Taller de Administración de Servidores Linux

CC5308

Clase 14: 04 de Abril de 2011

Extensiones de Seguridad para DNS

Marco Díaz
mdiaz [at] nic . cl

¿Qué es DNS?

- Protocolo que permite traducir nombres de dominios a números IP y viceversa
- Características
  - Sistema distribuido.
  - Autónomo.
  - Jerárquico.
  - Coherente.
  - Replicado.
  - Tolerante a fallas.
- Ejercicio mental: Guía telefonos

DNS - Definiciones...

- Nombre de host (Fully Qualified Domain Name):
  - Nombre de equipo + dominio.
  - Ejemplo ***ftp.inf.utfsm.cl.***
- Dominio:
  - Identificador para equipo o grupo de equipos.
  - Ejemplo ***inf.utfsm.cl.***

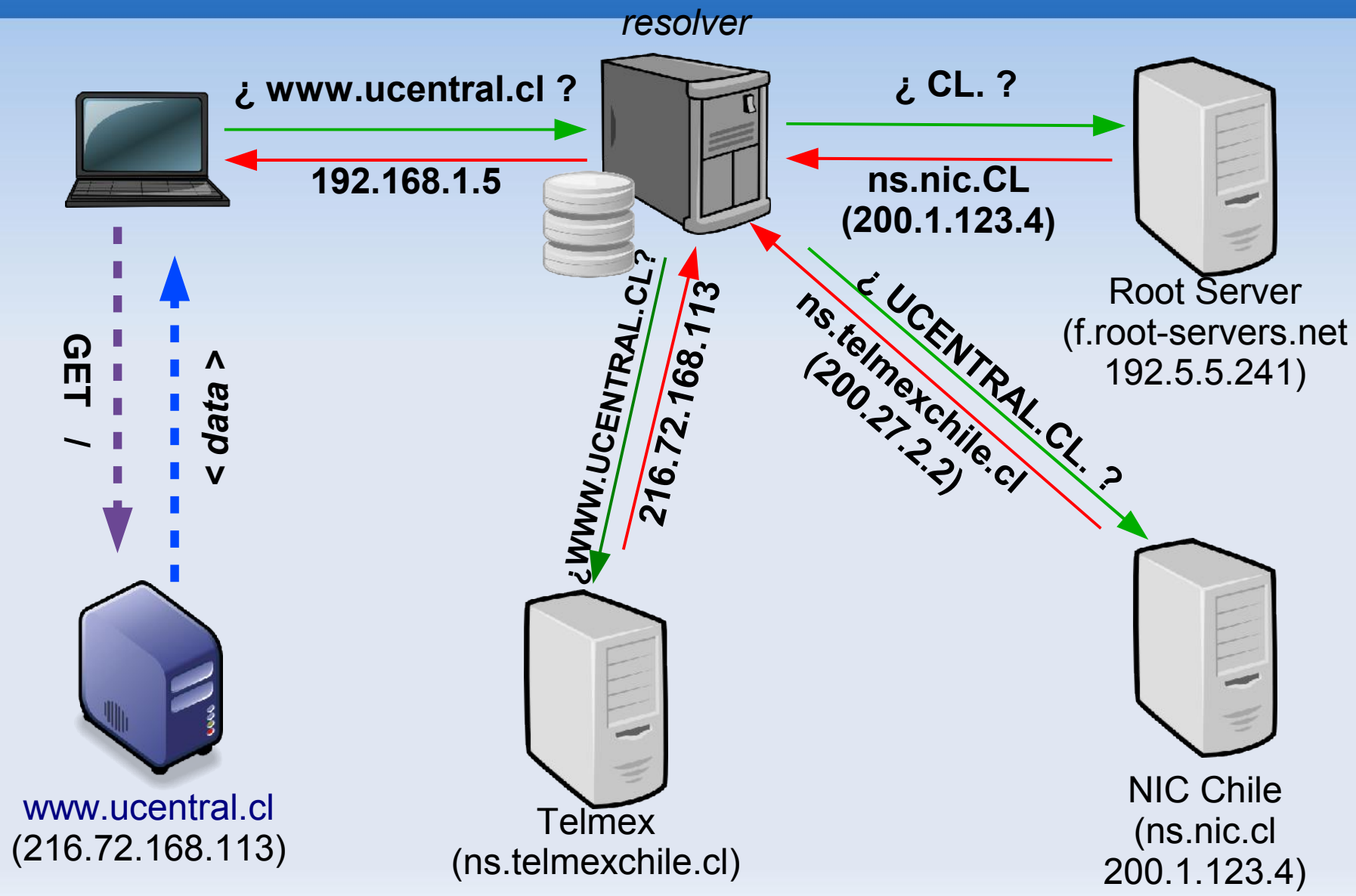
DNS - Definiciones...

- Zona:
  - Archivo (BD) con información sobre el dominio.
- Root-Server:
  - Servidores raíz. Tienen info sobre los TLD.
- Top Level Domain (TLD):
  - Pueden ser ccTLD o gTLD

DNS - Definiciones...

- 2 Funciones principales de sus servidores:
  - Los que preguntan (resolver, caché)
  - Los que responden (autoritativos)
- Resolvers:
  - Restringidos por ISP/organización
  - SW recomendado: BIND, Unbound
- Autoritativos:
  - Primarios, Secundarios
  - SW recomendado: BIND, NSD

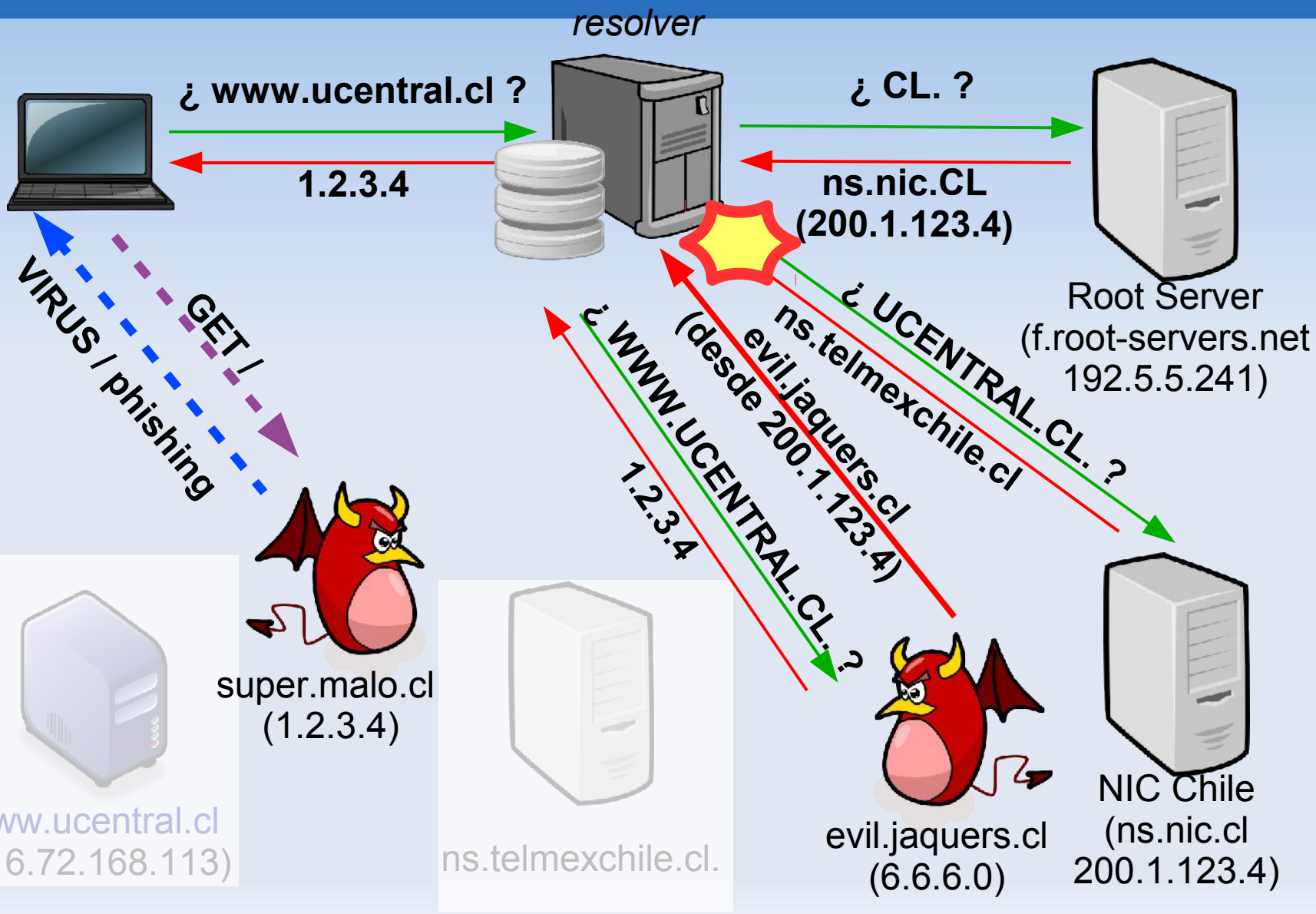
Cómo funciona el DNS?



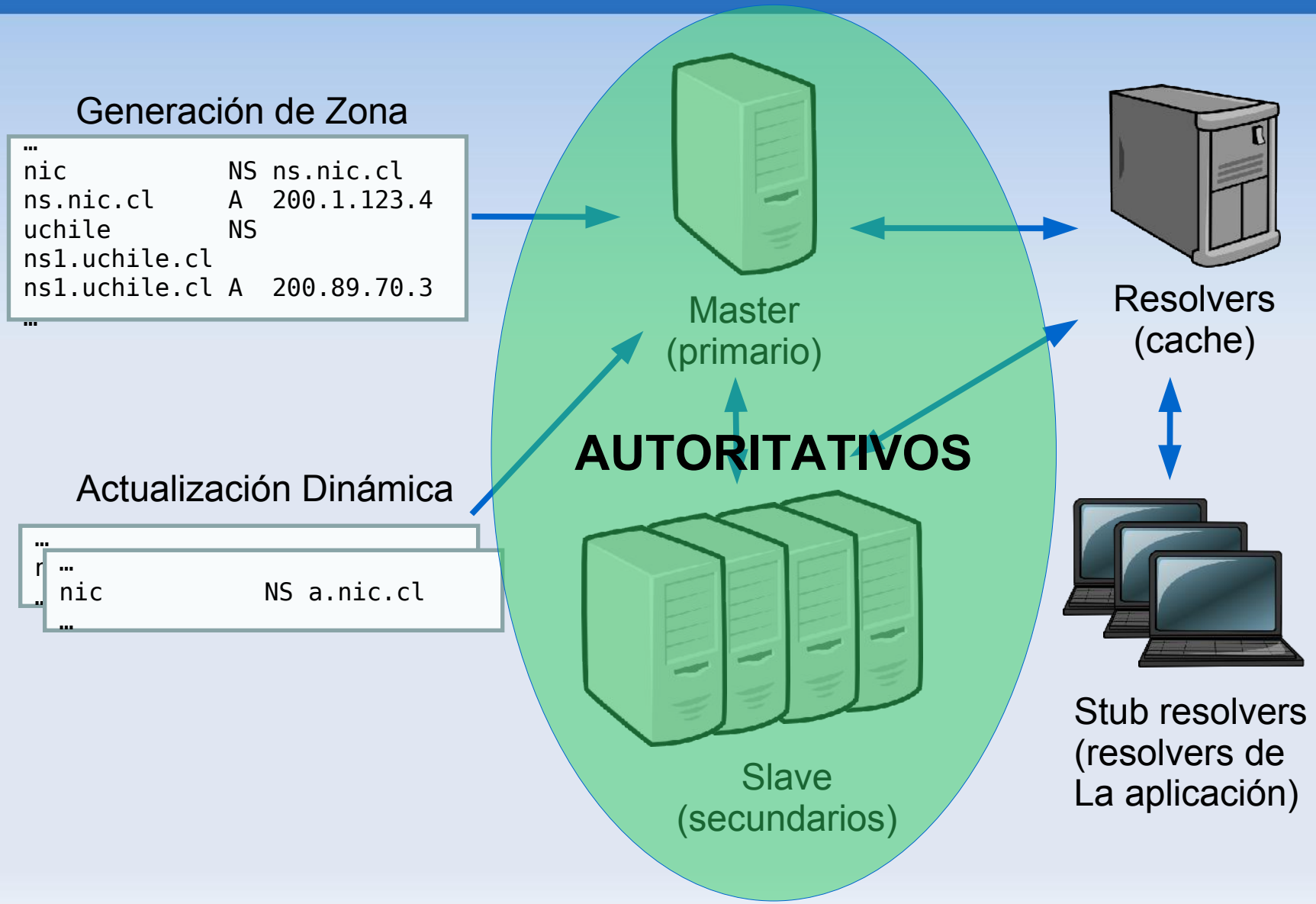
Problemas potenciales

- DNS “normal” no tiene formas inequívocas de garantizar la autenticidad de la información
- Tampoco puede garantizar la integridad de la información
- Es una base de datos altamente distribuida
  - No hay un ente centralizado de verificación
  - Varios posibles puntos de falla
- Ejemplos varios: Cache posioning, Kaminsky, Conficker, etc..

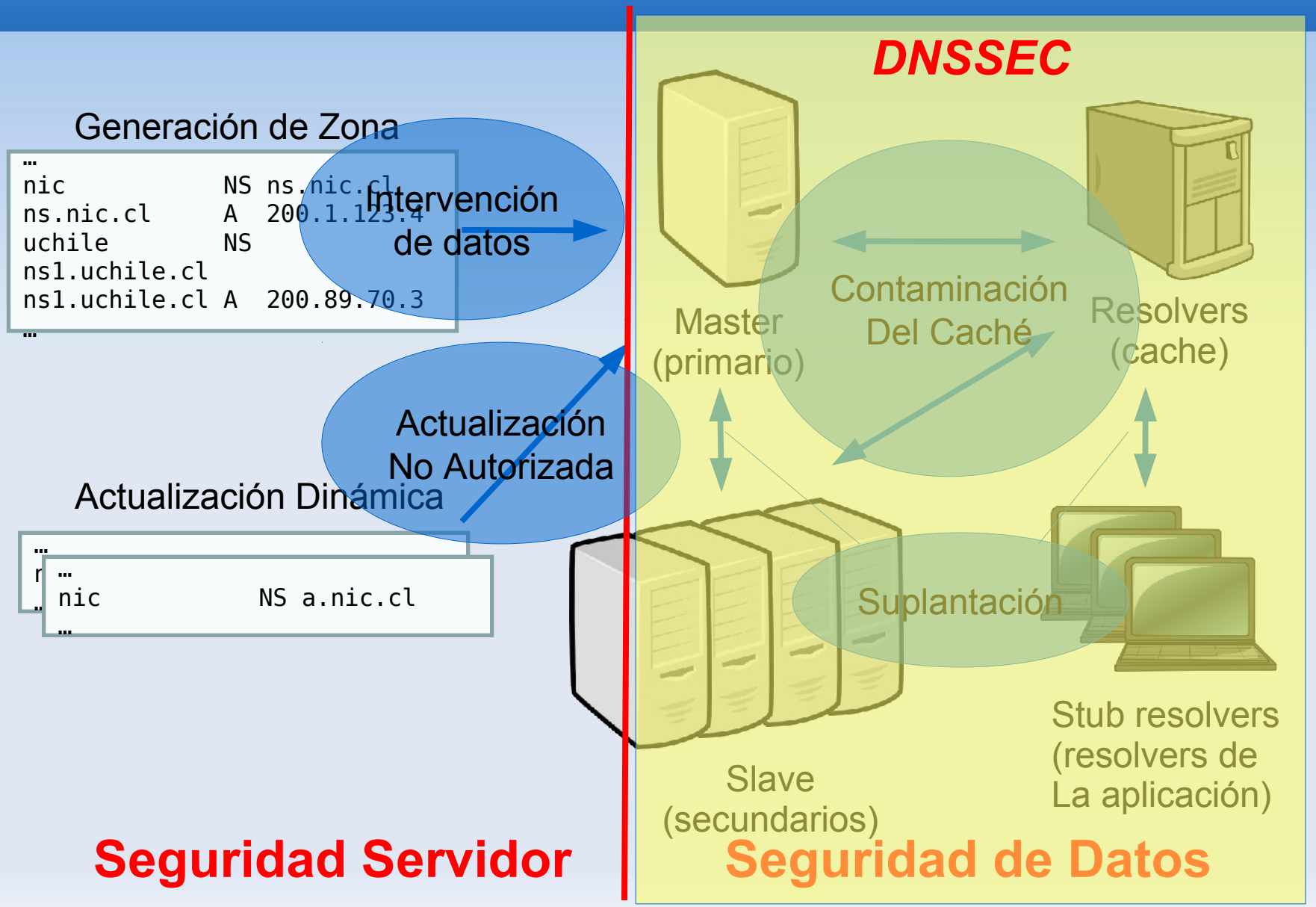
Problemas potenciales...



Flujo de DNS


Generación de Zona
…
nic NS ns.nic.cl
ns.nic.cl A 200.1.123.4
uchile NS
ns1.uchile.cl
ns1.uchile.cl A 200.89.70.3
…
Actualización Dinámica
…
nic NS a.nic.cl
…
Master
(primario)
AUTORITATIVOS
Slave
(secundarios)
Resolvers
(cache)
Stub resolvers
(resolvers de
La aplicación)

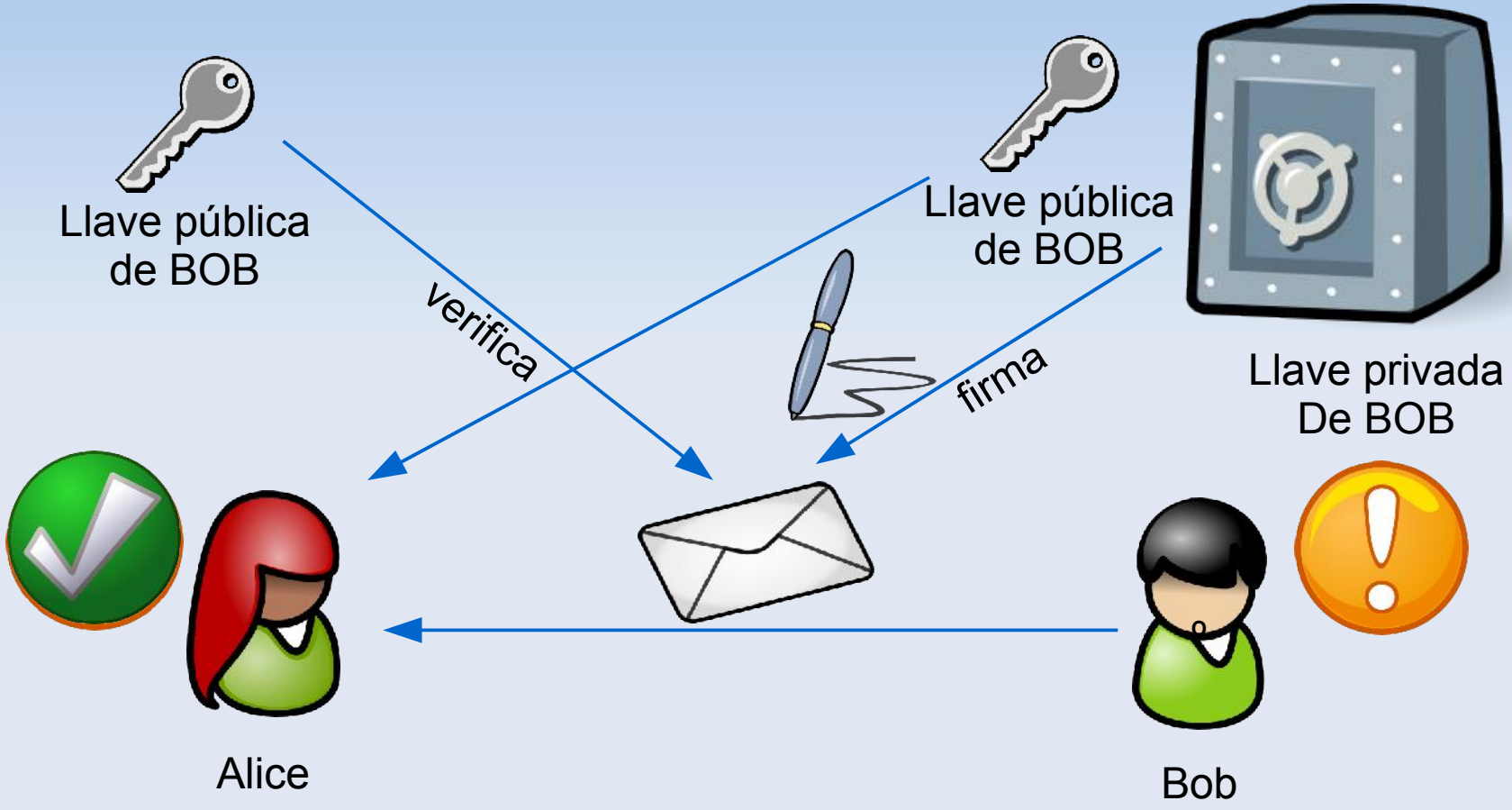
Vulnerabilidades...



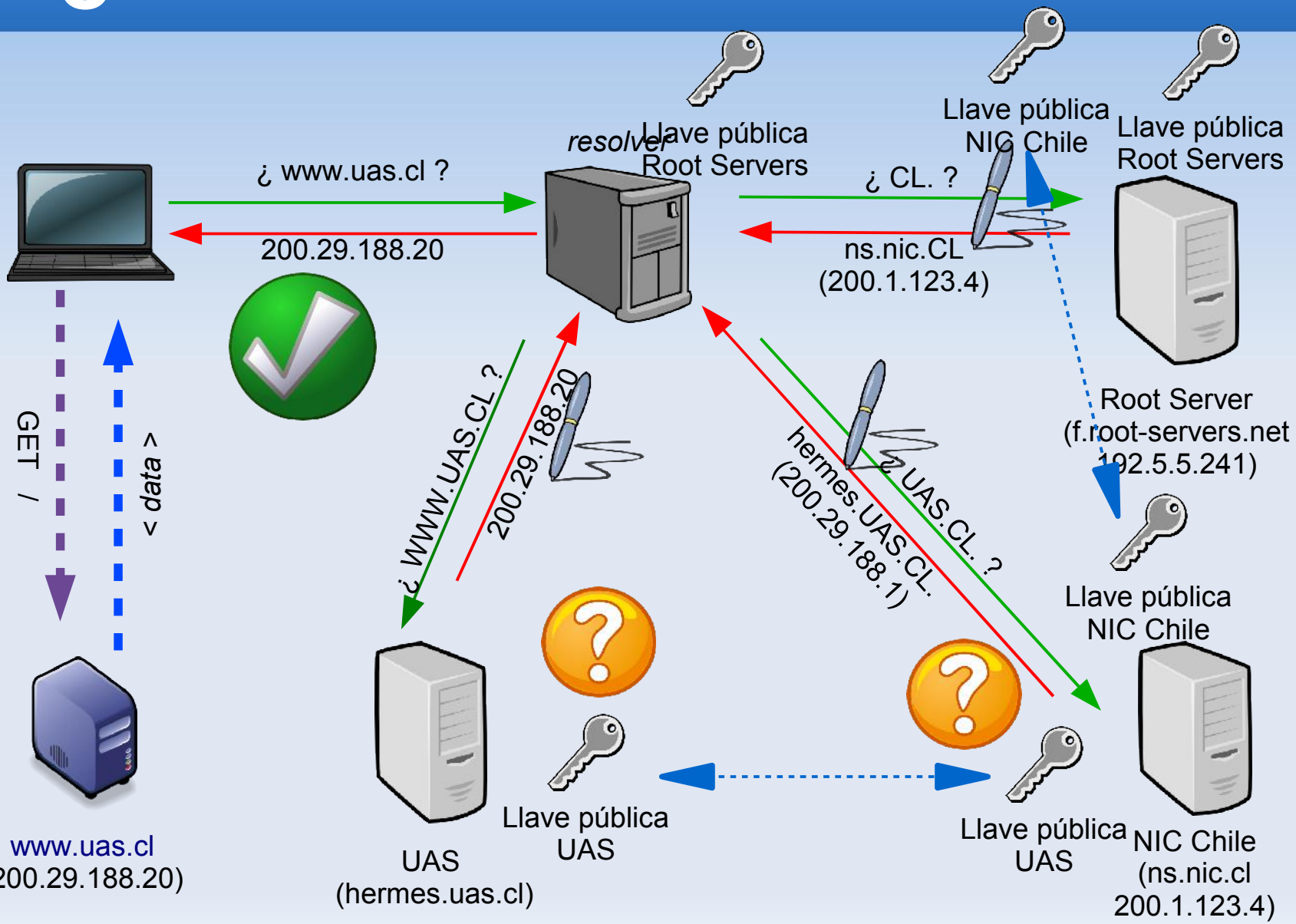
Extensiones de Seguridad para DNS: DNSSEC

- Garantiza la Autenticidad y la Integridad de los datos
  - Usando firmas digitales
- Utiliza cadenas de confianza partiendo desde la raíz, hasta el dominio consultado
- Parte de la premisa que todos confían en la raíz

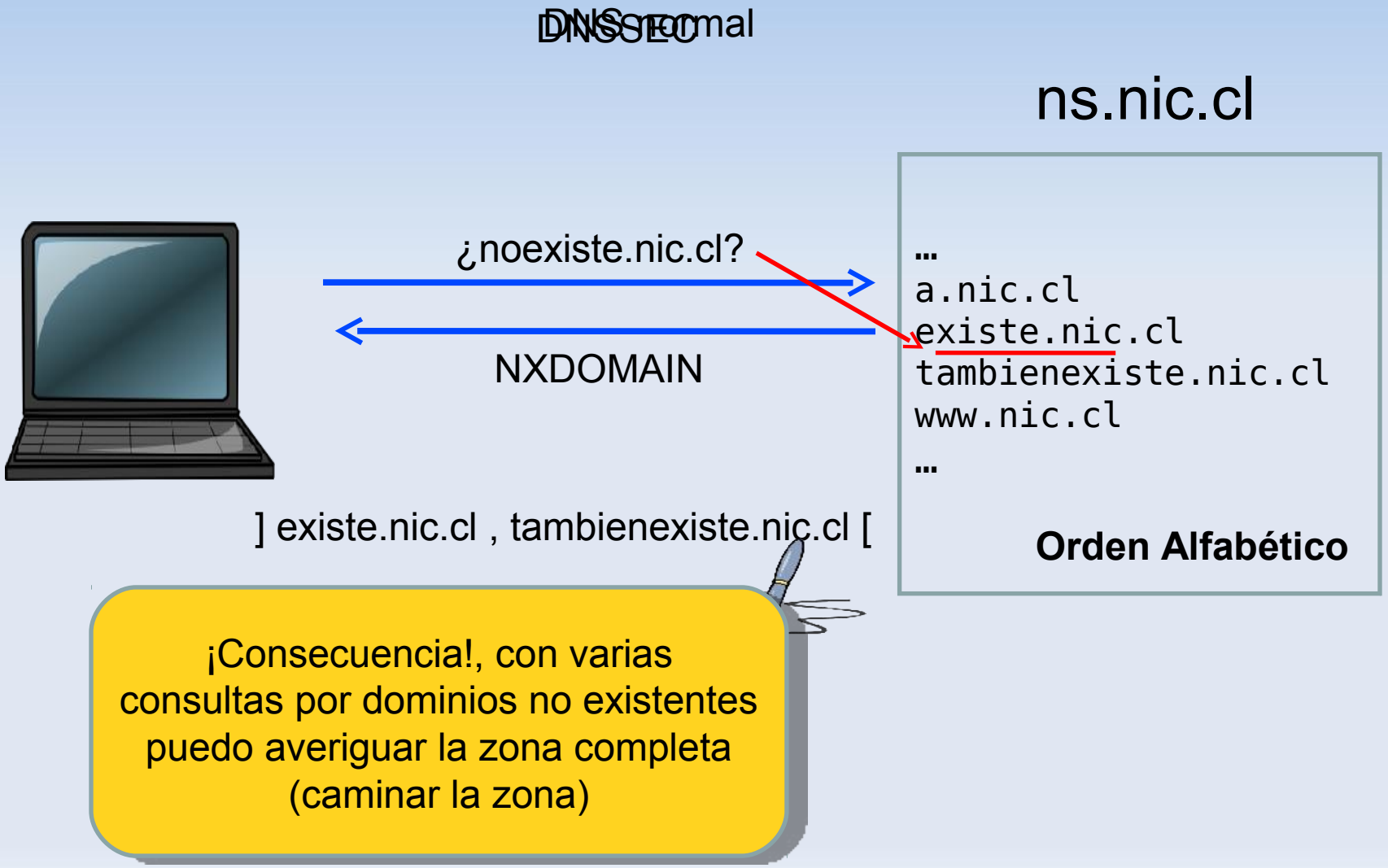
Firma digital



¿Cómo funciona DNSSEC?

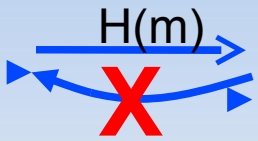


Dominios no existente



Dominios no existente

Nueva extensión NSEC3, soluciona “caminar la zona”



H(noexiste.nic.cl)

¿noexiste.nic.cl?

NXDOMAIN

] H(otro.nic.cl) , H(mail.nic.cl) [

ns.nic.cl

…
a.nic.cl
existe.nic.cl
tambienexiste.nic.cl
www.nic.cl
…

Orden alfabético

Por lo tanto, lo nuevo...

- 2 tipos de llaves
  - KSK (Key Signing Key)
  - ZSK (Zone Signing Key)
- Nuevos registros
  - DNSKEY (Llaves)
  - RRSIG (Firma)
  - DS (Delegación padre)
  - NSEC / NSEC3 (inexistencia)

Utilizando BIND

- Sugerido version 9.7.1-P2 (en adelante)
  - dnssec-keygen
  - dnssec-signzone
  - En named.conf:
    - dnssec-enable “yes”;
    - dnssec-validation “yes”;
- OpenSSL > 0.9.8o

Decisiones para DNSSEC

- NSEC o NSEC3 ?
- Tamaño de las llaves ?
  - Llaves KSK (Key Signing Key) y ZSK (Zone Signing Key)
- Tiempo de vida de las llaves/firmas ?
- Firmar todo a la vez ?
- Cuánto cuesta DNSSEC
  - Cómputo, memoria, tiempo, ancho de banda, esfuerzo, desarrollo
- Revocación de llaves (Procesos)
  - Expiración, Compromiso de llave privada, pérdida de la llave privada
  - Traslape de llaves viejas y nuevas (viejas firman nuevas)
  - Padre, Hijos ?

Decisiones para DNSSEC

- Comportamiento del resolver
  - Dominio seguro, inseguro, falso, indeterminado
- Procedimiento de inscripción de dominios
- Como solucionar dominios “aislados”
  - Secure Entry Point & DNSSEC Look-aside validation
- Como desistir de DNSSEC ?
- Qué/cuántos problemas soluciona efectivamente
  - Vale la pena el costo/complejidad ?

Ejemplo práctico

- Generar la llave ZSK:
  - `dnssec-keygen -r /dev/urandom -a RSASHA1 -b 1024 -n ZONE ejemplo.cl`
- Generar la llave KSK:
  - `dnssec-keygen -r /dev/urandom -f KSK -a RSASHA1 -b 2048 -n ZONE ejemplo.cl`
- Incluir las llaves en la zona:
  - `$include Kejemplo.cl.+$ID_ZSK.key ; ZSK`
  - `$include Kejemplo.cl.+$ID_KSK.key ; KSK`

Ejemplo práctico

- Firmar la zona:
  - ```
    dnssec-signzone \
     -r /dev/random \
     -o ejemplo.cl  \
     -N INCREMENT \
     -k Kejemplo.cl.+$ID_KSK.key \
     ejemplo.cl.zone \
     Kejemplo.cl.+$ID_ZSK.key
    ```
- Agregar el registro DS en el SEP
    ```