El gran agujero del DNS

João Damas
ISC

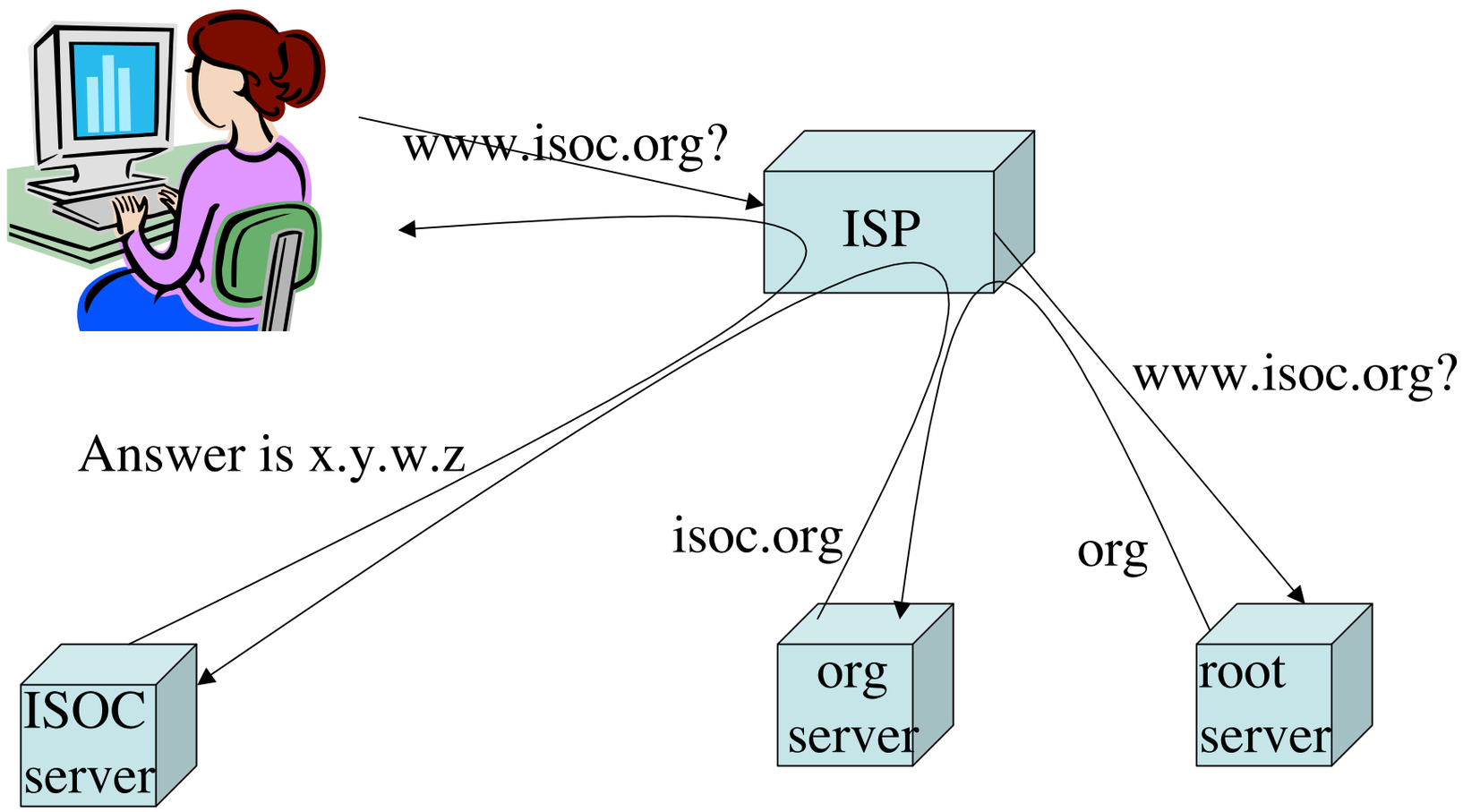
Indice

- DNS y caches
- Cronología
- Descripción del ataque Kaminski
- Soluciones

Proceso de resolución del DNS

INTERNET SOFTWARE CONSORTIUM

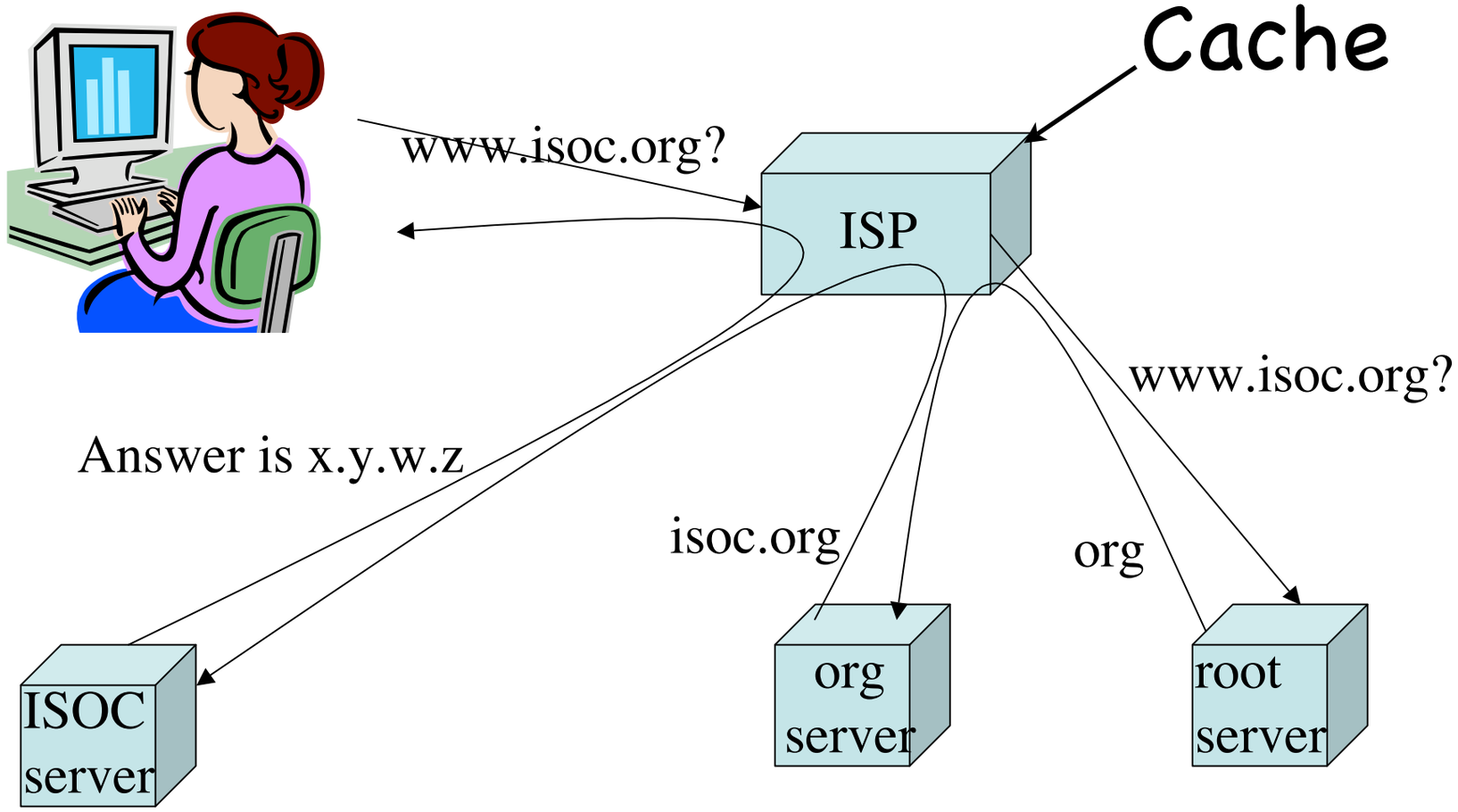
What is it? (2)



Proceso de resolución del DNS

INTERNET SOFTWARE CONSORTIUM

What is it? (2)



Cronología

- 1996: kashpureff cache poisoning
  - problema en BIND 4 y 8 permitió redirigir el nombre de InterNIC a AlterNIC
- Feb 2008 - Llamada de Dan Kaminski
- Mar 2008 - Reunión en Seattle
- Julio 2008 - parches de varios fabricantes
- Ago 2008 - Blackhat 08

El ataque de Kaminski

El ataque de Kaminski

- Al contrario que el ataque de Kashpureff, este no se basa en un bug de los servidores, sino en las limitaciones del protocolo DNS
- Mucho más eficaz, mucho más difícil de defender

El ataque de Kaminski

En episodios anteriores...

```
$ dig @ns1.example.com www.example.com
    ;; ANSWER SECTION:
    www.example.com.    120     IN    A    192.168.1.10

    ;; AUTHORITY SECTION:
    example.com.        86400   IN    NS   ns1.example.com.
    example.com.        86400   IN    NS   ns2.example.com.

    ;; ADDITIONAL SECTION:
    ns1.example.com.    604800  IN    A    192.168.2.20
    ns2.example.com.    604800  IN    A    192.168.3.30
    www.isc.org. 86400  IN    A    204.152.184.88
```

Empieza la carrera...

El ataque de Kaminski

```
$ dig meloinvento.example.com
    ;; ANSWER SECTION:
    meloinvento.example.com.  5    IN  A    10.10.10.10

    ;; AUTHORITY SECTION:
    example.com.              86400    IN  NS   www.example.com.

    ;; ADDITIONAL SECTION:
    www.example.com.          386400   IN  A    10.10.10.20
```

Aquí el atacante puede repetir todas las veces que quiera, y como el QID solo tiene 16 bits, al poco tiempo gana.

Soluciones

- Inmediata: Aumentar "entropía"
- Mejor: DNSSEC

Aumentar entropía

- Varias soluciones
  - Utilizar los 16 bits que designan el puerto UDP como algo más que el atacante tiene que adivinar.
  - Utilizar todas las posibles direcciones IP del servidor.
  - Idea 0x20 y 0x20 extendida.

Aumentar entropía

- Problemas con el uso de puertos e IPs
  - el API de sockets de Unix no está pensado para abrir y cerrar miles de puertos por segungo
  - algunos kernels no lo aguantan
  - select() es lento(isimo)
  - hay mecanismos (e.j. epoll) mejores pero no son portables.

Aumentar entropía

- 0x20
  - ¡idea genial!
  - parece que todos los servidores devuelven el bit 0x20 (00100000) sin tocar, igual que les llegó en la pregunta. Es el que distingue mayúsculas de minúsculas en el código ASCII

La solución definitiva

DNSSEC

- DNSSEC utiliza **firmas** criptográficas para verificar los datos del DNS
- si no tienes la clave, no puedes mentir de forma creíble

DNSSEC - cosas pendientes

- Es un cambio significativo en las operaciones de DNS
- El funcionamiento automático necesita que se firme la raíz, los TLDs, etc
- Algunos equipos (firewalls) no lo dejan pasar
  - en general es cierto de cosas como EDNS(0)

DNSSEC - cosas pendientes

- Las utilidades son un poco primitivas
  - ldns de NLNetlabs
  - BIND 9.7 - "one button DNSSEC"

DNSSEC - pasos adelante

- El gobierno de EEUU ha publicado una orden por la que el dominio .gov tiene que estar firmado antes del 31/12/08 y los dominios de segundo nivel tienen que publicar un plan para firmarlos durante 2009 antes del 31/12/08

- DoC ha publicado una solicitud de comentarios sobre dos propuestas para firmar la raíz, la de ICANN y la de Verisign. Resultados después de las elecciones.

¿qué me importa DNSSEC si ya está ahí SSL/X.509?

http://computerworld.co.nz/news.nsf/NL/FCC8B6B48B24CDF2CC2570020018FF73

Invalid banking cert spooks only one user in 300

Users remain the weakest link

By Stephen Bell Wellington | Monday, 16 May, 2005

Up to 300 BankDirect customers were presented with a security alert when they visited the bank's website earlier this month — and all but one dismissed the warning and carried on with their banking.

The bank's logs show about 300 customers used the single affected server during the 11-hour period when the certificate was out of date and only one backed out of the page, says Clayton Wakefield, head of technology for BankDirect owner ASB.

Peter Benson, chief executive of Auckland-based Security-Assessment.com, says he is "not at all surprised" at the statistics. "In my experience, the single weakest point in the chain of [computer] security is the space between the keyboard and the floor."

¿Preguntas?