NIC Chile:
DNSSEC

Relator: Hugo Salgado H.

junio / 2014

Temario

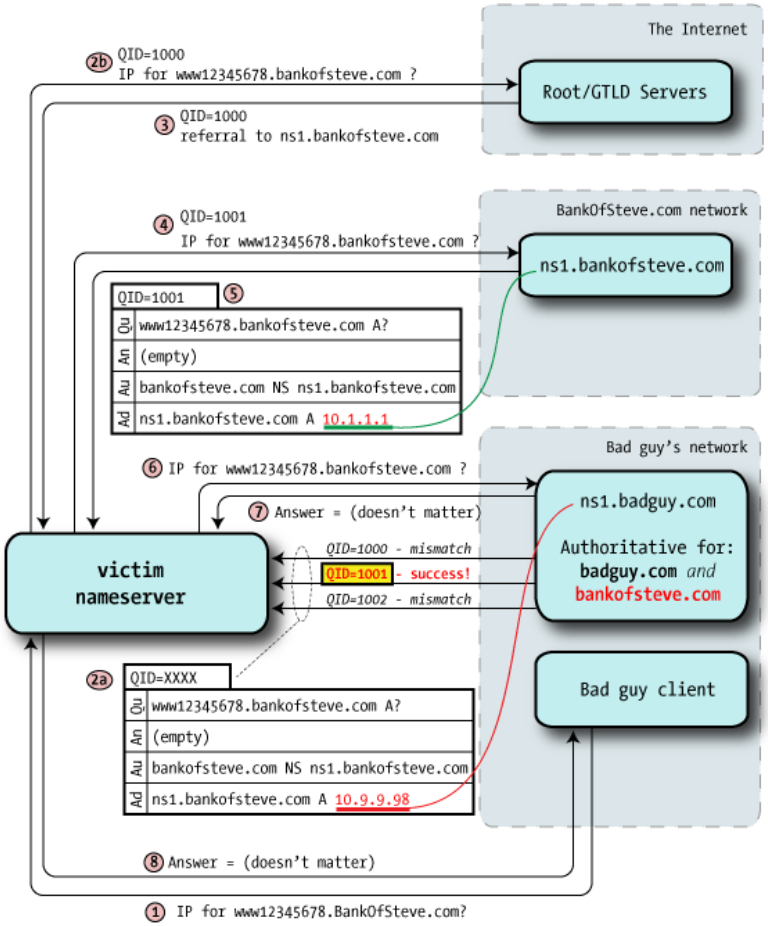
1. Ataques al DNS
2. Protocolo
3. Cambios al DNS
4. Implantación
5. Ejemplo de firmado de zona

1. Ataques al DNS

Dan Kaminsky

- 2008, cache poisoning
- Seguridad sólo en TXid (16 bits, 64k)
  - Starter pistol
    - No es necesario estar dentro de red ACL recursiva
  - Flood de respuestas
    - Mejores anchos de banda, 10 segundos
  - Spoof de NS
    - Secuestro de jerarquía completa
    - Permite usar siempre nombres frescos

Dan Kaminsky



"DNSSEC"

Soluciones corto plazo

- Aumentar entropía
  - Port variable (2k)
    - 2^16 x 2^11 = 134 millones
  - Query case
- Aceptar solo respuestas in-domain
- Monitoreo de txids malos
- Switch a TCP (?)

Solución a mediano plazo

- BCP38: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.
- Control de source spoofing
- 15 años y no se ve solución.

Solución definitiva: DNSSEC

- DNS con autenticación interna de “datos”, sin importar transporte.
- DNSSEC, RFCs 4033, 4034, 4035 y 5155
- Autenticidad e Integridad.
- Abre nuevos riesgos:
  - Agrega “timing” al DNS
  - Aumento de tamaños zonas y respuestas
  - Coordinación llave raíz
  - Falsa sensación de seguridad, no soluciona todo!

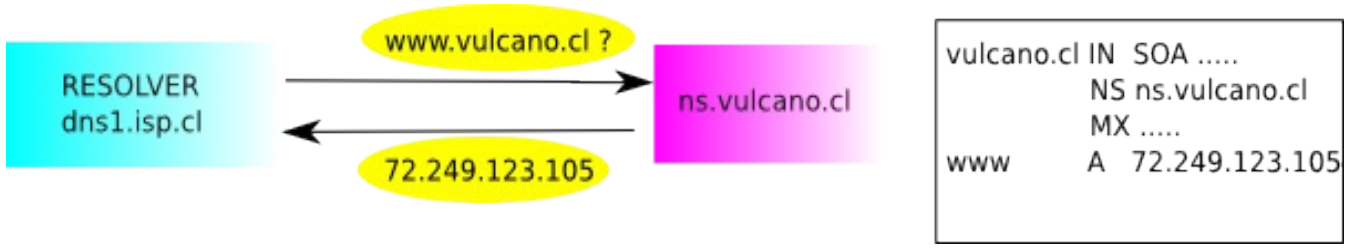
2. Protocolo

Criptografía asimétrica

- Llave pública y privada
  - Privada
    - firma zona offline
  - Pública
    - se publica en la zona
    - se envía al padre
- MD5 (muerto), SHA1, SHA256, SHA512, GOST, ECDSA.

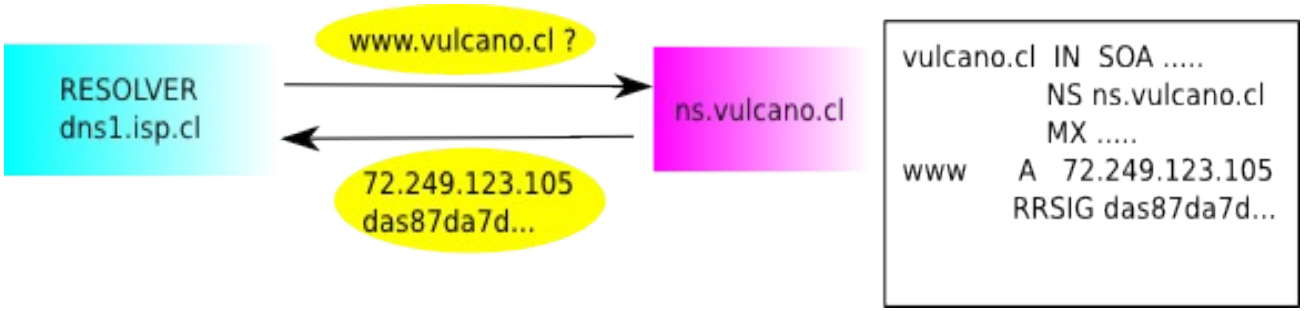
2. Protocolo

DNS clásico



2. Protocolo

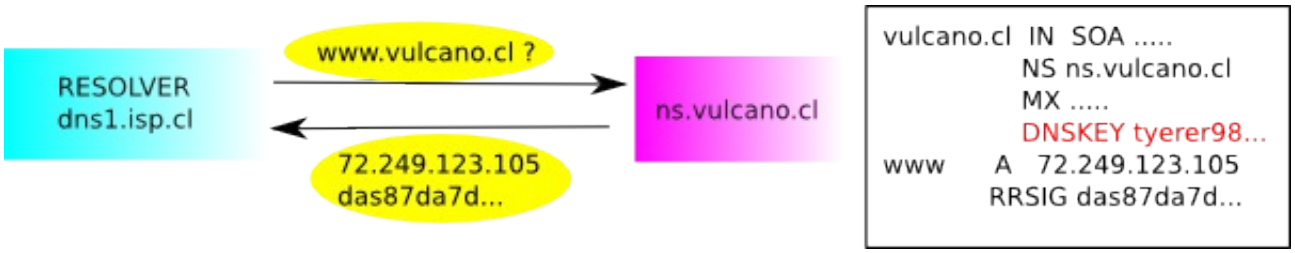
Agregamos firma



Autenticidad – Integridad

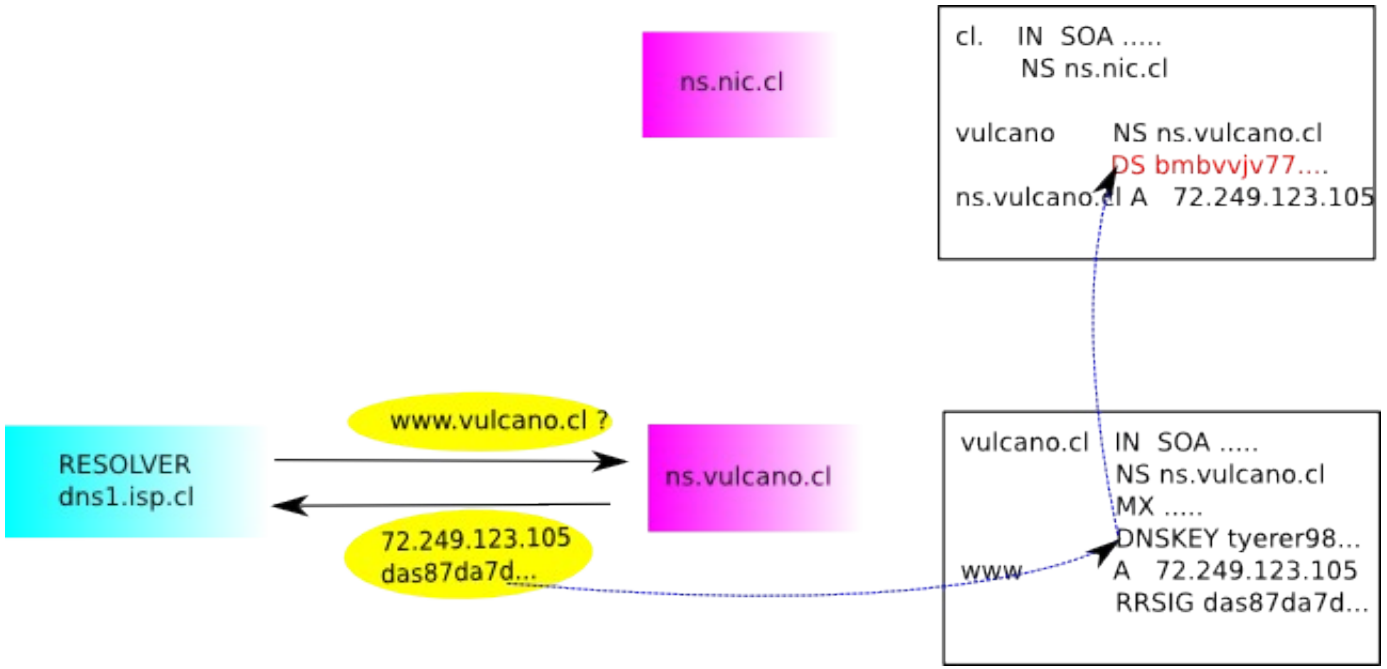
2. Protocolo

La llave pública del DNS autoritativo



2. Protocolo

Verificación: cadena de confianza

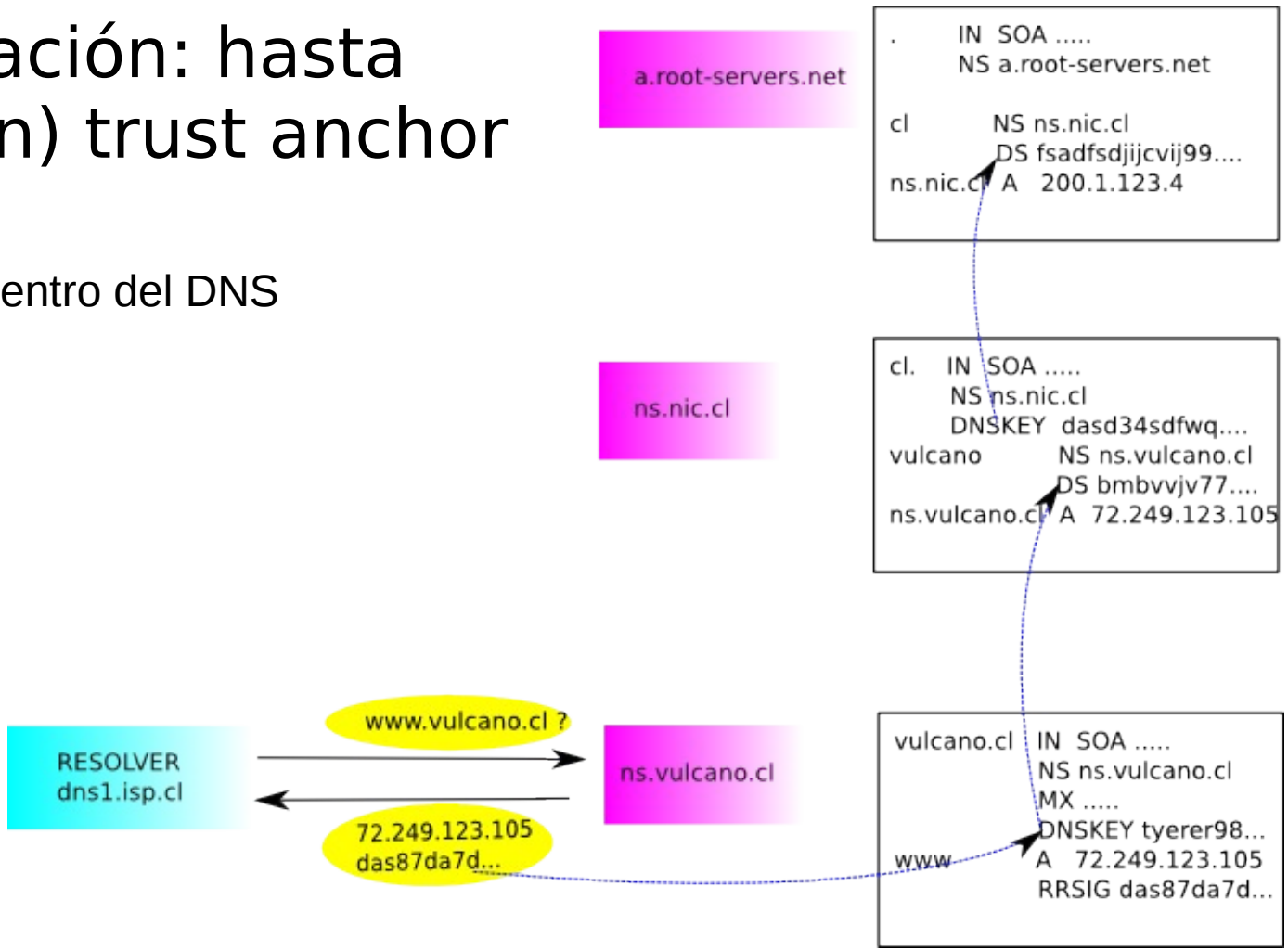


"DNSSEC"

2. Protocolo

Verificación: hasta el (un) trust anchor

PKI dentro del DNS



"DNSSEC"

3. Cambios al DNS

3. Cambios al DNS

4 resource records nuevos

- DNSKEY
- RRSIG
- DS
- NSEC

2 bits de header nuevos

- CD (checking disabled)
- AD (authenticated data)

Otros:

- CNAME con RRSIG y NSEC
- NSEC3
- EDNS0
- DO (DNSSEC OK)

3. Cambios al DNS -> DNSKEY

DNSKEY: la(s) llave(s) pública(s)

KSK y ZSK

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2De
                                       IQ3Cbl+BBZH4b/0PY1kxkmvHj
                                       cZc8nokfzj31GajIQKY+5CptL
                                       r3buXA10hWqTkF7H6RfoRqXQe
                                       ogmMHfpftf6zMv1LyBUgia7za
                                       6ZEzOJBOztyvhjL742iU/TpPS
                                       Edhm2SNKLijfUppn1UaNvv4w=
                                       =  )
```

3. Cambios al DNS -> RRSIG

RRSIG: las firmas

- por RRset
- Sólo los autoritativos:
  - No NS delegados
  - No glue records

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 (
                                20030220173103 2642 example.com.
                                oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
                                PYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
                                B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3t
                                GNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
                                J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

3. Cambios al DNS -> DS

DS: Delegation Signer

- Forma la cadena con el padre
- Hash del dnskey

```
dskey.example.com. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A
                                           98631FAD1A292118 )

dskey.example.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9Xz
                                             fwJr1AYtsmx3TGkJaNXVbfi/
                                             2pHm822aJ5iI9BMzNXxeYCmZ
                                             DRD99WYwYqUSdjMmmAphXdvx
                                             egXd/M5+X7OrzKBaMbCVdFLU
                                             Uh6DhweJBjEVv5f2wwjM9Xzc
                                             nOf+EPbtG9DMBmADjFDc2w/r
                                             ljwvFw==
                                             ) ;  key id = 60485
```

"DNSSEC"

3. Cambios al DNS -> NSEC

NSEC: Next Domain Name Field

- Respuestas negativas autenticadas
- Cómo firmamos si no hay RDATA?
- Solución: firmamos la brecha en el authority
- Orden canónico, se encadena los autoritativos y las delegaciones. No hay NSEC para glues.

```
alfa.example.com. 86400 IN NSEC host.example.com. (
                                    A MX RRSIG NSEC )
```

3. Cambios al DNS -> CD

CD: checking disabled

- Permite deshabilitar la validación de firmas
- Dirigido a resolvers donde el cliente “asume la responsabilidad”


```
% dig @172.30.67.102 evil.nic.cl +dnssec +short

% dig @172.30.67.102 evil.nic.cl +dnssec +short +cd
6.6.6.0
A 5 3 43200 20081112234200 20081013234200 22617 nic.cl. VIx6/h...
```

3. Cambios al DNS -> AD

AD: authenticated data

Indica que los datos fueron validados

```
% dig @172.30.67.102 e.nic.cl +dnssec +cd
...
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ...
...

% dig @172.30.67.102 www.nic.cl +dnssec
...
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ...
...
```

3. Cambios al DNS -> NSEC3

- Hashed authenticated denial of existence
- Define 2 RR's nuevos
  - NSEC3
  - NSEC3PARAM
    - Sólo para autoritativos
- Closest encloser proof
  - Hasta 3 NSEC3 RR's
    - Uno que demuestra el “closest encloser”
    - Otro el “next closest encloser”
    - Otro que demuestra la inexistencia de wildcards

3. Cambios al DNS -> NSEC3 ej.

Ejemplo:

```
example. 3600 IN SOA  ns1.example. bugs.x.w.example. 1 3600 300 (
                           3600000 3600 )
            DNSKEY  256 3 7 AwEAAaetidLzsKWUt4swWR8yu0wPHPiUi8LU (
                    sAD0QPWU+wzt89epO6tHzkMBVDkC7qphQO2h
                    TY4hHn9npWFRw5BYubE= )
            DNSKEY  257 3 7 AwEAAcUlFV1vhmqx6NSOUOq2R/dsR7Xm3upJ (
                    j7IommWSpJABVfW8Q0rOvXdM6kzt+TAu92L9
                    AbsUdblMFin8CVF3n4s= )
            NSEC3PARAM 1 0 12 aabbccdd

0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.example. NSEC3 1 1 12 aabbccdd (
                    2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                    SOA NSEC3PARAM RRSIG )

2t7b4g4vsa5smi47k61mv5bv1a22bojr.example. A 192.0.2.127
            NSEC3   1 1 12 aabbccdd (
                    2vptu5timamqttgl4luu9kg21e0aor3s A RRSIG )
...
```

4. Implantación

4. Implantación

¿Qué significa DNSSEC para

- Un usuario final?
- Un administrador de zona?
- Un registry (TLD)?
- Un ISP?
- Internet?

¿Qué NO es DNSSEC?

4. Implantación: usuario final

Idealmente: nada

- DNSSEC cubre desde el resolver hasta la raíz
- El “último paso” (stub resolver) debería ser transparente

En la realidad

- Uso de TSIG, SIG0 en el último paso
- Tener recursivos locales?
- Validadores locales.

4. Implantación: dnsadmin

- Generar las llaves
  - KSK, ZSK
- Comunicar registro DS al registry padre
- Firmar la zona (7x)
- Coordinar con subzonas
- Tareas nuevas críticas
  - Firmado después de cada cambio Y regular
  - Reloj sincronizado (ntp)
  - Rollover de llaves
    - Normal
    - De emergencia

4. Implantación: registry

- Definir política zone-walking
  - NSEC
  - NSEC3
  - Minimally covering NSEC (online signing)
- Tener políticas claras para
  - Rollover normal
  - Actuación de emergencia
- Obtener DS de clientes en forma segura
- Uso de opt-in (experimental)?

4. Implantación: ISP

- Grandes “resolvers”
  - Configurar trust anchors
  - Definir el tipo de “failover”
    - seguro (ad=1)
    - inseguro
    - bogus (rcode=2, “server failure”)
    - indeterminado
  - Asegurar la comunicación con usuarios finales
    - TSIG
    - SEC0
    - Ipsec
- Cajas negras: Xelerance, Secure64

4. Implantación: Internet

FIRMAR LA RAÍZ!

- Distribución de la llave
- Cómo actuar en casos de emergencia?
- Política, política, política...

Respeto a estándares por software y hardware

- EDNS0 (512-4096)
- TCP fail over (4K-64K?)
- End-to-end en firewalls, SoHo, etc.

4. Implantación: qué NO es

DNSSEC no es

- un mecanismo de confidencialidad
- no provee ACL's
- no hay protección frente a DOS. Al contrario
  - respuestas más grandes (reflectors)
  - carga criptográfica
- nada que ver con transferencias
- nada que ver con dynamic updates

5. Ejemplo real

5. Ejemplo: la zona normal

```
% cat ejemplo.cl.zone
$ORIGIN ejemplo.cl.
@       1D  IN   SOA  ns.ejemplo.cl. hsalgado.ejemplo.cl. (
                      2008101401 28800 14400 14400 3600000 86400)
        1D  IN    NS  ns.ejemplo.cl.
        1D  IN    NS  secundario.nic.cl.
        1D  IN     A  172.30.10.58
        1D  IN    MX  10 mail.ejemplo.cl.

www     1D  IN CNAME  ejemplo.cl.
ns      1D  IN     A  172.30.10.58
mail    1D  IN     A  172.30.10.58
```

5. Ejemplo: firmamos

```
% sudo yum install dnssec-tools
..........
% zonesigner -genkeys -zone ejemplo.cl ejemplo.cl.zone
..........

% ls
dsset-ejemplo.cl.                Kejemplo.cl.+005+34369.key
ejemplo.cl.krf                   Kejemplo.cl.+005+34369.private
ejemplo.cl.zone                  Kejemplo.cl.+005+35766.key
ejemplo.cl.zone.signed           Kejemplo.cl.+005+35766.private
Kejemplo.cl.+005+22347.key       keyset-ejemplo.cl.
Kejemplo.cl.+005+22347.private
```

5. Ejemplo: copiamos zona

Las llaves se mantienen en un lugar seguro

En el servidor vulnerable solo tenemos el archivo de zona firmado

```
% scp ejemplo.cl.zone.signed named@ns.ejemplo.cl:/var/named
..........
```

5. Ejemplo: configuramos bind

```
ns% vi /etc/named.conf

...

  options {
            ....
            dnssec-enable yes;
  };


  zone "ejemplo.cl" {
            ....
            file "ejemplo.cl.zone.signed";
  }


ns% /etc/init.d/named restart
```

5. Ejemplo: probamos

```
% dig @ns.ejemplo.cl a www.ejemplo.cl +dnssec +multiline
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50453
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.ejemplo.cl.                IN A

;; ANSWER SECTION:
www.ejemplo.cl.          86400 IN CNAME ejemplo.cl.
www.ejemplo.cl.          86400 IN RRSIG CNAME 5 3 86400 20081113175701 (
                                 20081014175701 35766 ejemplo.cl.
                                 Nlfjv9VHxbYEUa2OrhRKa/yhR0IDWhJHvE7qN6Qu062D
                                 l16meIoxg/GtqFeJSFPNNcF/uetX5LcKmEtSK9jtTKoG
                                 x/sHW7RcTOS4VPohu/5hwMMgkTf4zFE+y9e5MHegchWH
                                 Z4pRe0dqBUlaSIjqe3rVxQL+tPd7N66x1apqo/o= )
ejemplo.cl.              86400 IN A 172.30.10.58
ejemplo.cl.              86400 IN RRSIG A 5 2 86400 20081113175701 (
                                 20081014175701 35766 ejemplo.cl.
                                 gozkXB66oLLUVYXalGuVi3hfO/1lrMD2zRqDJWfycU3B
                                 7NsLPZS0gGRgN+693rGhqJGhl30OcBOzWk7w2HopNKQC
                                 A2iwzBGpaWt2jWl3lY809cQt7PnLJtga4NJFo6bFuCer
                                 ksnDHpvjUS11iJqrzE07HyuA3aRK+WQHqTTMPow= )

.... AUTHORITY SECTION ... ADDITIONAL SECTION

;; Query time: 0 msec
;; WHEN: Tue Oct 14 16:23:07 2008
;; MSG SIZE  rcvd: 831
```

5. Ejemplo: pasar DS a alguien

- Establecer cadena de confianza
- Para pruebas o zonas internas puede ser solo un trust-anchor en algún resolver
  - trusted-keys de BIND
  - DNSKEY completo
- Para pruebas nivel dos, DLV de ISC
- La vida real, enviar el DS a NIC Chile ;)
  - Panel de control
  - Escribir a dnssec@nic.cl

5. Ejemplo: mantención

- zonesigner por defecto tiene firmas válidas por 30 días
  - Recordar volver a firmar antes que expiren
    - zonesigner -zone ejemplo.cl ejemplo.cl.zone
    - scp ejemplo.cl.zone named@ns.ejemplo.cl:....
    - En ns basta hacer un
      rdnc reload ejemplo.cl
- O usar otras herramientas dnssec-tools
  - OPENDNSSEC
  - BIND
  - crontab+zonesigner (llaves en server)
  - Rollerd, donuts

5. Ejemplo: la zona insegura

```
$ORIGIN ejemplo.cl.
@       1D  IN   SOA  ns.ejemplo.cl. hsalgado.ejemplo.cl. (
                      2008101401 28800 14400 14400 3600000 86400)
        1D  IN    NS  ns.ejemplo.cl.
        1D  IN    NS  secundario.nic.cl.
        1D  IN     A  172.30.10.58
        1D  IN    MX  10 mail.ejemplo.cl.

www     1D  IN CNAME  ejemplo.cl.
ns      1D  IN     A  172.30.10.58
mail    1D  IN     A  172.30.10.58
```

5. Ejemplo: la zona segura

```
% cat ejemplo.cl.zone.signed
; File written on Tue Oct 14 15:57:01 2008
; dnssec_signzone version 9.5.0-P2
ejemplo.cl.          86400   IN SOA  ns.ejemplo.cl. hsalgado.ejemplo.cl. (
                                     2008101403 ; serial
                                     28800      ; refresh (8 hours)
                                     14400      ; retry (4 hours)
                                     3600000    ; expire (5 weeks 6 days 16 hours)
                                     86400      ; minimum (1 day)
                                     )
                     86400   RRSIG   SOA 5 2 86400 20081113175701 (
                                     20081014175701 35766 ejemplo.cl.
                                     N2jPzPPG/6bYBUdtrLPFDNZqVU4nfkISttBY
                                     8TrDulLxElEhjo6CeqNmeQyh7FiP8wfCP8YM
                                     NOOLoVb51WOff81J+mYhYH5ewCnT5XjOpmt1
                                     tPXBPr/wmQbxgACglWstnmTLkIXWkD01NMw/
                                     /QbxCRu/McaLh4QipN9u7r7QbCU= )
                     86400   NS      ns.ejemplo.cl.
                     86400   NS      secundario.nic.cl.
                     86400   RRSIG   NS 5 2 86400 20081113175701 (
                                     20081014175701 35766 ejemplo.cl.
                                     hlxkMYSW+Ksbzw2+/jjuFE2mbDpdu5AKYFKX
                                     6pQQC59p9UeYceqUo4RmR/X3m3lG7qcnBlhK
                                     tYnepzOq8HNBojNkwlCmLkhlwffZpHzcrEji
                                     MXfiQYm1Nl+T6zG61NIUO6iXKlMqFzrkIYiy
                                     cfQHcvewIp0L7dABz638hPOuYUI= )
                     86400   A       172.30.10.58
                     86400   RRSIG   A 5 2 86400 20081113175701 (
                                     20081014175701 35766 ejemplo.cl.
```

Enlaces útiles

Teoría

RFC's 4033, 4034, 4035 y 5155

Buena intro:
http://ispcolumn.isoc.org/2006-08/dnssec.html

Herramientas

BIND (dnssec-*, dig)

OpenDNSSEC (www.opendnssec.org)

Portal ISOC

- Deploy 360
internetsociety.org/deploy360/dnssec/

Relator

Hugo Salgado H.
Ingeniero de Proyectos
NIC Chile
hsalgado@nic.cl