¿Cómo puedo hacer el DNS más resiliente y seguro?

Una charla sobre algunas amenazas y posibles soluciones …

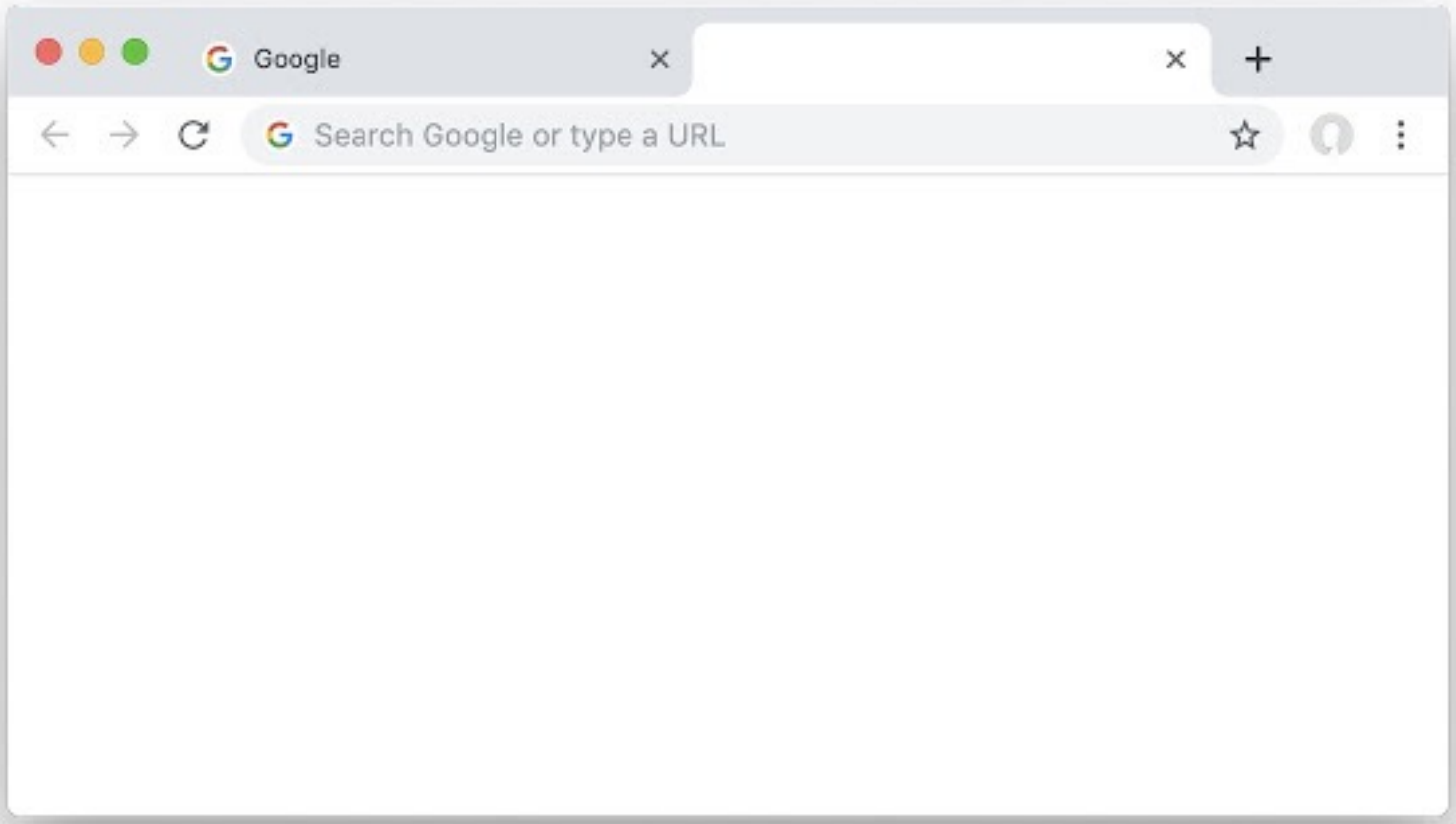
Nicolás Antoniello

LACRALO
18 de Abril, 2022

ICANN

Internet hoy

¿?


Google
Search Google or type a URL

Algunos elementos de un sistema a considerar…

Servicios de correo y calendario…

- E-mail
- Calendario
- Contactos

Servicios de Base de Datos…

- Datos del negocio
- Datos de clientes
- Datos de funcionarios
- Inventarios

Servidores de archivos…

- Información financiera
- Documentación interna
- Procesos y procedimientos de la organización

Sistemas de control y operación…

- Control de equipamiento
- Monitoreo
- Aprovisionamiento

Mecanismos de seguridad…

- Contraseñas
- Control de accesos
- Control de cambios
- VPNs

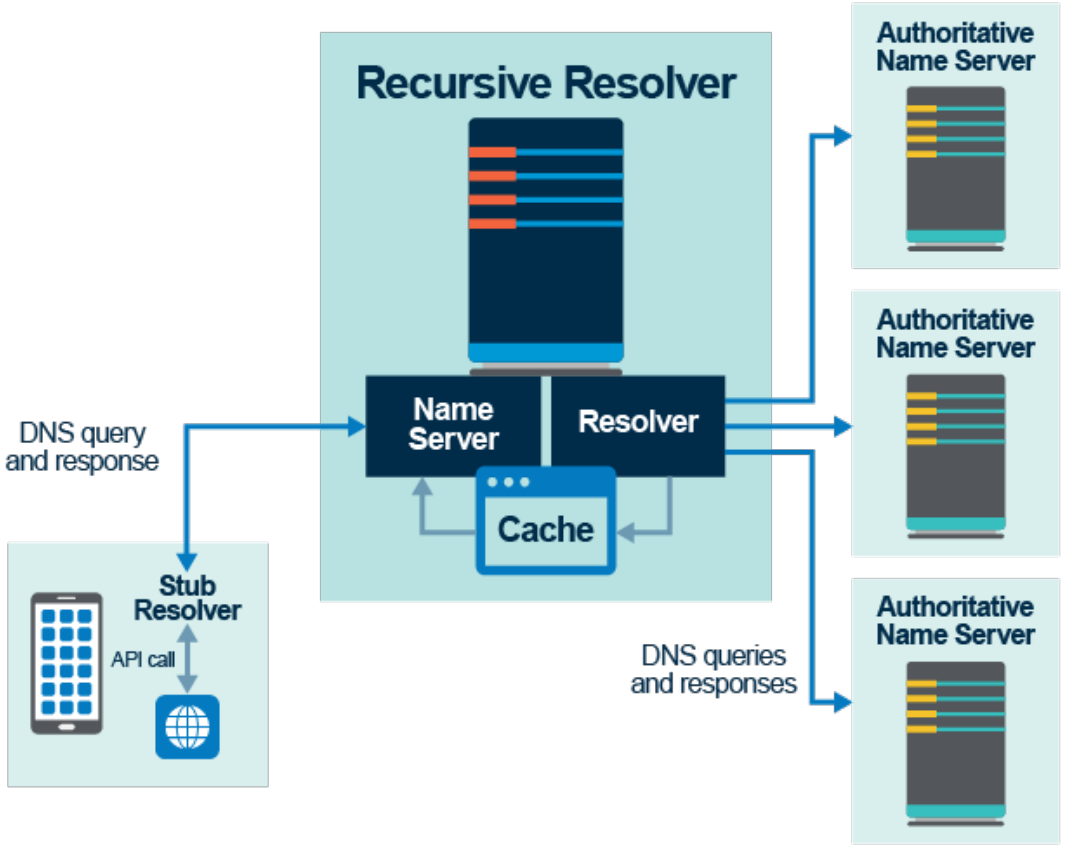
Sistema de registro y auditoría…

- Información para auditoría de seguridad
- Sentido común
- Más sentido común

El Sistema de Nombres de Dominio

DNS

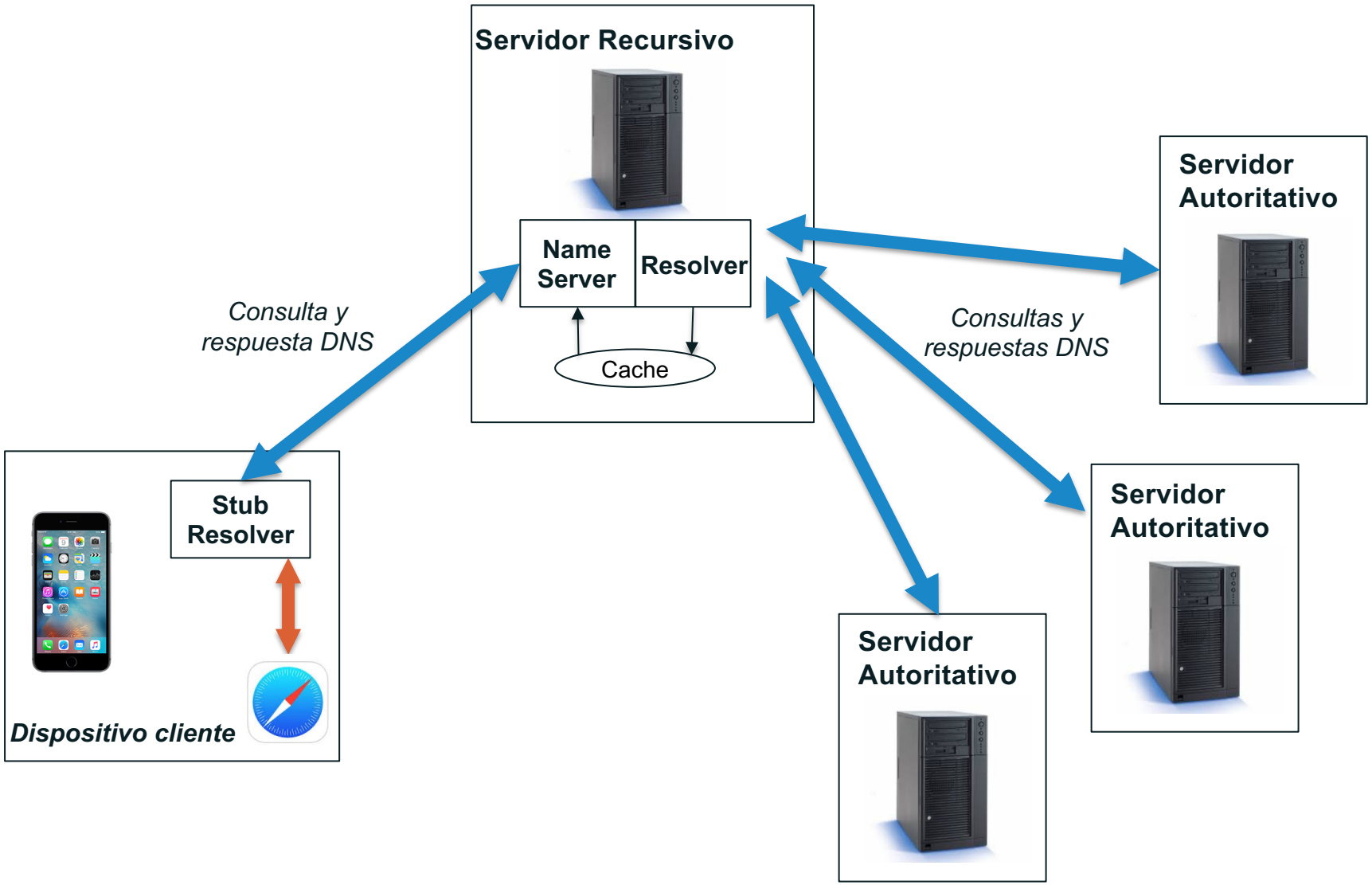
- El espacio de nombres se divide para permitir la **administración distribuida**.
- Las divisiones administrativas se denominan **zonas**.
- Un administrador de cualquier zona puede delegar la administración de un subárbol de su zona, creando así una nueva zona.
- La **delegación** crea zonas.
- **Servidores**
  - Servidores autorizados.
  - Resolvedores (Caching, etc).



El Sistema de Nombres de Dominio (DNS)

- Recordar que el DNS es una base de datos distribuida con el objeto de traducir o asociar nombres a números… para que podamos recordar y usar nombres (nombres de dominio) mientras los dispositivos siguen usando números (direcciones IP) como identificadores..
- ***Resolver*** (o servidores recursivos): envían consultas (son como proveedores de servicio de resolución, encargados de buscarnos los datos, para no tener que buscarlos nosotros mismos en esa base de datos).
- ***Servidores autoritativos***: responden consultas (son las cajas o contenedores que contienen toda la información almacenada en esa base de datos).
- El ***proceso de resolución*** es la implementación de la traducción de una dirección IP a un nombre de dominio, o más general, obtener la respuesta para una consulta específica.

El Sistema de Nombres de Dominio (DNS)



Algunos tipos communes de amenazas

Phishing

La práctica fraudulenta de enviar correos electrónicos que pretenden ser de empresas o servicios de renombre para inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito.

Malware

Software diseñado específicamente para interrumpir, dañar u obtener acceso no autorizado a un sistema informático.

- E.j.: ransomware, key logger, root kit, virus

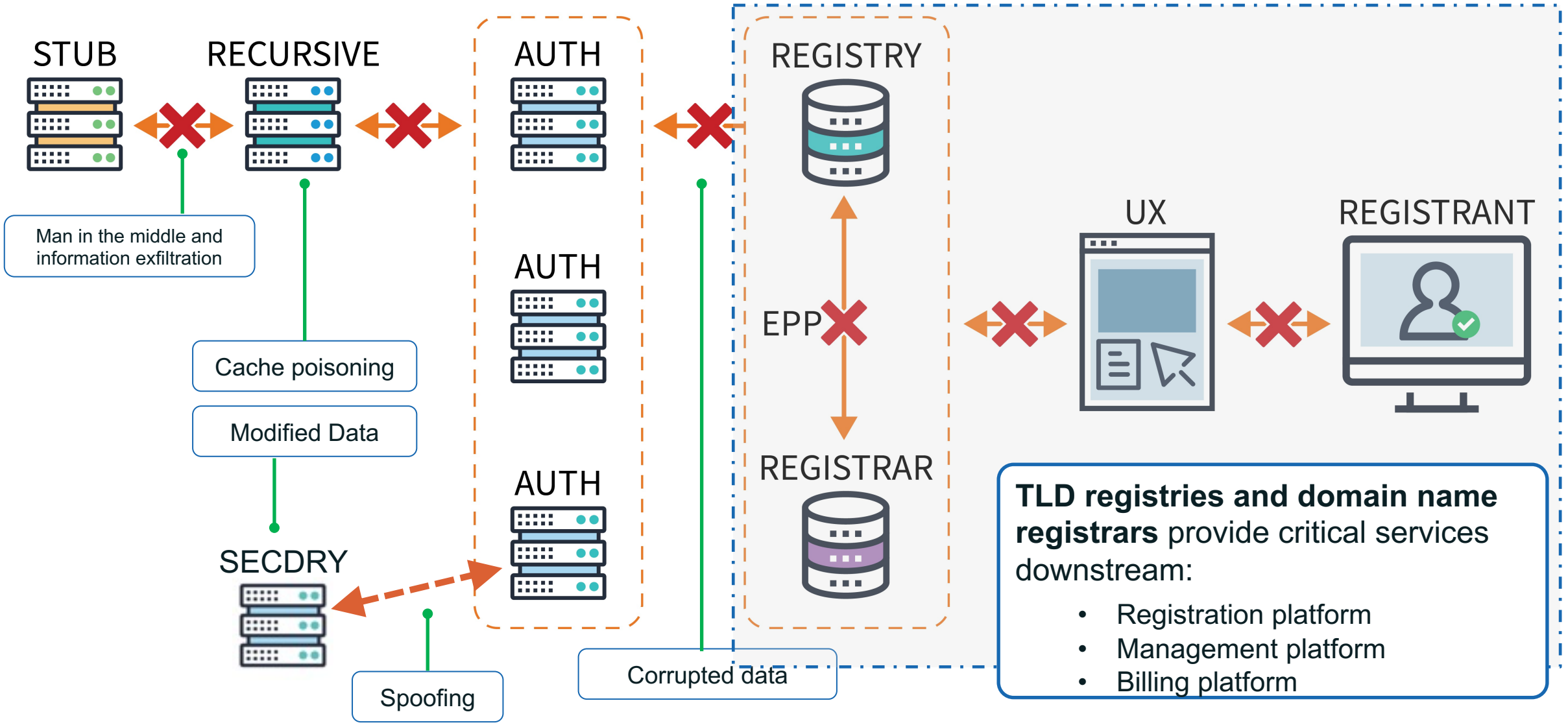
Botnets

Una red de computadoras privadas infectadas con software malicioso y controladas como grupo sin el conocimiento de los propietarios.

Amenazas al (o con) el Sistema de Nombres de Dominio

- Todos usamos el Sistema de Nombres de Dominio (DNS) para resolver nombres (fáciles de recordar) en direcciones de Protocolo de Internet (IP).
- Interrumpe el DNS e interrumpes las transacciones comerciales, los servicios (gubernamentales y no gubernamentales, las redes sociales, educación, salud…
- Explota el DNS y puedes engañar y defraudar a los usuarios.
- Algunos vectores de ataque:
    - Registrar nombres de dominio de forma maliciosa.
    - Secuestro de servicios de registro o resolución de nombres.
    - Alteración, en general, de datos de DNS.
    - Recolección de datos mediante sitios comprometidos.
    - Extracción de datos utilizando el servicio DNS (puerto 53).

Potenciales amenazas y puntos de ataque @ ecosistema DNS



La cruda realidad…

Esto difícilmente termine algún día…

- Los atacantes están motivados para encontrar nuevas vulnerabilidades.
- Los atacantes pueden ser creativos, y en ocasiones, muy sofisticados.
- Los atacantes casi siempre van por delante de "los buenos”.
- Algún nuevo mecanismo de ataque se encuentra siempre a la vuelta de la esquina. . .

Algunos mecanismos de solución o mitigación a considerar, aplicar y/o desplegar

Mantener múltiples servidores autoritativos

Mantener múltiples servidores autoritativos

- Las zonas pueden y deberían (siempre en la medida de lo posible) tener múltiples servidores autoritativos:
  - Proporciona redundancia y resiliencia
  - Distribuye la carga de consultas
- La replicación de zona es parte del protocolo DNS por lo que esta funcionalidad esta prevista en los estándares y la implementan todos los software de servidores DNS.

Utilización de la técnica de Anycast para el DNS

Anycast

Anycast podría definirse como una combinación de direccionamiento IP y esquema de enrutamiento, donde:

- la misma dirección IP se asigna a muchos dispositivos de destino; y
- la decisión de a qué destino llegará el paquete la deciden los mecanismos y métricas de enrutamiento de la red.

Anycast no requiere ninguna configuración especial a nivel de aplicación ni a nivel de cliente. Es un proceso transparente para el cliente.

El objetivo es que los paquetes lleguen al destino Anycast más cercano de acuerdo con las métricas de enrutamiento que la red considere importantes (por ejemplo, la cantidad de saltos).

Anycast para servidores DNS

- Los operadores de servidores raíz suelen emplear **Anycast**, distribuyendo muchas **instancias** de su servidor raíz en todo el mundo.

- Anycast también es comúnmente utilizado por los operadores de resolución recursiva, distribuyendo muchas instancias de sus recursivos en todo el mundo.

- Algunos de los beneficios de Anycast aplicado al DNS:
  - Proporciona redundancia y resiliencia a la infraestructura de DNS global.
  - Distribuye la carga de consultas y respuestas en muchos servidores.
  - Reduce la latencia al permitir más instancias más cerca de más clientes.
  - Proporciona más solidez, lo que ayuda a mitigar eventos como ataques DoS en la infraestructura de DNS.

- La técnica se puede aplicar en autoritativos de cualquier nivel tanto como en recursivos.

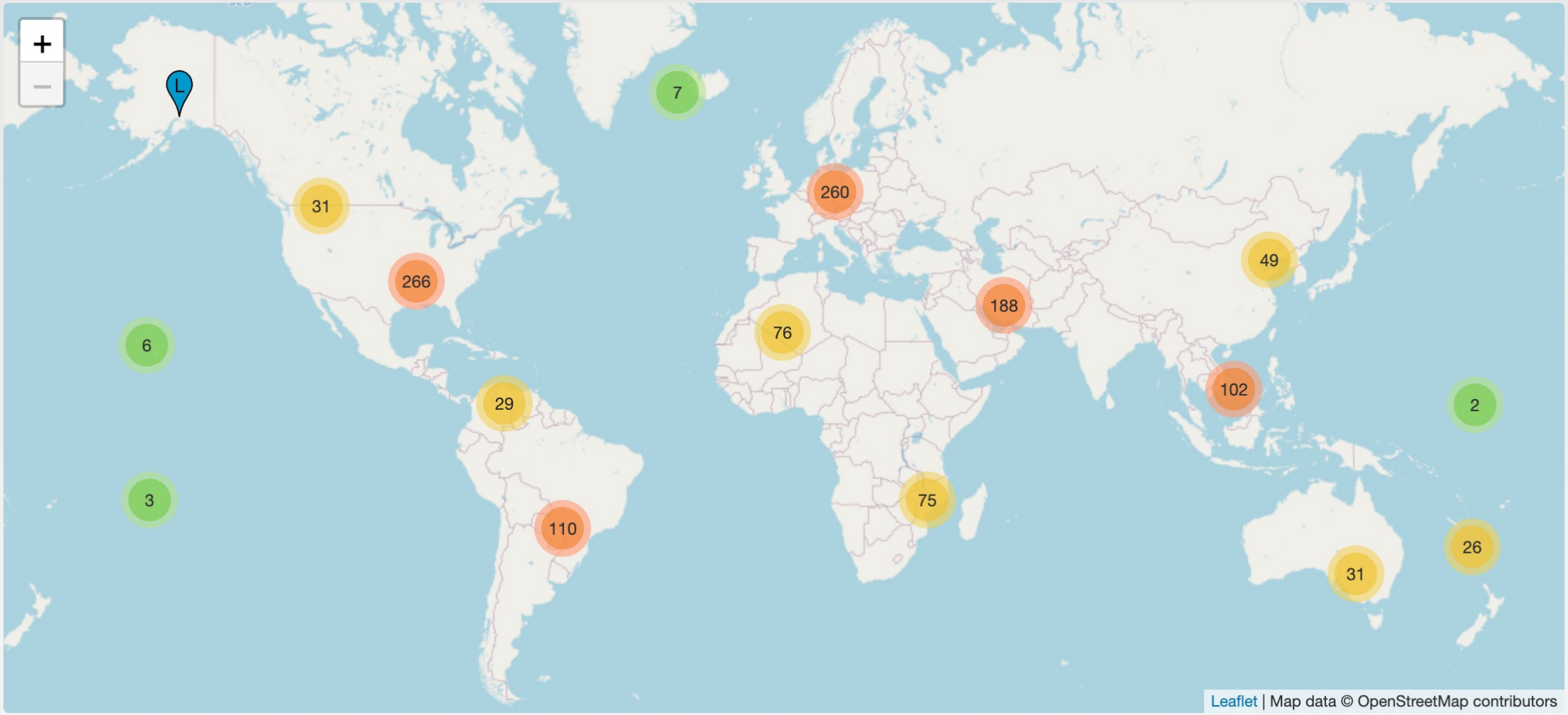
- En caso de aplicarla en servidores Autoritativos, todos deben mantener la misma información con la finalidad de que la respuesta sea la misma sin importar cual de las copias es consultada.

Copias de los servidores Raíz…

The Root Servers Operators

- **A** Verisign
- **B** University of Southern California Information Sciences Institute
- **C** Cogent Communications, Inc.
- **D** University of Maryland
- **E** United States National Aeronautics and Space Administration
  (NASA) Ames Research Center
- **F** Information Systems Consortium (ISC)
- **G** United States Department of Defense (US DoD)
  Defense Information Systems Agency (DISA)
- **H** United States Army (Aberdeen Proving Ground)
- **I** Netnod Internet Exchange i Sverige
- **J** Verisign
- **K** Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- **L** Internet Corporation For Assigned Names and Numbers (ICANN)
- **M** WIDE Project (Widely Integrated Distributed Environment)

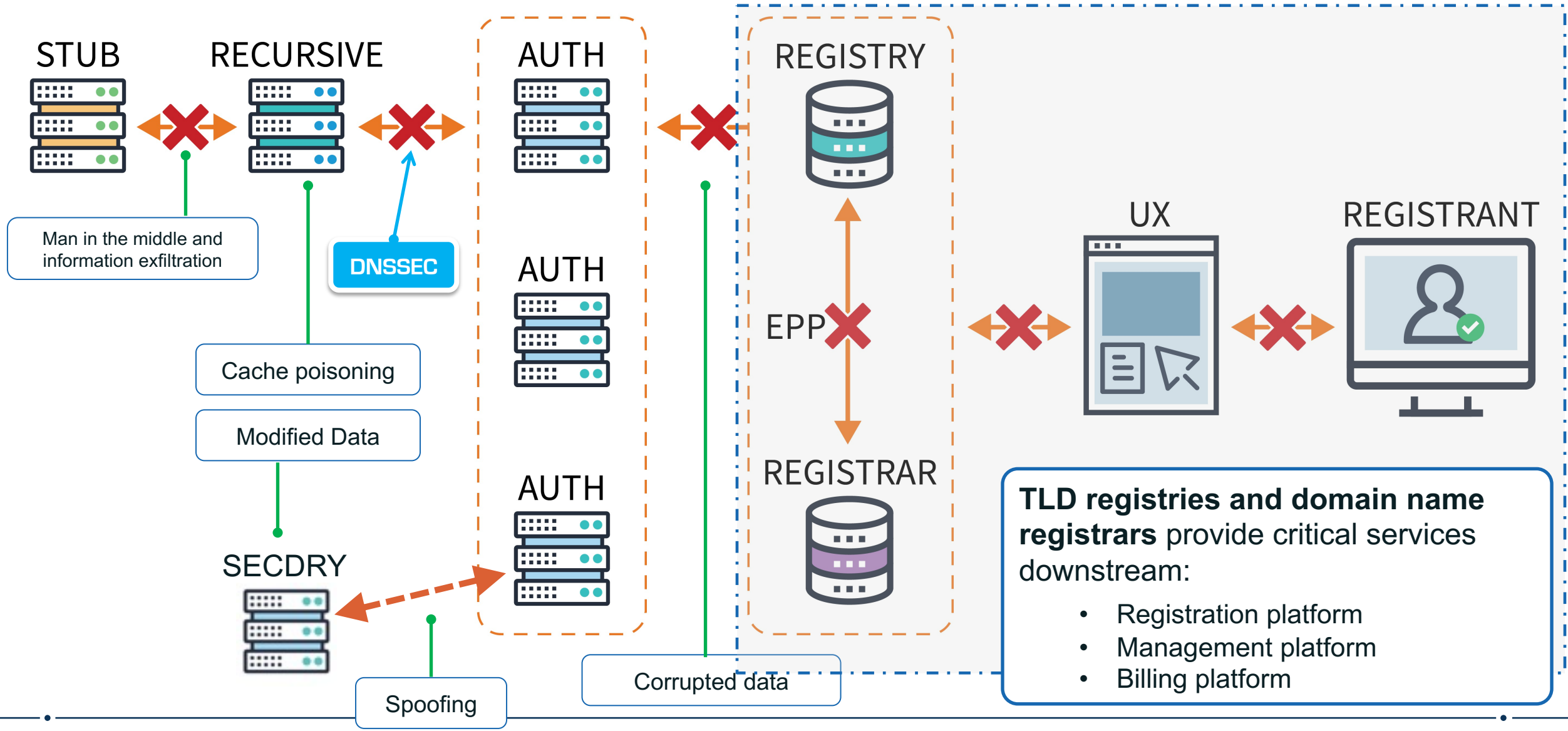
El sitio root-servers.org



As of 04/18/2022 8:33 p.m., the root server system consists of 1533 instances operated by the 12 independent root server operators.

Seguridad: DNSSEC …

Potenciales amenazas y puntos de ataque @ ecosistema DNS



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

DNSSEC: Autenticación de origen e integridad

DNSSEC

Utiliza criptografía de clave pública y firmas digitales para proporcionar:
* Autenticación de origen
* Integridad de los datos

Ofrece protección contra la falsificación de datos de DNS

Evitar ataques de envenenamiento de cache

Proveer confidencialidad en el intercambio de datos de DNS

Evitar ataques de Dos

Beneficios de DNSSEC

Beneficios técnicos

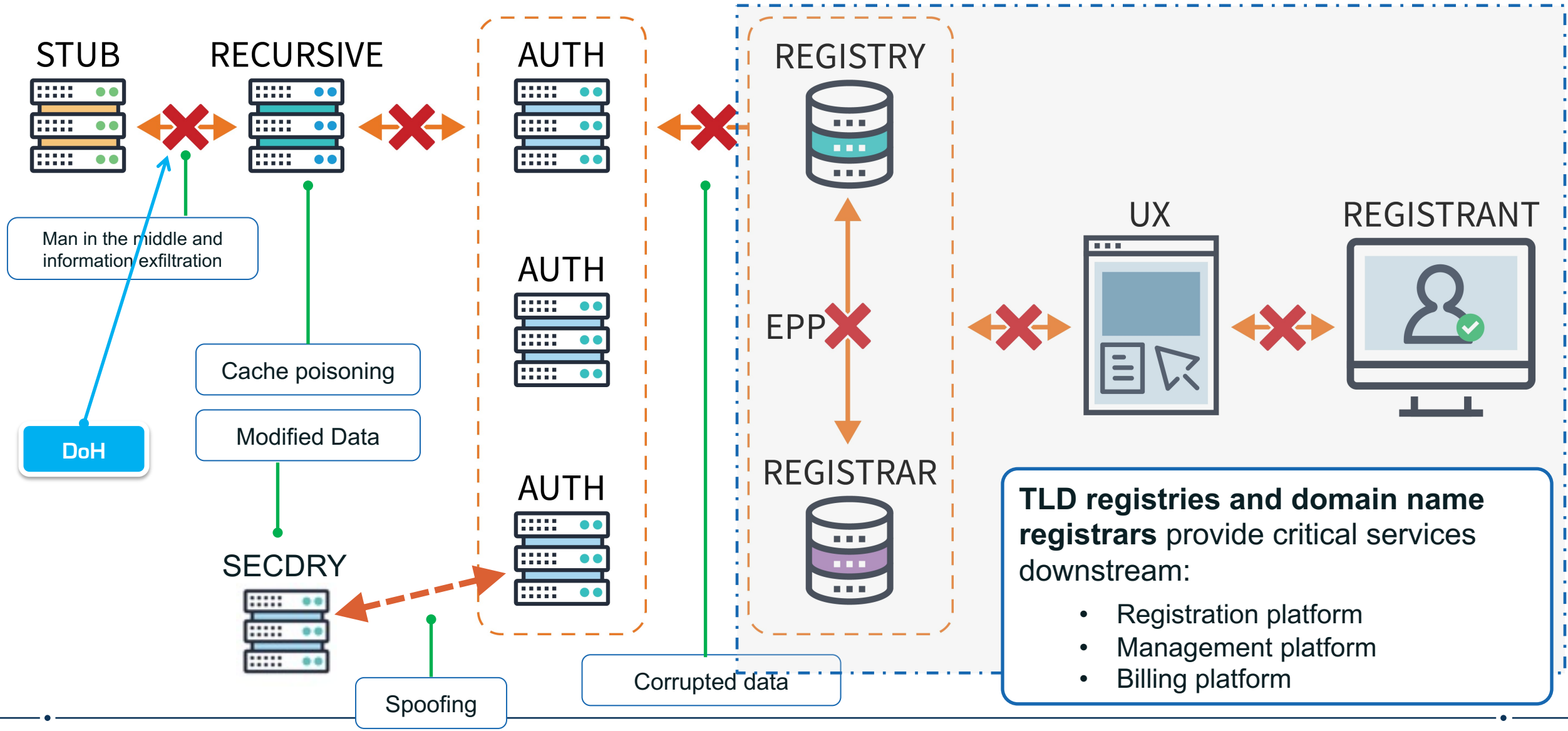
- **Proporcionar autenticación/validación de origen.**
- **Garantizar la integridad y no manipulación de los datos de DNS.**
- **Negación autenticada de existencia de datos DNS (NSEC).**

Impacto en los diferentes miembros del ecosistema

- **Usuario final:** confianza de llegar al sitio web deseado/correcto (complemento de https).
- **Registrante:** mitigación del fraude y mayor protección de marca (reputación del código de país).
- **Registrador:** cumpla con los estándares de la industria y satisfaga las demandas de los registrantes para una mayor seguridad (atraer y retener a los registrantes centrados en la seguridad y la reputación).
- **Registro:** cumpla con las mejores prácticas de la industria y las demandas de los registradores para una mayor seguridad de los dominios.

Privacidad: DoT & DoH …

Potenciales amenazas y puntos de ataque @ ecosistema DNS



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

DoT y DoH… en un slide ☺

La idea principal detrás de DoT y DoH es proporcionar **privacidad** mediante el cifrado de consultas y respuestas DNS entre el equipo terminal y el servidor DNS recursivo elegido.

De esa manera, aumenta la resiliencia contra la interceptación, el bloqueo, la interferencia y/o la manipulación de ese tráfico (principalmente lo mismo que busca cualquier método de encriptación punto a punto).

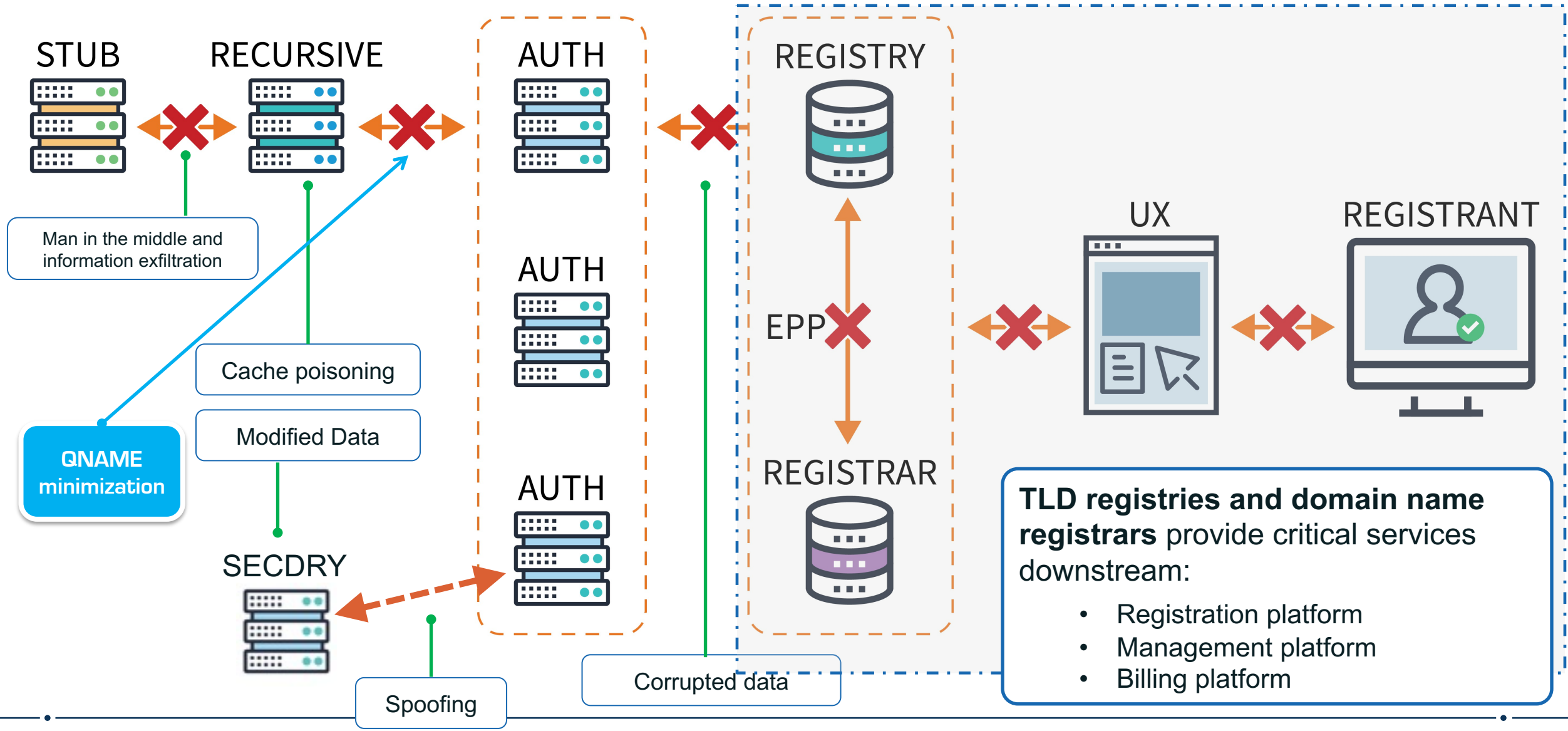
- DoT significa DNS sobre TLS.
- DoH significa DNS sobre HTTPS.

Como casi todos los métodos que involucran temas de privacidad, tanto DoT como DoH (y especialmente DoH) han suscitado algunas discusiones tanto a nivel político como técnico…

… una idea importante que vale la pena considerar es la separación entre los estándares y las implementaciones de lo mismos, que, a menudo conducen a algún debate. … desde una perspectiva técnica, podría considerarse mas conveniente desde el punto de vista de seguridad y resiliencia del sistema global de DNS, el habilitar estos mecanismos en sus propios recursivos en lugar de reenviar todas las consultas a uno público (y de esa forma, fomentar la descentralización de la resolución de DNS).

Privacidad: QNAME minimization …

Potenciales amenazas y puntos de ataque @ ecosistema DNS



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

QNAME minimization… en un slide ☺

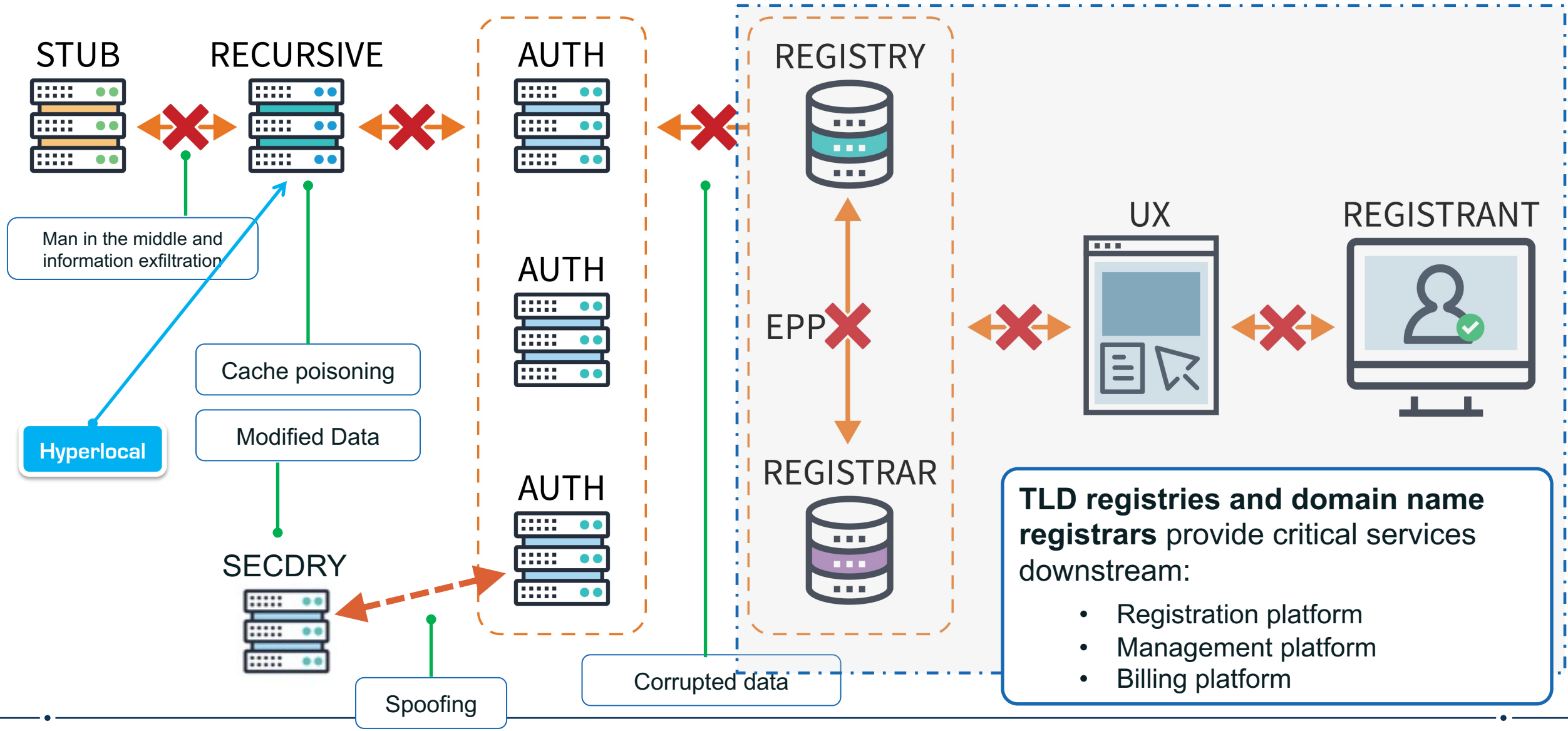
La minimización de QNAME sigue el principio explicado en la Sección 6.1 de [RFC6973]: cuantos menos datos envíe, menos problemas de privacidad tendrá.

La minimización del nombre de consulta de DNS (QNAME) se define en el RFC 7816 para mejorar la privacidad del usuario final en el proceso de resolución de DNS.

Cambia las consultas DNS “estándar” del servidor recursivo para incluir solo tantos detalles en cada consulta como sea necesario para ese paso en el proceso de resolución. El RFC 7816 de IETF lo describe como una técnica "en la que el sistema de resolución de DNS ya no envía el QNAME original completo al servidor de nombres autoritativo".

Acelerando la resolución & mejorando la privacidad: Hyperlocal …

Potenciales amenazas y puntos de ataque @ ecosistema DNS



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

Hyperlocal

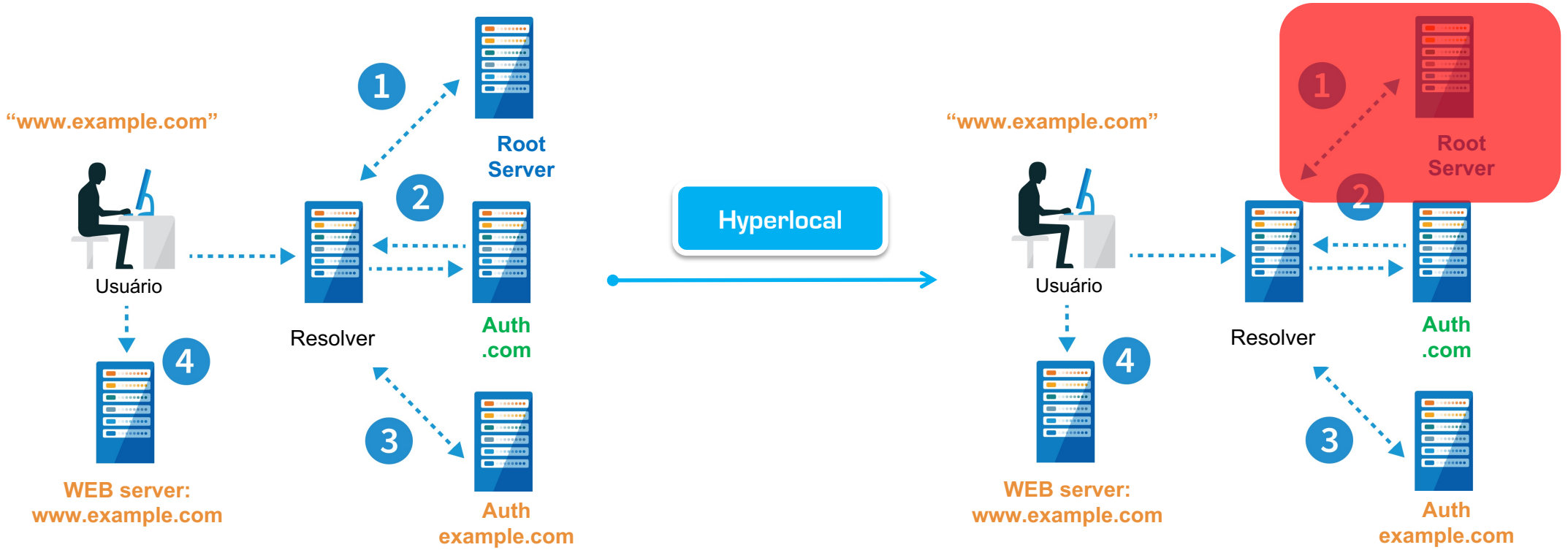
¿Qué es esto?

- Se trata de mantener una copia local de la Raíz del DNS en la misma máquina que ejecuta resoluciones recursivas (servidor recursivo).
- Incluido en ese objetivo está el garantizar que siempre se tenga acceso a los datos de la zona raíz.
- Steve Crocker nombró a esta técnica Hiperlocal.

Estandarizado en el RFC 8806, ”Corriendo un Servidor Raíz localmente en un Recursivo"

- El servidor raíz debe ejecutarse en la misma máquina que el servidor recursivo.
- Solo puede responder consultas de la máquina local y de ninguna otra máquina.
- Se recomienda mantener y aplicar el mecanismo de resolución estándar en caso de error o cuando la copia local no está disponible o está desactualizada.

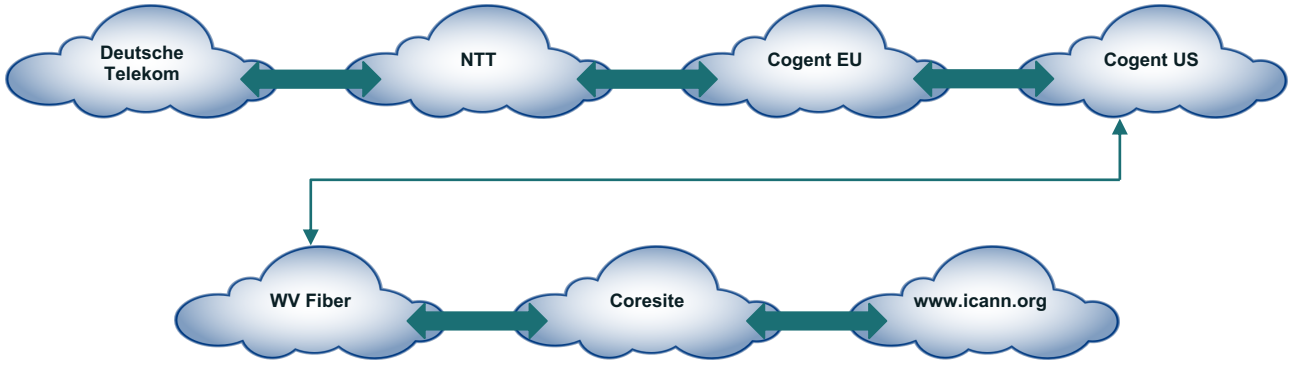
DNS & Hyperlocal



Algunas otras buenas prácticas a considerar …

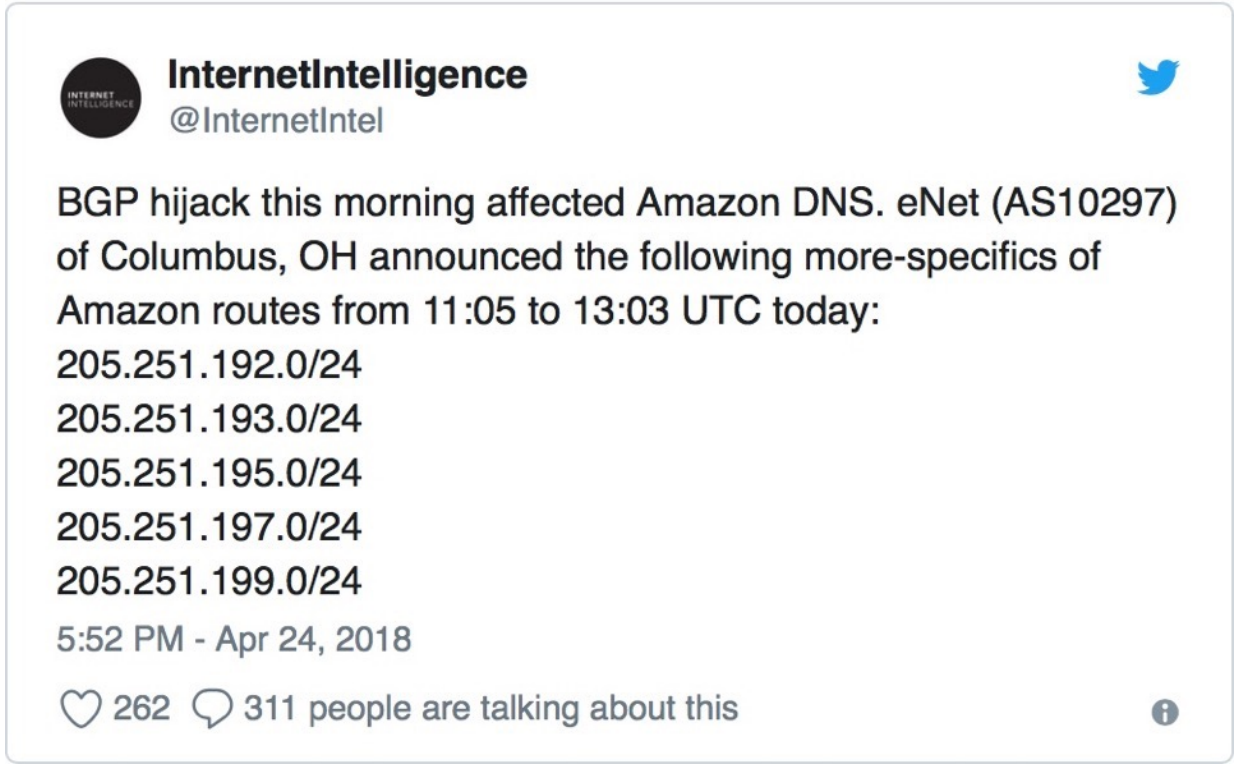
Enrutamiento global en Internet

- Asegurar la infraestructura de DNS con cosas como DNSSEC es, hoy día, muy necesario.
- La infraestructura de enrutamiento también es parte del ecosistema: los paquetes deben enrutarse desde el origen al destino, y es posible manipular esos paquetes para abusar de la infraestructura de DNS y de Internet en general.



RPKI

- Routing Public Key Infrastructure (RPKI)
- Una serie de certificados y autoridades de certificación para proteger la información del origen de la ruta.



MANRS

MANRS es una iniciativa creada por la Internet Society (ISOC) cuyo objetivo es asegurar el enrutamiento global de Internet. Sus principales participantes son proveedores de servicios de Internet, proveedores de nube, puntos de intercambio de Internet y redes de distribución de contenido.

https://www.manrs.org/

KINDNS

KINDNS es una iniciativa recientemente creada por ICANN. Corresponde a las siglas de **Knowledge-Sharing and Instantiating Norms for DNS and Naming Security** y es un programa para desarrollar un marco que se centra en las mejores prácticas operativas o instancias concretas de las mejores prácticas de seguridad del DNS.

Knowledge-sharing and
Instantiating
Norms for
DNS and
Naming
Security

https://community.icann.org/display/KINDNS

Algunas sugerencias adicionales

Seguir y mantener un conjunto de medidas de ciberseguridad que todas las redes deberían implementar para fortalecer la infraestructura de DNS local contra ataques.

Los pasos incluyen la implementación de sólidas prácticas de ciberseguridad para:

- Autorización
- Autenticación
- Cifrado
- Actualización
- Monitoreo y sistemas IDS
- Seguridad del correo electrónico (considerar también aspectos de Aceptación Universal para DNS)

Interactúa con ICANN: gracias y preguntas

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann