¿Que está pasando en el IETF?

DNS

Carlos Martínez (@carlosm3011)

LACNOG 2017 - LACNIC 28

Montevideo

Tres áreas mayores de trabajo

a. “Endureciendo” (*hardening)* del DNS
   i. Aumentar su resistencia a diferentes formas de abuso y ataque
b. Mejorar las características de privacidad del DNS
   i. Evitar divulgar información innecesariamente
   ii. Evitar todo lo que sea posible transportar información personal
c. Colaborar con las CDNs brindando información en el DNS que las ayude a dirigir los usuarios al contenido más cercano

Hardening del DNS

Privacidad en el DNS - ¿cual es el problema?

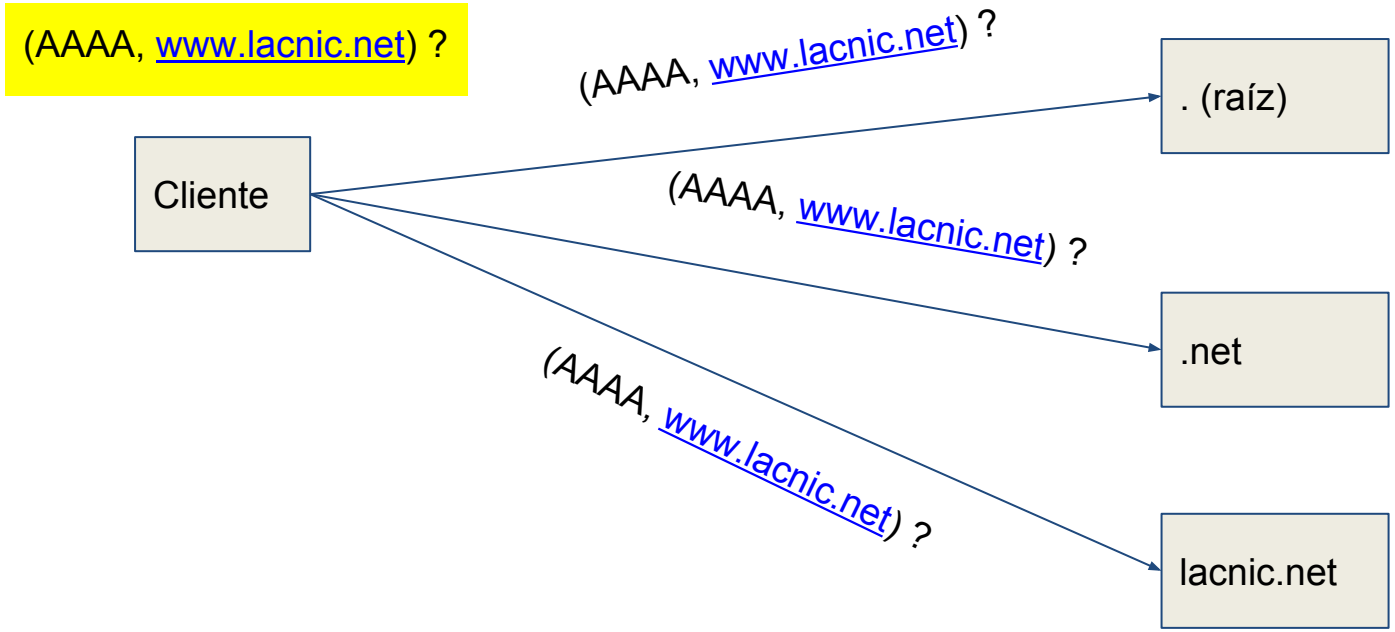
- la información contenida en el DNS es pública
- pero… las **consultas específicas** que hacemos no necesariamente lo son
- ¿Por qué? Imaginen:
  - *Un activista consultando un sitio no autorizado por su gobierno*
  - *Un empleado de una empresa consultando por un sitio con información sobre una cierta enfermedad*

Privacidad en el DNS

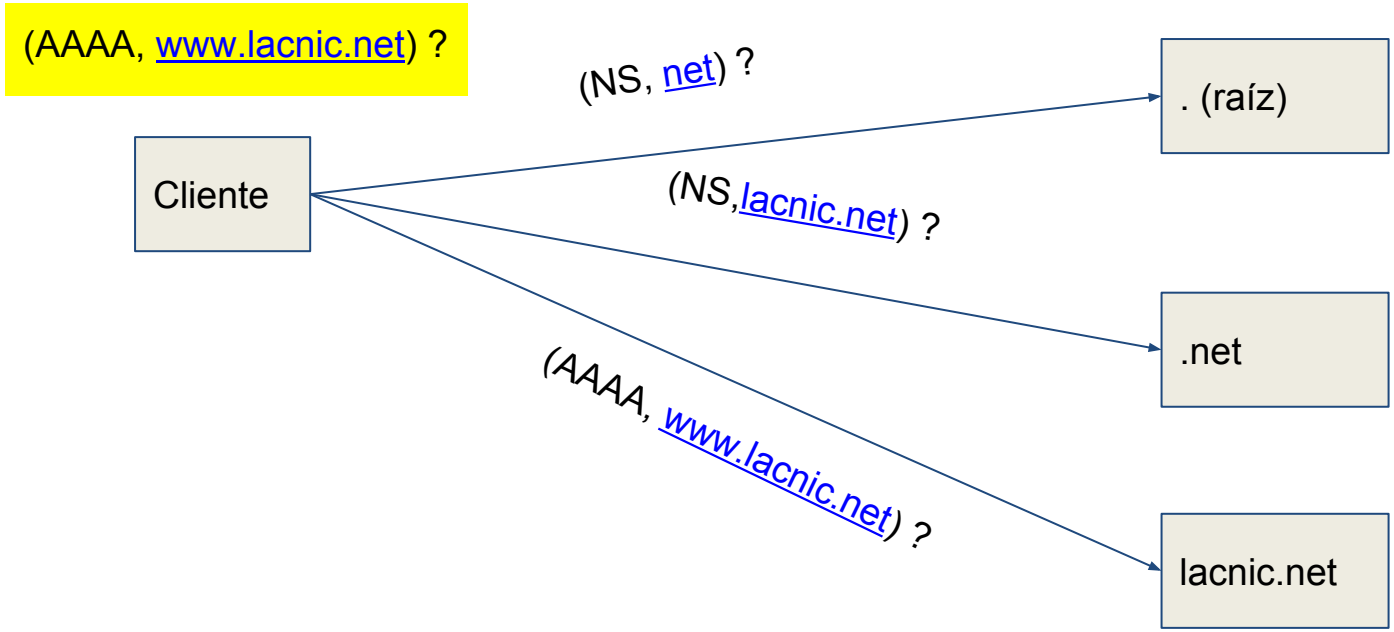
QNAME minimization - RFC 7816

- *Evitar divulgar demasiado las consultas que se realizan en el DNS*
- En la resolución recursiva tradicional se divulga demasiada información
- ¿Como podemos minimizar esta fuga de datos?
- https://tools.ietf.org/html/rfc7816

Resolución recursiva "tradicional"



Resolución recursiva “minimizada”



Transporte seguro

- QNAME-minimization resuelve parte del problema, pero las consultas siguen viajando en “texto plano”
- El WG “DPRIVE” está analizando diferentes transportes que cifren la información de consultas
  - DNS sobre TCP sobre TLS - RFC 7858
    - https://tools.ietf.org/html/rfc7858
  - Es la aproximación más “obvia”, ya que DNS sobre TCP ya está definido, y TCP sobre TLS también
    - *“... over some reliable transport protocol..” (RFC 5246)*
    - puerto 853

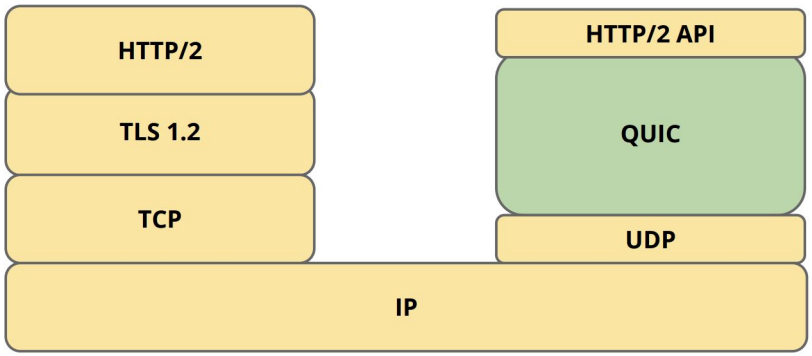
Transporte seguro (ii)

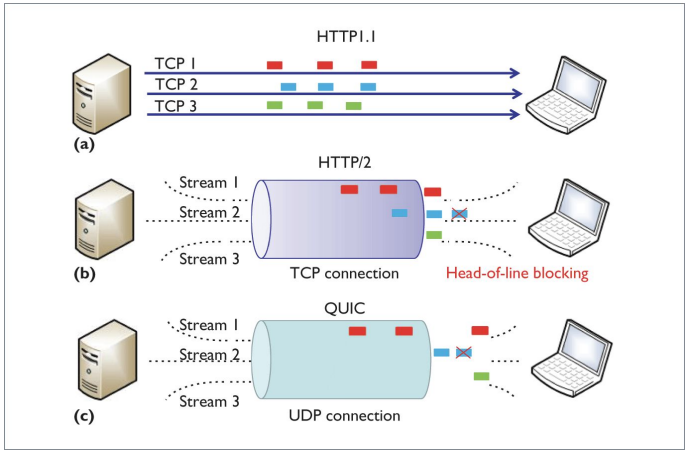
Pero… "*... the good thing about standards is that there are a lot of them*"

- DNS over HTTPS (¡si, en serio!)
  - Existe una visión de que el transporte "de facto" en Internet es ahora HTTP, y en particular HTTPS
  - https://tools.ietf.org/html/draft-hoffman-dns-over-https-01
- DNS over DTLS (RFC 8094)
  - DTLS es TLS para UDP
  - https://tools.ietf.org/html/rfc8094

Transporte seguro (iii)

- DNS over QUIC
  - ¿¿ Q U I … C ?? ¿ de qué hablas hijo?
  - **Q**uick **U**DP **I**nternet **C**onnections





  - QUIC es:
    - cifrado por defecto, multiplexa conexiones (*streams*), no sufre de NAT, basado en UDP (0-RTT connection establishment)

Transporte seguro (iv)

- DNS sobre QUIC parece encerrar la mejor proposición general en el sentido de tener
  - *cifrado “automático”*
  - *no sufre de problemas de fragmentación*
  - *está basado en UDP*
  - En general las implementaciones de QUIC son en modo usuario y no en modo kernel, permitiendo una evolución más ágil del protocolo
- https://tools.ietf.org/id/draft-huitema-quic-dnsoquic-02.txt

ANAME vs CNAME

- ANAME: https://tools.ietf.org/html/draft-ietf-dnsop-aname-00
- CNAME no puede coexistir con otros registros para el nombre de la propia zona (p.ej. el NS o MX)
- ANAME si puede coexistir con otros registros y permite compartir
- Útil para por ejemplo delegar servicios a CDNs sin “hardcodear” direcciones en el “zone apex”

Registros DNS a granel

- “Bulk DNS Resource Records”: https://tools.ietf.org/html/draft-woodworth-bulk-rr-06

```
example.com. 86400 IN BULK A (
      pool-A-[0-255]-[0-255].example.com.
     10.55.${1}.${2}    )
```

- (A, *pool-A-47-24.example.com)?* -> ***(A, 10.55.47.24)***
- Zonas repetitivas con valores numéricos de tamaño muy grande pero sin gran consumo de memoria ni tráfico
- **Reversos IPv6**

Localización vía DNS

- El problema que tienen las CDNs:
  - "*El valor de la respuesta DNS debería ser la dirección del nodo CDN más 'cercano' al cliente*"
  - (para alguna definición de 'cercano')
- Tradicionalmente esto era "sencillo" de hacer cuando cada ISP centralizaba sus consultas y proveía sus propios recursivos
  - Alcanza con responder lo más cercano a cada recursivo
- Sin embargo cuando se utilizan recursivos públicos (Google, OpenDNS) esta hipótesis falla

Localización vía DNS

- Solución ya existente: “EDNS Client Subnet” option (RFC 7871)
  - Transporta la subred del cliente que origina la consulta, es insertada por el recursivo
  - Limitación: no considera puertos de origen (CGN!!)
  - Queja: privacidad
- Nueva propuesta: “DNS X-Proxied-For” (draft-bellis-dns-x-proxied-for)

DNS XPF

- Se define un resource record, XPF
- El draft propone:

> The XPF RR contains the entire 5-tuple of (protocol, source address, destination address, source port and destination port) of the packet received from the client by the proxy.

- Resuelve la limitación de la “client subnet option”
- Los problemas de privacidad parecen bastante más serios

DNS XPF (ii)

- En realidad el XPF no debería llegarle a más nadie que al destino final de la consulta
  - *yeah… but…*
- Un tema más de fondo:
- Que el IETF no trate un tema no quiere decir que luego no se implemente igual
  - Ya lo hemos sufrido con el NAT

Agradecimientos

- Geoff Huston
  - [https://blog.apnic.net/2017/07/25/ietf-99-prague-theres-lot-going-dns/]
- Reporte de CENTR y su traducción
  - [https://www.centr.org/library/library/external-event/centr-report-on-ietf99.html#]
  - [http://www.lactld.org/wp-content/files_mf/ietf2017.pdf] - Hugo Salgado

¡Muchas gracias! ¿Preguntas?

lacnic 15 años 2002•2017 CONSTRUYENDO COMUNIDAD