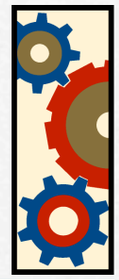
Cuestiones de seguridad en el DNS

João Damas
Internet Systems Consortium

Agenda

- Protocolo
  - TSIG/GSS-TSIG
  - DNSSEC
- Operación
  - Ataques al DNS
  - Ataques usando el DNS

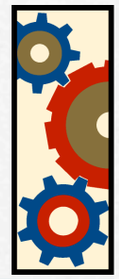
Seguridad en el protocolo



Antes todo el mundo se podía fiar de todo...

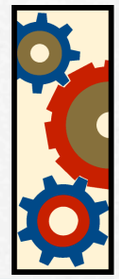
...después la vida se complicó

Cambios



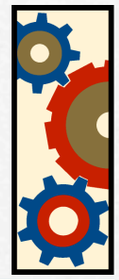
- TSIG/GSS-TSIG
- DNSSEC(bis)

Primero lo fácil



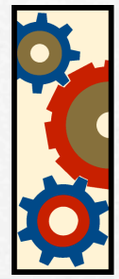
- TSIG es un mecanismo de secreto compartido para identificar a dos servidores de DNS entre si
- Permite controlar quien puede acceder al servidor para preguntas de DNS

TSIG/GSS-TSIG



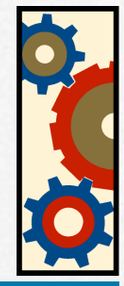
- Sencillo, eficaz, pero un latazo si hay muchos servidores involucrados
- se usa frecuentemente entre servidores de la misma zona
- configuración manual, secreto compartido

TSIG/GSS-TSIG



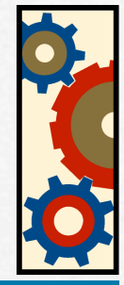
- TKEY permite una cierta automatización pero requiere una relación establecida anteriormente
- GSS-TSIG es la aplicación de GSS-API (General Security Service) al TSIG

GSS-TSIG



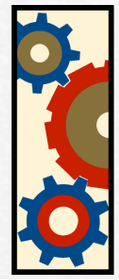
- Generalmente se usa Kerberos como sistema de autenticación local sobre el que se construye después el intercambio de las claves para TSIG
- Este mecanismo es fundamental para el funcionamiento de MS Active Directory

DNSSEC



- Asegurar, criptográficamente, la fiabilidad de las respuestas de DNS
- Historia de un desastre
  - 1997: RFC 2065
  - 1999: RFC 2535
- Sólidos desde el punto de vista formal pero...

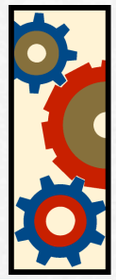
DNSSEC



...se les olvidó hablar con la gente que administra zonas de DNS.

No se podía implementar en zonas con más de unas pocas delegaciones por el exceso de tráfico administrativo que implicaba

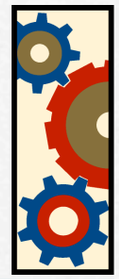
Una nueva esperanza



Con ayuda de varias personas y pruebas de lo que haría falta para operar DNS con DNSSEC, en particular usando la zona .nl, se modificó el estándar

11

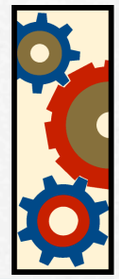
DNSSECbis



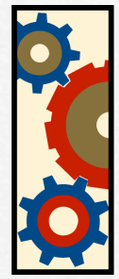
- RFC 4033/4034/4035

12

DNSSECbis



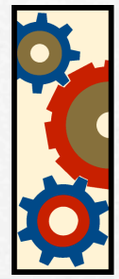
DNSSECbis



Pareja de Claves
KSK

13

DNSSECbis

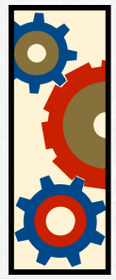


Pareja de Claves
ZSK

Pareja de Claves
KSK

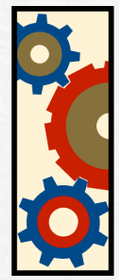
13

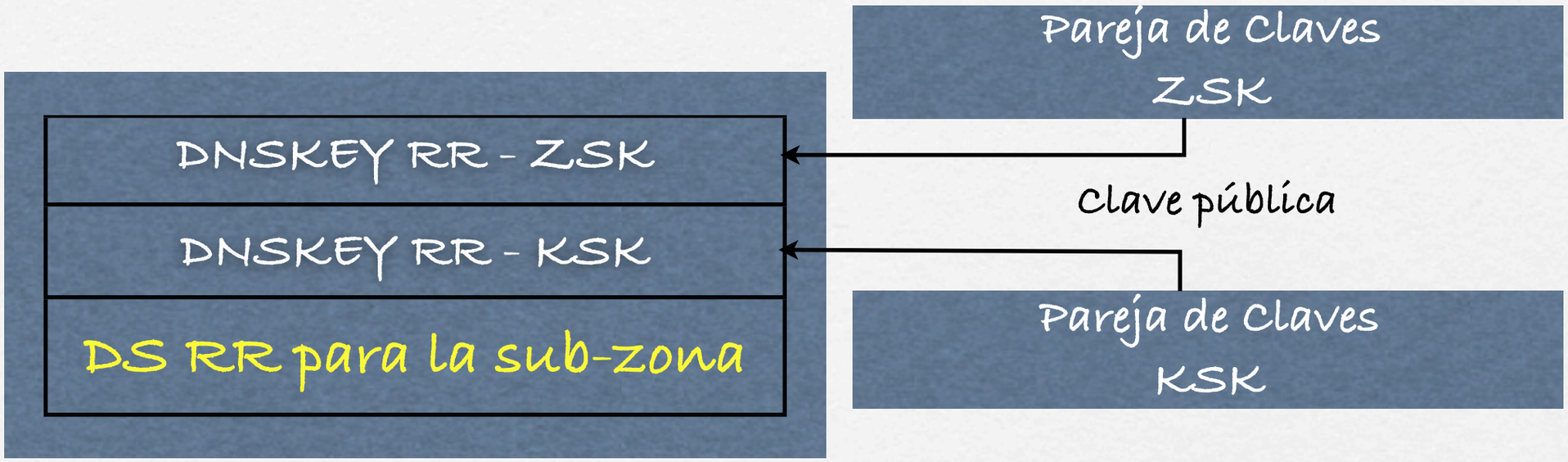
DNSSECbis



13

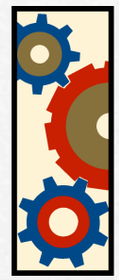
DNSSECbis

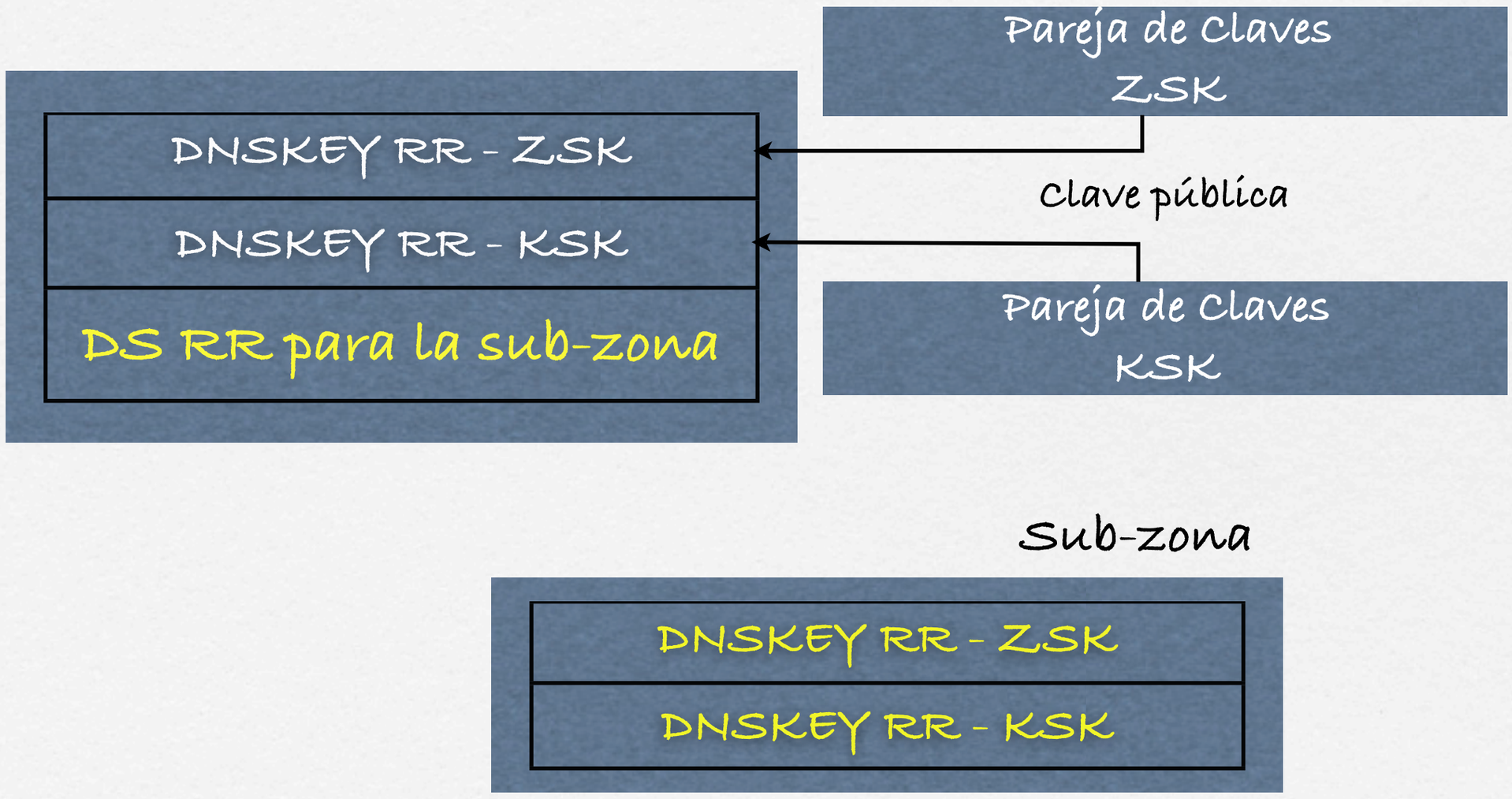




13

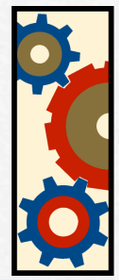
DNSSECbis

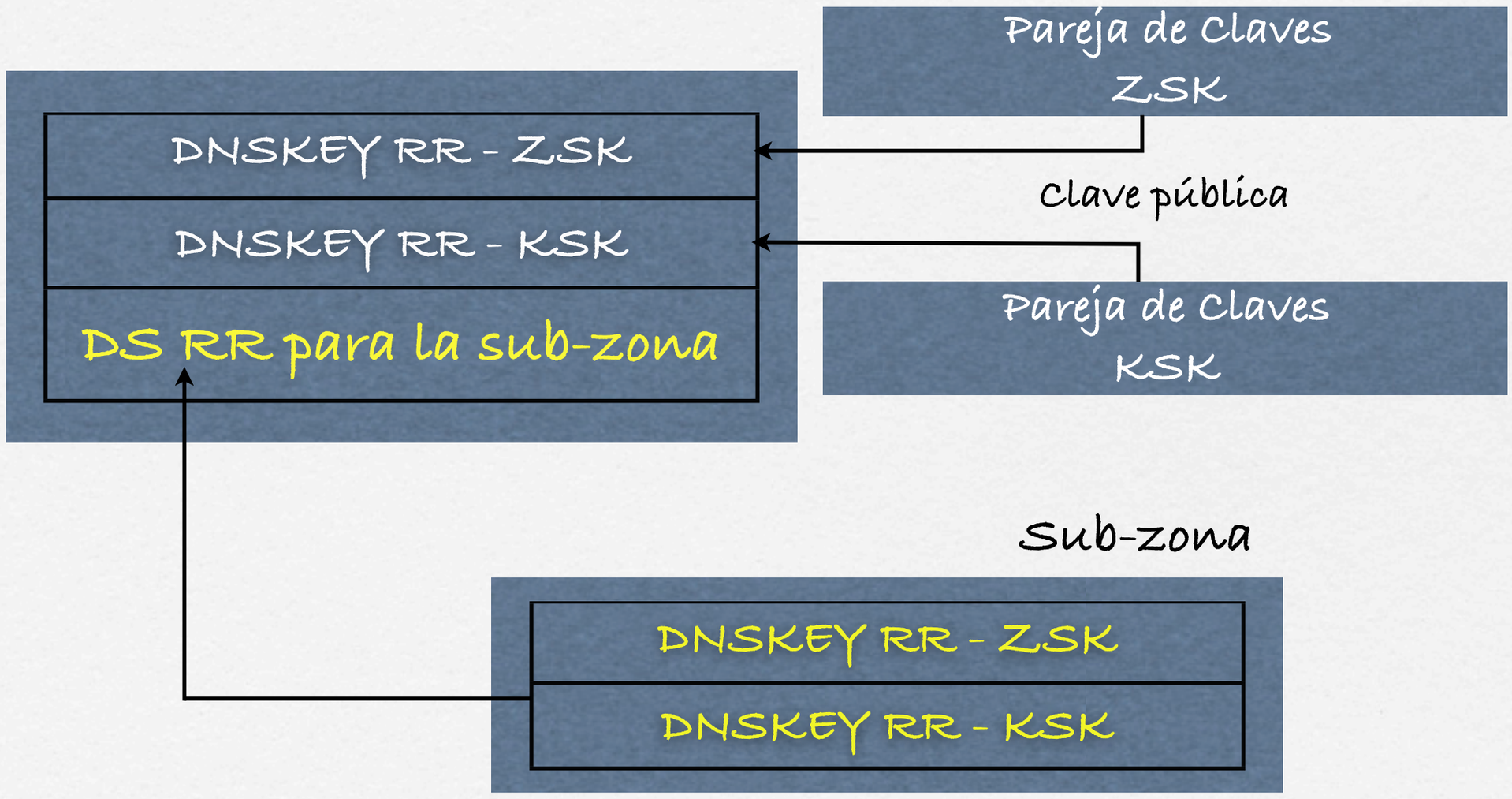




13

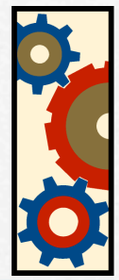
DNSSECbis

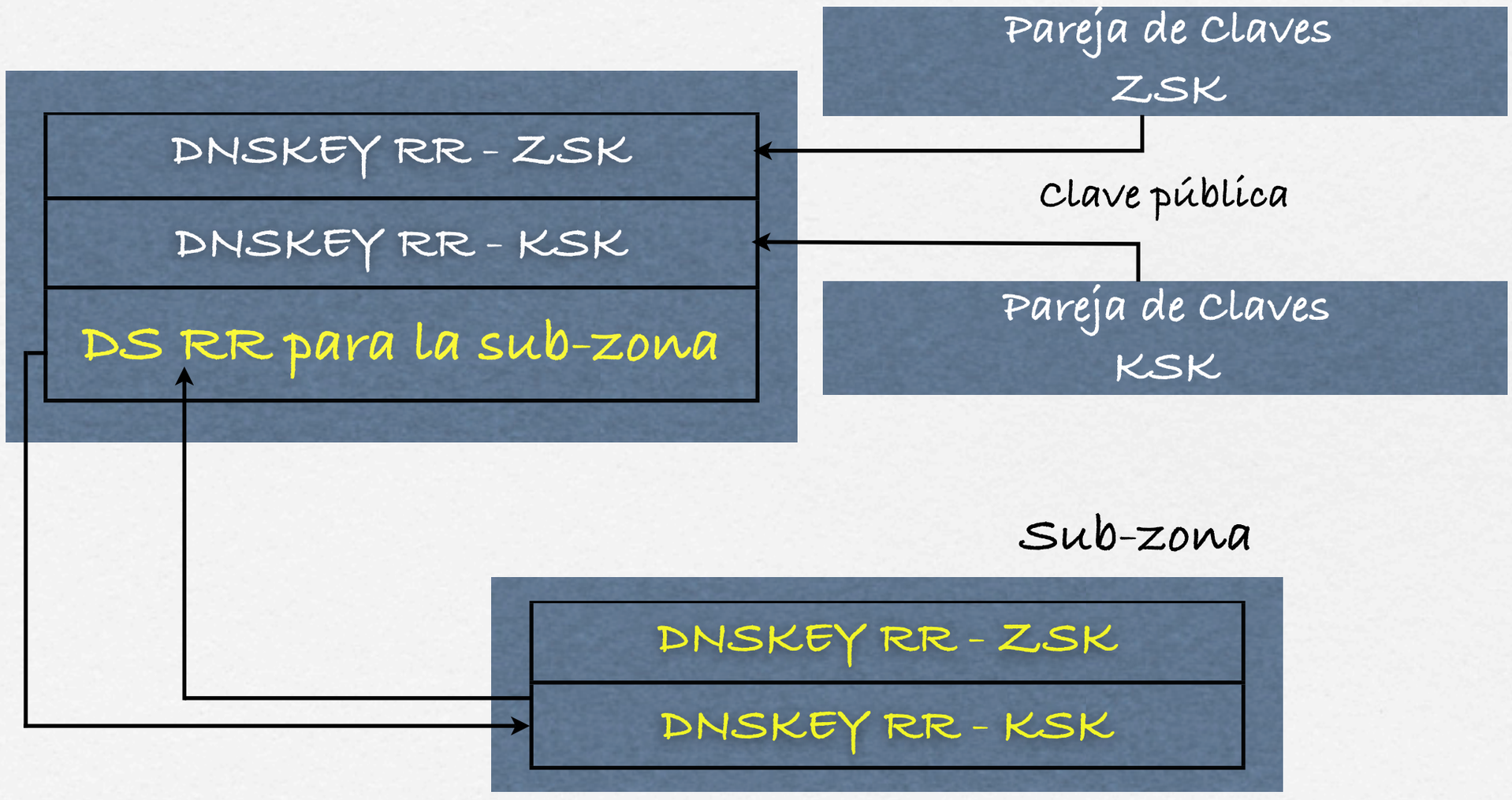




13

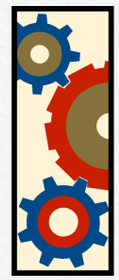
DNSSECbis

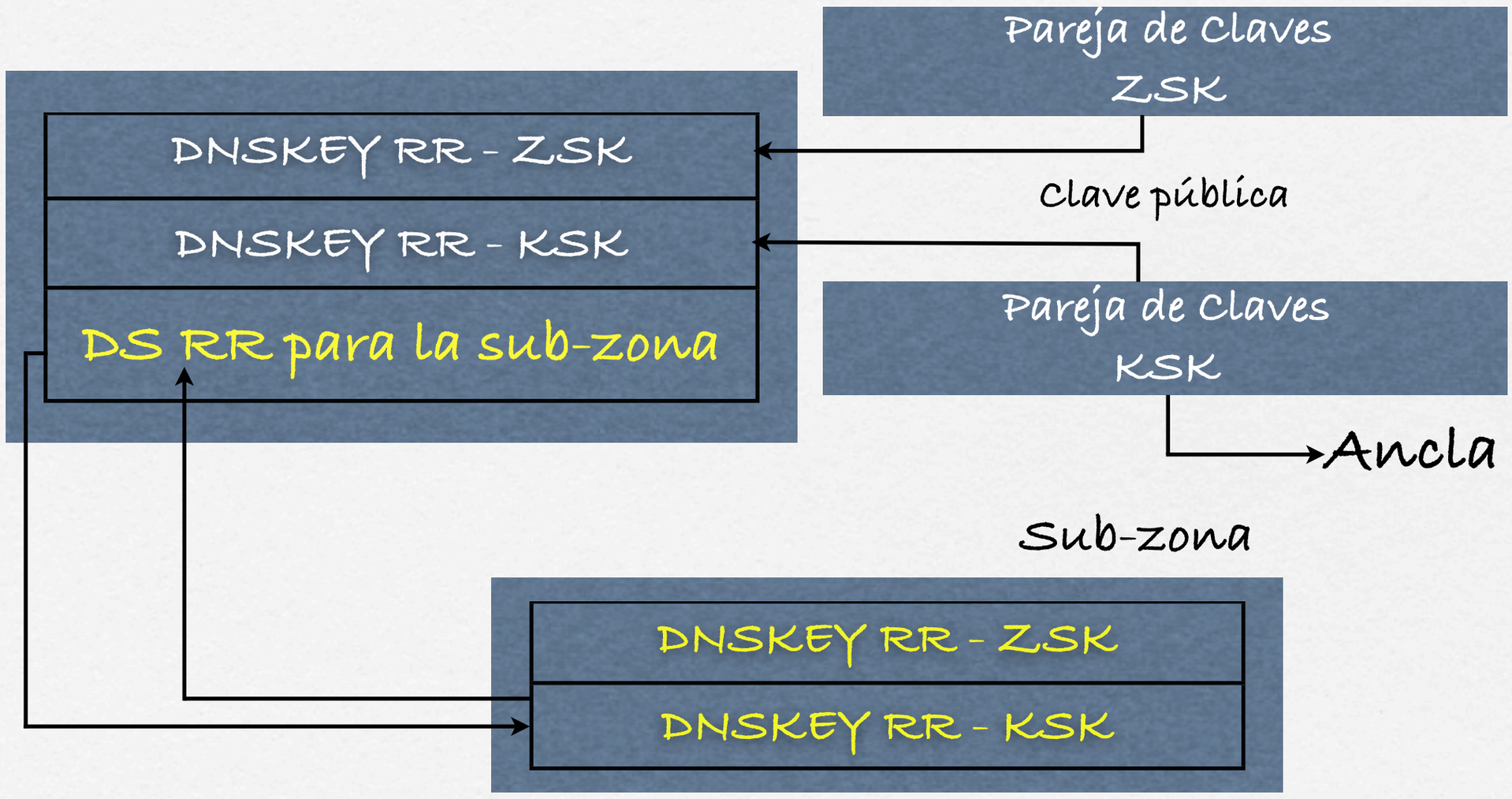




13

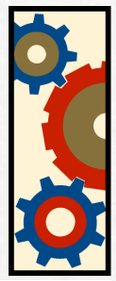
DNSSECbis





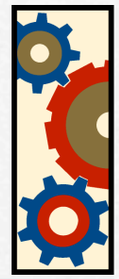
13

DNSSECbis



```
$ dig @ns.c-l-i.net c-l-i.net. soa +dnssec

; <<>> DiG 9.4.0a5 <<>> @ns.c-l-i.net c-l-i.net. soa +dnssec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42850
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;c-l-i.net.                IN     SOA

;; ANSWER SECTION:
c-l-i.net.          172800  IN     SOA     ns.c-l-i.net. hostmaster.c-l-i.net. 2006102701 43200 7200 1209600 7200
c-l-i.net.          172800  IN     RRSIG   SOA 5 2 172800 20061126144710 20061027144710 40259 c-l-i.net. bW2beSgoUSQGa0JfOmxY4utH03O0FKBbULetDHK/
XtEwvjLZ6uQ6wf+Y UxRRvuIxf5+u+fzvl3OTssgfrZNx6+MT0QftfFJKA/UqN6mgn4ak3MKG Xz3W0yX6Z5QJi01O9x2gj4UGKVvG6gHWuPtLVi8OSSHYc+lZPKObX451 wzE=

;; AUTHORITY SECTION:
c-l-i.net.          172800  IN     NS      ns.c-l-i.net.
c-l-i.net.          172800  IN     NS      borg.c-l-i.net.
c-l-i.net.          172800  IN     RRSIG   NS 5 2 172800 20061126144710 20061027144710 40259 c-l-i.net. RJ+s8eoVU1JAYP3f6KX/3lq2irfKNvJ6mFzCIkoFPtBzKFf9BFvfNCKb
QWoK351XcYvABo9UvRiyEmlCgxYOISVLshcd40KrzTbU2Q2yJAv0ZSsG 3jz2029WyHfQNn+Uptm2++jdbRRTDs1GbkNRivmnCz8E4VkUoy9VLWPW 6qc=

;; ADDITIONAL SECTION:
ns.c-l-i.net.       172800  IN     A       204.152.186.152
borg.c-l-i.net.     172800  IN     A       192.16.192.99
ns.c-l-i.net.       172800  IN     RRSIG   A 5 3 172800 20061126144710 20061027144710 40259 c-l-i.net. rP7/oxORWmLr01t9Sfqaj7PcJdW4d+TU0BLe7mG+4/xqdgaCowOvtqsK
8DdsCPEH4E8gM2iYaQ8aO9eCXhrbqvRWy5dhMGj2lFl7elXd2cexJuNR fp5GNS/QeSMLNV30MgCoI/KB7m2nDXciE1i0Ted1YkaAt/XeimYUwrhM Dec=
borg.c-l-i.net.     172800  IN     RRSIG   A 5 3 172800 20061126144710 20061027144710 40259 c-l-i.net. VUlHap6CySvPDJJ29CM75pN+raPZgNyRWifG0JxLVfklvgARV
+sW7kQX Xwd6HrCYurZZGtPdFfkplcFKA16wNFCz0X1tFGgj25VjEivoQTTcvS1y nW9r7rq7VILZKkSi1HGY31uPKdo6+A12ILcp1aPm0AirxG3pfJytwXOj Emk=
```

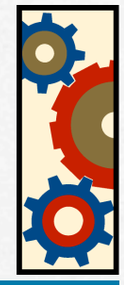
DNSSECbis



- Prueba de no existencia
  - Registros NSEC
  - Decriben intervalos entre dos nombres consecutivos en la zona

15

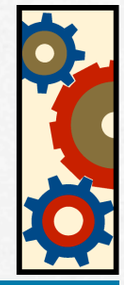
DNSSECbis



- implica que la zona tiene que estar ordenada
- lleva información sobre que tipo de registros existen o no en ese espacio

16

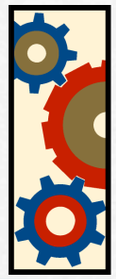
DNSSECbis



- Permite "caminar por la zona"
- Algunos TLDs perciben esto como un problema de privacidad
  - el problema real está en el whois, no en el DNS
- Desarrollo de NSEC3 y "online signing"

17

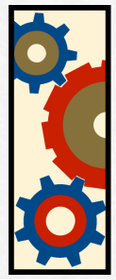
El problema de las anclas



- Todo este árbol necesita un sitio donde anclar su raíz
- Tener una raíz firmada va a tardar un rato
- Como esto era de esperar, se define el concepto de islas de seguridad, cada una con un punto de entrada

18

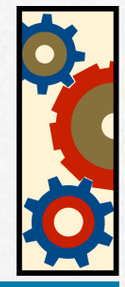
Islas de seguridad



- Permite uso de DNSSEC a falta de que esté el árbol completo
- Permite claves para ciertas partes del árbol
- Es tedioso si hay muchas islas
  - mantener al día las claves

19

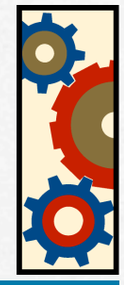
DLV



- Domain Lookaside Validation
- Funciona con BIND
  - Especificación pública pero no un RFC
  - Código RR asignado por la IANA
- Configuración local de cada servidor

20

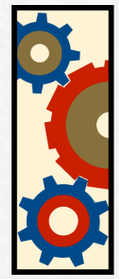
DLV



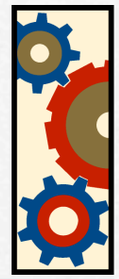
- Algoritmo
  - búsqueda según el modelo de DNSSEC estándar (anclas)
  - cuando se detecta una zona con información de DNSSEC, sí todo falla, se busca en la zona dlv.isc.org
  - la búsqueda es de más a menos específico, lo demás es igual

21

DLV



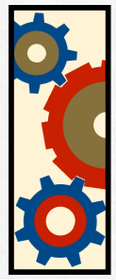
DLV



Raíz (.)

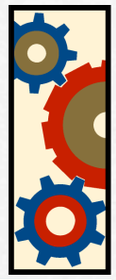
22

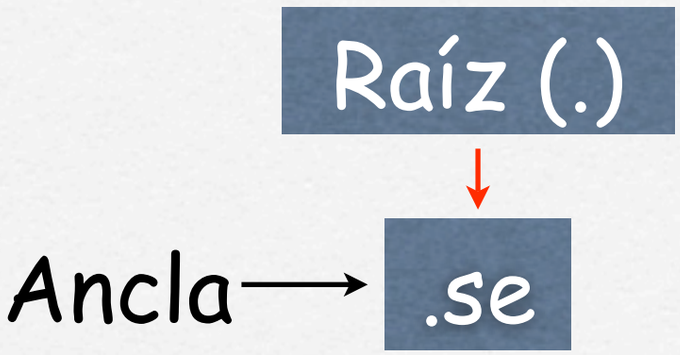
DLV



22

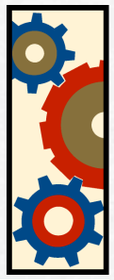
DLV

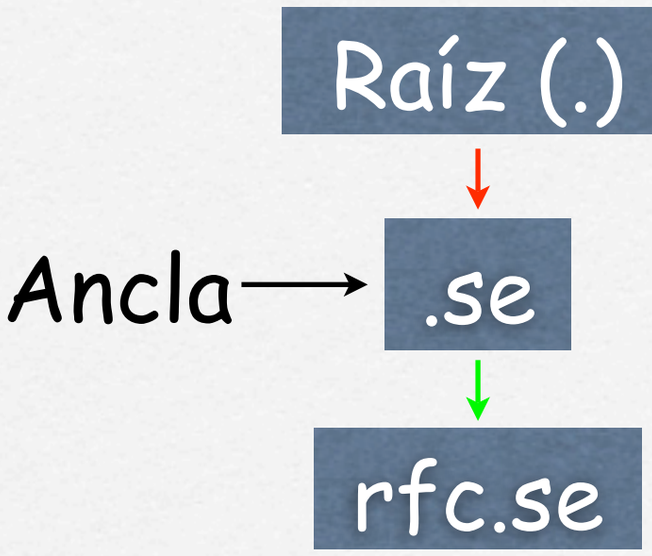




22

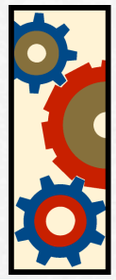
DLV

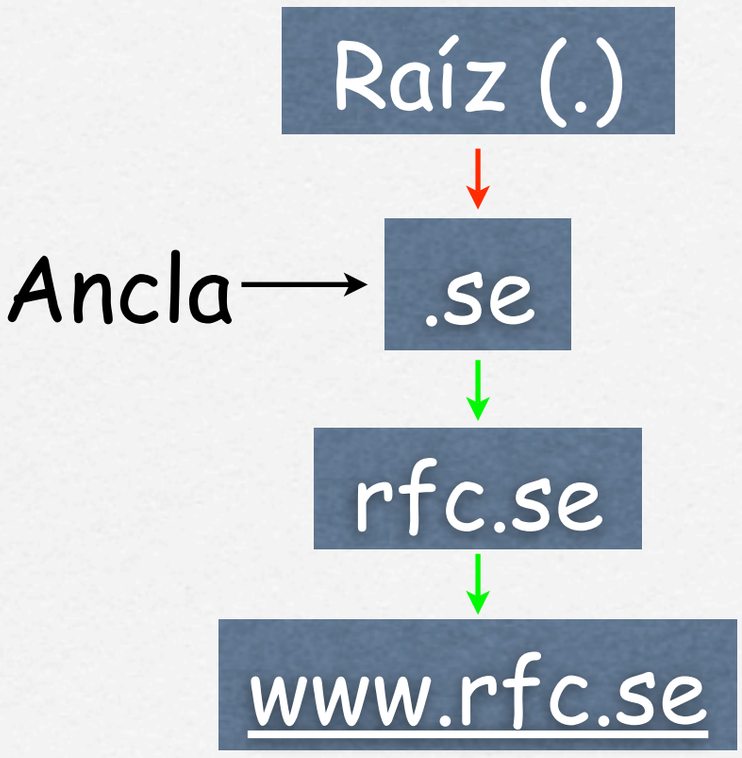




22

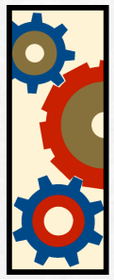
DLV

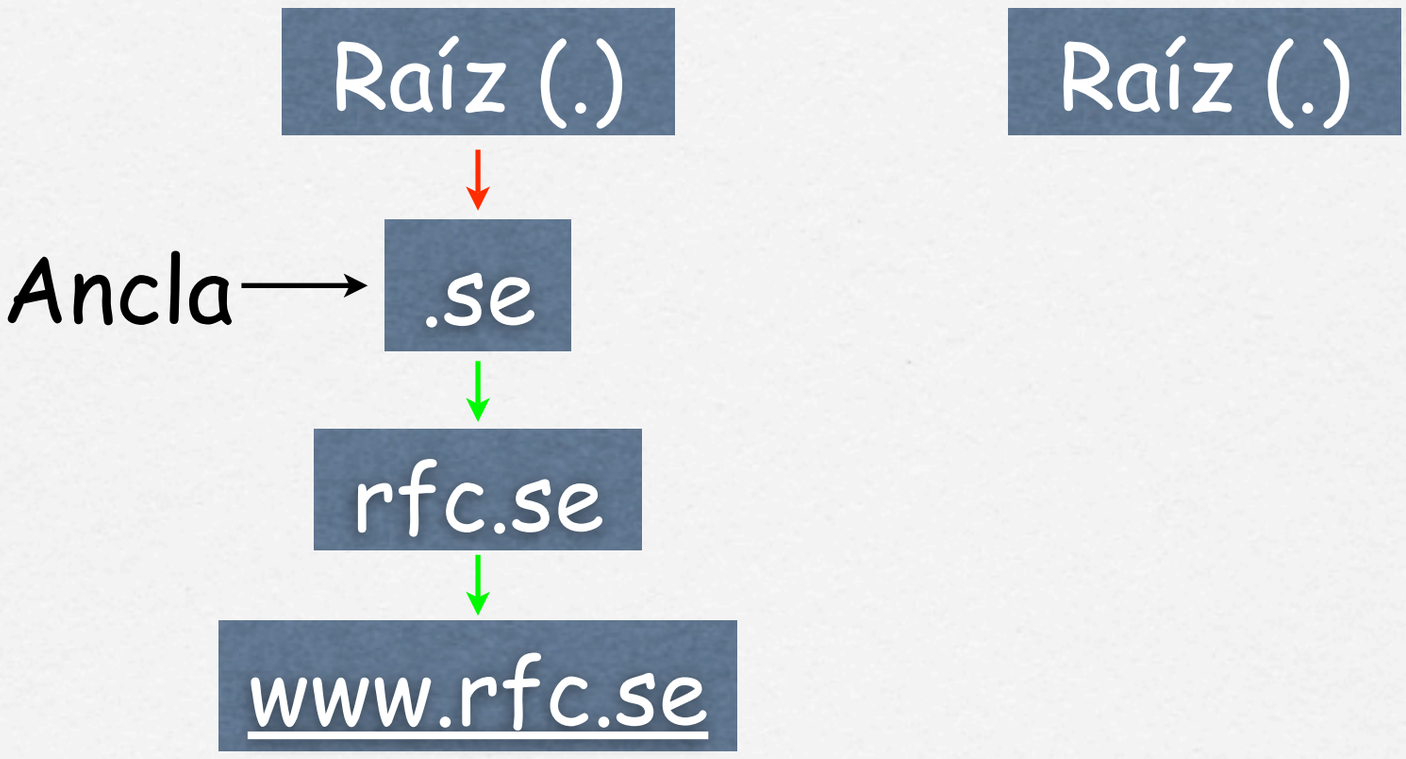




22

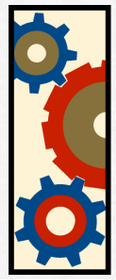
DLV

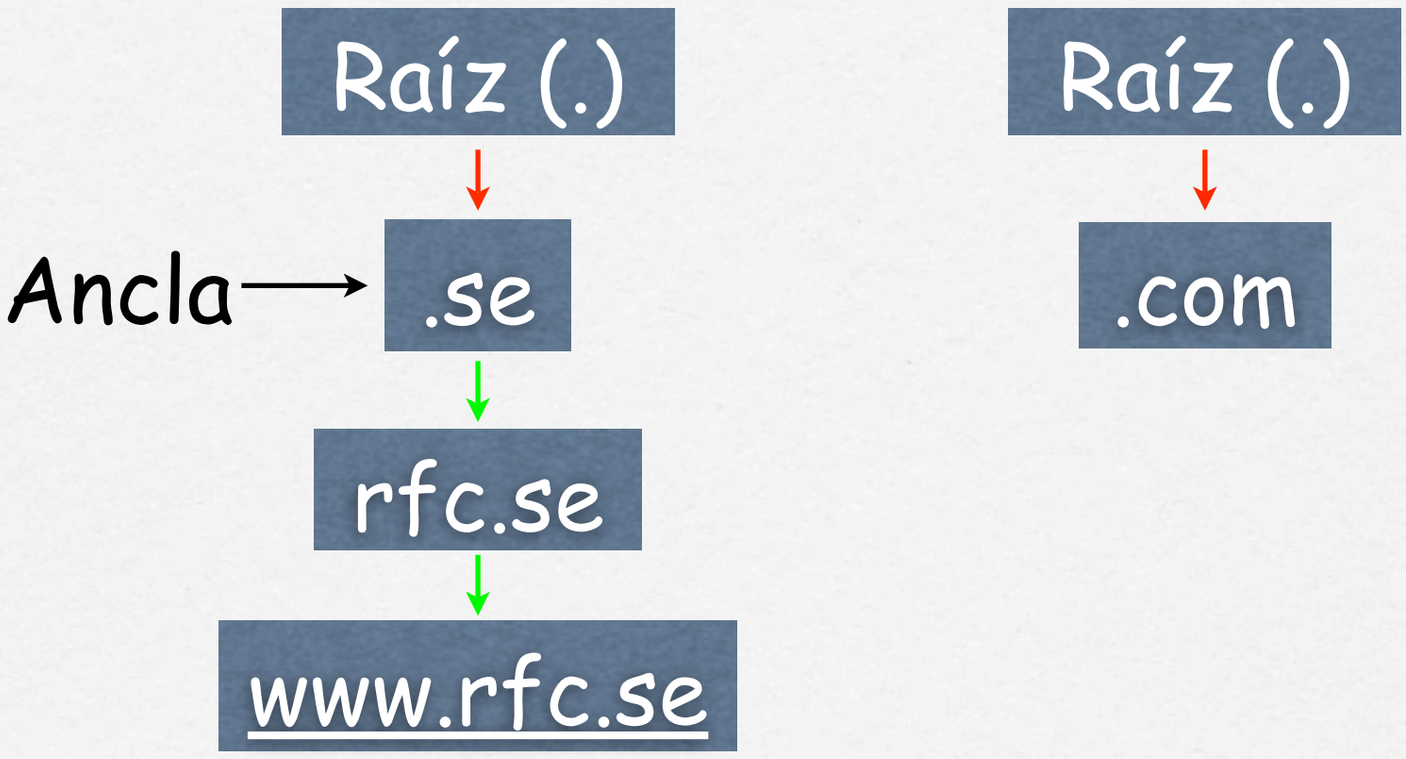




22

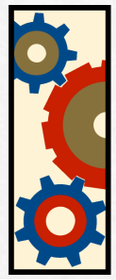
DLV

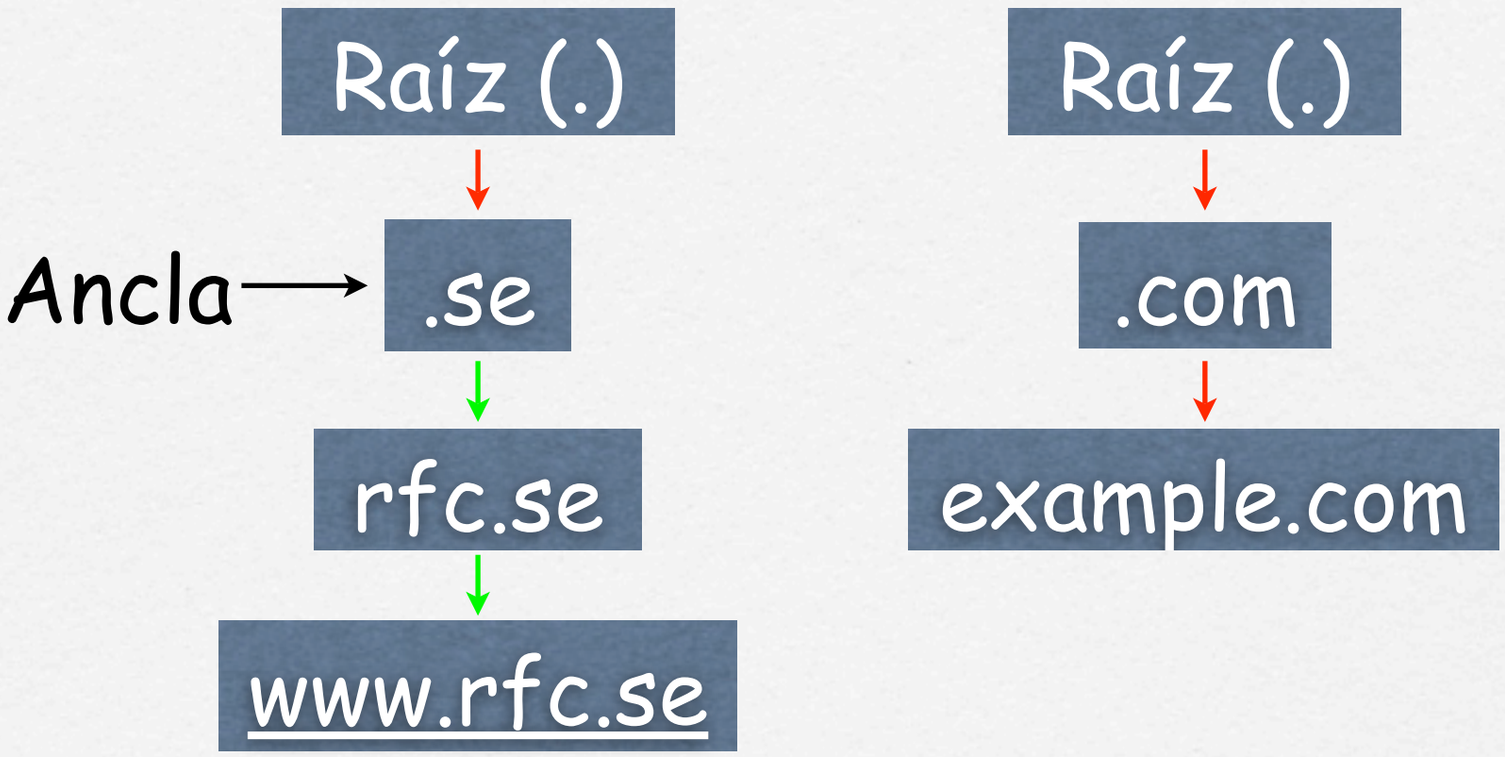




22

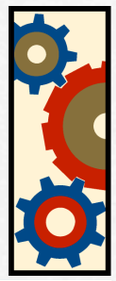
DLV

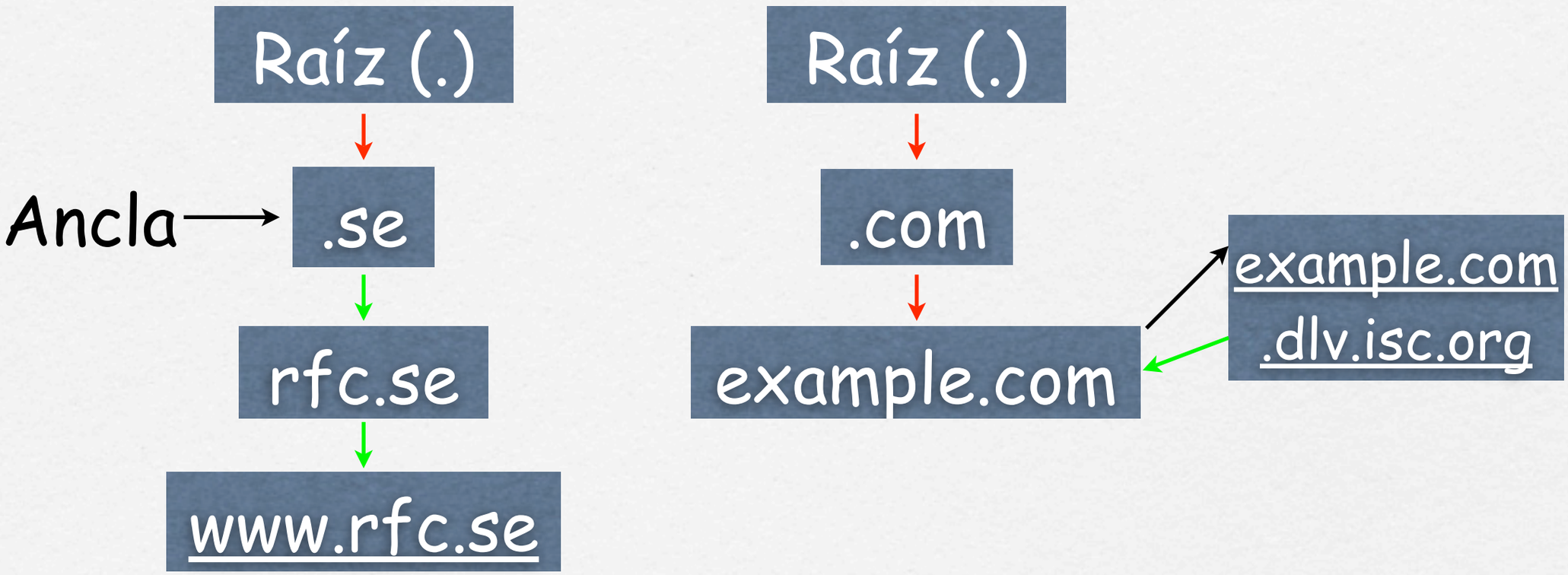




22

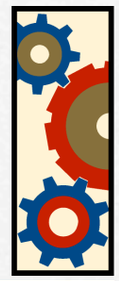
DLV

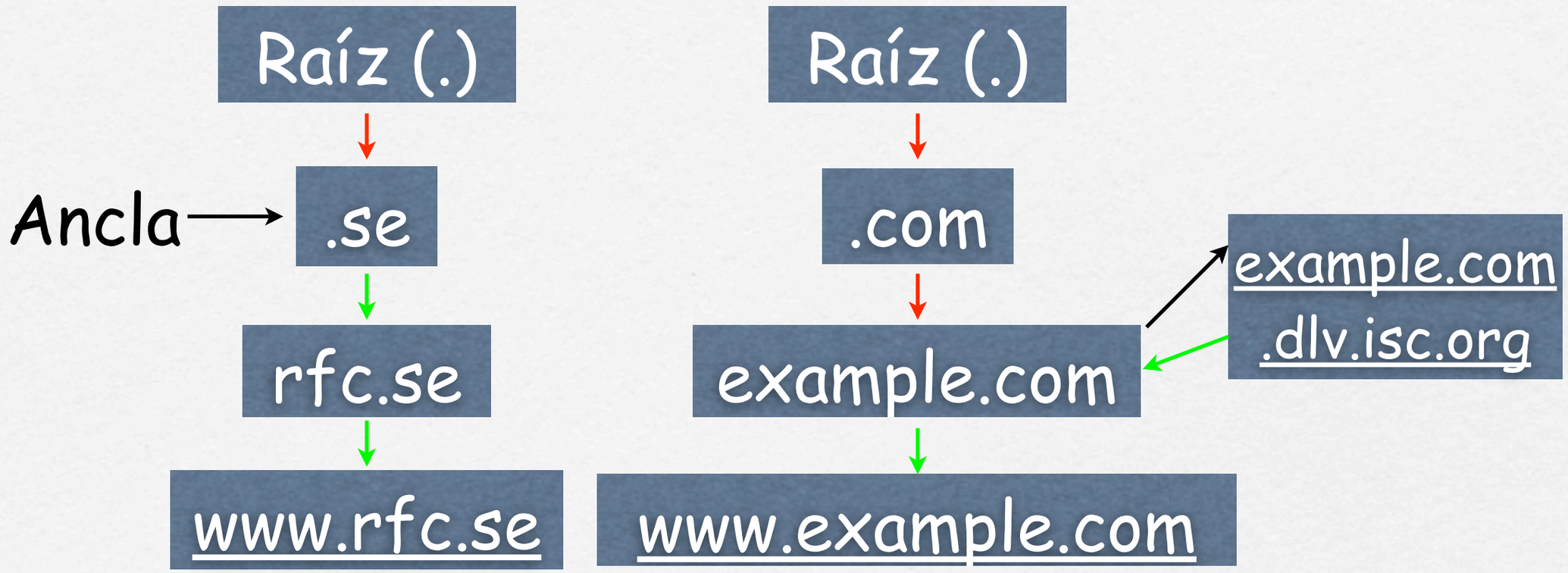



Raíz (.)
Ancla
.se
rfc.se
www.rfc.se
Raíz (.)
.com
example.com
example.com
.dlv.isc.org

22

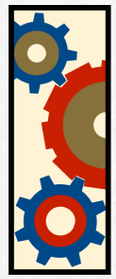
DLV




Raíz (.)
Ancla
.se
rfc.se
www.rfc.se
Raíz (.)
.com
example.com
www.example.com
example.com
.dlv.isc.org

22

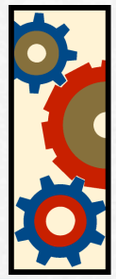
Operación



- Todo esto es muy bonito pero el DNS es más que solamente el protocolo
  - ataques, abuso, configuración

23

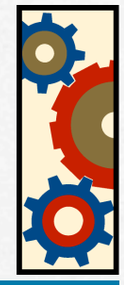
Software y configuración



- Diversidad de software
  - BIND, en especial BIND 9
  - NSD, para servidores autoritarios
  - Nominum
  - PowerDNS
  - etc...

24

Software y configuración



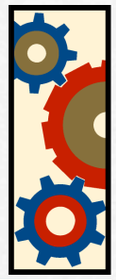
- Esconderse no ayuda

```
options {
    version "Esto no es un BIND"
};
```

- fpdns (http://www.rfc.se/fpdns/) te sacará los colores :)

25

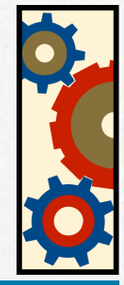
Software y configuración



- Usar los menores privilegios posibles
- Usar chroot
- Mantener el software actualizado
  - suscribirse a las listas del software elegido
  - Preferir Open Source

26

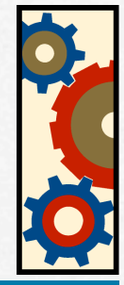
Software y configuración



- Generación de la zona
  - Permisos para alterar datos en la zona
  - Verificación del proceso de generación de la zona
  - Acuerdos de operación con servidores secundarios

27

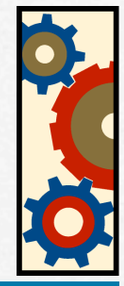
Ataques al DNS



- Tradicionalmente se había intentado contaminar caches de servidores con información falsa
  - Famoso caso de Kashpurev con alternic
- Todavía son posibles técnicas similares aunque cada vez es más difícil

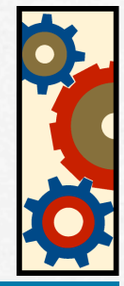
28

Ataques al DNS



- Ahora se estilan más los ataques a lo bruto
  - usando botnets para ahogar a los proveedores con tráfico
  - El uso de firewalls resulta perjudicial

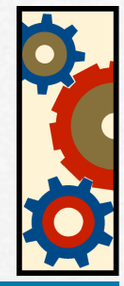
Ataques al DNS



- se requieren métodos de coordinación entre ISPs y proveedores.
  - Ej. OARC (http://oarc.isc.org)
- Cada vez más son ataques con fines de extorsión o con ánimo de tirar el sistema.

30

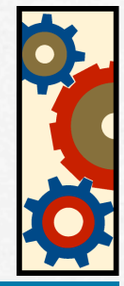
Ataques usando DNS



- DNS usa fundamentalmente UDP para transporte.
- No hay un concepto de sesión
- Interacciones cortas
- aunque hay otros protocolos que usan UDP, DNS es más fácil de usar.

31

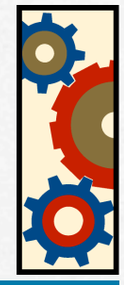
Ataques usando DNS



- Ataques de reflexión-amplificación
  - Falsifica la dirección IP de origen en el paquete de UDP
  - Se mandan varios paquetes de este estilo a servidores recurrentes abiertos, que dan servicio a cualquiera

32

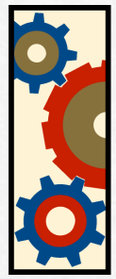
Ataques usando DNS



- Las respuestas convergen sobre la dirección IP falsificada, que es la víctima.
- Si se llena el cache de los servidores con respuestas grandes, se consiguen factores de amplificación bastante grandes.
- Difíciles de contrarrestar, ahogan las conexiones, no los servidores.

33

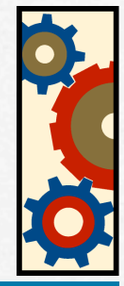
Ataques usando DNS



- Ver draft internet draft-ietf-dnsop-reflectors-are-evil-02.txt
  - No dar servicio a toda la Internet, solo a los clientes propios
  - Filtrar tráfico con direcciones de origen que no pertenecen a la propia red (BCP 38 y BCP 84), uRPF, etc

34

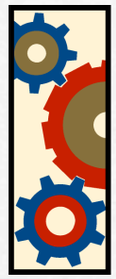
Resumen



- DNSSEC
  - Ha sido una aventura
    - El protocolo está listo
    - El software está listo
    - hay mecanismos para usarlo ya
- Evolución de los ataques

35

Gracias



Preguntas

36