Privacidad en el DNS

Fernando Gont

LACNIC 31
Punta Cana, República Dominicana. Mayo 6-10, 2019

Enunciado del Problema (I)

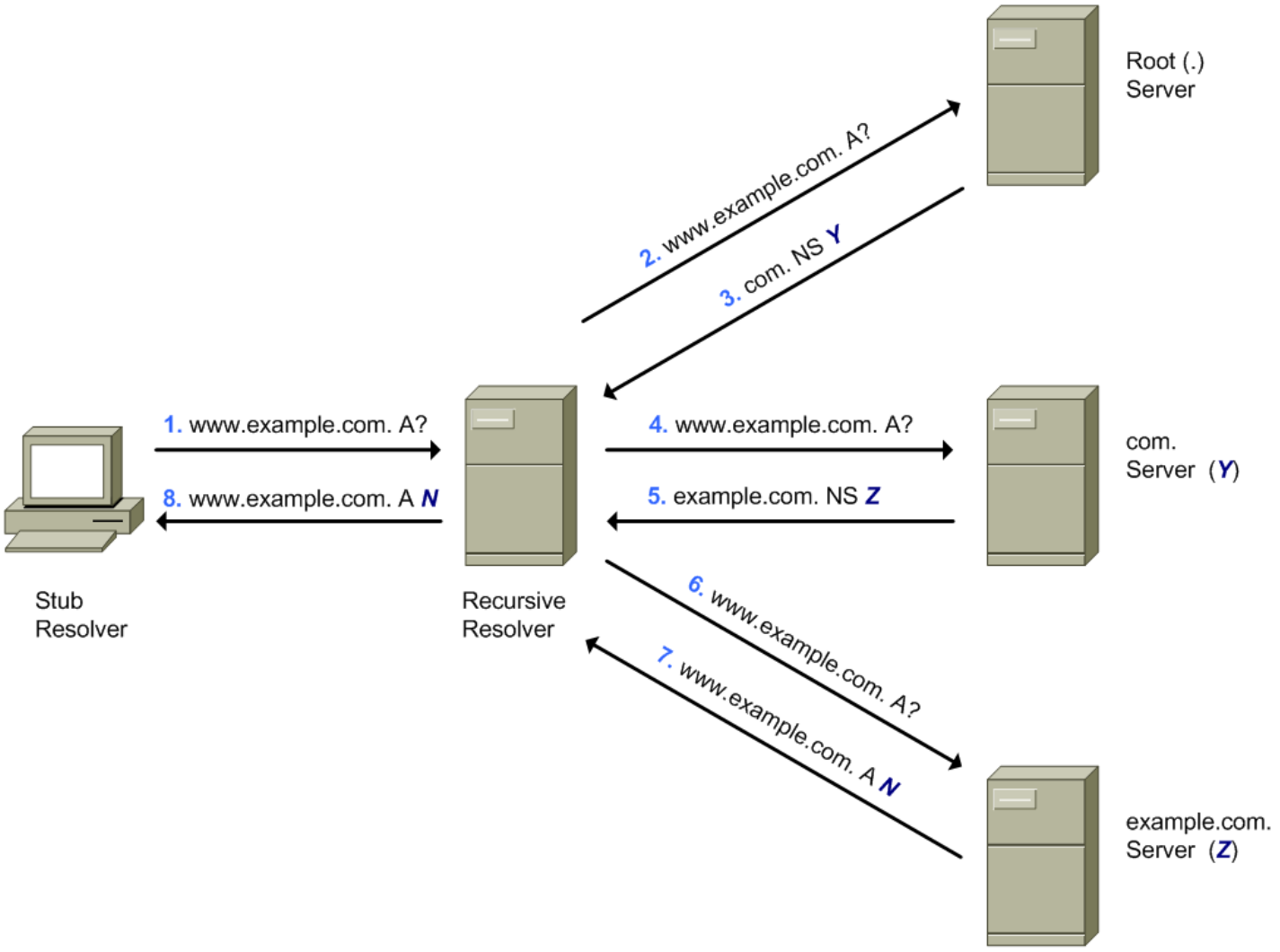
- Casi toda actividad de red está precedida por transacciones DNS
- Estas transacciones revelan información sobre nuestras comunicaciones:
  - Sitios web que visitamos
  - Aplicaciones que utilizamos
  - Personas con las que nos comunicamos
- Ejemplos:
  - www.clarin.com A? -> Visita a una página de fake news
  - whatsapp.com A? -> Uso de whatsapp
  - gont.com.ar MX? -> correo a alguien de mi familia

Enunciado del Problema (II)

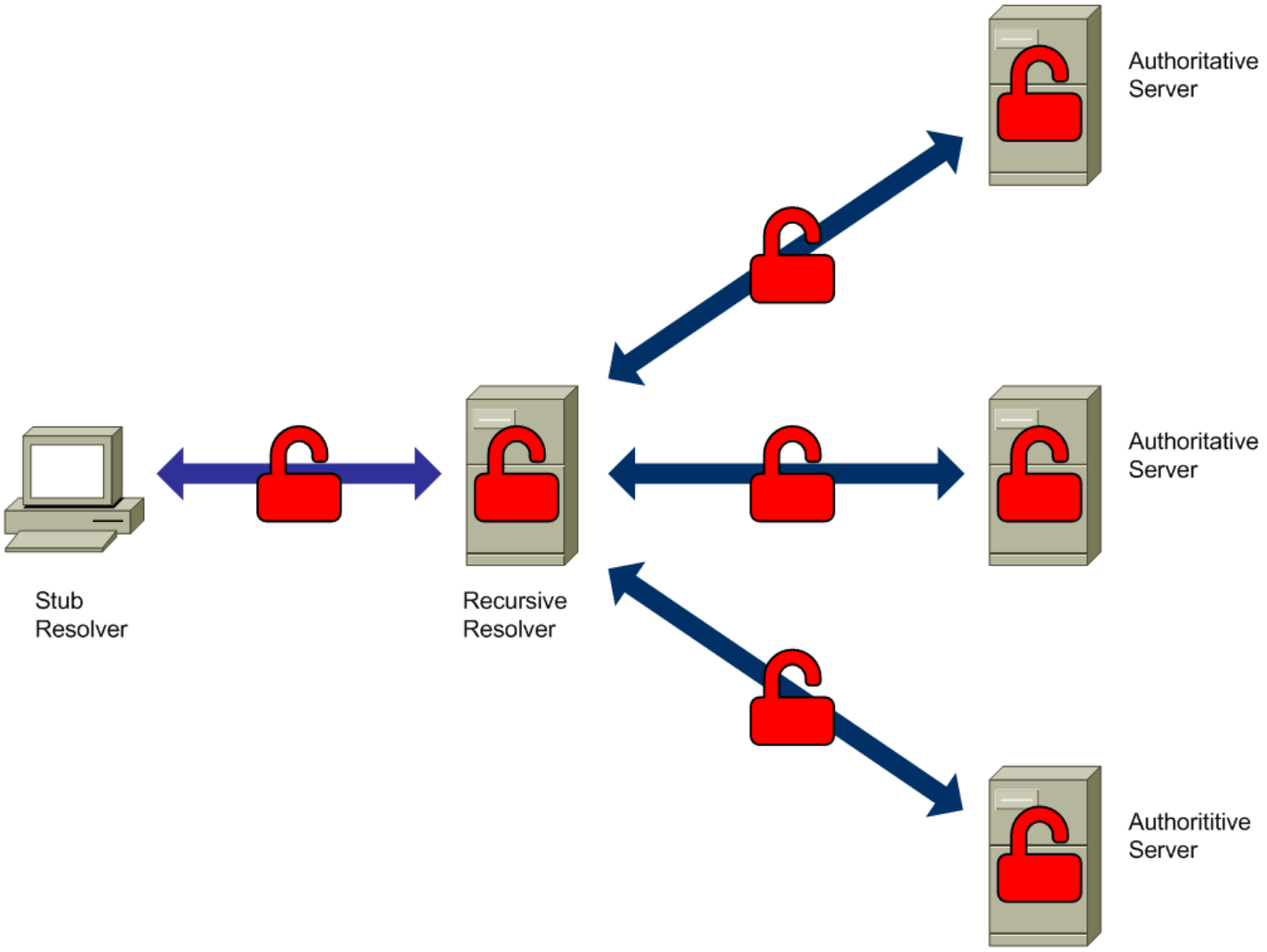
- Las transacciones DNS ocurren en texto plano
  - DNSSEC no provee privacidad a las transacciones DNS
- Esta cuestión ha sido abordada:
  - Proactivamente: DNScrypt
  - Reactivamente: Recientes esfuerzos en IETF

Problemas de Privacidad en DNS

Revisión sobre Peticiones DNS

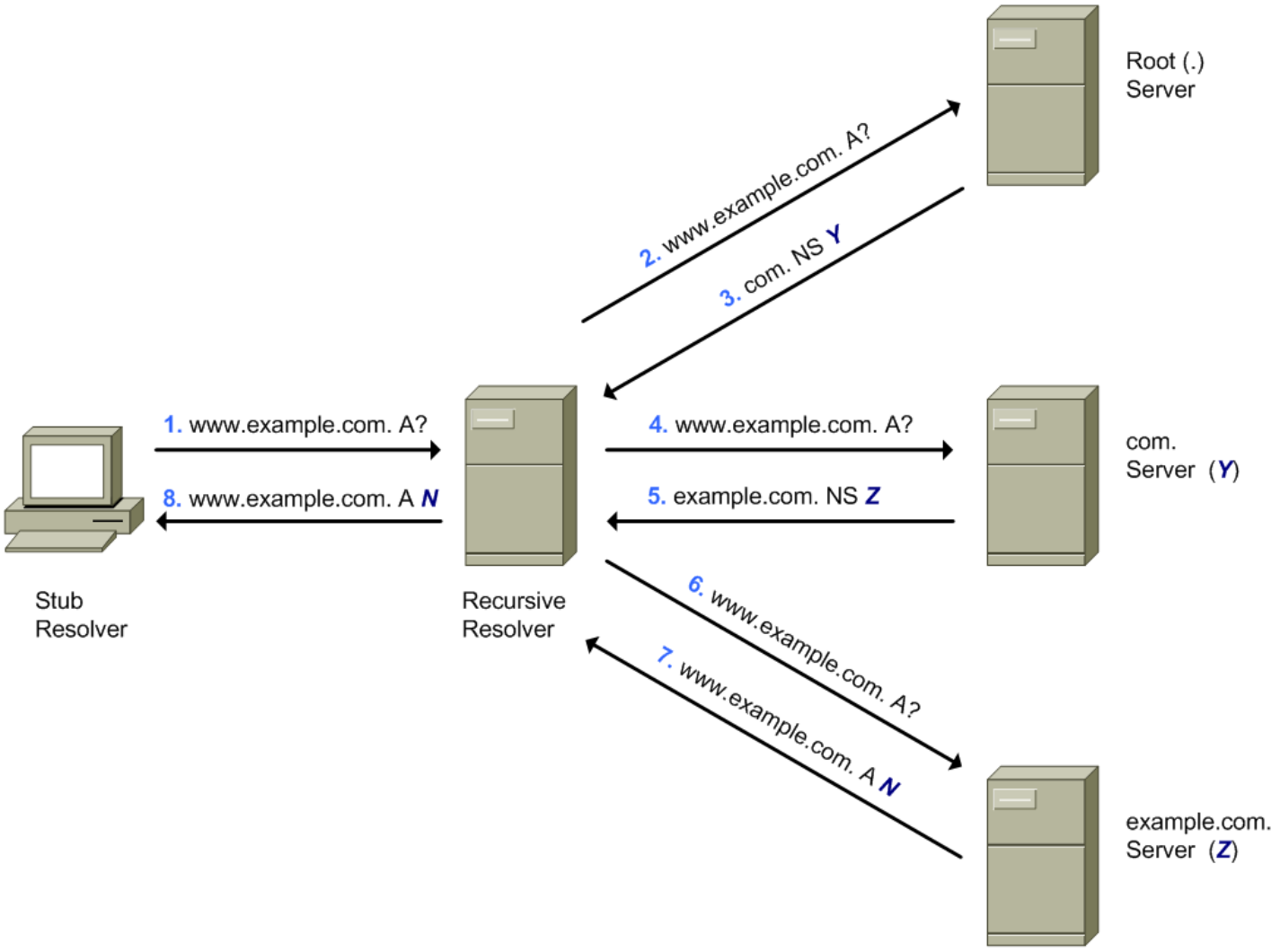


Posibles Fugas de Información

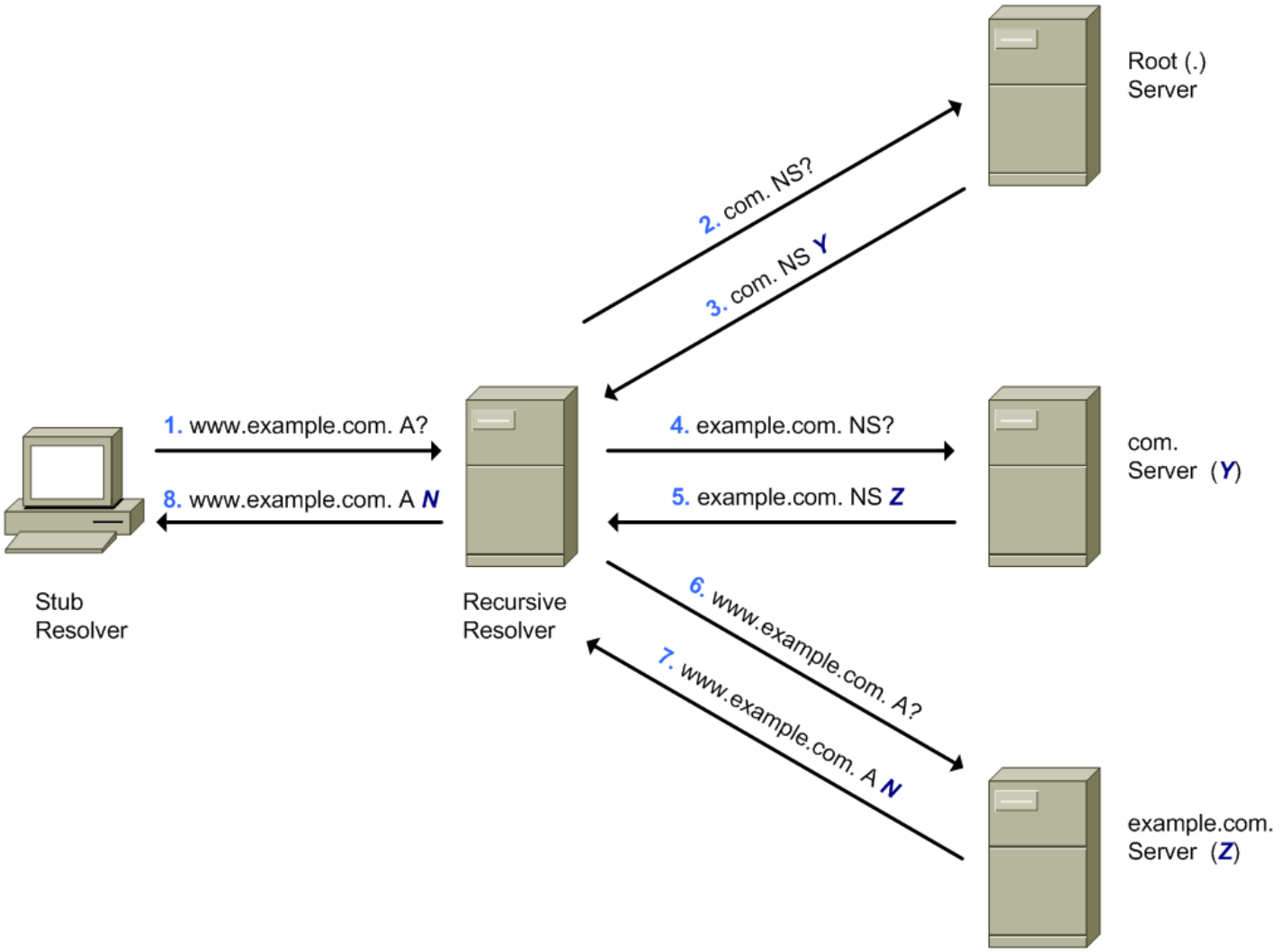


Mejoras en Privacidad DNS
Minimización de QNAME

Resolución Normal

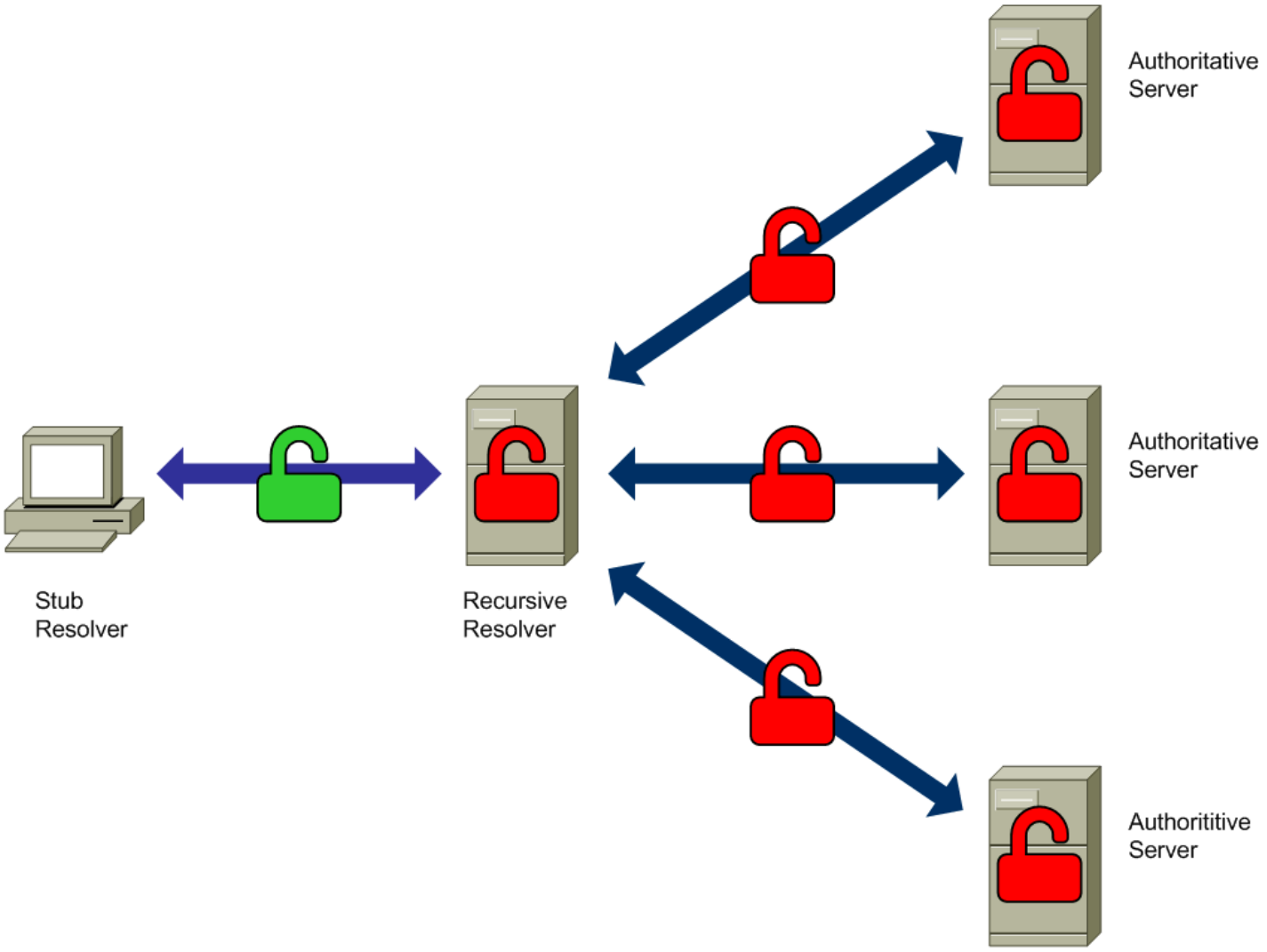


MInimización de QNAME (RFC7816)



Mejoras en Privacidad DNS
Cifrado de Transacciones

Cifrado de Transacciones



Cifrado de comunicación con resolutores

- Existen diversas técnicas para cifrar la comunicación con resolutores:
  - DNSCrypt -- pioneros, no-IETF
  - DNS over TLS (DoT) [RFC7858]
  - DNS over DTLS (DoD) [RFC8094]
  - DNS over HTTPS (DOH) [RFC8484]
- DoH codifica DNS queries/responses en HTTPS
- DoD y DoT tienen el potencial de usarse entre nameservers

Ubicación del Resolutor Recursivo

- La localización del resolutor recursivo tiene implicancias en numerosas áreas
- Registro de peticiones:
  - Dónde es posible registrar peticiones sin siquiera hacer sniffing?
- Identidadad expuesta
  - Qué identidad se expone a los servidores autoritativos?
- Jurisdicción legal:
  - Qué leyes aplican al resolutor recursivo?
- Respuestas dependientes de la topología?
  - Por ej., nombres de dominio que resuelven a IPs “cercanas”

Ubicación del Resolutor

Resolutor	En host	En CPE	En ISP	Tercera Parte
Registro de peticiones	No	No	Si	Si
Sniffing	Cualquier parte	Cualquier parte	Del host al ISP	No
Identidad expuesta a Servidores Autoritativos	Host	Red	ISP	Tercera Parte
Jurisdicción Legal	Misma que el host	Misma que el host	Misma que el host	Misma de la Tercera Parte
Respuestas dependientes de la topología	Si	Si	Si	No

Mejoras en Privacidad DNS
Cifrado de Transacciones: Despliegue

Implementaciones

- DNScrypt, DoH y DoT:
  - Implementaciones varias: stubby, Firefox, Chrome
  - Pueden estar habilitadas por defecto (con resolutores abiertos)
  - En ocasiones se utilizan en paralelo con la resolución tradicional
- Minimización de QNAME:
  - Implementación en resolutores recursivos populares (por ej. BIND)

Resolutores DNS “con privacidad”

- Existen resolutores abiertos que implementan mecanismos de privacidad:
  - Google (8.8.8.8)
  - Cloudflare (1.1.1.1)
  - ....
- El argumento es algo así como:

“Tendrás más privacidad si nos envías todos tus peticiones DNS a nosotros”

Conclusiones

Hasta que punto tiene sentido?

- Cosas que (en principio) tienen sentido:
  - Cifrar las transacciones DNS es algo positivo
  - Minimización de QNAME
- Impacto:
  - Dominios de dominios en HTTPS son leakeados por la extensión SNI
  - Las direcciones IP a veces proveen información similar
  - El impacto real es cuestionable

Si la privacidad es una preocupación, pensar en VPNs, TOR, etc.

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

www.si6networks.com