DNS

Amenazas - Prevención - Mitigación

Nicolás Antoniello

LAC DNS FORUM – Montevideo, Uruguay
3 de Setiembre, 2025

ICANN

Menú de hoy …

- ❑ DNS como objetivo de una amenaza
- ❑ DNS como vector de ataque
- ❑ Ataques más específicos
- ❑ Registro de nombres de dominio maliciosos
- ❑ Algunos mecanismos de solución o mitigación a considerar, aplicar y/o desplegar
- ❑ Algunas otras buenas prácticas a considerar

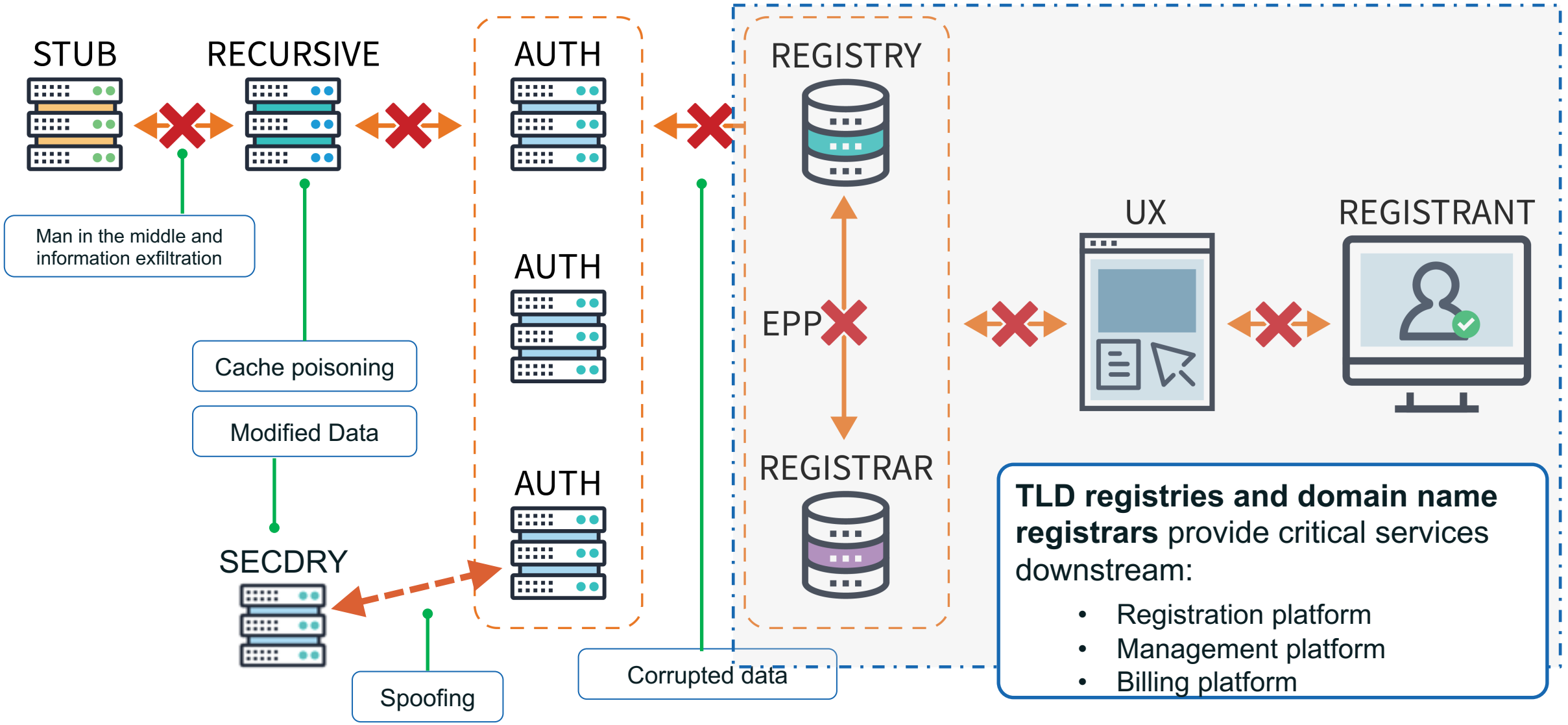
Un baño de realidad . . .

A los criminales les gusta ocultarse:

- Los atacantes están motivados a descubrir nuevas vulnerabilidades
- Los ataques pueden ser muy creativos, innovadores y sofisticados
- Algunos atacantes disponen de muchísimos recursos
- Los atacantes casi siempre están un paso adelante
- Redirección: los sitios web pirateados utilizan acortadores de URL
- Recursión: las URLs acortadas se vuelven a acortar
- URLs de un solo uso
- Contenido específico de un país o script; contenido no visible
- Los delincuentes utilizan ACL para impedir que los investigadores vean los sitios
- Los comportamientos delictivos pueden emular comportamientos legítimos
  - EJEMPLO: Fast Flux frente a redes adaptativas (p. ej., CDN)

DNS como objetivo de una amenaza

Potenciales amenazas y puntos de ataque @ ecosistema DNS



DNS como vector de ataque

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.

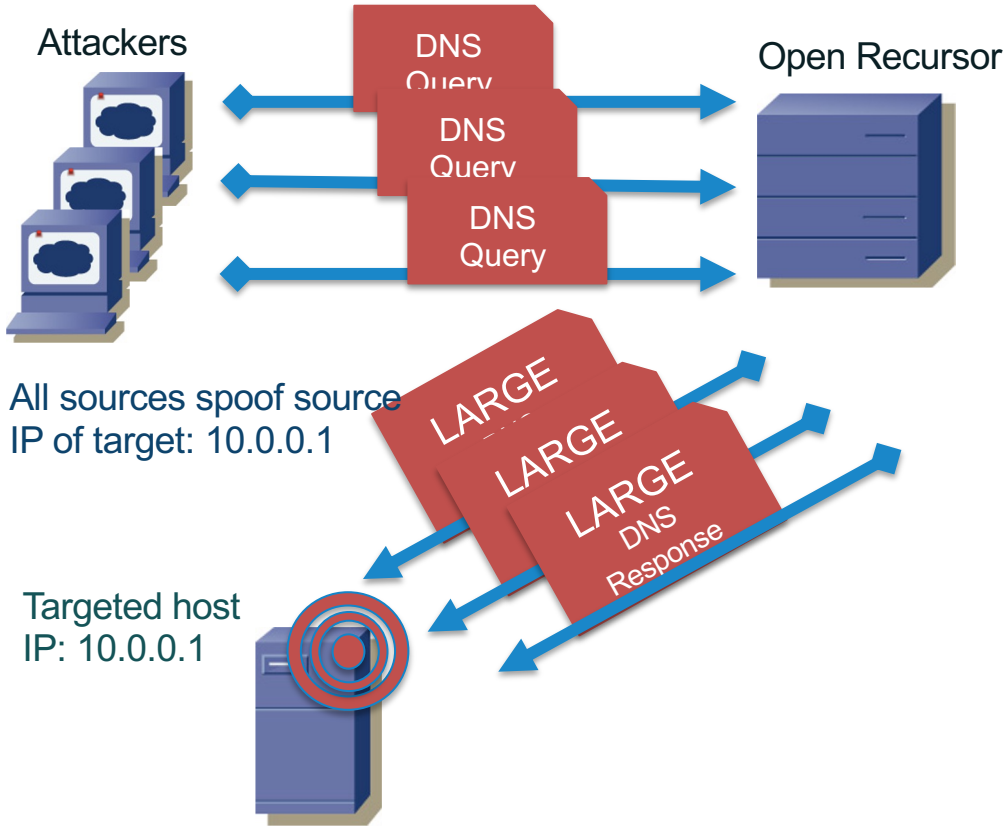
- E.j.: ransomware, key logger, root kit, virus

Botnets

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

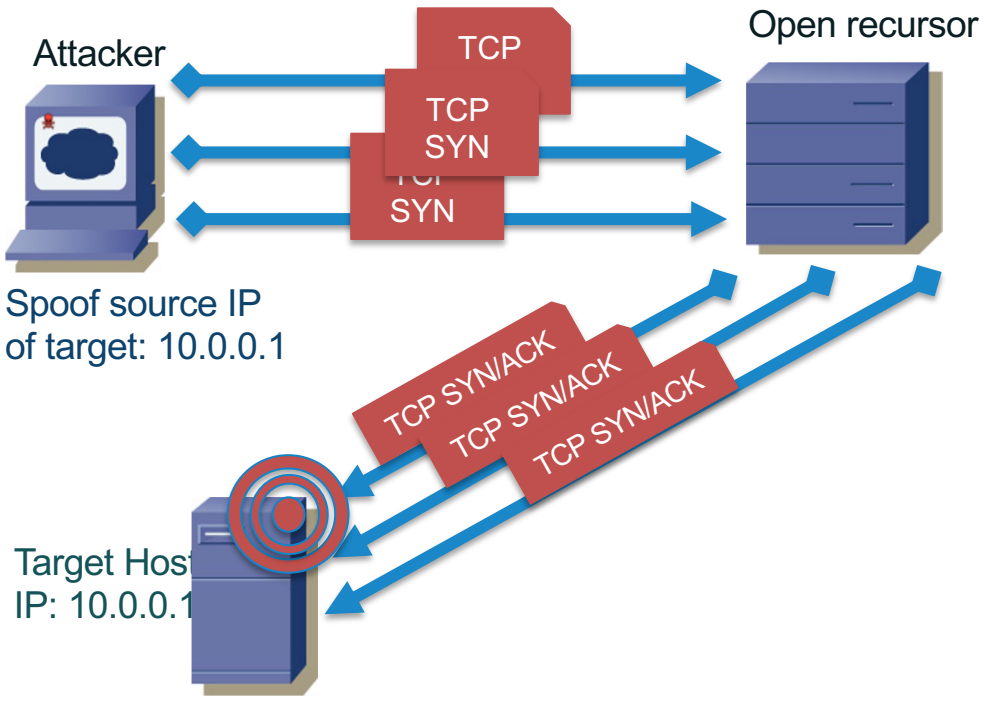
Ataque distribuido de reflexión y amplificación

- Lanzar un ataque de reflexión y amplificación desde miles de orígenes
- Reflejar a través de un servidor DNS recursivo abierto
- Entregar miles de respuestas grandes al objetivo



Consumo de recursos

- El atacante envía una avalancha de mensajes DNS a través de TCP desde la dirección IP falsificada del objetivo
- El servidor de nombres asigna recursos para conexiones TCP hasta que se agotan los recursos
- La resolución de nombres está degradada o interrumpida



Envenenamiento de Cache

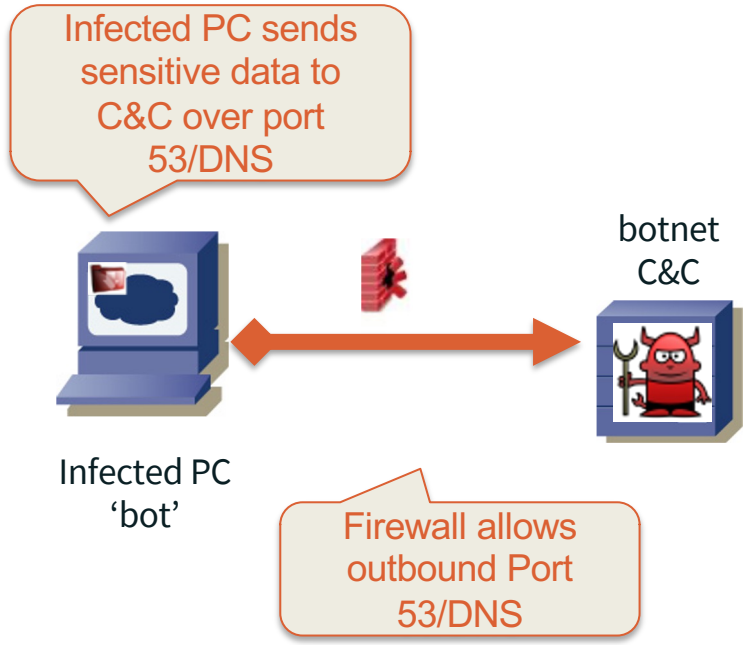
- Un usuario es víctima de spam/phishing y dirige el navegador del objetivo a un sitio malicioso:
  - http://LoseWeightFast.biz
- El servidor de nombres responde a la solicitud de BajaDePesoRapidamente.biz con datos DNS maliciosos para un sitio web legítimo (por ejemplo, Amazon.com)
- Estos datos maliciosos se almacenan en caché en los recursivos.
- Durante la vida útil del caché, cada vez que el usuario intenta ir a Amazon.com, termina en un sitio muy malo en el que no quiere estar. Y pasan cosas malas...

Cambiar en secreto el servidor DNS recursivo de un usuario

- Un usuario está configurado para utilizar los solucionadores de DNS recursivos del proveedor de servicios. O quizás el usuario configura manualmente el dispositivo para usar el DNS público de Google en 8.8.8.8 (por ejemplo).
- El malware (p. ej., DNSChanger) ataca el dispositivo del usuario y reescribe silenciosamente la opción de resolución recursiva para que sea un servidor recursivo bajo el control del atacante.
- El atacante redirige todas las consultas de DNS a sitios realmente malos donde suceden cosas malas.

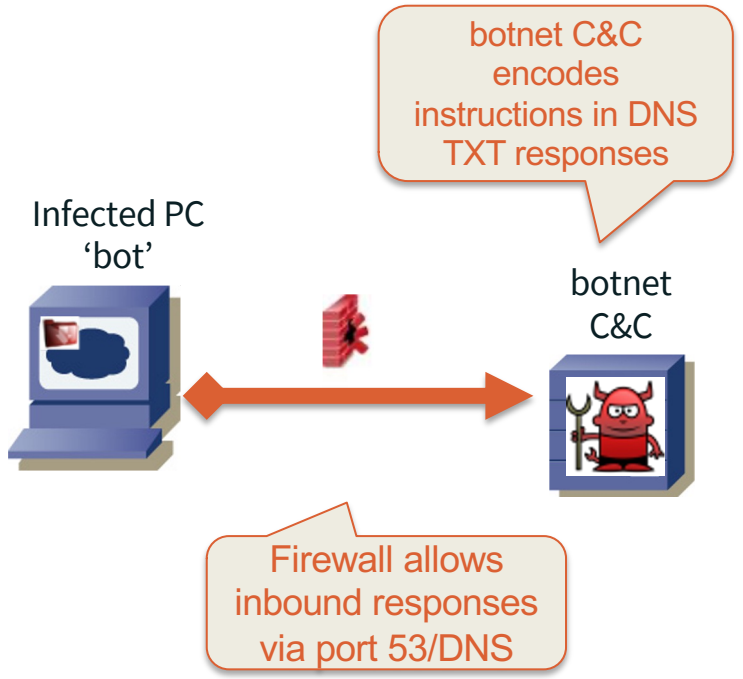
DNS como canal de exfiltración encubierto

- Mensajes DNS manipulados para reenviar datos confidenciales desde la PC infectada a través del firewall al comando y control de botnet (C&C).
- Prueba de concepto: exfiltrar los resultados de los ataques de inyección SQL



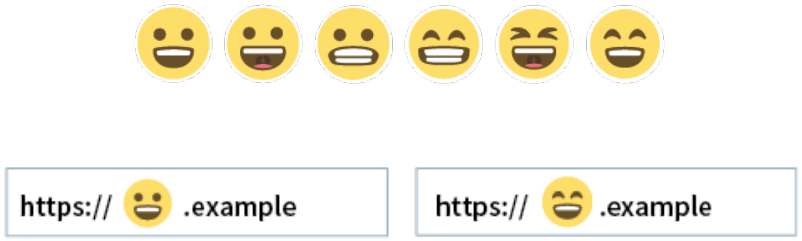
DNS como un canal de malware encubierto

- El malware en la PC infectada realiza búsquedas de registros DNS tipo TXT en el DNS controlado por el comando y control de la botnet (C&C).
- Las respuestas TXT contienen instrucciones para el bot.
- Algunos ejemplos:
  - Feederbot
  - Morto



Emojis en nombres de dominio

Divertido, pero puede ser peligroso



Users could easily confuse the "Grinning face" emoji (left) and "Grinning face with smiling eyes" emoji (right).

Los emojis pueden ser demasiado similares visualmente para distinguirlos, especialmente cuando se muestran en fuentes más pequeñas o en diferentes aplicaciones.

"Dizzy face" emoji (Unicode: 1F635) as displayed by:

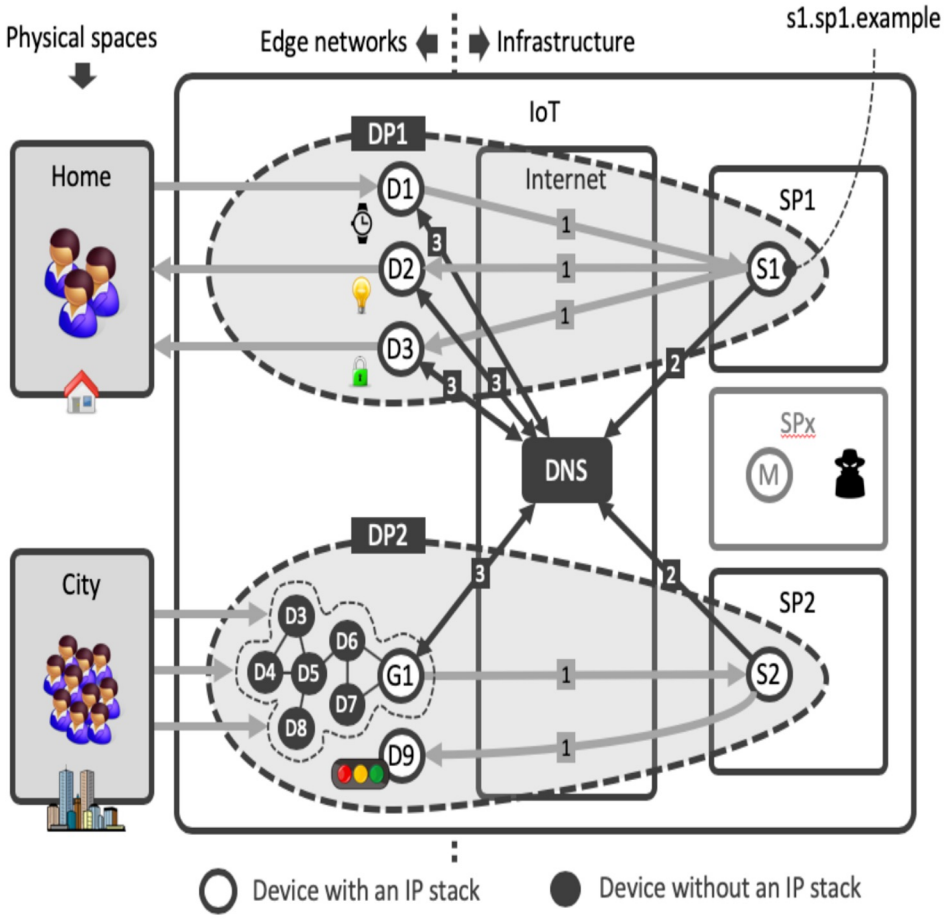
Los emojis no se muestran de manera uniforme en todas las plataformas porque actualmente no existe un estándar que especifique cómo deben verse.

Users could easily confuse the "Detective-medium light skin" emoji (left) with the"Detective-medium skin" emoji (right).

Algunos emoji permiten a los usuarios aplicar uno de los cinco modificadores de tono de piel. Estos pueden hacer que los emojis sean difíciles de distinguir y están sujetos a interpretación.

IoT & DNS

- El DNS (al igual que muchos sistemas) es vulnerable a diversos vectores de ataque diferentes
- Si escalamos Internet agregando 50 mil millones de dispositivos IoT, el área de amenazas tanto para el DNS como para Internet en general aumenta exponencialmente.
- IoT puede representar un riesgo significativo para la seguridad, la estabilidad y la flexibilidad de Internet si cometemos los mismos errores que cometimos antes de IoT



Ataques más específicos …

DDoS

Ataque Distribuido de Denegación de Servicio

Posibles caminos para mitigar:

- Proporcionar respuestas de tamaño mínimo a consultas DNS que tienen QTYPE=ANY (RFC 8482)
- Rate Limit
- Utilización de Cookies de DNS
- Si se implementa DNSSEC, utilizar Agresive NSEC
- Utilizar un proveedor DNS que utilice la técnica de ANYCAST (o mejor aún, más de un proveedor que utilice ANYCAST)
- Separar DNS para la gestión de infraestructura (NOC) del DNS público a fin de no perder el control del la misma

ICANN

Lame Delegations

Registros de delegación que apuntan a servidores DNS inexistentes

Posibles caminos para mitigar:

- Mantener actualizados los registros de delegación

ICANN

Dangling Records

Registros DNS tipo A, AAAA o CNAME que apuntan a servidores o servicios inexistentes

Posibles caminos para mitigar:

- Mantener actualizados los registros DNS (sobre todo cuando damos de baja por ejemplo un servidor en un servicio de nube o dejamos de utilizar un registro CNAME).

ICANN

Toma de control de servidor DNS

Un atacante logra inyectar registros de delegación (NS) maliciosos mediante el acceso a la información de registro

Este tipo de acción es prácticamente indetectable por el cliente DNS ya que los atacantes suelen re-dirigir las consultas al verdadero servidor DNS, pero todas las consultas pasan por ellos.

Posibles caminos para mitigar:

- Asegurar y monitorizar los servicios de registros y registradores.

ICANN

Fast Flux

En este tipo de ataque, un actor malicioso va cambiando rápidamente los registros de delegación (NS) y/o los registros A, AAAA, CNAME, etc., a fin de evitar los sistemas de detección y mitigación.

Posibles caminos para mitigar:

- Este tipo de ataque es muy difícil de mitigar ya que por lo general los mismos son de muy corta duración y con un objetivo bien definido.
- Una forma de intentar prevenirlo es mediante mecanismos de valoración y pseudo-detección de registro de dominios con fines maliciosos… pero nuevamente, en términos generales en un tipo de ataque muy difícil de mitigar una vez que comienza.

ICANN

Registro de nombres de dominio maliciosos

¿Cómo reconocer un dominio malicioso?

No siempre es fácil saberlo, pero hay algunos indicadores fiables:

- Valores sospechosos en los datos de la zona DNS (p. ej., TTL)
- Suplantación o uso confuso de una marca
- Punto de control de malware o DGA conocido
- Alojado en servidores de nombres sospechosos (notorios)
- Alta frecuencia/volumen de errores de nombre
- Ubicación de alojamiento sospechosa (notoria)
- Operador de servicio sospechoso (notorio)
- El contenido del sitio base es inexistente o incorrecto
- El contenido enlazado es sospechoso o incorrecto
- Encabezados, remitente o contenido de correo sospechosos
- En algunos casos la metodología de pago

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

Monitoreo

El monitoreo es esencial y se debe monitorizar no solamente parámetros generales sino algunos atributos propios del servicio DNS que estemos prestando

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.
- Se puede hacer de varias formas, por ejemplo manteniendo varios registros de delegación (NS) en el caso de servidores Autoritativos o mediante el uso de ANYCAST (aplica también a servidores Recursivos).

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 utilizadas (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.

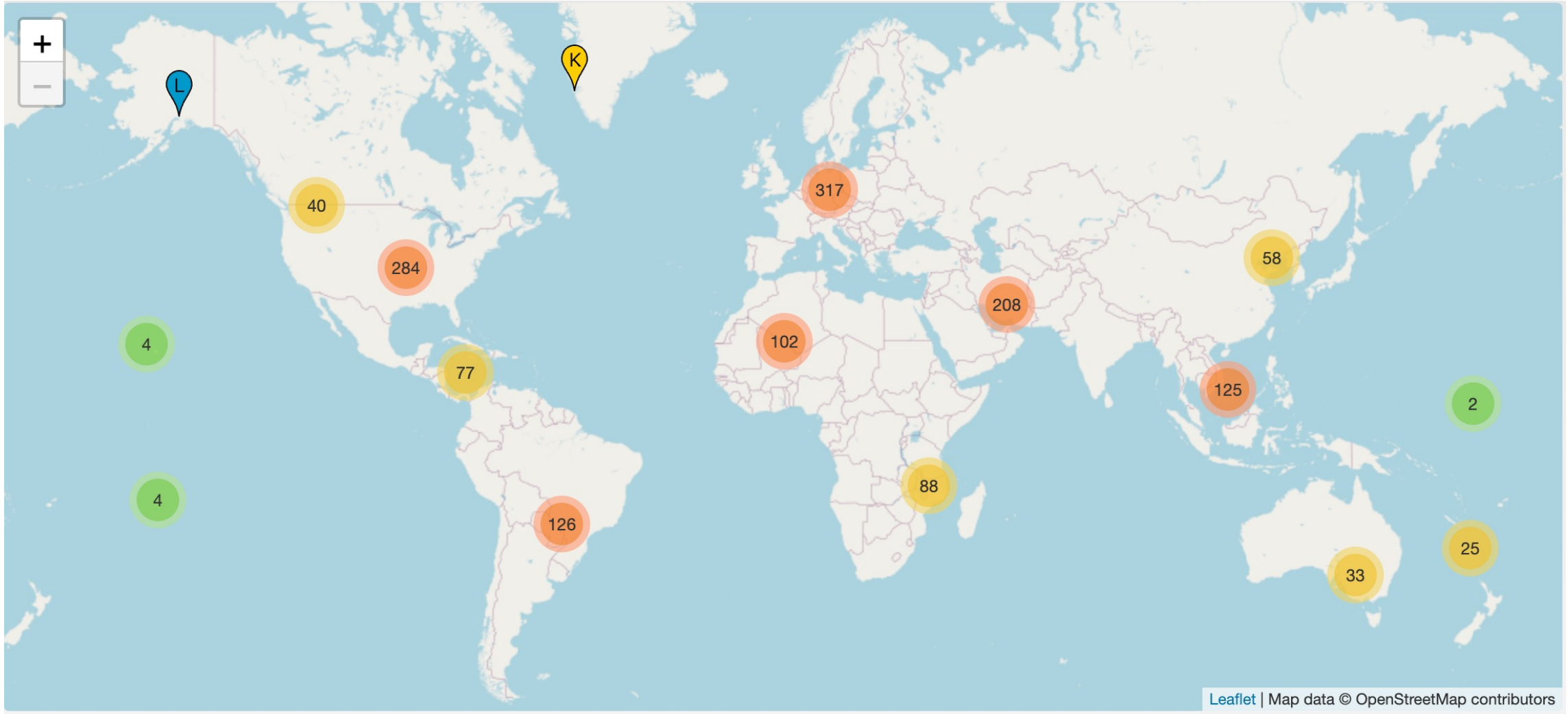
- En caso de aplicarla en servidores Autoritativos, todos deben mantener la misma información con la finalidad de que la respuesta sea la misma sin importar cual de las copias es consultada.

Copias de los servidores Raíz…

Operadores de servidores Raíz

- **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)

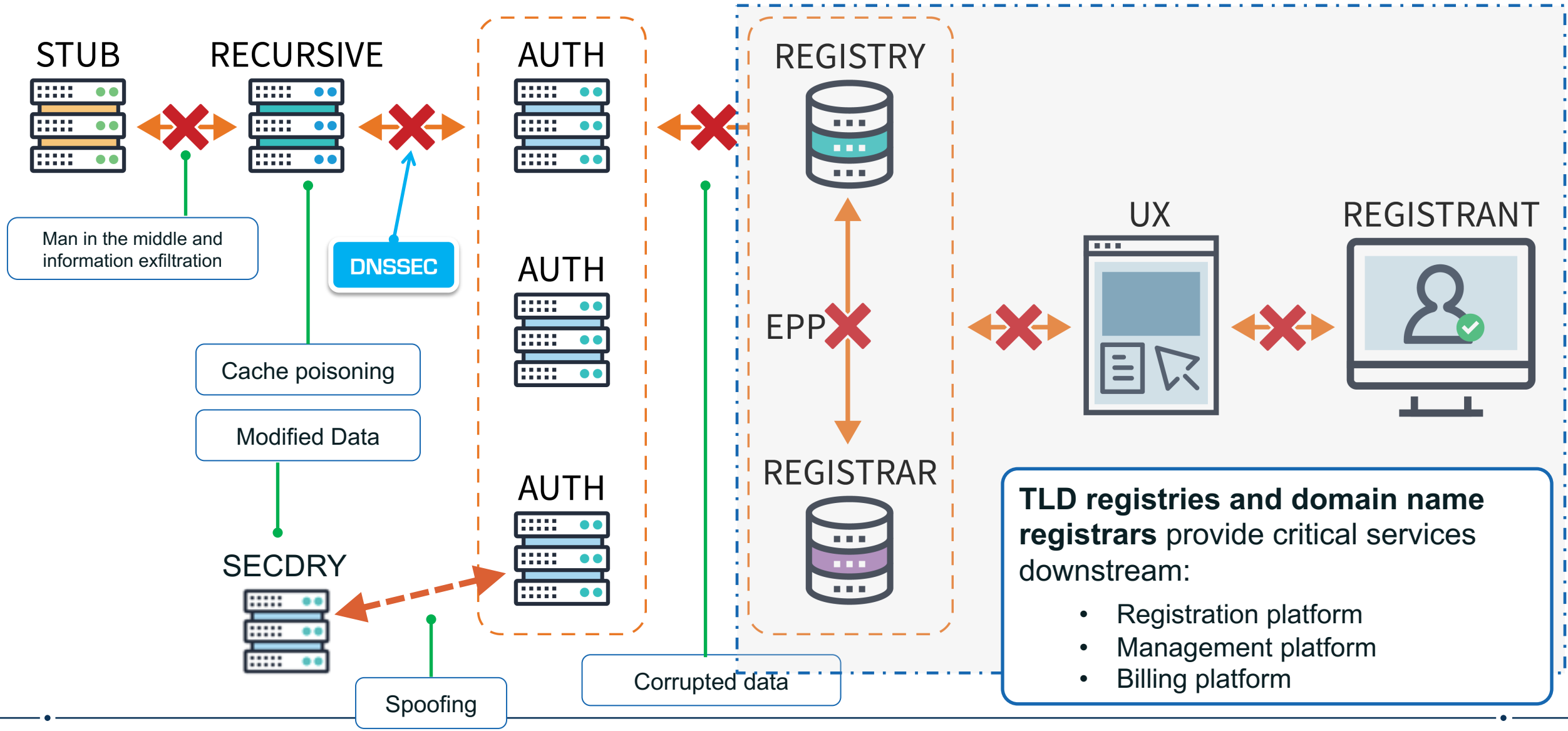
El sitio root-servers.org



As of 2023-06-05T19:21:48Z, the root server system consists of 1707 instances operated by the 12 independent root server operators.

Seguridad: DNSSEC …

Potenciales amenazas y puntos de ataque @ ecosistema DNS



DNSSEC: Autenticación de origen e integridad

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.

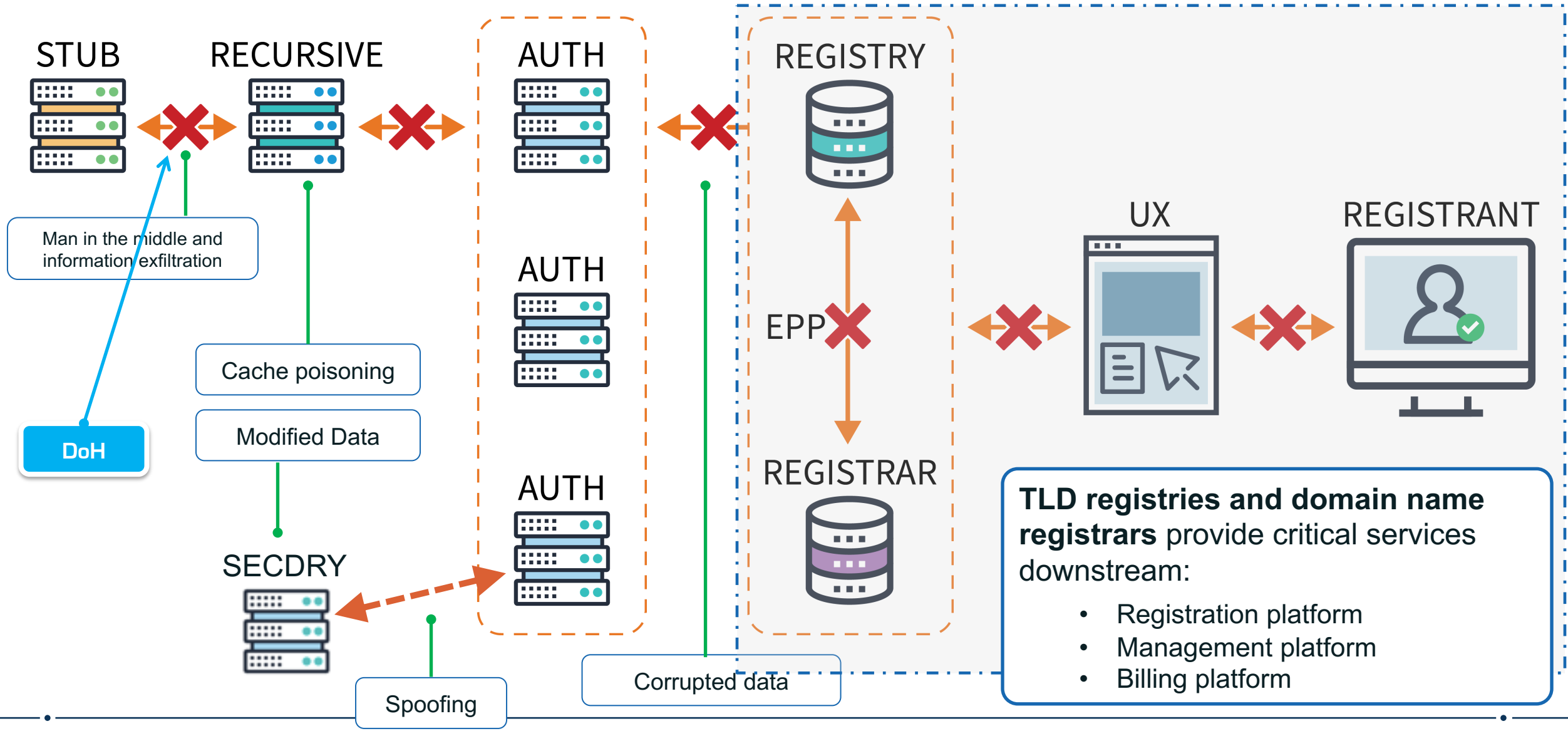
No mantener servidores Recursivos abiertos

A excepción de la prestación específica del servicio de recursivo público, un proveedor de servicios genérico que dispone de un servidor recursivo DNS para sus clientes debe siempre vigilar que el mismo sea únicamente accesible por sus clientes (en otras palabras evitar siempre mantener un servidor recursivo abierto a todo el mundo).

ICANN

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).

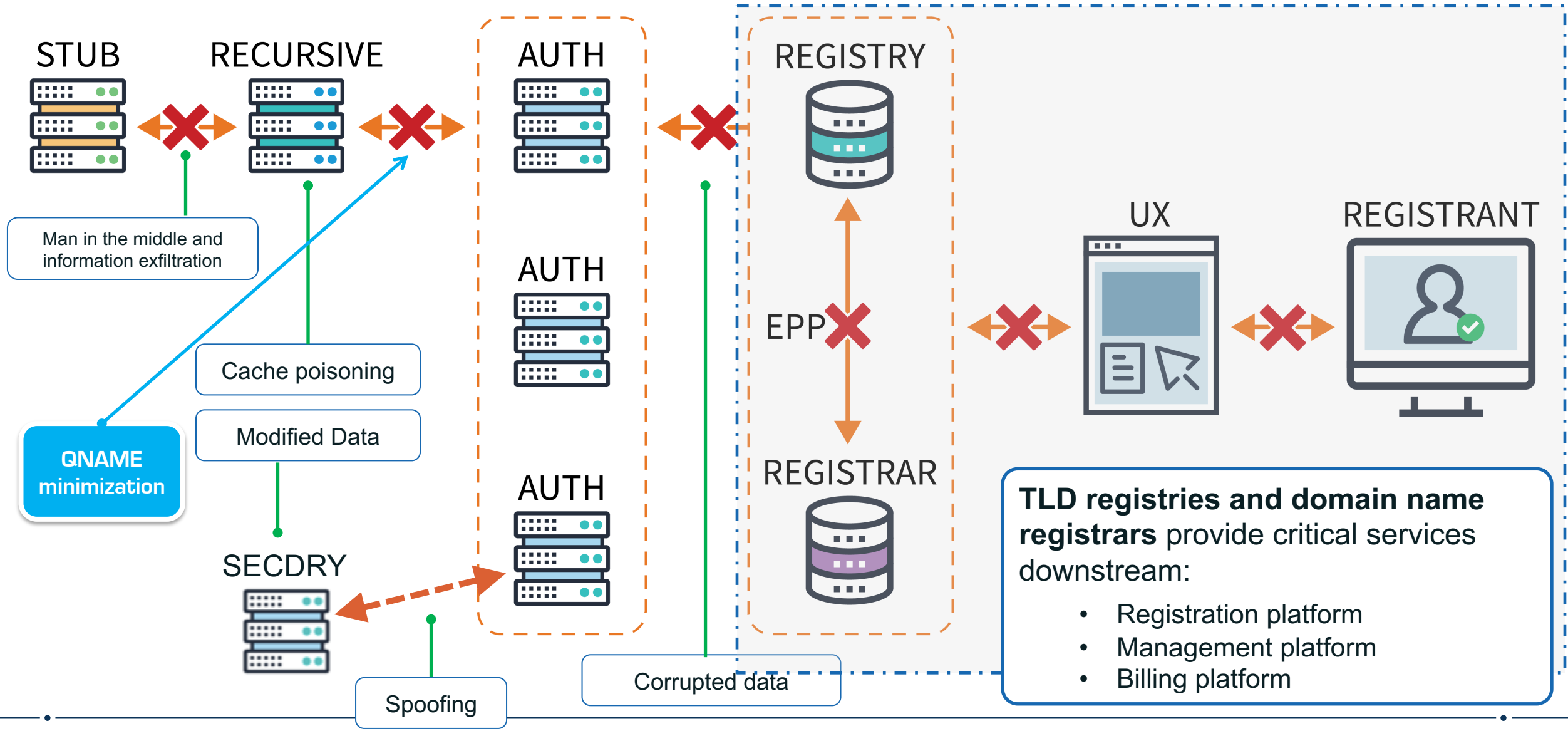
- DoT significa DNS sobre TLS.
- DoH significa DNS sobre HTTPS.

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 ☺

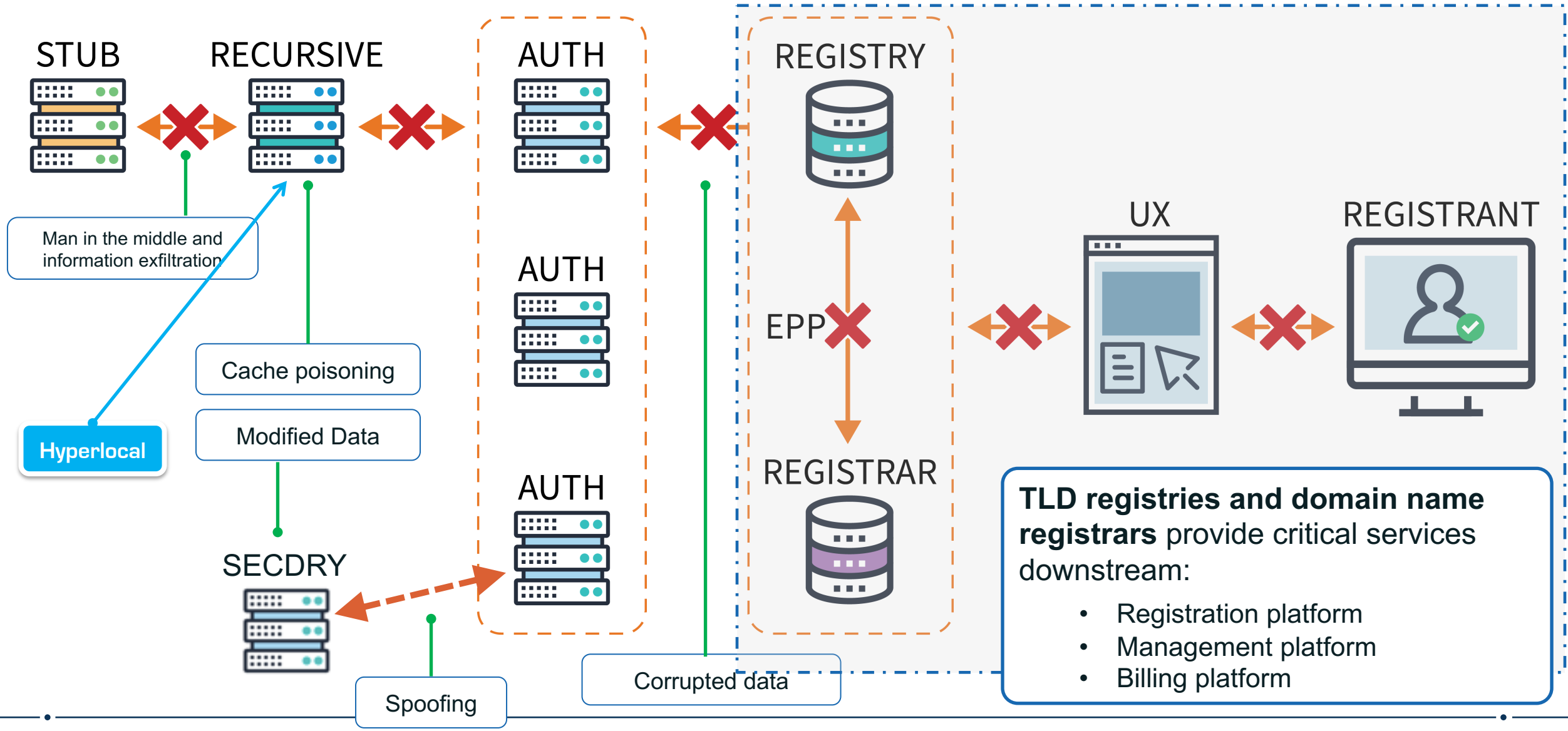
La minimización de QNAME sigue el principio explicado en la Sección 6.1 de [RFC6973]: cuantos menos datos envíe, menos problemas de privacidad tendrá.

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

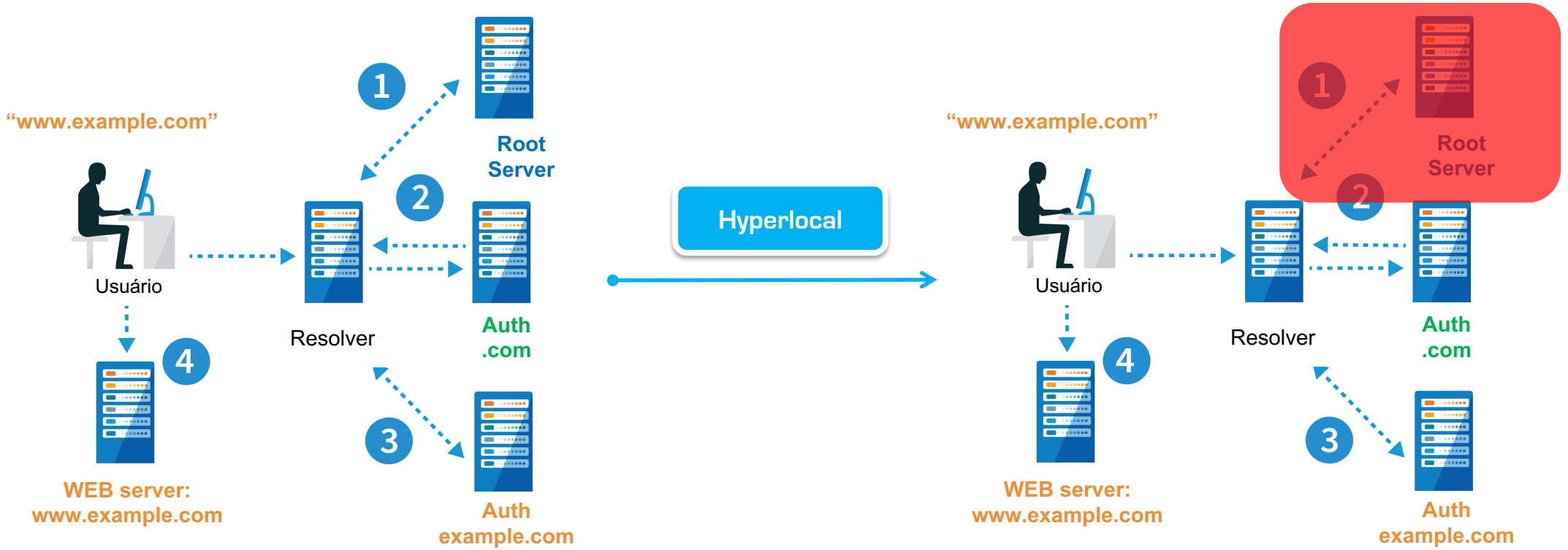
¿Qué es esto?

- 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 …

MANRS

MANRS es una iniciativa creada originalmente 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 y correcta configuración de los reversos DNS)
- Mantener todos los servidores correctamente sincronizados en materia de tiempo (NTP), *muy importante cuando implementamos DNSSEC*

Sugerencias adicionales para Registradores/Registros

- Posibilidad de ofrecer DNSSEC para los casos de hosting de DNS
- Mecanismo de transferencia de registro DS para DNSSEC
- Sistema de manejo de credenciales de acceso a la plataforma de gestión de los clientes
- Monitoreo de los dominios registrados con fines maliciosos
- Sistema ágil de atención de reclamos, respuesta a incidentes y colaboración con organizaciones de aplicación de la ley locales, regionales e internacionales
- Mantenimiento y sanidad de la zona (eliminación de registros en desuso, etc.)
- **Generar, difundir internamente y mantener actualizados todos los procedimientos operativos para todas las tareas de Registro** (procedimiento para mantenimiento y rotación de llaves para DNSSEC; casos en los que se utilice el DNS como mecanismo de bloqueo de acceso a sitios; etc.)

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