CAPÍTULO 2

DNSSEC

2.1 DNSSEC

El proyecto de DNSSEC surgió en 1993 con los organismos de regularización y normalización, que se encargan de aprobar y regular las nomas y estándares elaborados para la comunidad del internet, como principal objetivo la mejora y ampliación de la existente estructura.

Esto se lleva a cabo mediante las solicitudes que son sujetas a procesos de análisis y revisión, por algunos grupos especializados en temas propuestos, para posteriormente con toda la comunidad de internet para así llegar a un conceso con las partes involucradas y así generar la aprobación y difusión de nuevas normas y estándares.

2.2 ORGANISMOS DE REGULACIÓN

2.2.1 ISOC

La Sociedad de Internet (ISOC), es un organismo sin fines de lucro fundada en 1992 dedicada a asegurar el desarrollo, evolución, cooperación y coordinación del internet a nivel mundial de protocolos, estándares y temas asociados a internet que actualmente cuenta con 100 organizaciones y más de 28,000 miembros individuales y para brindar un mejor servicio creo 5 oficinas alrededor del mundo como son:

- Oficina Africana
- Oficina de Asia
- Oficina de Europa
- América latina y Buros del Caribe
- Norte América Bureau

Su financiamiento es por los miembros, a través de organizaciones e individuos, donaciones e inscripciones a talleres, cursos y eventos se encuentra representada por el siguiente logo en la figura 2.1.

Figura 2.1 Logotipo de la ISOC

La ISOC cuenta con el premio “Jonathan Bruce Postel” premio que es entregado anual a un individuo o una organización que destaca y se dedica, al impulso de nuevas mejoras del esquema del internet.

“*Jonathan B. Postel Service Award* fue creado por la Sociedad de Internet para honrar a una persona que haya realizado contribuciones sobresalientes en el servicio a la comunidad en comunicaciones de datos. El premio se centra en las contribuciones técnicas continuas e importantes, el servicio a la comunidad, y liderazgo.”[3]

Dentro de esta asociación se encuentra un grupo dedicado a la administración de los procesos de Internet. Para cumplir sus objetivos, este grupo toma como base reglas y procedimientos anteriormente ratificados por un Consejo Administrativo. Su principal importancia, radica en el proceso establecido para la generación de nuevos estándares y protocolos de Internet, el cual va desde la documentación, publicación y difusión de especificaciones, hasta la aprobación final, por parte del Consejo.

La sociedad de Internet, cuenta con diversas organizaciones encargadas de la administración, investigación y desarrollo de algunos temas de Internet, entre las más importantes destacan las siguientes:

[3]Tomado y traducido de http://www.isoc.org/awards/postel/

- Internet Assigned Numbers Authority (IANA)
- Internet Architecture Board (IAB) que proporciona supervisión arquitectónica
- Internet Engineering Steering Group (IESG) se encarga de anunciar las mejora del internet

2.2.2 IETF

En 1986 surge la *The Internet Engineering Task Force (IETF Fuerza de Tarea de Ingenieros de Internet)*, es la comunidad internacional abierta a cualquier persona interesada, en participar en la evolución y mejora operacional de Internet, es la principal organización de la ISOC.

La IETF está organizada en diferentes grupos de trabajo encargados de un tema específico dentro de las distintas áreas de Internet. Estos grupos cuentan con un Director de Área (ADs) responsable de la dirección, administración y avance técnico, dentro del grupo de trabajo. Cada uno de estos directores es miembro activo de la Inty rnet Enginnering Steering Group (IESG), grupo responsable de la dirección técnica de las actividades y de los procesos de estandarización dentro de la IETF su logotipo es el siguiente como se muestra en la figura 2.2.

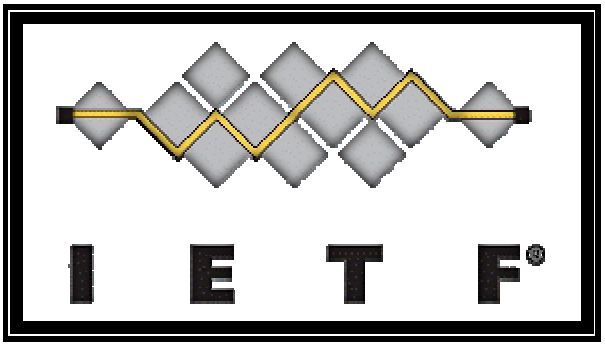

Figura 2.2 Logotipo de IETF

La IEFT se reúne tres veces al año, en las cuales se analizan las actividades y procesos de estandarización de Internet. A pesar de que este organismo tiene objetivos establecidos, una parte de su definición está basada en RFCs, ya que se encuentran en constante actualización, revisión y consulta por parte de los participantes de todo el mundo.

Dados sus objetivos y el grupo de personas que lo conforman, existen diversos mecanismos de contribución y aportación por parte de sus miembros, dentro de estas contribuciones se encuentran las participaciones orales y escritas por parte de los asistentes a los eventos y sesiones de este grupo de trabajo, además de las aportaciones realizadas en el proceso de estandarización.

2.3 ORÍGENES DE DNSSEC

En una de las publicaciones de IEFT en agosto del 2006 volumen 2 pública James M. Galvin donde describe las diferentes evoluciones que ha tenido la seguridad DNS a partir de 1999, ya que el internet va cambiando constantemente ocasionando que la seguridad no se concluirá por dicha evolución así como los requisitos.

El 30 de noviembre de 1993 identificaron las amenazas, a los servicios de seguridad así como los requisitos de interés para los DNS, dando origen al grupo de trabajo encargado de la seguridad designado por la IETF, así como evaluaría todas las propuestas con el objetivo de crear una sola propuesta.

Este grupo fue constituido hasta marzo del 2004 con la Descripción de Seguridad en el Servidor de Nombre de Dominio (DNSSEC), este se encargaría de especificar las mejoras en el protocolo DNS para evitar las posibles modificaciones no autorizadas, en la base de datos que cada servidor contiene y así la autenticación del mismo.

Así como el mecanismo que se agregaría del protocolo mediante una firma digital. Este servicio se añadiría de tal manera que los registros de recursos (RRs) del DNS serian firmados, distribuidos y verificados dando la confianza en la exactitud de datos recibidos. Esto dio dos cuestiones de estudio y revisión.

1. Los registros deben ser firmados por el DNS primario o secundario para lograr la distribución de los registros de recursos.
2. El mecanismo para identificar y verificar las claves públicas para la firma digital.

Dando origen a los supuestos como es la compatibilidad y convivencia con los servidores DNS y los clientes que no son compatibles con el servicio y los datos que se consideran de información pública, así proporcionando a la discusión de cómo realizar confidencialidad a los datos y control de acceso.

Las especificaciones se tenían claras, limitadas y estimando que se realizaría la implementación en un año (estimación que se les fue de control), debido a la falta de documentación de las discusiones que llevo a la elección de servicio de la seguridad para crear la primera obra llamada Domain Name System Security Extensions (DNSSEC) escrito por Donald Eastlake y Charlie Kaufman que se publicó en el RFC 2067 en Enero de 1997, a tres años de la creación del grupo de trabajo.

El no documentar retrasó por varios años, ya que causaba conflictos, puesto que no se entendía por qué se realizaba dicha aplicación de DNSSEC qué funcionalidad tenia y esto dio origen años después a un análisis de las amenazas más frecuentes, esto proporcionaba el estudio de todos los servidores de nombre de dominio con qué riesgos y lo que se necesitaba para realizar, este documento posiblemente habría servido como base importante para la revisión de futuras aplicaciones y para entender como implementar lo que en primera instancia se tenía.

Este documento fue publicado en agosto del 2004 llamado Análisis de Amenazas del Domain Name System (DNS) escrito a nombre de Derek Atkins y Rob Austein en el RFC 3833., en base a lo anterior las extensiones DNSSEC parecen resolver un conjunto de problemas que es necesario resolver.

Tomando en cuenta que el objetivo principal de DNS es:
"Los nombres de dominio a direcciones IP facilita la comunicación entre dos sitios. Si la información no está disponible o es inaccesible, los sitios no serán capaces de comunicarse"[4].

Aunque los datos en el DNS deben ser disponibles para ser de utilidad, el protocolo limita la rapidez de búsqueda a un dominio inherente que cualquier cliente pueda acceder a todos los datos de una zona, la seguridad añade una funcionalidad, si un cliente consulta un dominio inexistente, la respuesta sería correcta y el servidor asegurara que la firma del dominio no existe pero, además de indicar que la siguiente etiqueta del dominio es válido en la zona. A través de consultas repetidas, un cliente puede conocer y descargar todo el contenido de una zona.

Las extensiones de seguridad DNS en actualización dinámica llamo la atención de la comunidad de DNS. Esto se especifica en el RFC2065 que incluía una cobertura limitada de los problemas de actualización dinámica, pero en última actualización se especifica en el RFC 2137 de nombre Secure Domain Name System escrita por Donald Eastlake que se publicó en abril de 1997, de acuerdo a la aplicación y la experiencia operacional de los desarrolladores y los primeros usuarios. RFC2535 - Domain Name System Security Extensions escrito por Donald Eastlake se publicó en marzo de 1999.

[4] Tomado y traducido de http://isoc.org/wp/ietfjournal/?p=97#more-97

En mayo del 2000 fue publicado TSIG como el RFC 2845 que es la autentificación en la transacción de nivel mediante el uso de secreto compartido mediante la firma.

Los operadores de dominio sueco y holandés de nivel superior, NLnet Labs y RIPE NCC. Descubrieron problemas de funcionamiento con los intercambios de claves entre primarios y secundarios. Esta fue una de las principales cuestiones que dieron lugar a una reescritura importante que se convirtió en tres especificaciones en los RFC4033, RFC4034 y RFC4035 - publicado en marzo de 2005, aunque esta vez ya tenía un grupo de trabajo comprometido a resolver el problema de privacidad.

2.4 AMENAZAS DEL DNS

Las amenazas es todo aquello que intenta o pretende destruir algún sistema, explotando los fallos de seguridad que se denominan vulnerabilidades ocasionando incidentes que originan pérdida o daños a las empresas.

Una vulnerabilidad son defectos o debilidades en los diseños, implementación, controles o procedimientos de seguridad que se le proporciona a un sistema que pueden ser explotados intencionalmente.

Es por ello que las amenazas son las situaciones que pueden hacer explotar en muchas ocasiones intencionalmente para los servidores de nombre de dominio o accidentales de las vulnerabilidades que tiene.

En la red de comunicación (internet) existen muchos riesgos y es por ello que, es necesaria la implementación de seguridad para reducir los niveles de vulnerabilidades y así no tener pérdidas o alteración de la información.

2.5 VULNERABILIDADES QUE TIENEN LOS DNS

En los servidores de nombre de dominio (DNS) existen diferentes amenazas que se mencionan en el RFC 3833 comunes o que han ocasionado problemas al haber sido explotadas así como mencionando una posible solución para proteger los servidores.

2.5.1 INTERCEPTACIÓN DE PAQUETES

En el internet existe dos tipos de comunicaciones TCP (Transmission Control Protocol) es el protocolo de control de trasmisión que crea una conexión donde se mandar todo el flujo de datos es decir que se establece un canal de comunicación que garantizara la entrega de datos correctamente y UDP (User Datagram Protocol) es el protocolo basado en el intercambio de datagramas sin que se establezca una conexión ya que el datagrama contiene la información de direccionamiento, no incluye el control del flujo, por lo que los paquetes pueden llegar en diferente orden y no garantiza que llegue completamente la información. Es por ello que una es más segura que la otra los DNS trabajan con una conexión UDP es decir el usuario consulta a los DNS y este le envía la información en un solo paquete sin firmar y garantizar que realmente es lo que el usuario busca, esta información puede ser modificada y redireccionar al usuario a otra página.

La interceptación de paquetes es una de las amenazas en contra de los DNS especificado en el RFC donde es la apropiación de los paquetes en el medio de comunicación y es causada por no contener una firma o un canal seguro permitiendo a un ente ajeno a la conversación y enterarse de todo lo que el usuario busca para después poder emplear la información como a él le convenga.

Esta vulnerabilidad se puede mejorar si se firmara los servidores como en una zona de seguridad como por ejemplo TSIG donde existe una relación de confianza entre un cliente especifico y particular que comprobara la firma por

que garantiza la integridad de la comunicación de los servidores o DNSSEC que realiza la comprobación de las firmas y cuando se aplica correctamente prevé la integridad de datos.

2.5.2 ID GUESSING AND QUERY PREDICTION

Puesto que los DNS en su mayor parte se utiliza sobre el protocolo UDP/IP, es relativamente fácil para un atacante generar paquetes que coinciden con el protocolo de transporte.

Dado que el DNS crea la siguiente cabecera especificada en la figura 2.3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	Opcode				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

Figura 2.3 Cabecera del DNS

Donde:

ID es el identificador utilizado para relacionar solicitudes y respuestas.

QR identifica el mensaje como una solicitud (Query **0**) o una respuesta (1)

Opcode: de 4 bits describe el tipo de solicitud.

- 0 estándar es decir una solicitud normal (nombre a dirección).
- 1 inverso, solicitud Inversa (dirección a nombre).
- 2 status del servidor, estado del servidor.
- 3-15 reservado para un uso a futuro.

AA indica que la respuesta fue por un servidor autoritativo.

TC Indica que el mensaje fue truncado.

RD indica la solicitud de un servicio recursivo por parte del servidor de nombre. Este servicio normalmente no está disponible.

RA Indica la disponibilidad del servicio recursivo.

Z es un campo de 3 bits reservado para un uso futuro, y su valor definido por 0.

RECODE este campo lo escribe los servidores de nombre de dominio, y sirve para indicar el tipo de búsqueda como puede ser:

- ***0:*** Sin error.
- ***1:*** Format Error es decir que es imposible interpretar el formato de la búsqueda.
- ***2:*** Server Failure es el error que indica que es imposible procesar el servidor.
- ***3:*** Name Erro el nombre no existe.
- ***4:*** Not implemented es el tipo de búsqueda que no es soportada.
- ***5:*** Refused es la solicitud rechazada.

QDCOUNT indica el número de entradas en la sección de Preguntas.

ANCOUNT que indica el número de Resource Records en la sección de Respuesta.

NSCOUNT define el número de Resource Records en la sección de Autoridad.

ARCOUNT define el número de Resource Records en la sección de Archivos Adicionales.

El campo ID en la cabecera del DNS es sólo un campo de 16-bits y el puerto UDP del servidor DNS asociados a una pregunta es de 16 bits, es decir sólo hay 2^{32} posibles de que el ID y puerto UDP, sin embargo el paquete del ID en algunas implementaciones de servidores de DNS no cambian aleatoriamente y el puerto es fijado para compatibilidad con firewalls a un cliente determinado.

Es por ello que existe una posibilidad de 2^{16} de que se realice el ataque que se basa en la predicción del canal cuando éste se encuentra ocupado y que la probabilidad de éxito cuando la víctima se encuentra en un estado, ya que la

víctima reinicia continuamente o posiblemente su comportamiento sea influenciado por algún atacante o porque la víctima está respondiendo (de una manera predecible) a alguna tercera persona y esta acción es conocida por el atacante.

Este ataque no necesita estar en un tránsito o de red compartida. Es similar a la intercepción de paquetes. Una solución es que la firmas de DNSSEC controle y sean capaces de detectar la respuesta, han sido falsificadas y en caso de no ser utilizado DNSSEC se sugiere utilizar TSIG o algún mecanismo equivalente para garantizar la integridad de sus comunicaciones con un servidor de nombre recursivo que lleva a cabo la revisión de la firma.

2.5.3 NAME CHAINING

Tal vez la clase más interesante en las amenazas del DNS es la llamada name chaining, ya que son un subconjunto de ataques basados en nombres, llamadas "envenenamiento de caché". Los ataques basados en nombres pueden ser parcialmente mitigados por una la larga duración de control en los mensajes de respuesta para la consulta original, pero esas excepciones de no captura dan origen al ataque.

Hay variaciones en el ataque, pero lo que todos tienen en común es afectar los *Resource Records* (RR) en el DNS sino que directamente se asigna a un nombre. Cualquier *Resource Records* que al principio permita a un atacante introducir mal los datos en la caché de la víctima.

Los registros de tipo: CNAME, NS, y DNAME pueden redirigir la consulta de la víctima a un lugar dependiendo de la elección del atacante. *Resource Records* (RR) con MX y SRV son menos peligrosos, pero en principio también se puede utilizar para desencadenar otras búsquedas en lugar de ser asignada por el atacante.

La forma general del ataque de encadenamiento de nombre es descrita como:

- La Víctima emite una consulta, tal vez a instancias del atacante o un tercero, la consulta puede ser sin relación, bajo el nombre del ataque (es decir, el atacante sólo utiliza esta consulta como un medio para introducir información falsa acerca de algún otro nombre).
- El atacante inyecta respuesta, ya sea a través de la interceptación de paquete, o por ser un servidor de nombres legítimos que está implicado en algún momento en el proceso de respuesta a la consulta que la víctima publicará en breve.
- La respuesta del atacante incluye uno o más *Resource Records* con nombres DNS; dependiendo de la forma particular, este ataque tiene el objeto que puede inyectar datos falsos relacionados con los nombres en la caché de la víctima, o puede ser para redirigir la siguiente etapa de la consulta a un servidor de la elección del atacante (con el fin de inyectar o colocar las mentiras de la Autoridad o de *Resource Record* de una respuesta, donde tendrán una mejor oportunidad de defensas de un programa de resolución).

Cualquier atacante que puede insertar en los *Resource Records* en la caché de una víctima puede realizar algún tipo de daño, por lo que hay ataques al envenenamiento de caché o encaminamiento de nombre. Sin embargo, en el caso del ataque de encadenamiento de nombres es la relación causa-efecto entre el ataque inicial y el resultado final puede ser mucho más compleja que en los otros las formas de envenenamiento de caché, así que el nombre encadenar ataques merecen una especial atención.

El thread común en todo el nombre del encadenamiento de los ataques es el mensajes de respuesta que permitirá al atacante la introducción del nombre al DNS de forma arbitraria y facilitar más información que las reclamaciones con el

atacante, así asociando los nombres, a menos que la víctima conozca los datos asociados con el nombres y pueda detectarlos de lo contrario la víctima va a tener dificultades para defenderse de esta clase de ataques.

Con los DNSSEC se pretende que se proporcione una buena defensa contra la mayoría de variaciones en esta clase de ataque. Al revisar las firmas, se puede determinar si los datos asociados a un nombre realmente se insertaron por la autoridad delegada por esa porción del espacio de nombres DNS.

Las firmas DNSSEC no cubren los registros de cola, dando así la posibilidad de que un nombre de encadenamiento en el ataque con la cola, pero con DNSSEC es posible detectar el ataque de forma temporal y así dando origen a la aceptación de la cola con el fin de recuperar la versión firmada autorizada de los mismos datos, a continuación, comprobar las firmas en la versión auténtica.

2.5.4 BETRAYAL BY TRUSTED SERVER

Otra variación sobre el ataque de interceptación de paquetes es la confianza del servidor que en muchos casos resulta no ser tan confiable, ya sea por accidente o por intentos del cliente servidor que es configurado como resolvers y este utiliza los servidores de confianza para realizar toda consulta del nombre de dominio.

En muchos casos la confianza del servidor es proporcionada por los usuarios ISP y de publicidad destinada al cliente a través de DHCP o por opciones de PPP. Además de la traición accidental de esta relación de confianza (A través de errores de servidor, servidor de éxito robos, etc).

El servidor puede ser configurado para devolver las respuestas que no son lo que el usuario desea, ya sea en un intento sincero de ayudar al usuario o para promover algún otro objetivo, como la promoción de una sociedad comercial entre el ISP y algunos terceros.

Este problema en particular es especialmente grave para los travelers que llevan a su propio equipo y esperar que funcione en la mayor parte, de la misma manera donde quiera que vayan. Estos travelers necesitan de confianza en el servicio DNS sin tener en cuenta que opera la red a la que su equipo está conectado.

Aunque la solución obvia a este problema sería que el cliente eligiera un servidor más confiable, en la práctica esto no puede ser una opción para el cliente. El entorno de la red de un cliente tiene sólo un número limitado de servidores de nombres recursivos que elegir, y ninguno de ellos puede ser particularmente digno de confianza. El filtrado de puertos u otras formas de intercepción de paquetes puede evitar que el cliente sea capaz de ejecutar una resolución interactiva. Así, mientras que la fuente inicial de este problema no es un ataque al protocolo de DNS, este tipo de traición es una amenaza para los clientes DNS, y simplemente cambiando a un servidor de nombre recursivo en otro diferente no es una defensa adecuada.

Visto estrictamente desde el punto de vista del protocolo DNS, la única diferencia entre este tipo de traición y un ataque de intercepción de paquetes es que el cliente ha enviado voluntariamente su solicitud al atacante. La defensa contra un ataque a la intercepción del paquete: es la resolución de cualquiera que debe comprobar las firmas de DNSSEC o el uso TSIG (o equivalente) para autenticar el servidor en el que ha depositado su confianza.

Teniendo cuenta que el uso de TSIG pero que por sí mismo no garantiza que un servidor de nombres es en absoluto fiable. TSIG puede hacer una resolución de ayudar a proteger su comunicación con un servidor de nombre que ya ha decidido confiar por otras razones. La protección de una resolución de la comunicación con un servidor que está dando falsas respuestas no es particularmente útil.

También hay que tener en cuenta que si el trozo de resolución no confía en el servidor de nombres que está realizando un trabajo en su nombre y quiere comprobar las firmas de DNSSEC, la resolución realmente tiene que tener conocimiento independiente a la clave pública DNSSEC (s) que necesita para llevar a cabo el chequeo. Por lo general, la clave pública para la zona de las raíces es suficiente, pero en algunos casos el conocimiento de claves adicionales puede también ser adecuada.

2.5.5 DNS DENEAL OF SERVICE (“NEGACIÓN DE SERVICIO” O “DNS DOS”)

Los ataques de negación de servicio utilizando la vulnerabilidad del DNS, puede llevarse a cabo de distintas maneras. Una de ellas es aprovechando las respuestas negativa que genera como respuesta un servidor de nombre de dominio ejemplo se quiere saber en la ubicación de ingeneria.unam.mx, los servidores mandan la respuesta de que no existe el nombre de dominio esto se toma como denegación del servicio. También cuando la consulta te manda a otra página que no contiene lo que el usuario requiere. El DNS es vulnerable a la denegación de servicio, y no existe mecanismo de protección, por lo que DNSSEC no ayudaría a este tipo de vulnerabilidades.

2.6 ¿QUÉ ES DNSSEC?

En la solución de las vulnerabilidades de los servidores de nombre de dominio (DNS) en el RFC 3833 se recomienda utilizar TSIG y DNSSEC, pero ¿Qué es TSIG y DNSSEC como funciona?

Como se vio anteriormente el DNS realiza una consulta en forma de árbol invertido donde parte de los Root Server (DNS), y preguntando a diferentes DNS dependiendo del nivel hasta encontrar la ubicación de donde se localiza en nombre que apunta a una IP.

Ya que la actualización de los mensaje de los Servidores de Nombre de Dominio, como son las respuestas y actualizaciones es complicado, surge el protocolo TSIG (Secret Key Trasaction Authentication for DNS Firma de transacción) publicado en el RFC 2845 utilizado sobre DNS, la implementación consta en autoriza a dos sistemas que estén intercambiando información mediante una llave compartida que permite el nivel de autenticación.

La transmisión de datos de una manera segura mediante la utilización de funciones hash para proporcionar medios de autenticación a los servidores, protección en los mensajes (como trasferencia de zonas) y actualizaciones de zonas de los DNS de una forma dinámica.

TSIG utiliza la función has MD5, con la variable HMAC-MD5 una función con un valor de 128 bits. La firma de TSIG incluye el tiempo que el mensaje firmo el DNS, esto para ayudar a combatir los ataques ya que a un hacker captura la firma.
DNSSES en el periódico El Universal se define como:

“DNSSEC es un protocolo que verifica y valida las respuestas del servidor de nombres a través de redes de confianza, lo que permite que el sistema de nombres de dominios sea más seguro.”[5]

En otras palabras el Domain Name System Security Extensions o Extensión de seguridad (DNSSEC) especificado en el RFC 2535, es el protocolo que aporta autentificación e integridad a los registros de recursos de las zonas de los DNS mediante la utilización de cadenas de confianza mediante la firma de cada servidor que realice la consulta.

[5] Periódico EL UNIVERSAL 24 de junio del 2010 http://www.eluniversal.com.mx/articulos/59265.html

Es por ello que proteger a los DNS de ciertos ataques anteriormente mencionados que requieren por lo que se necesita cambiar el protocolo del DNS tiene los *Resource Records (RR) los más conocidos o utilizados* son*:*

- **NS** (**N**ame **S**erver): Es el nombre de los servidores DNS tanto primarios como secundarios que se encuentran definidos dentro del archivo de zona es decir que disponen de la dirección y nombre para el dominio.
- **A** (**A**ddress)**:** Indica la dirección IP asociada al nombre host.
- **MX** (**M**ail E**x**changer)**:** Es el nombre del servidor encargado del correo en ese dominio asi como la prioridad.
- **CNAME** (**C**anonical **Name**)**:** Indica cuál sea el nombre canónico de un alias.
- **PTR** (**P**oin**t**e**r**)**:** Host Name – Pointer Indica el dominio asociado a una dirección IP.
- **TXT** (**T**e**xt**)**:** – datos del Host arbitrariamente utilizados para las listas negras.
- **SOA** (**S**tart **of A**uthority) indica los datos de la autoridad para el domino o zona en cuestión, por lo que cada dominio deberá de existir.

DNSSEC agrega cuatro tipos de recursos nuevo registro: registro de recursos Firma (RRSIG), DNS de Clave Pública (DNSKEY), Delegación Firmante (DS) y Next segura (NSEC).

Así también se agrega dos bits como cabecera (header) en el DNS como indicadores como son:

Checking Disabled (comparación de movilidad reducida CD).
Authenticated Data (Autenticacion de datos AD)

2.7 RRSIG

El registro Resource Record Signature (RRSIG) almacena la firma digital de un RRset.

Un RREset es un grupo de registros de recursos con el mismo propietario, clase y tipo, esto ahorra tiempo de estar buscando un registro de direcciones, es decir el propietario seria iingeneria.unam.mx se creo que registro ww2.iingeneria.unam.mx como se muestra en la figura 2.4

```
; File written on Fri Aug 13 13:02:11 2010
; dnssec_signzone version 9.4.2-P2
iingen.unam.mx.         7200    IN SOA  kate.nic.unam.mx. dns.unam.mx. (
                                        2010081100 ; serial
                                        3600       ; refresh (1 hour)
                                        1200       ; retry (20 minutes)
                                        604800     ; expire (1 week)
                                        7200       ; minimum (2 hours)
                                        )
                        7200    RRSIG   SOA 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        X9bBDUmYufjs9ImihAFm6Jgf3ncDASWDm9tZ
                                        sSEUMYF7K8m0mzWVqv5EfiYd793vqOP2/EOw
                                        1aOoCPliX6u6NQ== )
                        7200    NS      kate.nic.unam.mx.
                        7200    NS      jack.nic.unam.mx.
                        7200    RRSIG   NS 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        lVIdmco8P0ppDUbOC+hnBN1nzaSFt7vsRUSl
                                        Xo/eIzjj4OZgGhJikHqVGjxjwzBn9ucgnbyn
                                        9rTo7/+FH/uipg== )
                        7200    NSEC    ww2.iingen.unam.mx. NS SOA RRSIG NSEC DNSKEY
                        7200    RRSIG   NSEC 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
                                        nF2LeC1+R4txo5BviP+vasF9We1oQA97FEN3
                                        iV5PoURuHoic9YbLqnFPejOzSE0ZWqUo+1Gz
                                        zVjqvMGly111rg== )
                        7200    DNSKEY  256 3 5 (
                                        AwEAAayDoYmhLfOs8baHUsqfU4yGjprYlDa5
                                        1aLiLknbPKm/3N01maneP0Yn/qwOM6mgSIyz
                                        +eE2u30TdPiioojHU3ws=
                                        ) ; key id = 21306
                        7200    DNSKEY  257 3 5 (
                                        AwEAAb6JRoTbURvDYkg+qMya3LDvqaOzWali
                                        gtPdcn9LABB15A4416l1MHGyeGzgO2mfDZjS
                                        A5EUFmbQ42WdmIP75dc=
                                        ) ; key id = 12604
                        7200    RRSIG   DNSKEY 5 3 7200 20100912170211 (
                                        20100813170211 21306 iingen.unam.mx.
iingenunam.signed 52%
```

Figura 2.4 Resource Record Signature (RRSIG) con RRset

En donde el propietario es iingeneria.unam.mx y todo lo que se encuentre registrado bajo el está firmado de la siguiente manera como se visualiza en la figura 2.5.

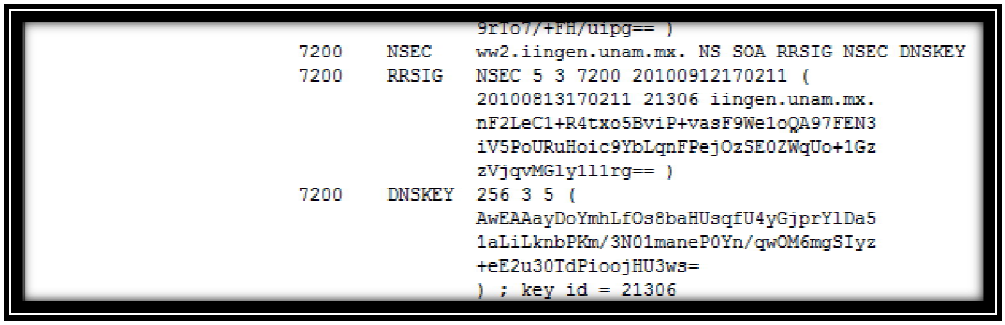

Figura 2.5 Firma de RRSIG.

- ***Tipo de cubierta*** *es el primer campo*. Eso nos dice que es NSEC que tiene por registro ww2.iingen.unam.mx
- ***Algoritmo con valor 5 es el segundo campo.*** Este es uno de los mismos valores utilizados en el registro DNSKEY, para cada RRset, es con un número 5 algoritmo RSA/SHA-1 y un 3 el algoritmo DSA.
- **Campo de etiqueta:** es el número de etiquetas que hay en el nombre del propietario de los documentos firmados ww2.iingen.unam.mx, contiene 3 etiquetas.
- **El *TTL original*** en los registros de la RRset que se firmó. (Todos los registros en un RRset se supone que tienen el mismo TTL.) El TTL necesita ser almacenado porque un servidor de nombres caché de la RRset que este en el registro se cubre RRSIG disminuir el TTL en los registros almacenados en caché. Este número es imposible reconstruir los registros de direcciones originales para verificar la firma digital.
- Los dos campos siguientes son de **inicio y expiración** de firma, respectivamente, los dos registros son almacenados con números enteros sin ningún signo de segundos son presentados en el YYYYMMDDHHMMSS (año, mes, día, hora, minuto y segundo). El

tiempo de creación de firma es por lo general el tiempo que el programa firmo la zona.

- ***Etiqueta de clave*:** es una huella digital derivada de la clave pública que corresponde a la clave privada que firmo la zona Si la zona tiene más de una clave pública, la verificación de software DNSSEC utiliza la etiqueta clave para determinar qué tecla de usar para verificar esta firma.
- **El campo de sesiones** en este caso iingen.unam.mx, es el que *firma el nombre del* campo. Es el nombre de dominio de la clave pública que un verificador debe utilizar para comprobar la firma. Es la etiqueta de clave, identifica el registro usado DNSKEY. El nombre del firmante del campo es siempre el nombre de dominio de la zona de los registros firmados.
- **El *campo de firma*:** esta es la firma digital de la clave privada de la zona en los registros de firma y del lado derecho del registro RRSIG, y esta se encuentra codificada en base 64.

RRSIG es calculada utilizando la clave privada. Un servidor con soporte DNSSEC intentará devolver los RRs solicitados y sus correspondientes registros RRSIG para poder ser chequeados posteriormente.

2.8 DNSKEY

El registro DNSKEY se utiliza para almacenar una clave pública necesaria para verificar los registros RRSIG.

La zona de clave privada se almacena en un lugar seguro, en un archivo en el sistema de archivos localizado en el Servidor de Nombre de Dominio primario o maestro, la clave pública de la zona que se anuncia como un registro vinculado al nombre de dominio de la zona y es por ello que solo almacena la clave de una zona como se muestra en la siguiente figura 2.6.

Figura 2.6 firma de DNSKEY

Después del tipo de firma que es DNSKEY siguen los siguientes campos:

Es 257 es el valor de la bandera, este es de longitud de dos bytes y codifica un conjunto de valores como se observa en la siguiente figura2.7.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
							ZK								SEP

Figura 2.7 campo de banderas disponibles

Donde los primeros bists del 0 al 6 y del 8 a 14 están reservadas y deben de tener un valor de 0.

En bit octavo es el tipo de calve:

- **0** es una clave de zona DNS y no se puede utilizar para verificar los datos firmados por la zona.
- **1** es la clave de zona DSN. El nombre de registro DNSKEY, el propietario es el nombre de dominio de al zona.3757.

El valor 3 es el campo de protocolo: es un vestigio de la versión DNSSEC.

El valor 5 es el campo de algoritmo, donde DNSSEC puede trabajar con diferentes algoritmos en la clave los valores son los siguientes:

- **0** Reservados.

- **1 RSA/MD5**. El uso de RSA/MD5 ya no se recomienda, sobre todo debido a las deficiencias descubiertas recientemente en el algoritmo de hash MD5 de un solo sentido.
- **2 Diffie-Hellman** no se puede utilizar para firmar las zonas, pero puede ser utilizado para otros fines relacionados con DNSSEC.
- **3 DSA/SHA-1** (además de cualquier algoritmo obligatorio) es opcional.
- **4Reservado** para un algoritmo de clave pública elíptica curva basada en.
- **5 RSA/SHA-1**. El uso es obligatoria.
- ***253-254*** **.**Estos números algoritmo son reservados para uso privado por RFC 4034.
- ***255*****Reservados.**

El último campo en el registro DNSKEY es la clave pública y se codifica en base 64.

DNSSEC admite claves de longitudes de muchos. Cuanto más larga sea la clave, más segura (porque es más difícil para encontrar la clave privada correspondiente), pero cuanto más tiempo se tarda en firmar datos de la zona con la clave privada y verificar con la clave pública, y más largo es el de la DNSKEY registro y firmas creadas.

2.9 NSEC

Este registro es utilizado para la comprobación de la consistencia interna. Indica qué RRset es el próximo en la zona y qué tipo de códigos están disponibles para el nombre actual.

El registro NSEC resuelve el problema de la firma de respuestas negativas. Abarca una brecha entre dos nombres de dominio consecutivos en una zona, que le dice que el nombre de dominio que sigue después de un name hacen el dominio dado el nombre del registro: "Siguiente segura"

Pero no la noción de "nombres de dominio consecutivos" implica un orden canónico a los nombres de dominio en una zona. Para ordenar los nombres de dominio en una zona, se empieza por la clasificación por la etiqueta más a la derecha en los nombres de dominio, a continuación, en la etiqueta junto a la izquierda, y así sucesivamente. Las etiquetas son ordenadas mayúsculas y minúsculas y lexicográficas (por orden de diccionario), con los números que vienen antes de las letras y los números de las etiquetas antes inexistentes como se muestra en la siguiente figura 2.8.

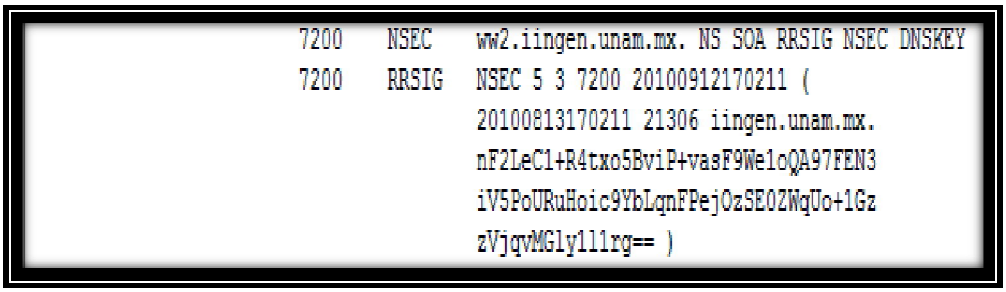

Figura 2.8 Figura NSEC

El nombre de dominio a lado en la zona después de iingen.unam.mx es ww2.iingen.unam.mx tiene registros como son NS, SOA, RRSIG, un registro NSEC y un registro DNSKEY.

El último registro NSEC en una zona contendrá el nombre de la zona, tratando el espacio de nombre como circula, dado que no hay realmente ningún nombre de dominio que sigue después, este indica que no hay otro registro de iingen.unam.mx mas que los anteriores.

El registro NSEC, en su totalidad identifica y especifica lo que existe bajo una zona, indicando “Eso no existe” y con ello reduce las demandas falsas de nombres de dominio o registros que no existen.

2.10 DS

El registro Delegation Signer (DS) es un puntero para construir cadenas de autenticación, DS o firma de delegación identifica la clave pública autorizada para firmar el iingen.unam.mx los datos de la zona. El registro DS en el registro RRSIG, da fe de que si pertenece a la zona.

2.11 COMPARACIÓN DE MOVILIDAD REDUCIDA (CD) Y AUTENTICACIÓN DE DATOS (AD)

En la cabecera del DNS como se muestra en la figura 2.9 se anexaron dos banderas de consulta AD y CD ambos son parte de la consulta estándar del encabezado como se puede visualizar en la siguiente figura 2.10.

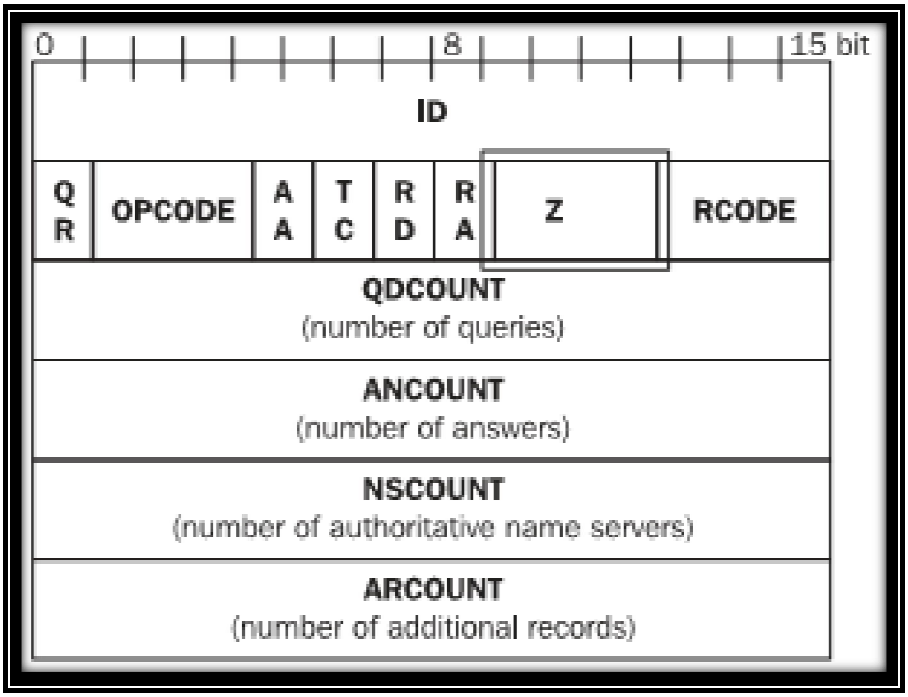

Figura 2.9 Cabeceras DNS

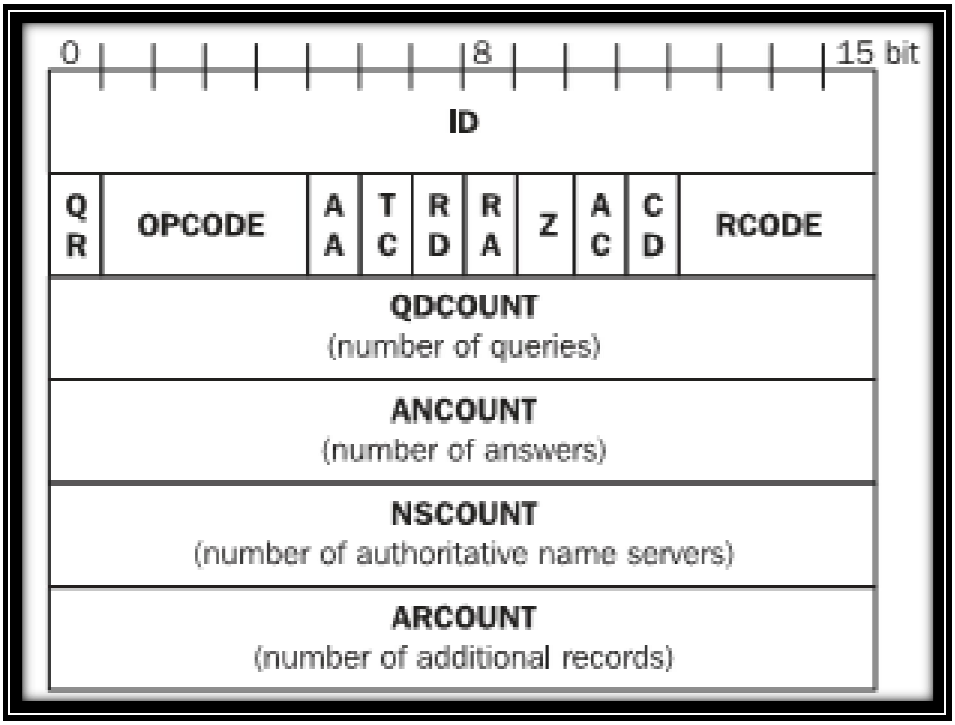

Figura 2.10 Cabeceras de DNSSEC

El bit AD está diseñado para permitir que los resultados de la consulta de un servidor de nombres que admite DNSSEC, pero no pueden comprobar los registros DNSSEC para determinar si una respuesta ha sido validada. Sin embargo, estos solucionadores sólo deben confiar en el valor del bit AD si su canal de comunicación con el servidor de nombres es secureusing IPSEC o TSIG, por ejemplo.

El bit de CD, por el contrario, es para el uso de resultados que *pueden* comprobar los registros DNSSEC, que es una abreviatura para la comprobación de movilidad reducida, le dice al servidor de nombres para no molestar a la verificación de los registros DNSSEC en la resolución de nombre, ya que puede manejar el trabajo en sí.