Un estudio comparativo en extensiones de seguridad para el sistema de nombres de dominio (DNS).

Sanchez Ernesto, Arias Figueroa Daniel, Rocabado Sergio, Aguero Verônica, Molina Gustavo/
Universidad Nacional de Salta
Av. Bolivia 5150
0387-4258614

esanchez@cidia.unsa.edu.ar; daaf@cidia.unsa.edu.ar; srocabado@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, lo que lo expuso a lo largo del tiempo, a constantes "ataques" de las más diversas formas, ataques que van desde la Denegación de Servicio, intercepción de los mensajes intercambiados entre clientes y servidores, suplantación de identidad mediante la técnica de Spoofing, hasta la técnica conocida como Envenenamiento de Cache.

Por su naturaleza de sistema público y por considerarse parte esencial para el funcionamiento de Internet, es que organizaciones y particulares, han puesto especial énfasis en la implementación de políticas y prácticas destinadas a dotar de seguridad al servicio proporcionado por DNS.

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 que permitirá analizar dos modelos que brindan extensiones de seguridad al Sistema de Nombres de Dominio, el primero de ellos, es el basado en criptografía de curva elíptica (DNSCurve), el segundo es el denominado DNSSEC, basado en el uso de criptografía asimétrica.

Palabras clave:
Internet, Sistema de Nombres de Dominio, DNS Seguro, DNSSEC, DNSCurve

CONTEXTO

El proyecto investigación "*Un estudio comparativo en extensiones de seguridad para el sistema de nombres de dominio (DNS)*", se desarrolla en el Centro de Investigación y Desarrollo en Informática Aplicada (C.I.D.I.A.) de la Facultad de Ciencias Exactas de la Universidad Nacional de Salta.

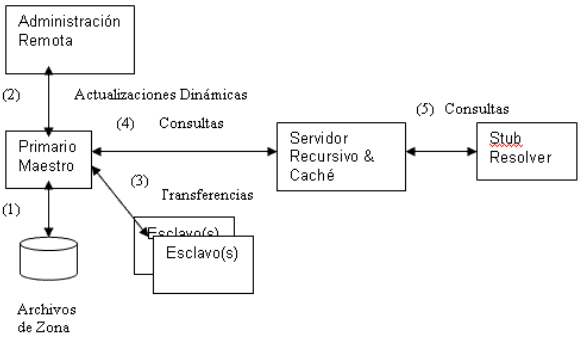
1. INTRODUCCION

A nivel macro, el servicio DNS es esencial para el funcionamiento de Internet. En un nivel micro o local, el servicio DNS podría ser esencial para el funcionamiento de una pequeña empresa con presencia en Internet a través de su sitio web. En todos los casos se debe poner especial atención en la seguridad, para garantizar la eficacia y la seguridad del sistema DNS.

Por su naturaleza de sistema público, desde sus comienzos el sistema DNS, es susceptible a "ataques" de los más diversos, por parte de usuarios mal intencionados, por lo que consideramos primordial en la definición de políticas y procedimientos de seguridad, conocer las vulnerabilidades del sistema DNS, representadas en las posibles fuentes de amenazas en los flujos de datos de dicho sistema.

Como parte de los resultados de trabajos de investigación, se presenta una clasificación de las amenazas a la seguridad de un sistema DNS, lo que permitirá la selección de los recursos y estrategias adecuadas para mitigar

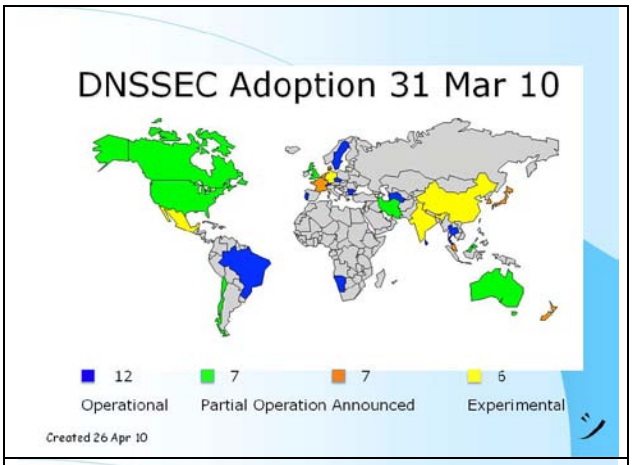
las mismas. La siguiente tabla [1] presenta un resumen de las amenazas más conocidas clasificadas según a que componentes afectan en un flujo de datos normal en un Sistema DNS.

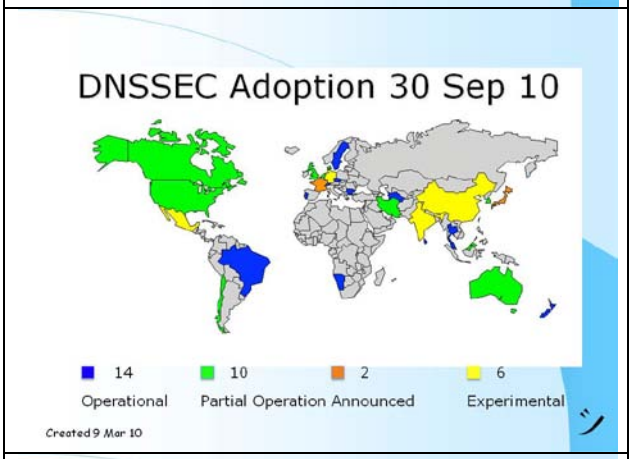


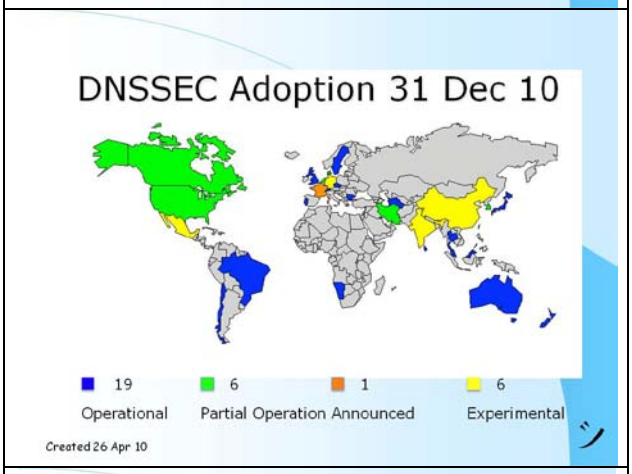
Etiqueta	Área	Amenaza	Clasificación	Solución
1	Archivos de Zona	Corrupción de archivos (accidental o mal intencionada)	Local	Políticas de administración
2	Actualizaciones dinámicas	Actualizaciones no autorizadas mediante la técnica de "IP Spoofing"	Servidor a Servidor	Arquitectura de red segura, Autenticación de solicitudes (TSIG, SIG(0)) o desactivadas.
3	Transferencias de Zonas	Suplantación de identidad del origen en la actualización de zonas mediante la técnica de "IP Spoofing"	Servidor a Servidor	Arquitectura de red segura, Autenticación de solicitudes (TSIG) o desactivadas.
4	Consultas remotas	Envenenamiento de Cache usando "IP spoofing", intercepción de mensajes mediante la técnica "Man in The Middle".	Servidor a Cliente	DNSSEC
5	Consultas a un Resolver	Envenenamiento de Cache usando "IP spoofing", intercepción de mensajes mediante la técnica "Man in The Middle".	Cliente remoto a Cliente	DNSSEC

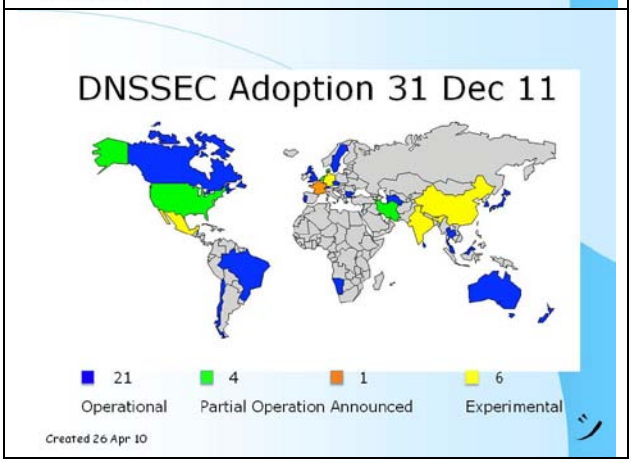
Estas formas de ataques descriptas anteriormente, son algunas de las que explotan vulnerabilidades de un diseño del protocolo de resolución de nombres (DNS) donde no se incluyeron medidas de seguridad como la autenticación y confidencialidad, razón por la cual hubo que ir añadiéndose a posteriori por medio de extensiones.

Dada la condición de sistema jerárquico, es que el proceso de migración a una alternativa que proporcione seguridad al proceso de resolución de nombres, no tiene una fácil solución y mucho menos rápida, ya que se hace necesaria una implementación a escala global. Por citar un ejemplo, para el caso de las extensiones de DNSSEC, son muy pocos los países que han adoptado tales extensiones para sus servidores raíz. A continuación se presentan los siguientes gráficos que muestran por un lado la situación actual de la implementación global de DNSSEC, y proyecciones de cómo el despliegue ira avanzando.









Fuente: DNSSEC Deployment Initiative

Consideramos que, el uso de extensiones de seguridad para DNS, no es una solución integral, sino que debe formar parte de una serie de medidas que pueden ayudar a minimizar la exposición a algunos de los ataques mencionados, es por esto que planteamos una investigación aplicada en la que se pretende estudiar y comparar alternativas de extensiones de seguridad para DNS y cual sería el impacto de su implementación dentro de una organización o red local. Del mismo modo nos encontramos trabajando en la elaboración de una guía a modo de políticas y conjunto de buenas prácticas a fin de evaluar un sistema DNS y tomar las medidas para hacer de ésta arquitectura lo más fiable y segura.

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 pública y Certificados digitales.
- Criptografía de curva elíptica.
- DNSSEC.
- DNSCurve.

3. RESULTADOS OBTENIDOS/ESPERADOS

En función a lo expresado en este trabajo, nuestra investigación tiende fundamentalmente a sentar las bases necesarias para la implementación de DNSSEC en el ámbito de la Universidad Nacional de Salta, tomando como referencia las especificaciones actuales del Sistema de Nombres de Dominio, estado del arte de vulnerabilidades y ataques en el Sistema anteriormente descrito y el aporte de los

resultados de los estudios comparativos de los modelos DNSSEC y DNS Curve. De un modo más amplio, pretendemos en una primera etapa, poner a disposición a la comunidad universitaria, la guía de políticas y buenas prácticas que permitan evaluar y asegurar un Sistema de Nombres de Dominio, que junto a la experiencia que resulte del caso de implementación, sirvan de referencia para entornos de red que requieran la implementación de un Sistema DNS con extensiones de seguridad.

.

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] Pro DNS and Bind – Ronald G. Aitchison (2005).
[2] DNSCurve: Usable security for DNS - Daniel J. Bernstein (2008).
[3] Elliptic Curve KEYs in the DNS - ECC Keys in the DNS - Richard C. Schroeppel, Donald Eastlake 3rd.
[4] An Illustrated Guide to the Kaminsky DNS Vulnerability - Steve Friedl's Unixwiz.net Tech Tips.
[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