre exatec1.itesm.mx.

Longitud de los nuevos registros

Las características que determinan el tamaño de los paquetes de DNS utilizando los nuevos registros que agregan las extensiones de seguridad se resume en la siguiente tabla:

Registro	Longitud
DNSKEY	16 + Public Key
RRSIG	72 + Owner Name + Signature
DS	16 + Digest
NSEC	Next Domain + Type Bit maps

Tabla 4: Longitud de los nuevos registros DNSSEC

Nuevos bits en el header

Acorde con el documento RFC 4035, DNSSEC agrega tres nuevos bits en header del mensaje de DNS, los cuales tienen especial importancia para los servidores de nombres recursivos.

- DNSSEC OK (DO).
- Checking Disabled (CD).
- Authenticaded Data (AD).

Bit DNSSEC OK (DO)

Este bit debe encenderse siempre que se desee hacer una petición del tipo DNSSEC ya que de esta manera se indica al servidor de nombres de dominio que las extensiones de seguridad son soportadas por el resolver. Si este bit no se enciende entonces el servidor que atiende la petición no agregará ninguno de los nuevos registros que implementa DNSSEC.

Bit Checking Disabled (CD)

Este bit debe encenderse cuando el stub resolver (cliente) que genera la petición de DNS desea realizar la validación de las firmas digitales y no limitarse a que la autenticación sea realizada por el servidor de nombres de dominio recursivo, es decir con este bit le indica que las firmas digitales deben enviarse junto con la respuesta de DNS hasta el stub resolver.

A continuación se presenta un ejemplo de la respuesta recibida por parte del servidor de nombres recursivo al realizar la petición www.itesm.mx utilizando las extensiones de seguridad (DNSSEC).

Es importante observar el tamaño de la respuesta (Ej. 418 Bytes) ya que con el bit de CD se solicita al servidor del nombres recursivo que todas las firmas digitales sean enviadas hacia el stub resolver.

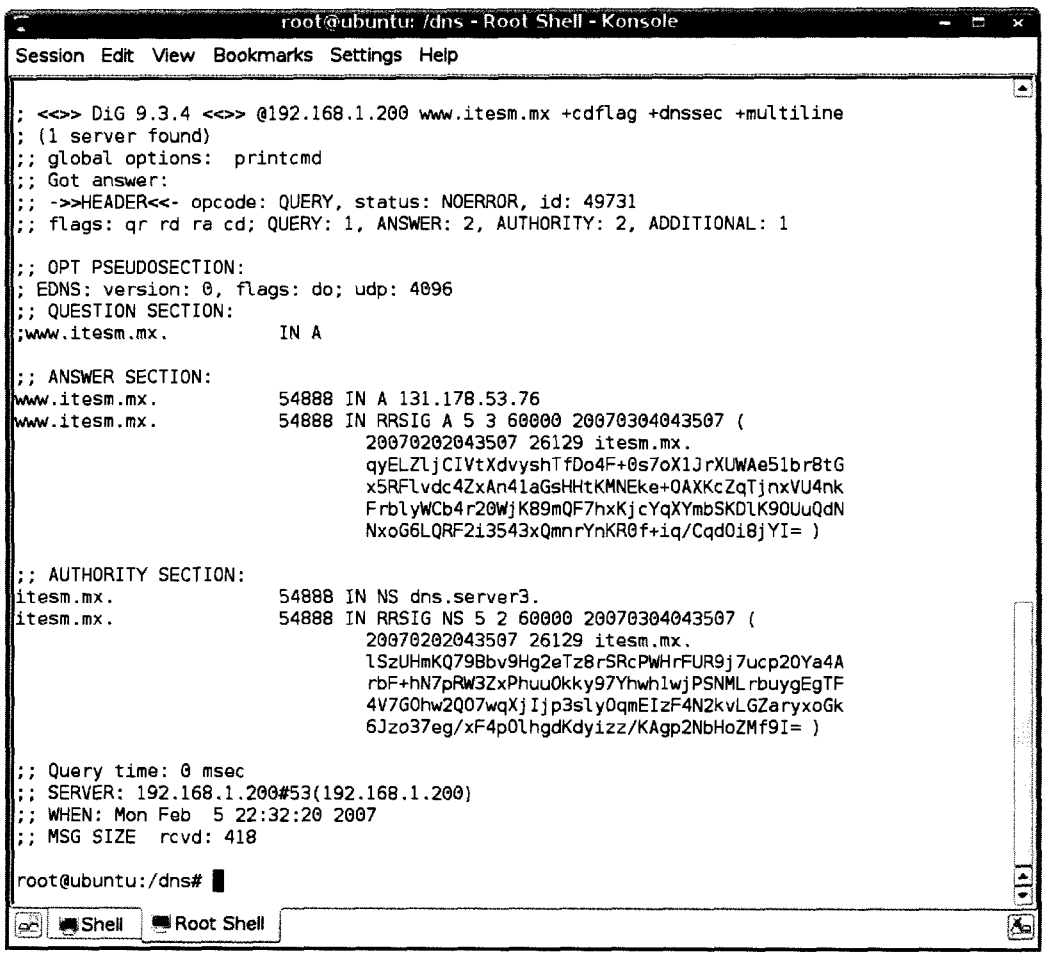


Figura 15: Ejemplo de respuesta DNSSEC con bit CD

Bit Authenticated Data (AD)

Este bit es encendido automáticamente por el servidor de nombres recursivo cuando todos los registros contenidos en la respuesta y en la sección de autoridad (Auhtority Section) han sido autenticados de manera correcta utilizando las firmas digitales y los nuevos registros de DNSSEC.

A continuación se presenta un ejemplo de la respuesta recibida por parte del servidor recursivo con el bit AD encendido, es importante observar que el tamaño de

la respuesta (Ej. 225 Bytes) es mucho menor a comparación de cuando se enciende el bit CD (Checking Disable) donde la longitud de la respuesta fue de casi el doble de tamaño (Ej. 408 Bytes).

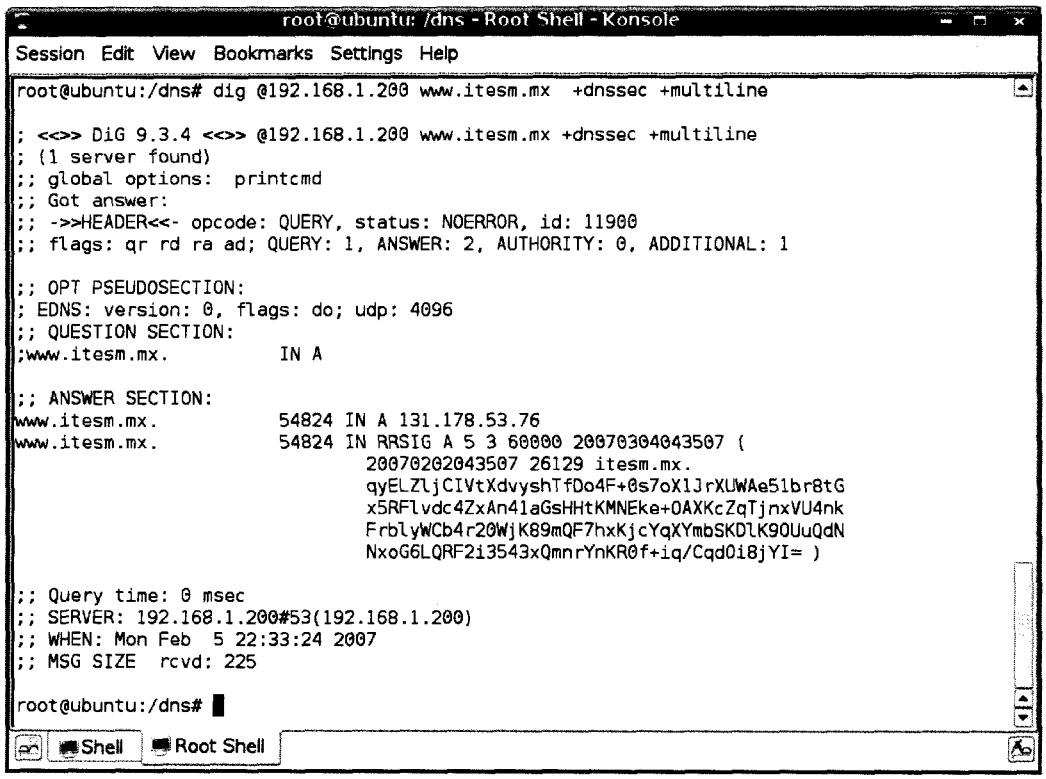


Figura 16: Ejemplo de respuesta DNSSEC con bit AD.

2.5 Cómo funciona DNSSEC

DNSSEC es un modelo que permite la autenticación de extremo a extremo de los participantes de la infraestructura de DNS.

DNSSEC construye una cadena de confianza basándose principalmente en la utilización de dos llaves criptográficas definidas como KSK (Key signing Key) y ZSK (Zone signing key).

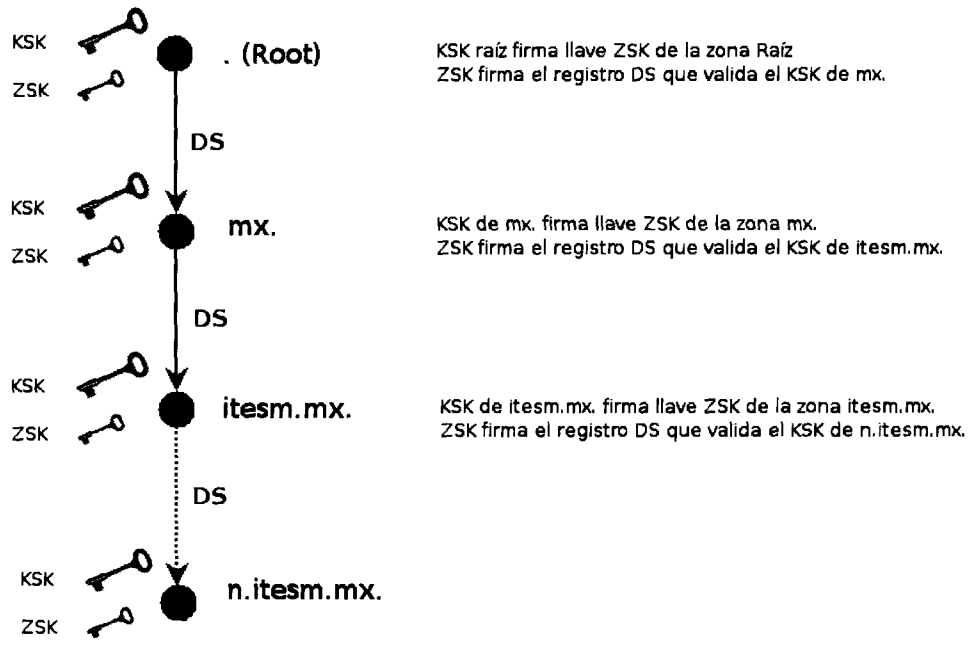


Figura 17: Ejemplo de generación de cadena de confianza utilizando registros DS y llaves KSK / ZSK.

La llave KSK es una llave que generalmente está construida con una mayor cantidad de bits que la llave ZSK. La bandera conocida como punto de entrada seguro (Secure Entry Point) se encuentra encendida. Esta llave sirve principalmente para firmar la llave ZSK.

Por otro lado la llave ZSK, es una llave construida con una menor cantidad de bits pero su tiempo de expiración es mucho menor que la KSK. La llave ZSK sirve principalmente para firmar el contenido de la zona y generar los nuevos registros que agregan las extensiones de seguridad.

Capítulo 3. Metodología

Con la finalidad de analizar e identificar el impacto que generarán estas nuevas extensiones de seguridad en servidores recursivos de DNS, se procederá a realizar la metodología que se detalla a continuación.

1. Análisis de un servidor DNS recursivo de producción
    - Capturar tráfico real de un servidor DNS recursivo con la finalidad de caracterizar primeramente el comportamiento y los recursos del servidor bajo el esquema de DNS tradicional.
2. Construcción del Ambiente de Pruebas
    - Depurar y seleccionar únicamente las peticiones entrantes a dicho servidor recursivo procedentes de los clientes ubicados en la LAN.
    - Reproducir el tráfico entrante en el servidor recursivo de producción solicitando se haga un recorrido "trace" completo de los servidores autoritativos con la intención de identificar la cantidad de peticiones iterativas que deberán de ser realizadas antes de obtener una respuesta. Este procedimiento es importante ya que permite caracterizar el tipo de estrés al que está sometido un servidor recursivo de producción si la respuesta a una petición no se encuentra en su caché.
    - Construcción del ambiente de pruebas para una arquitectura de servidores autoritativos que represente las diferentes zonas de los dominios que desean ser consultados por parte del cliente con base a los resultados de consulta iterativa del paso anterior. En este esquema estarán descartados los servidores de nombres secundarios dado que el objetivo de este estudio es el analizar únicamente los impactos en servidores de caché recursivos.
3. Firmado de las zonas autoritativas
    - Realizar el firmado de las zonas autoritativas, para ello deberán de considerarse los siguientes escenarios para las pruebas de desempeño:
        - DNS Unsigned

- ZSK = 512 bits KSK = 512 bits
- ZSK = 512 bits KSK = 1024 bits
- ZSK = 512 bits KSK = 2048 bits
- ZSK = 512 bits KSK = 4096 bits
- ZSK = 1024 bits KSK = 1024 bits
- ZSK = 1024 bits KSK = 2048 bits
- ZSK = 1024 bits KSK = 4096 bits
- ZSK = 2048 bits KSK = 2048 bits
- ZSK = 2048 bits KSK = 4096 bits
- ZSK = 4096 bits KSK = 4096 bits

El criterio que se está considerando es que la llave KSK sea mayor o igual la llave ZSK.

Una de las mejores prácticas operacionales para este protocolo es considerar el escenario para el cual la zonas son firmadas utilizando ZSK = 1024 y KSK = 2048.

4. Configuración de BIND para el soporte de DNSSEC.

    - Activar los parámetros en el archivo named.conf para el soporte de las extensiones de seguridad.

5. Comparativo Servidor ITESM de Producción DNS vs DNSSEC

    - Analizar el comportamiento considerando un tráfico similar de peticiones por segundo comparada con el servidor de producción del cual fueron extraídas las muestras de DNS tradicional.
    - Reproducir el tráfico entrante hacia el servidor recursivo considerando cada uno de los escenarios del paso anterior, para ello es importante analizar el comportamiento bajo los siguientes criterios de operación:
        - Caching (TTL) / CD = 0
        - No Caching (TTL nulo) / CD = 0
        - Caching (TTL) / CD = 1
        - No Caching (TTL nulo) / CD = 1

- Identificar los impactos en:
  - Tamaño promedio de la Respuesta (LAN)
  - Tamaño promedio de la Respuesta (WAN)
  - Distribución del tamaño de los paquetes. Es importante identificar aquellos paquetes superiores a 1500 Bytes dado que éste es el MTU para redes que utilizan el protocolo de Ethernet de capa 2.
  - Ancho de banda interno (LAN).
  - Ancho de banda externo (WAN).
  - Tiempo promedio de respuesta (delay).
  - Tiempo promedio de CPU.
  - Tamaño de la memoria caché.

6. Identificación de impactos generales
   - Considerar ambientes con alto número de peticiones por segundo que sometan a un mayor tráfico entrante hacía al servidor caché recursivo.
     - Generar un tráfico de aprox. 1 M de peticiones hacia el servidor DNSSEC recursivo.
   - Caracterizar impactos en el servidor recursivo:
     - CPU
     - Retraso de la respuesta

   Estos experimentos deberán de considerar los siguientes criterios:
   - ZSK = KSK {0,512,1024,2048}
   - Tarjeta criptográfica {No Instalada / Instalada}
     - Nota: Esta tarjeta fue facilitada por NIC MX – ccTLD mx.

Capítulo 4. Implementación de ambiente de laboratorio (Testbed).

A continuación se presenta el detalle de la información que fue capturada del servidor recursivo de nombres del ITESM Campus Monterrey con dirección IPv4 10.18.0.138. Dicho tráfico fue capturado con ayuda de la herramienta TCPDUMP ejecutada en un servidor IBM el cual se encontraba conectado en un puerto que redireccionaba todo el tráfico entrante y saliente dirigido hacia el servidor de caché del Campus durante 500 segundos de muestra. Este tráfico sirvió como entrada para la caracterización del comportamiento de un servidor real sometido a un diversidad de peticiones hacía Internet como sucede en una universidad.

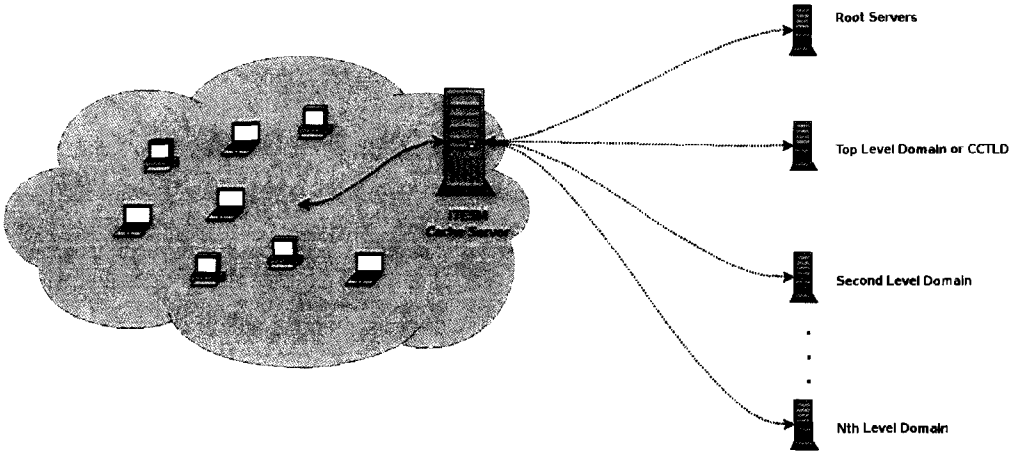


Figura 18: Diagrama de Operación de Servidor Recursivo del ITESM Campus Monterrey

Con base al tipo de peticiones que recibió el servidor recursivo del ITESM el comportamiento del tráfico entrante fue el siguiente:

Query Type on the source	# Queries	% Queries
A	11637	76.00%
PTR	1619	10.57%
NS	25	0.16%
AAAA	500	3.27%
TXT	1120	7.32%
SRV	192	1.25%
MX	146	0.95%
SOA	63	0.41%
ANY	9	0.06%
Total	**15311**	**100.00%**

Tabla 5: Tipo de Peticiones Entrantes al Servidor

Al analizar el destino hacia donde se dirigian las peticiones se encontró que cerca del 60% de las peticiones se repitieron en al menos 1 o más ocasiones.

Duplicated VS Non Duplicated Queries		
# Non duplicated queries	5855	38.24%
# Duplicated queries	9456	61.76%
# Total Query	**15311**	**100.00%**

Tabla 6: Porcentaje de peticiones repetidas hacia el servidor DNS recursivo (ITESM)

El desglose del comportamiento del tráfico bajo el esquema tradicional se incluye en la sección de anexos de este documento.

4.1 Detalle de interconexión del laboratorio

Para construir el ambiente de pruebas donde se realizaron las simulaciones para el análisis y comparativo del impacto DNSSEC vs DNS se procedió a extraer del archivo TCPDUMP todo el desglose de peticiones que fueron generadas desde la LAN del ITESM y que solicitaban resolución en su servidor de nombres recursivo. Las estadísticas de este comportamiento se presentaron en la sección anterior.

Posteriormente se regeneró la cantidad peticiones iterativas que este servidor debe realizar hacia Internet para obtener una respuesta y enviarla hacia el stub resolver que realizó dicha petición.

Se utilizó la herramienta "dig +trace" con la finalidad de conocer el recorrido que una petición debe realizar a través de los diferentes servidores de nombres autoritativos. A continuación se presenta un ejemplo del proceso que se sigue para conocer la resolución de la petición www.itesm.mx.

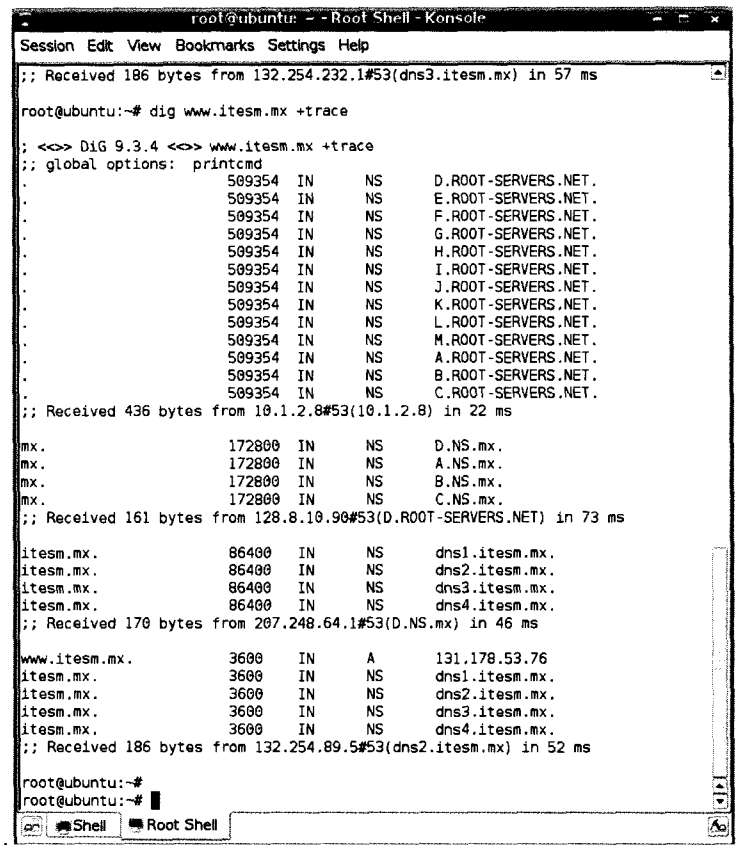


Figura 19: Identificación del número de peticiones iterativas (Internet)

Como podemos observar en la figura anterior el número de peticiones iterativas que el servidor recursivo tuvo que realizar para obtener una respuesta a la petición "dig www.itesm.mx" fue de 1 petición recursiva y 3 peticiones iterativas las cuales se desglosan a continuación:

- 10.1.2.8 Servidor DNS Caché (Petición Recursiva)
  - Responde indicando referal a la raíz.
- 128.8.10.90 Servidor DNS Autoritativo D.ROOT-SERVERS.NET (Iterativa)
  - Responde indicando referal a mx.
- 207.248.64.1 Servidor DNS Autoritativo D.NS.mx. (Iterativa)
  - Responde indicando referal a itesm.mx.
- 207.248.64.1 Servidor DNS Autoritativo dns2.itesm.mx. (Iterativa)
  - Responde indicando respuesta del tipo address para www.itesm.mx.

Este procedimiento fue ejecutado para cada una las 15311 peticiones que fueron capturadas con TCPDUMP dirigidas hacia el servidor caché del Campus. La razón principal por la que se detalló la cantidad de peticiones que deben realizarse es porque en el esquema de DNSSEC cada una de estas iteraciones representa un procesamiento adicional para el servidor de caché, por lo que se debe considerar este tipo de escenarios para una mejor aproximación del impacto que se desea medir.

Durante la simulación no se consideró la existencia de servidores secundarios para atender la respuesta, por lo que sólo se encuentran implementados el número de servidores autoritativos que deben de ser consultados antes de regresar una respuesta al stub resolver, para ello cada iteración o pregunta a un servidor es colocada en un servidor de DNS autoritativo independiente. Es importante mencionar que la máxima cantidad de iteraciones para la cantidad de peticiones simuladas (15311) no fue superior a 5 saltos.

A continuación se presenta el diagrama de interconexión y el direccionamiento lógico utilizado en la realización de las pruebas para las mediciones de impactos de desempeño del servidor recursivo (NSCACHÉ).

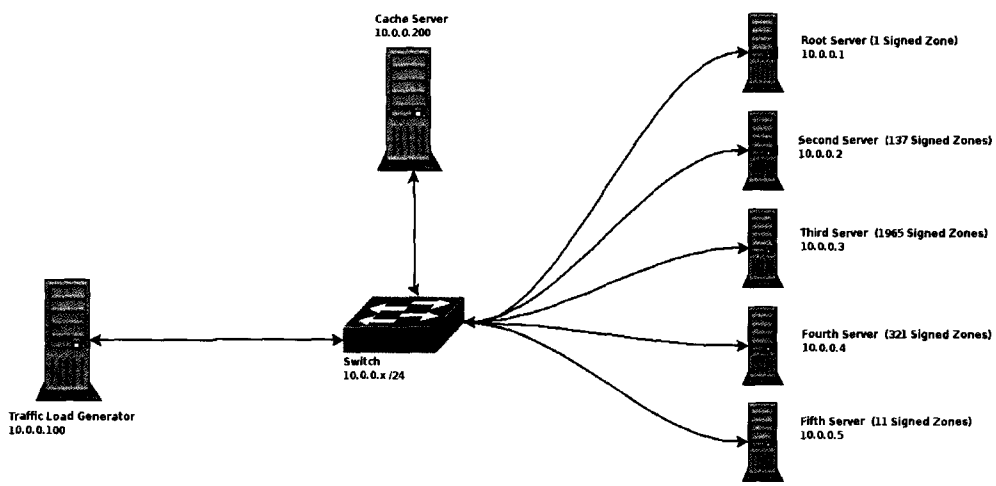


Figura 20: Diagrama de Interconexión de los Equipos de Laboratorio

Bajo este esquema, si repetimos la misma petición "dig www.itesm.mx" a los servidores de prueba en el laboratorio, la respuesta quedaría de la siguiente manera.

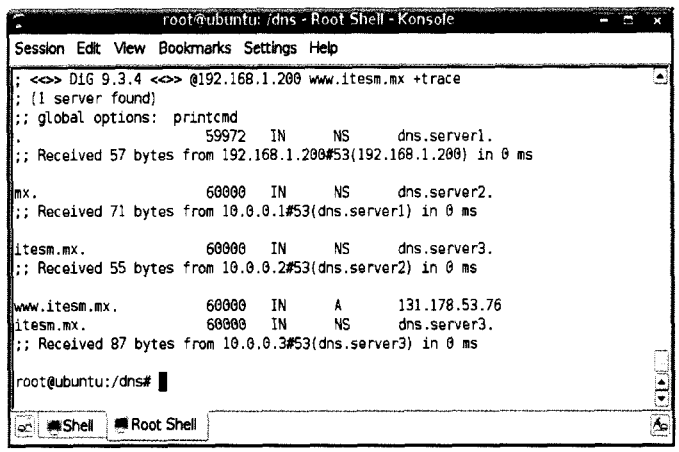


Figura 21: Identificación del número de peticiones iterativas (Laboratorio)

Observamos en la figura anterior que la cantidad de número de peticiones que el servidor de caché recursivo debe de realizar hacia los servidores autoritativos corresponde a los mismos que los que realizaría en un ambiente real en Internet.

Bajo este esquema se diseño un script en PERL que realizó la construcción del ambiente de pruebas asignando la distribución de zonas y nombres de dominio como se aprecia en la figura 18. Todas estas zonas han sido firmadas con la ayuda de las herramientas dnssec-keygen y dnssec-signzone utilizando diferentes tamaños de ZSK y KSK, todo ello con la finalidad de simular una reconstrucción del DNS pero ahora con las características y extensiones de seguridad de las cuales deseamos conocer su impacto sobre el servidores de nombres recursivo o de caché.

Es importante mencionar que al reproducir el tráfico entrante de 15311 peticiones la distribución hacia los servidores autoritativos en la arquitectura de laboratorio es la siguiente:

Destination	% Recursive Queries
10.0.0.1	1.57%
10.0.0.2	19.96%
10.0.0.3	61.21%
10.0.0.4	17.04%
10.0.0.5	0.22%
Total	100.00%

Tabla 7: Distribución de las peticiones realizadas hacia los diferentes servidores (Laboratorio)

A continuación se presenta el detalle del comportamiento de los flujos de información cuando el servidor de nombres recursivo ITESM es replicado en el

ambiente de pruebas, esto nos permite conocer y caracterizar el comportamiento del protocolo DNS tradicional sobre el servidor caché del Campus.

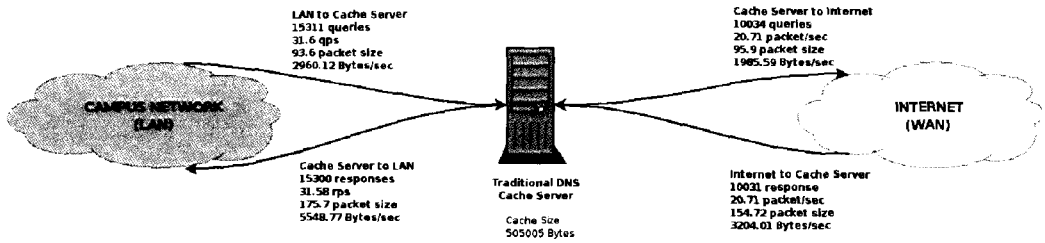


Figura 22: Identificación de los flujos de Información de entrada y salida (DNS Tradicional)

Capítulo 5. Análisis de impactos DNSSEC

5.1 Impactos DNSSEC en servidor DNS Recursivo (ITESM-Lab)

En la siguientes secciones se presentan los impactos en el servidor de Caché del Campus al implementarse DNSSEC y considerarse los criterios definidos en la metodología de este documento.

Para cada uno de los experimentos de la sección 5.1 que se presentan a continuación se realizó la medición considerando que el caché del servidor recursivo se encontrada sin ningún registro previamente almacenado, que la número de peticiones por segundo corresponde al servidor real de producción (30 qps) y que las extensiones de seguridad están soportadas en toda la arquitectura de DNS donde se realizan estos experimentos.

5.1.1 Impacto en tamaño de la respuesta

Primeramente se presentan los impactos que generan las extensiones de seguridad sobre las nuevas longitudes de las respuestas cuando:

1. El servidor recursivo recibe respuestas por parte de los servidores autoritativos y que impactan en el ancho de banda de la WAN (Conexión hacía el exterior del Campus).
2. El servidor recursivo envía hacia los stub-resolver (clientes) y que impactan en el ancho de banda de la LAN (Conexión interna del Campus).

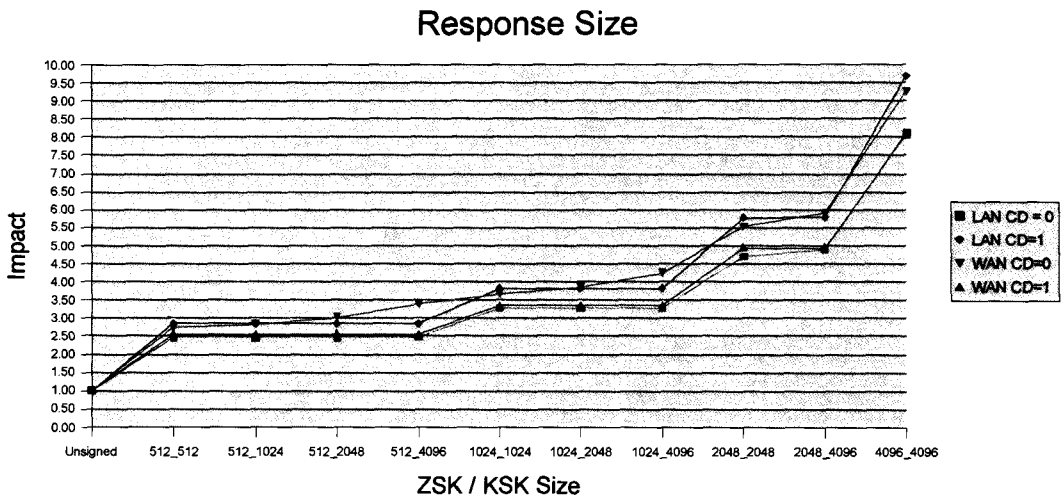
Los experimentos fueron realizados considerando los escenarios CD = 0 (El servidor recursivo es quién valida las firmas) y cuando CD = 1 (El cliente es quién valida las firmas).

	Response Size (LAN)		Response Size (WAN)	
Experiment	LAN CD = 0	LAN CD=1	WAN CD=0	WAN CD=1
Unsigned	1.00	1.00	1.00	1.00
512_512	2.47	2.85	2.74	2.56
512_1024	2.47	2.85	2.83	2.56
512_2048	2.47	2.85	3.03	2.56
512_4096	2.48	2.85	3.41	2.56
1024_1024	3.28	3.83	3.67	3.35
1024_2048	3.28	3.82	3.86	3.35
1024_4096	3.28	3.83	4.25	3.35
2048_2048	4.69	5.78	5.53	4.93
2048_4096	4.89	5.78	5.92	4.94
4096_4096	8.12	9.69	9.26	8.08

Tabla 8 Impacto normalizado de las longitudes de la respuesta DNSSEC (ITESM-LAB)

Se observa que las variaciones en KSK para cada escenario no afecta de manera considerable el resultado en el impacto general, sin embargo se aprecia un ligero efecto del tamaño de este tipo de llave KSK para el caso de la WAN (Conexión hacía el exterior del Campus) y cuando el bit CD = 0, debido a que bajo este escenario se observó se produce la mayor cantidad de peticiones de registros del tipo DNSKEY entre el servidor recursivo y los servidores autoritativos.

En la siguiente se figura se presentan los impactos de cada una las combinaciones ZSK / KSK.



Gráfica 1 Longitud de la respuesta DNSSEC (ITESM-LAB)

Las estadísticas anteriormente presentadas permiten realizar una prueba de concepto que puede resumirse de la siguiente manera:

- CD = 0 (El cliente delega la validación al servidor recursivo).
  - Mayor impacto en el tamaño de respuesta de la WAN.
  - Menor impacto en el tamaño de respuesta de la LAN.

- CD = 1 (El cliente es quien valida las firmas).
  - Mayor impacto en el tamaño de respuesta de la LAN.
  - Menor impacto en el tamaño de respuesta de la WAN.

5.1.2 Impacto en ancho de banda

El aumento en el tamaño de la respuesta tiene un impacto directo en el crecimiento del ancho que demandan estas nuevas extensiones de seguridad. En la siguiente tabla se presenta los impactos en esta variable. Es importante mencionar que la capacidad de "caching" en el servidor recursivo impacta exclusivamente en la información que es enviada y recibida en el segmento de WAN, razón por la cual se hace especial énfasis bajo este tipo de configuración. Los resultados que se presentan a continuación se encuentran normalizados respecto al escenario DNS tradicional (unsigned).

	LAN		WAN			
	Caching or No Caching		Caching		No Caching	
Experiment	CD = 0	CD=1	CD=0	CD=1	CD=0	CD=1
Unsigned	1.00	1.00	1.00	1.00	1.00	1.00
512_512	1.77	2.20	2.60	1.84	2.89	1.72
512_1024	1.77	2.21	2.69	1.83	3.04	1.71
512_2048	1.76	2.22	2.91	1.84	3.38	1.72
512_4096	1.76	2.21	3.32	1.84	4.17	1.71
1024_1024	2.22	2.80	3.32	2.30	3.78	2.07
1024_2048	2.20	2.84	3.64	2.30	4.64	2.13
1024_4096	2.23	2.83	3.96	2.30	4.97	2.13
2048_2048	3.12	3.92	4.86	3.19	5.50	2.80
2048_4096	3.13	4.11	5.27	3.15	6.29	2.95
4096_4096	4.93	6.41	7.83	4.87	8.75	4.36

Tabla 9 Impacto normalizado en el ancho de banda LAN/WAN al incluir DNSSEC (ITESM-LAB)

Podemos confirmar que el impacto en el ancho de banda al implementar estas extensiones de seguridad será mucho mayor en el segmento de WAN a comparación que el de LAN.

DNS por naturaleza es un protocolo ligero que no demanda un gran ancho de banda de los enlaces de Internet de los clientes, sin embargo es importante poner especial atención en el impacto que se produce en el segmento de WAN con la implementación de este nuevo protocolo ya que podría generar cuellos de botella en enlaces de baja capacidad hacia Internet (Ej. 512 Kbps).

La importancia del caching bajo este nuevo esquema de seguridad es importante ya que ayuda a reducir en 1 orden de magnitud el consumo de ancho de banda hacia el segmento de WAN.

Los límites superior e inferior del impacto en ancho de banda son establecidos principalmente cuando el bit de CD = 0, dado que esto implica la solicitud de registros DNSKEY a los servidores autoritativos para la validación de las firmas digitales.

5.1.3 Impacto en memoria caché

Respecto al impacto en memoria caché para el servidor recursivo se observa el siguiente comportamiento al incrementar el número de bits con que son firmadas las zonas de los servidores autoritativos. Los resultados que se presentan a continuación se encuentran normalizados respecto al escenario DNS tradicional (unsigned).

	Cache Memory	
Experiment	CD = 0	CD=1
Unsigned	1.00	1.00
512_512	7.69	4.93
512_1024	8.49	4.93
512_2048	10.10	4.93
512_4096	13.31	4.94
1024_1024	10.98	6.61
1024_2048	12.60	6.61
1024_4096	15.81	6.62
2048_2048	17.82	10.14
2048_4096	21.02	10.15
4096_4096	31.30	17.03

Tabla 10 Impacto normalizado en memoria caché al incluir DNSSEC (ITESM-LAB)

El impacto principal en esta variable se observa cuando la bandera de CD = 0, dado que con esta condición se le pide al servidor recursivo que efectué la validación de las firmas que ha recibido y que además las guarde temporalmente en su memoria caché durante el tiempo que indique el TTL. De igual manera bajo esta condición de CD = 0, el servidor recursivo realiza las peticiones necesarias para construir y validar la cadena de confianza hasta el servidor autoritativo que responde finalmente a la petición realizada en un inicio por el stub resolver.

5.1.4 Impacto en procesador (CPU)

Los impactos en el CPU considerando el tráfico actual en los DNS del Campus Monterrey representan una variación mínima dado que el servidor recibe una tasa promedio de 30 peticiones / seg. Bajo estas condiciones el CPU se ve ligeramente impactado.

Experiment	%CPU
Unsigned	0.00
512_512	2.00
512_1024	2.00
512_2048	2.00
512_4096	2.00
1024_1024	2.00
1024_2048	2.00
2048_2048	2.00
2048_4096	2.00
4096_4096	5.00

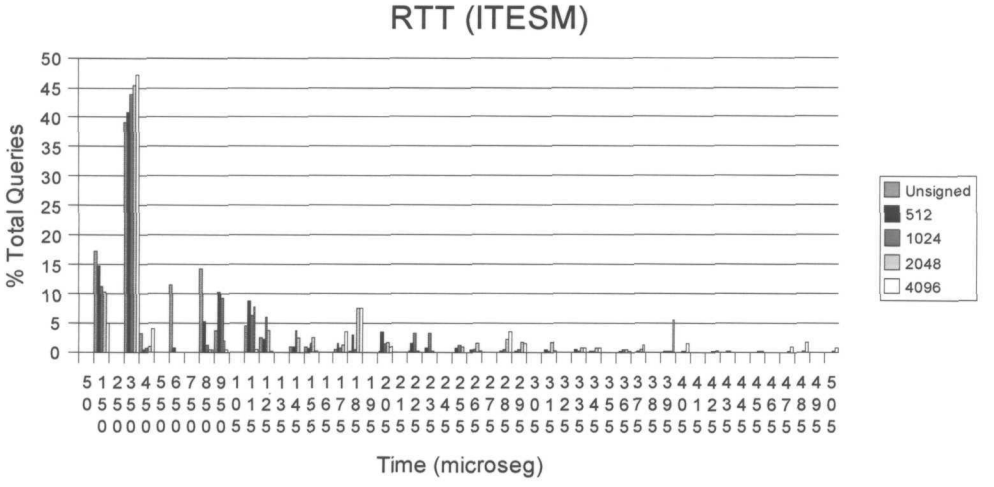
Tabla 11 Impacto en procesador (ITESM-LAB)

Se identifica un impacto constante con valor promedio del 2% para los escenarios que consideran los diferentes tamaños de las llaves de ZSK / KSK. Se puede identificar que dada las condiciones actuales de tráfico del ITESM, DNSSEC no representa una limitante desde el punto de vista del procesador. Estos resultados fueron obtenidos con ayuda del comando IOSTAT considerando la columna de utilización de %CPU.

5.1.5 Impacto en tiempo de respuesta

Al igual que el impacto en el CPU, los tiempos de respuesta se ven ligeramente impactados al implementar el protocolo de DNSSEC en los servidores del Campus

Monterrey, la distribución de los tiempos de respuesta. El máximo de la gráfica indica que para todos los escenarios el 45% de las peticiones corresponden a un RTT = 350 µsec



Gráfica 2 Tiempos de Respuesta promedio del servidor Recursivo al incluir DNSSEC (ITESM-LAB).

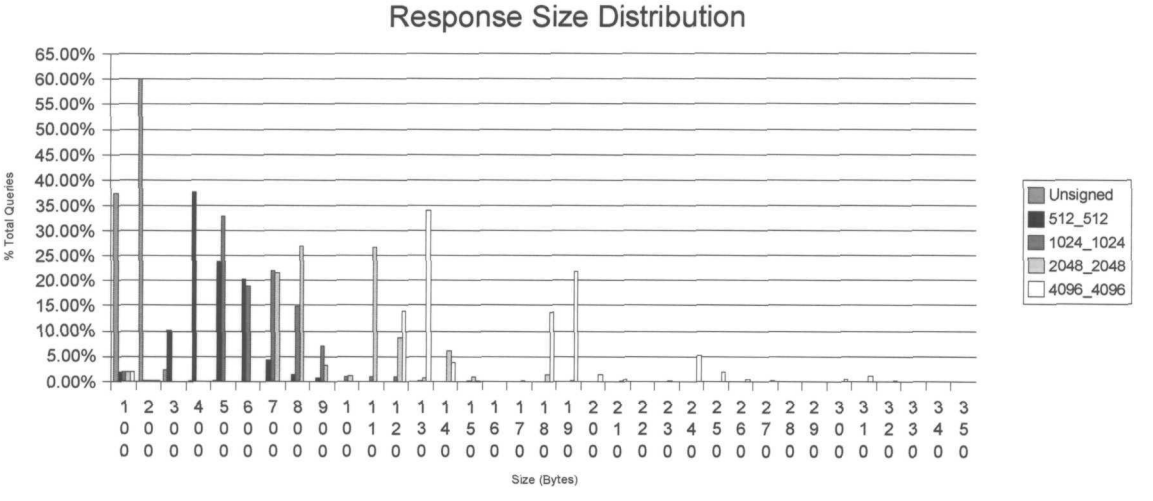
A medida que la longitud de la llave se incrementa se aprecia que existe un cierto porcentaje de paquetes sufren un mayor retraso, ocasionado por el proceso de validación de las firmas digitales.

5.2 Impactos Generales DNSSEC

En la sección anterior se detalló el comportamiento que sufriría el servidor recursivo del ITESM Campus Monterrey al implementar las extensiones de seguridad DNSSEC. A continuación se presentarán las estimaciones en los impactos que generarán las extensiones de seguridad cuando se presente un aumento en el número de peticiones por segundo que recibe un servidor recursivo.

5.2.1 Distribución del tamaño de la respuesta

Después de analizar el comportamiento de las 15309 peticiones que sirvieron como tráfico entrante para el esquema del servidor del ITESM, esta misma muestra ha servido para determinar una distribución genérica del tamaño de los paquetes al implementar las extensiones de seguridad.



Gráfica 3 Distribución del tamaño de la respuesta al incluir DNSSEC

Durante el experimento observamos que para implementar las extensiones de seguridad es mandatario hacer uso de ENDS0 para poder soportar longitudes de paquetes superiores a 512 bytes sobre UDP. Como podemos observar en la gráfica a medida que aumenta el tamaño de la firma digital, la cantidad de paquetes superiores a 512 bytes también es mucho mayor, lo cual implicaría hacer uso de TCP como protocolo de transporte para poder soportar las extensiones de seguridad al DNS.

ENDS0 es un esquema que ayuda a solucionar esta problemática permitiendo que el tamaño del paquete de UDP pueda ser de hasta 4096 bytes antes de utilizar TCP,

para el caso del experimento se observa que el paquete más grande llega a ser de una longitud aproximada a los 3100 bytes, por lo que no es necesario hacer uso de TCP aún y cuando se esté firmando con una longitud de llave de 4096 bits.

La finalidad de conocer el tamaño de la respuesta utilizando de DNSSEC ayuda a determinar tambien la cantidad de paquetes que pueden exceder un determinado tamaño de MTU sobre la línea de transmisión, lo cual implicaría realizar fragmentación sobre el paquete que desea ser enviado.

Por ejemplo, para el caso de las redes basadas en Ethernet, el MTU soportado es de hasta 1500 bytes. Considerando que Ethernet es el protocolo de capa 2 mayormente utilizado para ambientes LAN, lo que se deberá de tomar en cuenta al implementar DNSSEC es que acorde con la figura anterior los firmados superiores a 1024 bits, demandarán del uso de fragmentación antes de ser colocados en el medio de transmisión, generando retrasos en la respuesta o incluso pérdida de paquetes.

5.2.2 Carga máxima soportada

La carga máxima en función del número de peticiones por segundo soportado por el servidor bajo los diferentes escenarios de los tamaños de la llave son los siguientes:

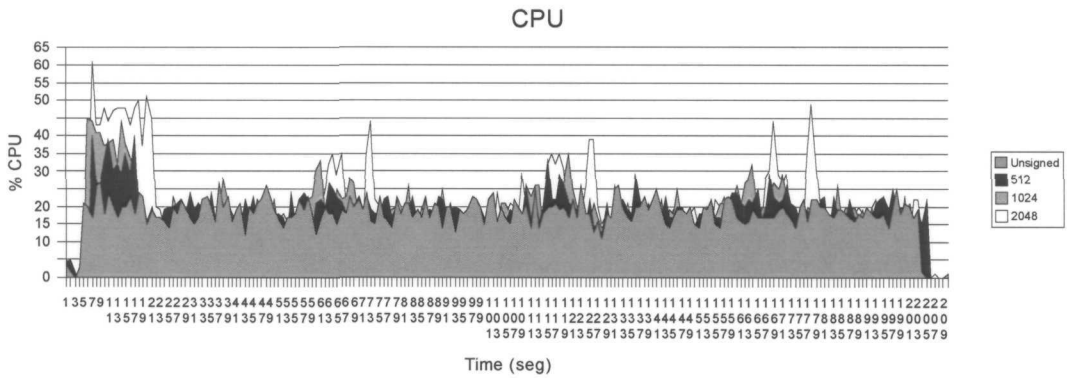
Longitud Llave	Peticiones por segundo soportadas
Unsigned	4058.83
512	3382.95
1024	3120.87
2048	2772.95

Tabla 12 Cantidad máxima de peticiones por segundo soportadas.

Para obtener los resultados de la tabla 12, se configuró el generador de tráfico de peticiones (queryperf) de tal manera que cada nueva petición enviada hacía el servidor recursivo fuera enviada hasta recibir la respuesta de la petición anterior, de esta manera se garantiza respetar el tiempo de procesador necesario para atender cada una de las peticiones y no generar una sobresaturación durante el proceso de firmado.

5.2.3 Impacto en CPU – Carga Máxima

El análisis de impacto al CPU del servido recursivo se hizo considerando el mayor número de peticiones por segundo soportadas por el servidor tomando en cuando los resultados de la tabla 12 y considerando que se implementan diferentes



longitudes de llave ZSK = KSK.

Gráfica 4 Impacto en el procesador del servidor recursivo DNSSEC

En la figura anterior observamos que a medida que la longitud de la llave de la firma digital es más robusta el impacto sobre el CPU también es mayor durante el proceso de validación.

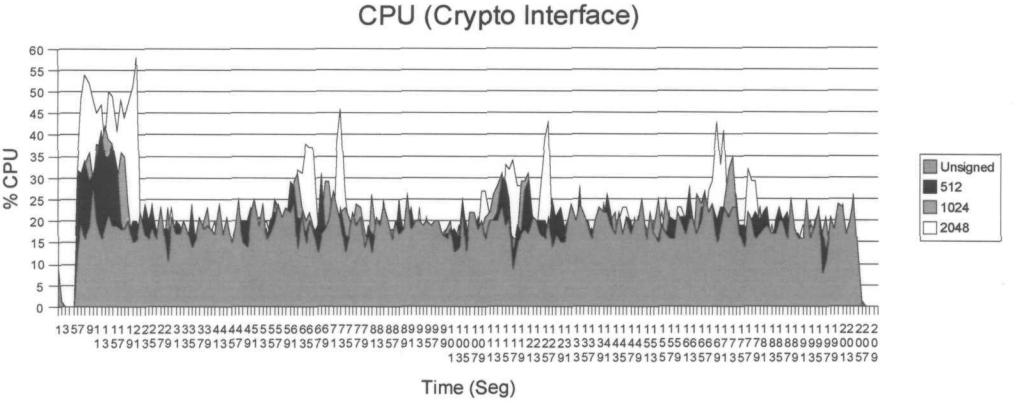
Se observa que el comportamiento inicial del uso del CPU se debe a que el servidor de caché se encuentra sin ningún registro en su memoria al inicio del experimento, razón por la cual todas las peticiones deberán de ser validadas contra su respectiva llave, sin embargo conforme el experimento avanza en el tiempo y al encontrarse en estado estable el impacto sobre el CPU permanece constante en todos los escenarios debido a que las firmas y los registros ya fueron almacenados en memoria caché, motivo por el cual las validaciones criptográficas son mínimas.

Los picos posteriores de la gráfica se debe a que los registros NXDOMAIN fueron configurados para este experimento con un Negative TTL = 50 seg con la intención de identificar que sucede con el procesador a medida que estos registros expiran de su caché.

Un valor más acertado para ambientes de producción es que el Negative TTL sea aproximadamente igual a 1800 segs, bajo esa perspectiva lo único que se

modificaría en la gráfica presentada es el instante de tiempo en el cual aparecerán los picos de consumo de CPU.

NIC Mx facilitó el uso de una tarjeta de criptografía con la finalidad de medir el desempeño del CPU cuando un dispositivo de aceleración para el firmado y verificación de firmas digitales se encuentra instalado en servidor de caché. Durante las pruebas surgieron los siguientes resultados considerando un esquema similar de número de peticiones por segundo al que fue sometido el servidor anterior.



Gráfica 5 Impacto en procesamiento del servidor recursivo DNSSEC al incluir tarjeta criptográfica.

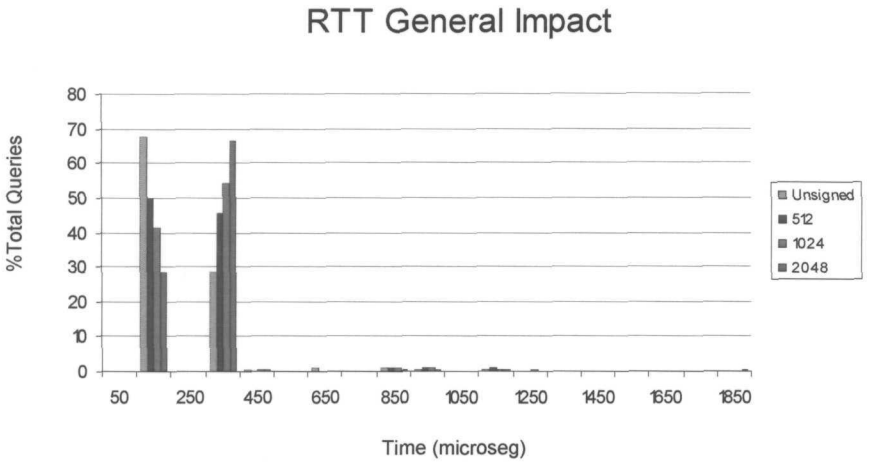
La diferencia en impacto de CPU es casi imperceptible respecto a la gráfica anterior, esto se debe principalmente a que al comparar la capacidad de verificación de firmas en ambos ambientes (con y sin tarjeta de criptografía) es muy similar considerando el número de peticiones por segundo entrantes, se concluyó que el servidor recursivo debería estar expuesto a una carga superior a las 20000 peticiones por segundo con la finalidad de identificar una mejora en el desempeño del CPU con el uso de este tipo de tarjetas de criptografía para la verificación de firmas. El estar sometido a estos niveles de peticiones por segundo en un ambiente de producción es poco probable o nulo.

El contar con una tarjeta de aceleración criptográfica para el esquema de DNSSEC, resulta de mayor utilidad para los servidores autoritativos de DNS los cuales su tarea principal es firmar una gran cantidad de zonas a diferencia de los recursivos que únicamente verifican firmas digitales.

Los resultados fueron obtenidos con ayuda del comando IOSTAT considerando la columna de utilización de CPU%

5.2.4 Impacto en RTT – Carga Máxima

El impacto en los tiempos de respuesta presenta la siguiente distribución ante los cambios en longitud de los bits de las firmas que son utilizadas.



Gráfica 6 Tiempos de respuesta promedio del servidor recursivo DNSSEC

El retraso en los tiempos de respuesta se ve afectado por los tiempos de verificación que realiza el servidor de caché antes de enviarlos hacia el cliente que realizó dicha petición.

Los resultados anteriores fueron obtenidos con ayuda de la opción Histograma RTT del programa Queryperf, el cual mide el tiempo de respuesta promedio (RTT) para el total de peticiones que son enviadas hacía al servidor recursivo durante la duración del experimento.

Conclusiones

A lo largo de este conjunto de experimentos que han sido presentados en este documento, se pudieron identificar los principales impactos que tendrán las extensiones de seguridad al ser implementadas en los servidores recursivos o de caché.

La cantidad de experimentos presentados han sido con la intención de poder identificar y caracterizar la mayor parte de los escenarios que pueden presentarse en un ambiente real o de producción para este tipo de servidores. Algunas de las pruebas han sido incluso ajustadas a los peores escenarios con la finalidad de poder conocer hasta qué nivel este protocolo seguridad será viable en su implementación.

Los resultados principales se sintetizan de la siguiente manera:

- El considerar variaciones en el ZSK / KSK ha permitido corroborar que las variaciones importantes en desempeño dependen de manera directa del tamaño de la llave con que los servidores autoritativos realizan el firmado de zona (ZSK).

- La llave KSK genera un ligero impacto en el tráfico de Internet cuando el servidor recursivo es el encargado de la validación de la cadena de confianza CD = 0.

- El incremento en el tamaño de la respuesta de DNSSEC afecta de manera directa el nuevo ancho de banda que será demandado para poder transportar los nuevos registros y firmas digitales que implementa este nuevo protocolo. Si los TTL de los ambientes de producción son muy bajos (No caching), la afectación en esta variable puede ser mayor si se combina incluso con que el servidor recursivo sea quien realice las validaciones. Los umbrales generales para esta variable estarían definidos desde un incremento de 1.72 a 8.75 veces la demanda que actualmente demanda DNS tradicional.

- Se identificaron escenarios donde el tamaño de la respuesta era superior a 1500 bytes, razón por la cual serían objeto de fragmentación al cruzar por redes del tipo Ethernet, generando un requerimiento extra para el procesador o incluso mayor número de pérdida de paquetes.

- Las afectaciones en CPU resultan considerables únicamente cuando existe un mayor número de peticiones por segundo; para los servidores recursivos del ITESM esta variable no se ve afectada dado que la cantidad de peticiones por segundo es relativamente baja para poder considerar impactos importantes en el desempeño.

- La tarjeta de procesamiento criptográfico que fue considerada en la última sección de los experimentos no significó un cambio considerable dado que la cantidad de peticiones para carga máxima se encontró dentro de los límites de verificación de firmas soportados por el servidor recursivo aún sin la tarjeta criptográfica. Para identificar beneficios importantes con este tipo de configuración es necesario elevar el número de peticiones por segundo entrante a niveles poco usuales en producción.

- El impacto en memoria caché es quizá el que mayor impacto sufre dada la cantidad de nuevos registros que el servidor recursivo tiene que almacenarse durante el proceso de validación de firmas digitales. El peor escenario para esta variable es cuando el cliente le solicita que lleve a cabo el proceso de validación de firmas. Los umbrales de impacto están definidos de 4.93 a 31.30 veces comparado con el tamaño del DNS tradicional.

Bajo estos resultados de experimentación se identifica que el costo principal que deberá de considerarse en el corto plazo para la implementación de las extensiones de seguridad será el aumento en el ancho de banda del segmento de WAN, los impactos en caché, memoria, tiempos de respuesta y CPU pudieran ser manejados de manera gradual e incluso pueden ser remediados con una menor inversión que permita hacer una actualización en las características técnicas de los servidores actuales de DNS.

Investigaciones Futuras

Los experimentos anteriores fueron realizados sin considerar la existencia de servidores autoritativos secundarios, por lo que se pude considerar como valor agregado importante a este modelo el diseñar un esquema que contemple este otro tipo de servidores, lo cual lo asemejaría en mayor grado a la realidad de los ambientes de producción.

Es importante contemplar un esquema que considere los TTL reales para los registros almacenados en las zonas de los servidores autoritativos con la finalidad de conocer cual es el tiempo real que un registro es almacenado en memoria caché, esto permitiría acotar en un mejor contexto el impacto de las variables que se ven afectadas por las extensiones de seguridad.

Los desarrollos actuales de este tema de investigación pueden ser la base para la implementación de un esquema de medición del desempeño que permita evaluar la propuesta NSEC3 cuya funcionalidad es la de corregir el tema de enumeración de zona, que en la actualidad es una vulnerabilidad detectada para el protocolo DNSSEC.

Bibliografía

[1] D. Atkins, et al, .Threat Analysis of the Domain Name System (DNS)., RFC 3833, Agosto 2004. http://www.ietf.org/rfc/rfc3833.txt

[2] P. Mockapetris, .Domain Names - Concepts and Facilities., STD 13, RFC 1034, Noviembre 1987. http://www.ietf.org/rfc/rfc1034.txt

[3] P. Mockapetris, .Domain Names - Implementation and Specification., STD 13, RFC 1035, Noviembre 1987. http://www.ietf.org/rfc/rfc1035.txt

[4] R. Arends, et al, .DNS Security Introduction and Requirements., RFC 4033, Marzo 2005. http://www.ietf.org/rfc/rfc4033.txt

[5] R. Arends, et al, .Resource Records for DNS Security Extensions., RFC 4034, Marzo 2005. http://www.ietf.org/rfc/rfc4034.txt

[6] R. Arends, et al, .Protocol Modifications for the DNS Security Extensions., RFC 4035, Marzo 2005. http://www.ietf.org/rfc/rfc4035.txt

[7] Paul Albitz and Cricket Liu. DNS and BIND. O'Reilley & Associates, Inc. Sebastopol, CA., 2006.

[8] A. Barbir, et al, Delegation Signer (DS) Resource Record (RR), RFC 3568, Julio 2003. http://www.ietf.org/rfc/rfc3568.txt

[9] D. Eastlake, Domain Name System Security Extensions., RFC 2535: Marzo 1999. http://www.ietf.org/rfc/rfc2535.txt

[10] P. Vixie, Extension Mechanisms for DNS (EDNS0),. RFC 2671: Agosto 1999.

[11] O. Kolkman, Measuring the resources requirement of DNSSEC, Ripe NCC - 352, Octubre 2005.

[12] B. Ager, H. Dreger, Exploring the Overhead of DNSSEC, Abril 2005.

[13] S. Rose, Secure Domain Name System (DNS) Deployment Guide, NIST SP800-81, Mayo 2006.

[14] R. Curtmola, A. Del Sorbo, On the Performance and Analysis of DNS Security Extensions, 2005.

[15] ISC Bind 9.3 Administrator Manual.

[16] O. Kolkman, et al, DNSSEC Operational Practices, RFC 4641, Septiembre 2006 http://www.ietf.org/rfc/rfc4641.txt

[17] O. Kolkman, DNSSEC How To, NLnet Labs, Enero 2007 http://www.nlnetlabs.nl/dnssec_howto/dnssec_howto.pdf

Anexo A: Comportamiento del tráfico (DNS – Tradicional)

Tomando en consideración la distribución del flujo de las peticiones hacia los diferentes destinos de los servidores autoritativos en Internet se obtuvo la siguiente estadística.

TLD	
com	40.00%
mx	19.10%
net	11.20%
in-addr.arpa	11.10%
org	9.70%
other	8.90%

Tabla 13 Distribución de las peticiones dirigidas a TLD o ccTLD (ITESM)

SLD	
itesm.mx	16.10%
senderbase.org	7.50%
10.in-addr.arpa	4.90%
msn.com	4.40%
com.mx	2.30%
yahoo.com	1.90%
microsoft.com	1.60%
200.in-addr.arpa	1.40%
llnwd.net	1.20%
google.com.	1.00%
hotmail.com	1.00%
akamai.net	1.00%
other	55.70%

Tabla 14 Distribución de las peticiones dirigidas a Dominios de Segundo Nivel SLD (ITESM)

3LD	
mty.itesm.mx	11.30%
sb-adfe2ko9.senderbase.org	3.80%
rf-adfe2ko9.senderbase.org	3.60%
16.10.in-addr.arpa	1.70%
rad.msn.com	1.60%
17.10.in-addr.arpa	1.50%
vo.llnwd.net	1.20%
sorteotec.itesm.mx	0.08%
other	75.22%

Tabla 15 Distribucion de las peticiones dirigidas a Dominios de Tercer Nivel 3LD (ITESM)

Anexo B: Detalle de análisis ITESM - DNSSEC

IMPACT Case 1: CACHING / CD = 0										
		Response Size (LAN)			Response Size (WAN)					
Experiment	Cache Memory	Success	NXDomain	SrvFail	Success	NXDomain	SrvFail	Referral	Bandwidth (LAN)	Bandwidth(WAN)
Unsigned	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
512_512	7.69	1.75	3.13	1.00	2.74	3.10	1.08	2.16	1.74	2.60
512_1024	8.49	1.75	3.13	1.00	2.94	3.11	1.00	2.16	1.74	2.69
512_2048	10.10	1.75	3.13	1.00	3.36	3.10	1.00	2.16	1.74	2.91
512_4096	13.31	1.75	3.13	1.00	4.19	3.10	1.00	2.16	1.73	3.32
1024_1024	10.98	2.31	4.17	1.00	3.83	4.12	1.00	2.71	2.17	3.32
1024_2048	**12.60**	**2.31**	**4.16**	**1.00**	**4.23**	**4.10**	**1.00**	**2.71**	**2.18**	**3.54**
1024_4096	15.81	2.31	4.16	1.00	5.07	4.11	1.00	2.71	2.18	3.96
2048_2048	17.82	3.44	6.21	1.00	6.03	6.10	1.00	3.80	3.05	4.86
2048_4096	21.02	3.44	6.21	1.00	6.85	6.11	1.00	3.80	3.07	5.27
4096_4096	31.30	5.70	10.32	1.00	10.44	10.17	1.00	5.98	4.81	7.83

Tabla 16 Impactos de las extensiones de seguridad Caching / CD = 0 (ITESM-LAB)

IMPACT Case 2: CACHING / CD = 0										
		Response Size (LAN)			Response Size (WAN)					
Experiment	Cache Memory	Success	NXDomain	SrvFail	Success	NXDomain	SrvFail	Referral	Bandwidth (LAN)	Bandwidth(WAN)
Unsigned	**0.00**	**0.92**	**1.00**	**1.00**	**0.98**	**0.99**	**1.00**	**0.95**	**0.94**	**4.19**
512_512	0.14	1.74	3.13	1.00	2.96	3.09	1.00	2.19	1.70	12.10
512_1024	0.16	1.74	3.13	1.00	3.32	3.09	1.00	2.19	1.69	12.75
512_2048	0.19	1.74	3.13	1.00	4.06	3.10	1.00	2.19	1.68	14.15
512_4096	0.26	1.74	3.14	1.00	5.51	3.10	1.00	2.19	1.69	17.45
1024_1024	0.20	2.30	4.16	1.00	4.29	4.10	1.00	2.73	2.13	15.84
1024_2048	**0.23**	**2.31**	**4.16**	**1.00**	**5.02**	**4.11**	**1.00**	**2.73**	**2.10**	**16.95**
1024_4096	0.30	2.30	4.16	1.00	6.50	4.10	1.00	2.73	2.16	20.81
2048_2048	0.31	2.68	6.22	1.00	6.97	6.12	1.00	3.82	2.99	23.06
2048_4096	0.38	3.42	6.22	1.00	8.43	6.13	1.00	3.82	3.00	26.37
4096_4096	0.55	5.67	10.32	1.00	12.25	10.16	1.00	6.01	4.76	36.67

Tabla 17 Impactos de las extensiones de seguridad No Caching / CD = 0 (ITESM-LAB)

Anexo C: Detalle de análisis ITESM - DNSSEC (Caching / CD = 1)

	IMPACT Case 3: CACHING / CD = 1									
		Response Size (LAN)			Response Size (WAN)					
Experiment	Cache Memory	Success	NXDomain	SrvFail	Success	NXDomain	SrvFail	Referral	Bandwidth (LAN)	Bandwidth(WAN)
Unsigned	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
512_512	4.93	2.43	3.13	1.02	2.41	3.16	1.00	2.17	2.09	1.84
512_1024	4.93	2.43	3.13	1.02	2.41	3.15	1.10	2.17	2.08	1.83
512_2048	4.93	2.43	3.13	1.02	2.41	3.16	1.01	2.17	2.08	1.84
512_4096	4.94	2.43	3.13	1.02	2.41	3.15	1.01	2.17	2.08	1.84
1024_1024	6.61	3.33	4.15	1.02	3.21	4.18	1.09	2.71	2.69	2.30
1024_2048	**6.61**	**3.32**	**4.15**	**1.02**	**3.21**	**4.17**	**1.09**	**2.71**	**2.68**	**2.30**
1024_4096	6.62	3.32	4.15	1.02	3.21	4.18	1.01	2.71	2.69	2.30
2048_2048	10.14	5.11	6.19	1.02	4.81	6.22	1.00	3.80	3.86	3.19
2048_4096	10.15	5.11	6.21	1.02	4.81	6.25	1.01	3.80	3.83	3.15
4096_4096	17.03	8.66	10.28	1.01	8.01	10.29	1.07	5.98	6.11	4.87

Tabla 18 Impactos de las extensiones de seguridad Caching / CD = 1 (ITESM-LAB)

	IMPACT Case 4: CACHING / CD = 1									
		Response Size (LAN)			Response Size (WAN)					
Experiment	Cache Memory	Success	NXDomain	SrvFail	Success	NXDomain	SrvFail	Referral	Bandwidth (LAN)	Bandwidth(WAN)
Unsigned	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
512_512	1.00	2.72	3.12	1.00	2.46	3.12	1.00	2.05	2.35	1.77
512_1024	1.00	2.72	3.13	1.00	2.45	3.12	1.00	2.05	2.09	1.55
512_2048	1.00	2.72	3.12	1.00	2.45	3.12	1.00	2.05	2.22	1.65
512_4096	1.00	2.71	3.13	1.00	2.45	3.12	1.00	2.05	1.63	1.21
1024_1024	1.00	3.68	4.14	1.00	3.30	4.13	1.00	2.56	2.84	2.06
1024_2048	**1.00**	**3.68**	**4.14**	**1.00**	**3.30**	**4.13**	**1.00**	**2.56**	**3.14**	**2.27**
1024_4096	1.00	3.69	4.16	1.00	3.30	4.14	1.00	2.56	2.89	2.10
2048_2048	1.00	5.62	6.20	1.00	4.99	6.18	1.00	3.58	3.95	2.81
2048_4096	1.00	5.62	6.20	1.00	4.98	6.19	1.00	3.58	4.49	3.07
4096_4096	1.00	9.52	10.28	1.00	8.34	10.24	1.00	5.63	6.56	4.33

Tabla 19 Impactos de las extensiones de seguridad No Caching / CD = 1 (ITESM-LAB)