TRANSACTION SIGNATURE (TSIG). UNA ALTERNATIVA DE SEGURIDAD PARA TRANSFERENCIAS DE ZONAS DNS.

Sánchez Ernesto, Di Mauro Juan, Silvera Jorge Arias Figueroa Daniel.
C.I.D.I.A./Departamento de Informática/Facultad de Ciencias Exactas/Universidad Nacional de Salta
Av. Bolivia 5150
0387-4255547

esanchez@cidia.unsa.edu.ar; juannombreapellido@gmail.com; jsilvera@arnet.com.ar; daaf@cidia.unsa.edu.ar

RESUMEN

Desde su creación el Sistema de Nombres de Dominio, ha carecido de un diseño que asegure la comunicación entre las partes que intervienen en el proceso de resolución de nombres. Y dada su condición de sistema público y estructura jerárquica, es que se encuentra expuesto a posibles vectores de "ataque" a lo largo de todo el flujo de datos intercambiado por los componentes (Clientes y Servidores) que lo conforman.

Es así que, en el Centro de Investigación y Desarrollo en Informática Aplicada (C.I.D.I.A.) perteneciente a la Universidad Nacional de Salta se formó un equipo de trabajo que se encuentra realizando una investigación aplicada cuyo objetivo es presentar de manera práctica el conjunto de vulnerabilidades presentes en el Sistema de Nombres de Dominio y definir las medidas a implementar para mitigar las mismas.

Se detalla a continuación un caso práctico sobre la vulnerabilidad presente en una transferencia de zona y la alternativa *TSIG (Transaction Signature)* como parte de un conjunto de medidas para dotar de seguridad a los procesos involucrados en tales transferencias.

Palabras clave:
Internet, Sistema de Nombres de Dominio, DNS Seguro, DNSSEC, TSIG. Transferencias de zonas DNS.

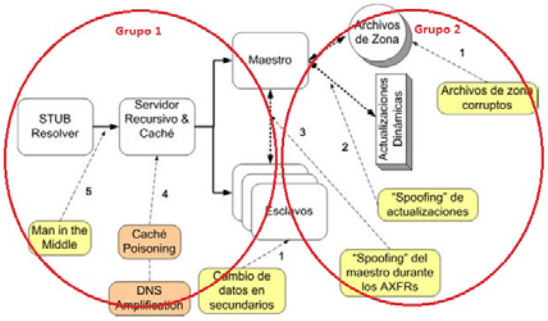
CONTEXTO

Lo expuesto en el presente trabajo, surge del proyecto de investigación "Extensiones de Seguridad para el Sistema de Nombres de Dominio" (Consejo de Investigación de la Universidad Nacional de Salta), en conjunto con el Centro de Investigación y Desarrollo en Informática Aplicada (C.I.D.I.A. – UNSa).

1. INTRODUCCION

La condición de sistema jerárquico del Sistema de Nombres de Dominio, lo expone a posibles vectores de "ataque" a lo largo de todo el flujo de datos intercambiado por los componentes (Clientes y Servidores) que lo conforman.

Las tareas iniciales en el marco del proyecto de investigación citado en el apartado anterior, fueron identificar y clasificar las amenazas a la seguridad de un Sistema DNS. El siguiente gráfico resume en términos generales los puntos críticos y se distinguen dos grandes grupos en el tráfico de red intercambiado [2]. El primer grupo se corresponde al tráfico intercambiado en procesos de consultas DNS (solicitud/respuesta) entre Clientes y Servidores, el segundo corresponde al tráfico correspondiente a la administración de archivos de zonas (actualización y transferencias de zonas) entre servidores maestro/esclavo.



En una etapa posterior, se seleccionó el segundo grupo de vulnerabilidades y se propuso el desarrollo de una aplicación en lenguaje Python, para enumeración y análisis de redes TCP/IP "Guesso" [4]. Mediante los módulos específicos para el protocolo DNS (*mydnsinterface y mydns*), basados en la librería *pydns* (bajo licencia OpenSource), se demostró la posibilidad de obtener información basada en transferencias de zonas DNS.

En resumen, la técnica consistió en hacer consultas DNS para cada uno de los tipos listados a continuación [2]:

Nombre	Descripción	código
A	dirección IP	1
NS	servidores DNS	2
CNAME	nombres canónicos	5
PTR	registro de puntero	12
HINFO	información de host	13
MX	Mail eXchange (servidores de correo)	15
AXFR	pedido de transferencia de zona	252

La tarea de obtención de información, se automatizó mediante el siguiente algoritmo, que volcaba los resultados obtenidos en una estructura de datos, lo que permitió enumerar los hosts pertenecientes a un dominio en particular:

```
def get_domain_hosts(dominio):
    tipos = ['NS','MX','A','PTR','CNAME','A']
    respuestas = []                    //lista vacía
    for t in tipo:
        respuestas.add(consulta(dominio,t))
    return procesar_respuesta(respuestas)
```

Se puede observar que la función recibe un nombre de dominio como argumento y retorna un diccionario indizado por tipo de consulta (o registro) cuyos valores son las respuestas de los servidores DNS para esa consulta.

Expuesta la vulnerabilidad para en caso de transferencia de zonas (tipo de consulta AXFR), y según se describe en [1], surge de manera natural como primera medida para mitigar este tipo de vulnerabilidad, denegar todo tipo de solicitud de transferencias de zonas y permitirlas, en caso de ser necesario, solo para un grupo restringido de host (listas de accesos de IP origen).
Del mismo modo que se presenta, como una rápida y sencilla alternativa a implementar, así se descarta, ya que la misma está expuesta a ataques de "suplantación de identidad" (*IP Spoofing*), mediante la técnica de "hombre en el medio" [7].

Es así que el siguiente nivel en el proceso de asegurar la transferencia de zonas fue implementar el protocolo TSIG [3], lo que permite la autenticación entre las partes basada en el uso de técnicas criptográficas, que aseguran que Cliente y Servidor son quienes dicen ser y por otro lado, asegurar la integridad de los datos (los datos recibidos por el Cliente son los que envió el Servidor).

Transaction Signature (TSIG): Definido en el RFC 2845, es un mecanismo que hace uso de una clave única mediante la implementación de Códigos de Autenticación de Mensaje entre servidores maestros y esclavos. La distribución de la clave hacia los servidores esclavos debe hacerse de manera segura utilizando medios como email seguro, fax o correo postal, se recomienda para la misma, periodos de actualización de entre 30 y 60 días. En caso de presencia de más de un servidor esclavo, se deben utilizar pares de claves (maestro-esclavo) diferentes, ya que al verse comprometida alguna de las claves, solo de deshabilitarían temporalmente las transferencias entre las partes afectadas, sin involucrar al resto de las transferencias.

A los fines prácticos, se menciona que TSIG fue configurado para DNS BIND versión

9.9.2-P1, sobre plataforma Linux Fedora 17. La clave compartida se generó mediante la utilidad *dnssec-keygen* [5][6].

Los resultados obtenidos en cada una de las etapas descritas anteriormente, nos permiten concluir que no existe una solución integral que permita dotar de seguridad al protocolo DNS y a las partes intervinientes en los procesos y operaciones de consultas, sino que se deben adoptar un conjunto de medidas que permitirán minimizar la exposición a los posibles ataques a la información intercambiada.

2. LINEAS DE INVESTIGACION y DESARROLLO

Los principales ejes temáticos que se están investigando son los siguientes:

- Sistema de Nombres de Dominio.
- Ataques típicos al Sistema de Nombres de Dominio.
- Criptografía de clave privada.
- DNSSEC.
- Transaction Signature (TSIG).

3. RESULTADOS OBTENIDOS/ESPERADOS

Con los resultados obtenidos en cada una de las etapas realizadas hasta ahora, se logró documentar un conjunto de políticas de seguridad que se espera sea el marco de referencia para los responsables de administrar un sistema DNS dentro del ámbito educativo. Por otro lado, en términos generales, se pretende acompañar el despliegue global que vienen teniendo las extensiones de seguridad para el sistema DNS.

.

4. FORMACION DE RECURSOS HUMANOS

La estructura del equipo de investigación es de 5 (cinco) miembros incluidos el Director y Co-director.
Dos miembros están realizando el trabajo de Tesis de Posgrado en Redes de Datos, dependiente de la Universidad Nacional de La Plata.
Otros dos participantes se encuentran realizando el trabajo de Tesis de Grado (*DNS Curve*), de la Carrera de Licenciatura en Análisis de Sistemas de la Universidad Nacional de Salta.

5. BIBLIOGRAFIA

[1] AITCHISON Ron, Pro DNS and BIND 10, 2da Edición, Apress, 2011, ISBN 978-1-4302-3049-6.
[2] FALL Kevin R. - STEVENS W. Richard, TCP/IP Illustrated, Volume 1. The Protocols, 2da Edición, 2012, ISBN-13: 978-0-321-33631-6.
[3] VIXIE P, GUDMUNDSSON O, EASTLAKE 3rd, D, WELLINGTON, B. RFC 2845: Secret Key Transaction Authentication for DNS (TSIG). Mayo 2000.
[4] Di Mauro Juan, trabajo de Tesis de pregrado “Guesso, software para enumeración y análisis de redes TCP/IP”. UNSa 2012.
[5] Clarifications and Implementation Notes for DNSSECbis - S. Weiler.
[6] RFC 4033: DNS Security Introduction and Requirements - R. Arends, R. Austein, M. Larson, D. Massey, S. Rose.
[7] RFC 3833: Threat Analysis of the Domain Name System (DNS) - D. Atkins, R. Austein