Seguridad en DNS

Miguel Angel Astor Romero

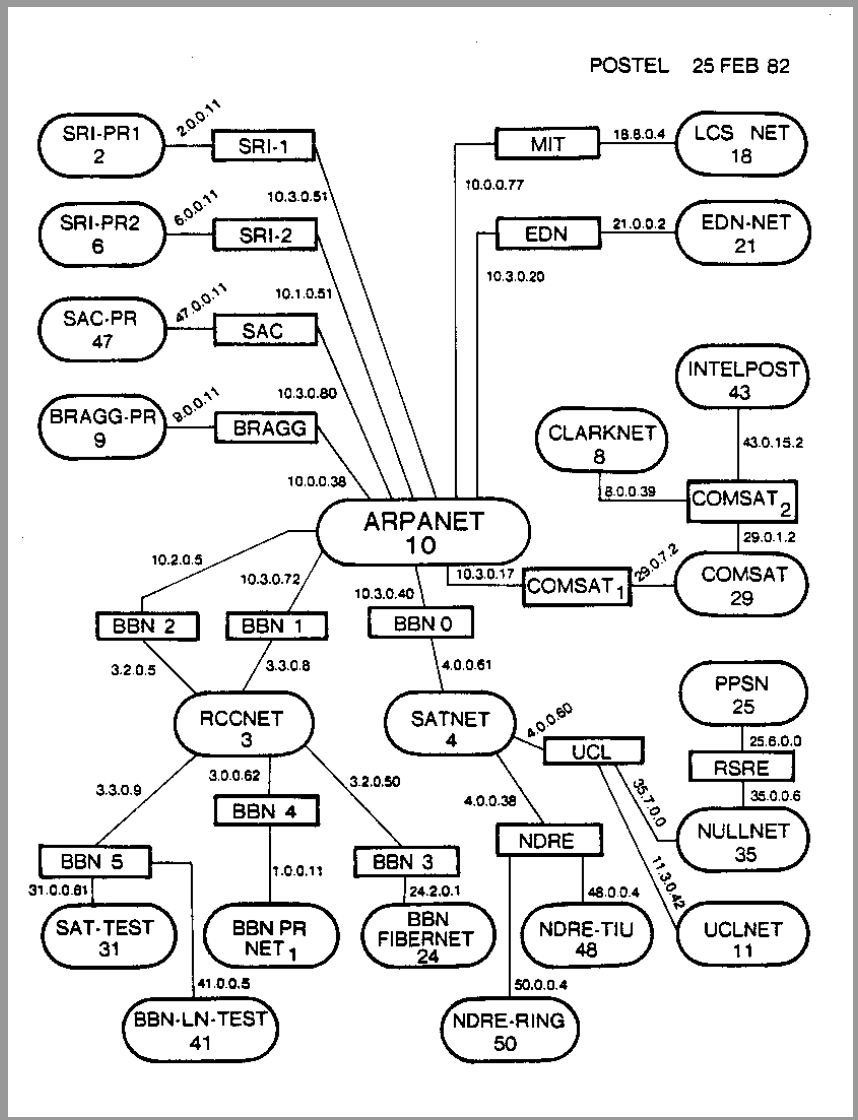
16 de Noviembre de 2017

Agenda

Consideraciones de Seguridad en DNS

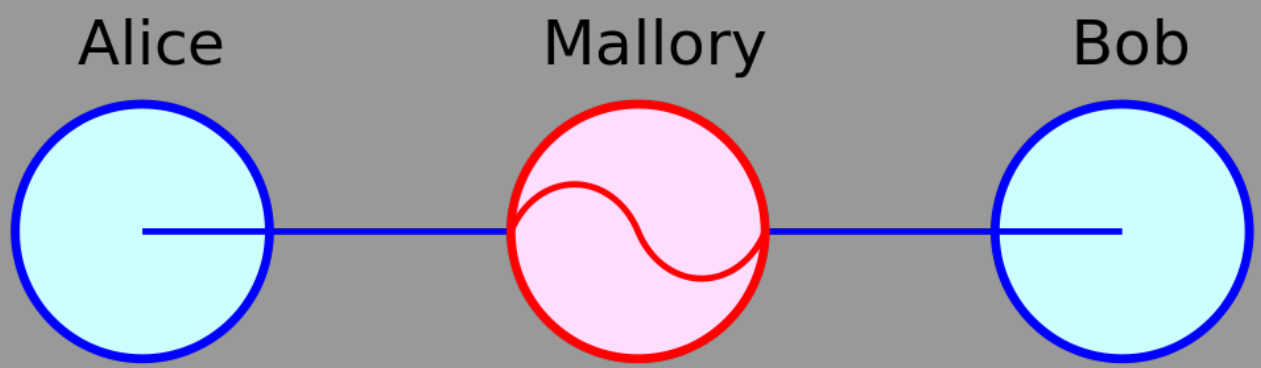
- DNS fue inventado en 1983 por Paul Mockapetris.
- El internet era muy pequeño en aquel entonces y "todos se conocían".
- La seguridad y privacidad de las comunicaciones no fueron consideradas en el diseño original de DNS.

Mapa de la Internet



J. Postel, febrero de 1982.

Ataques Man-in-the-Middle

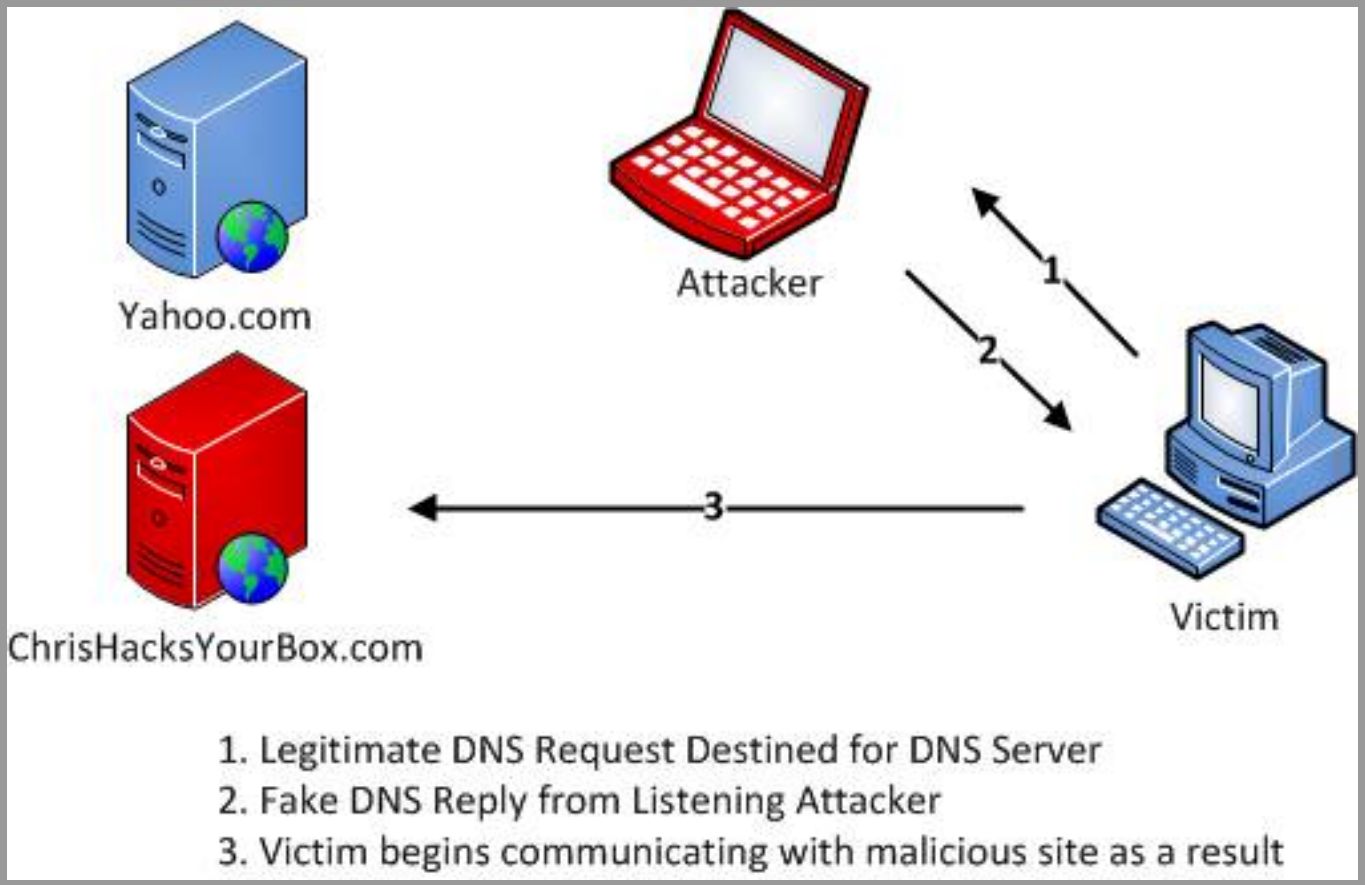


- DNS no posee mecanismos de autenticación de mensajes.
- Un atacante puede facilmente interceptar respuestas legítimas de servidores DNS y sustituirlas por respuestas adulteradas.

Envenenamiento de caché

- También llamado DNS *spoofing*.
- Consiste en sustituir las entradas de caché de un servidor o resolvedor DSN recursivo.
- Se realiza mediante ataques MITM, por ejemplo siguiendo un ataque de envenamiento de caché ARP.

Envenenamiento de caché

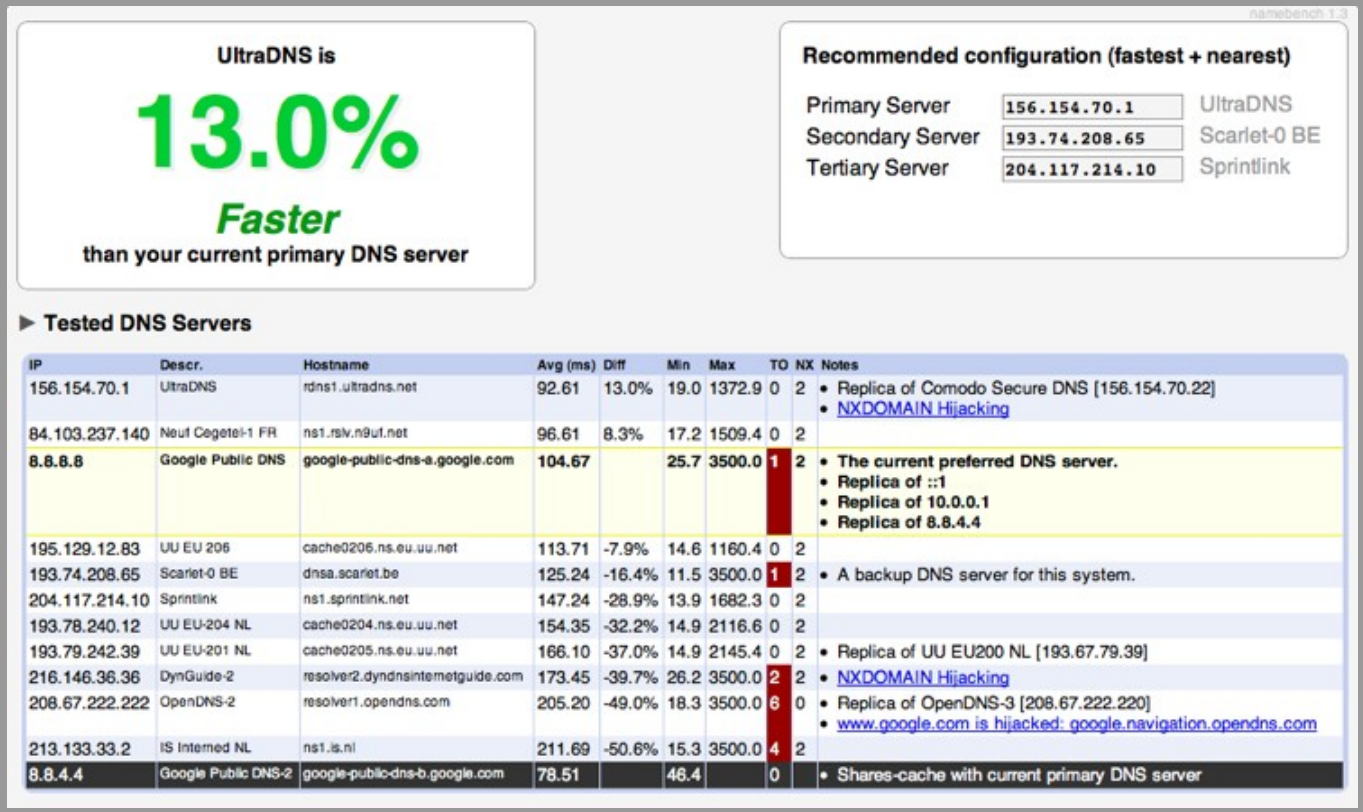


Imágen recuperada de `http://techgenix.com`

Secuestro de DNS

- Consiste en dos posibles ataques:
  1. Se sustituye el servidor DNS que se consulta en un cliente mediante algún ataque MITM.
  2. Se responde con información "falsa" cuando falla la resolución de un nombre (normalmente debería retornar una respuesta de tipo NXDOMAIN).
- El segundo "ataque" se utiliza institucionalmente:
  - En servicios de registro de nombres (publicidad).
  - En servidores DNS públicos (publicidad).
  - En ISP's (publicidad y censura).

UltraDNS



namebench 1.3

UltraDNS is

13.0%

Faster

than your current primary DNS server

Recommended configuration (fastest + nearest)

Primary Server	156.154.70.1	UltraDNS
Secondary Server	193.74.208.65	Scarlet-0 BE
Tertiary Server	204.117.214.10	Sprintlink

▶ **Tested DNS Servers**

IP	Descr.	Hostname	Avg (ms)	Diff	Min	Max	TO	NX	Notes
156.154.70.1	UltraDNS	rdns1.ultradns.net	92.61	13.0%	19.0	1372.9	0	2	• Replica of Comodo Secure DNS [156.154.70.22] • NXDOMAIN Hijacking
84.103.237.140	Neuf Cegetel-1 FR	ns1.rslv.n9uf.net	96.61	8.3%	17.2	1509.4	0	2	
8.8.8.8	**Google Public DNS**	**google-public-dns-a.google.com**	**104.67**		**25.7**	**3500.0**	**1**	**2**	• **The current preferred DNS server.** • **Replica of ::1** • **Replica of 10.0.0.1** • **Replica of 8.8.4.4**
195.129.12.83	UU EU 206	cache0206.ns.eu.uu.net	113.71	-7.9%	14.6	1160.4	0	2	
193.74.208.65	Scarlet-0 BE	dnsa.scarlet.be	125.24	-16.4%	11.5	3500.0	1	2	• A backup DNS server for this system.
204.117.214.10	Sprintlink	ns1.sprintlink.net	147.24	-28.9%	13.9	1682.3	0	2	
193.78.240.12	UU EU-204 NL	cache0204.ns.eu.uu.net	154.35	-32.2%	14.9	2116.6	0	2	
193.79.242.39	UU EU-201 NL	cache0205.ns.eu.uu.net	166.10	-37.0%	14.9	2145.4	0	2	• Replica of UU EU200 NL [193.67.79.39]
216.146.36.36	DynGuide-2	resolver2.dyndnsinternetguide.com	173.45	-39.7%	26.2	3500.0	2	2	• NXDOMAIN Hijacking
208.67.222.222	OpenDNS-2	resolver1.opendns.com	205.20	-49.0%	18.3	3500.0	6	0	• Replica of OpenDNS-3 [208.67.222.220] • www.google.com is hijacked: google.navigation.opendns.com
213.133.33.2	IS Interned NL	ns1.is.nl	211.69	-50.6%	15.3	3500.0	4	2	
8.8.4.4	Google Public DNS-2	google-public-dns-b.google.com	78.51		46.4		0		• Shares-cache with current primary DNS server

Forward Confirmed reverse DNS (FCrDNS)

- Se aplica con resolvedores recursivos al recibir respuesas no autorizadas (provenientes de caché).
- Consiste en realizar una búsqueda reversa para verificar que la IP obtenida efectivamente pertenece al dominio resuelto.
  - in-addr.arpa
  - ip6.arpa
- Por ejemplo, si un servidor responde que la dirección del dominio `www.example.com` es `190.169.74.203`, entonces se realiza la búqueda reversa `203.74.169.190.in-addr.arpa`, la cual debe retornar `www.example.com`.

DNS Security Extensions DNSSEC

- Agrega autenticación de las respuestas de los servidores DNS utilizando criptografía de clave pública con un modelo de cadena-de-confianza.
- Utiliza nuevos tipos de registros:

RRSIS	Firma de un conjunto de registros.
DNSKEY	Clave pública.
DS	Hash de un registro DNSKEY correspondiente.
NSEC	Registro para negación de existencia.

- Los registros (pe. AAAA) a autenticar se agrupan en conjuntos llamados *Resource Record Set* (RRS).

Autenticación de RRS en DNSSEC

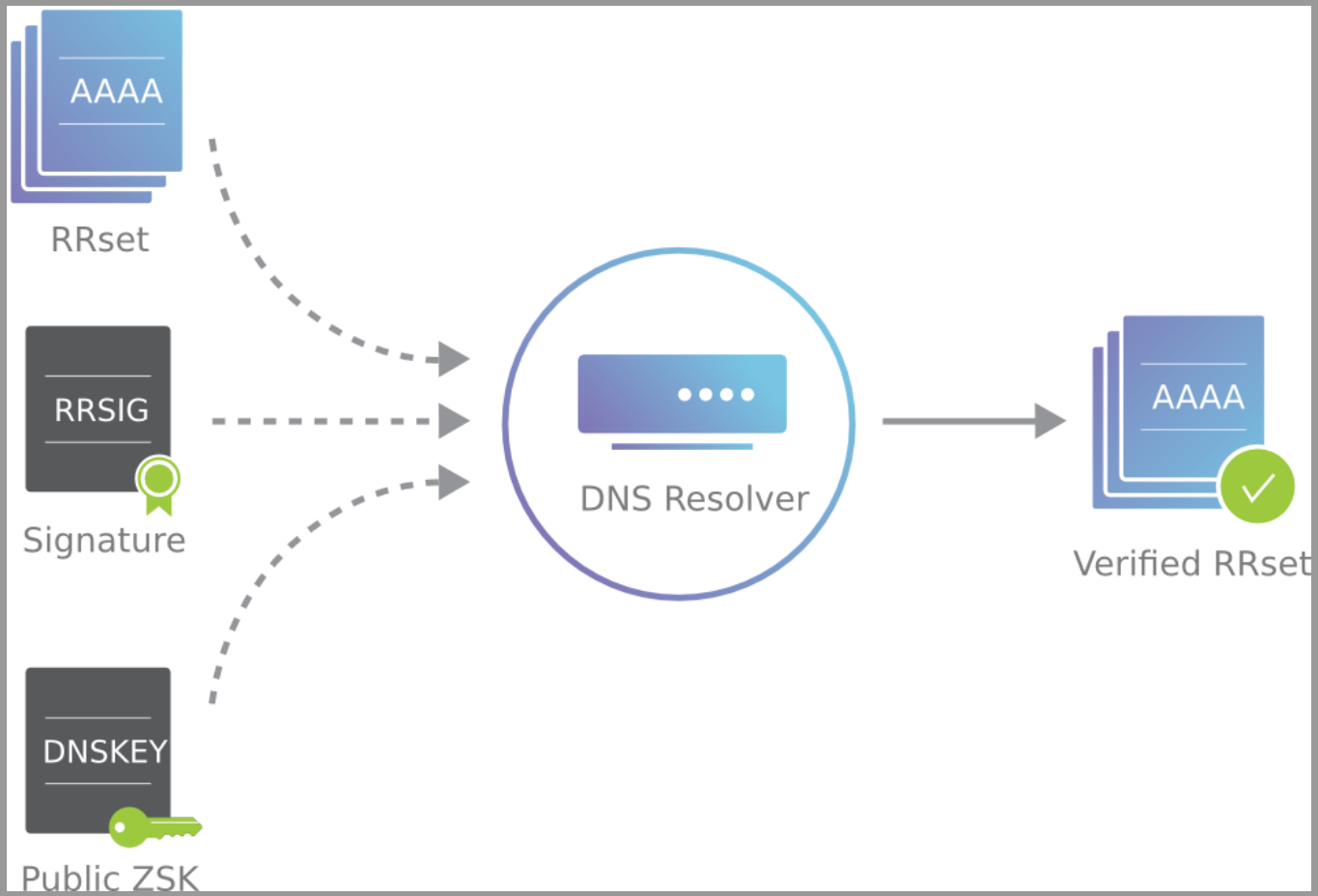


Imagen recuperada de `https://www.cloudflare.com`

El modelo de cadena-de-confianza

- Para garantizar que las claves usadas para firmar los RRS son válidas estas son firmadas también por un par de claves diferente.
- Estas claves usadas para firmar las primeras son firmadas a su vez.
  - Las claves para firmar claves son firmadas por el administrador de la zona padre.
- Se realiza la firma recursivamente hasta llegar a la zona raiz.
  - Se considera que los administradores de la zona raiz son 100 % confiables.

El modelo de cadena-de-confianza

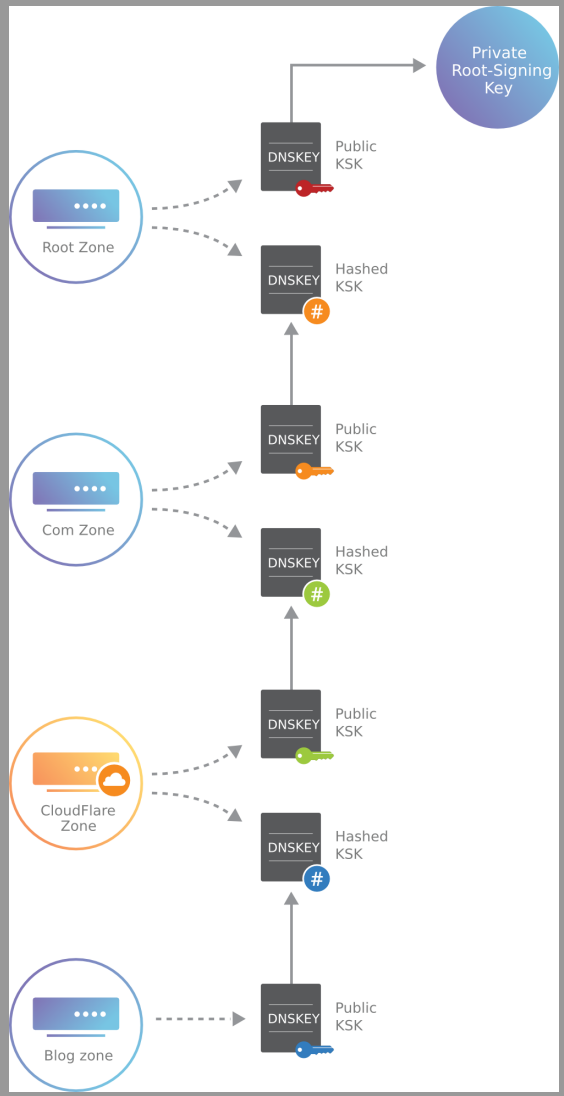


Imagen recuperada de
`https://www.cloudflare.com`

DNSCurve

- Es un protocolo para proveer privacidad en las comunicaciones de DNS.
- Utiliza cifrado asimétrico con algoritmos de curvas elípticas.
- El resolvedor debe disponer de una forma de obtener la clave pública del servidor de nombres que quiere contactar.
- Los servidores autoridad la colocan en el registro NS de la zona superior:

```
example.com. IN NS uz5bcx1nh8...q7rpj8l.example.com.
```

- Las claves siempre son de 51 bits, se representan en base 32, y siempre comienzan con los caracteres “uz5”.

Algoritmo de DNSCurve

- El funcionamiento es como sigue:
  1. El resolvedor genera un *nonce* de 96 bits.
  2. El resolvedor envía un paquete que contiene:
     1. Su propia clave pública.
     2. El *nonce*.
     3. Un bloque cifrado y firmado que contiene el paquete de solicitud DNS y el *nonce*.
  3. El servidor responde de manera similar.

RFC's importantes

- D. Atkins, *Threat Analysis of the Domain Name System (DNS)*, RFC 3833, IETF Informational, 2004.
- M. Dempsky, *DNSCurve: Link-Level Security for the Domain Name System*, draft-dempsky-dnscurve-01, IETF Network Working Group Draft, 2010.

¿Preguntas?