Securing DNS infrastructure

Light talk on securing DNS infrastructure …

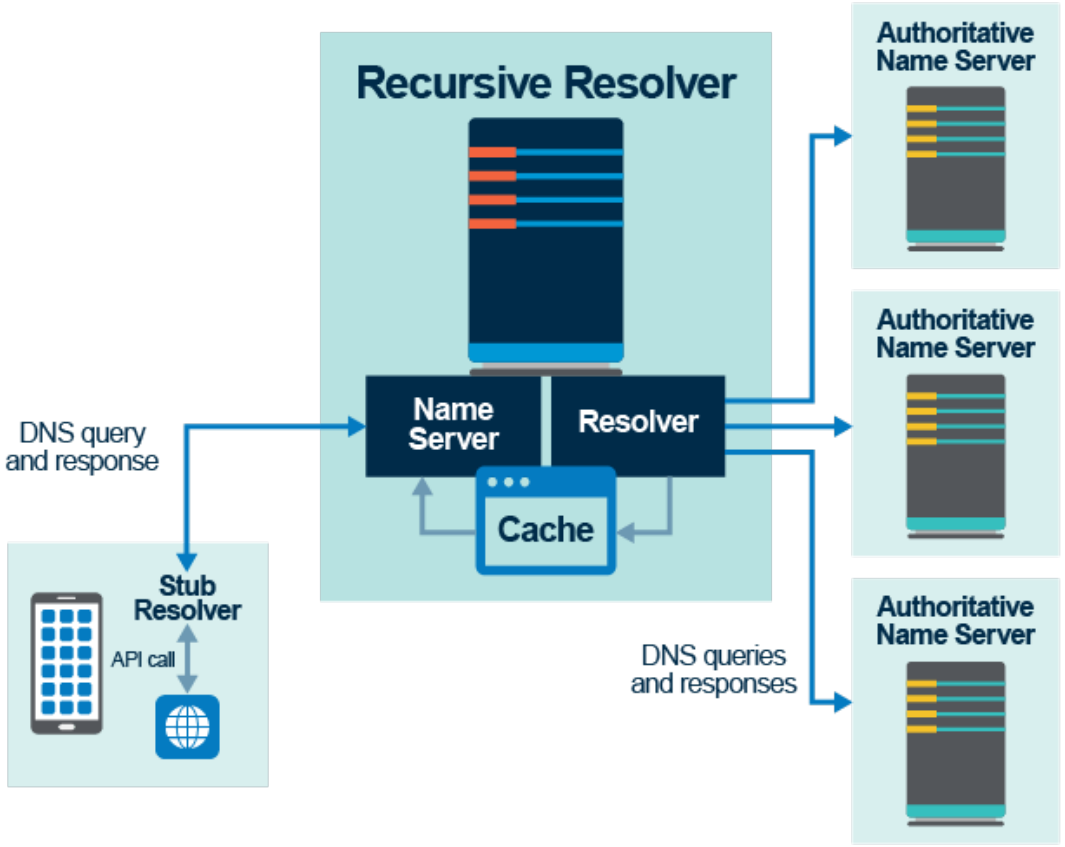
Nicolás Antoniello

CARIBNOG
15 May 2020

Recalling DNS

DNS

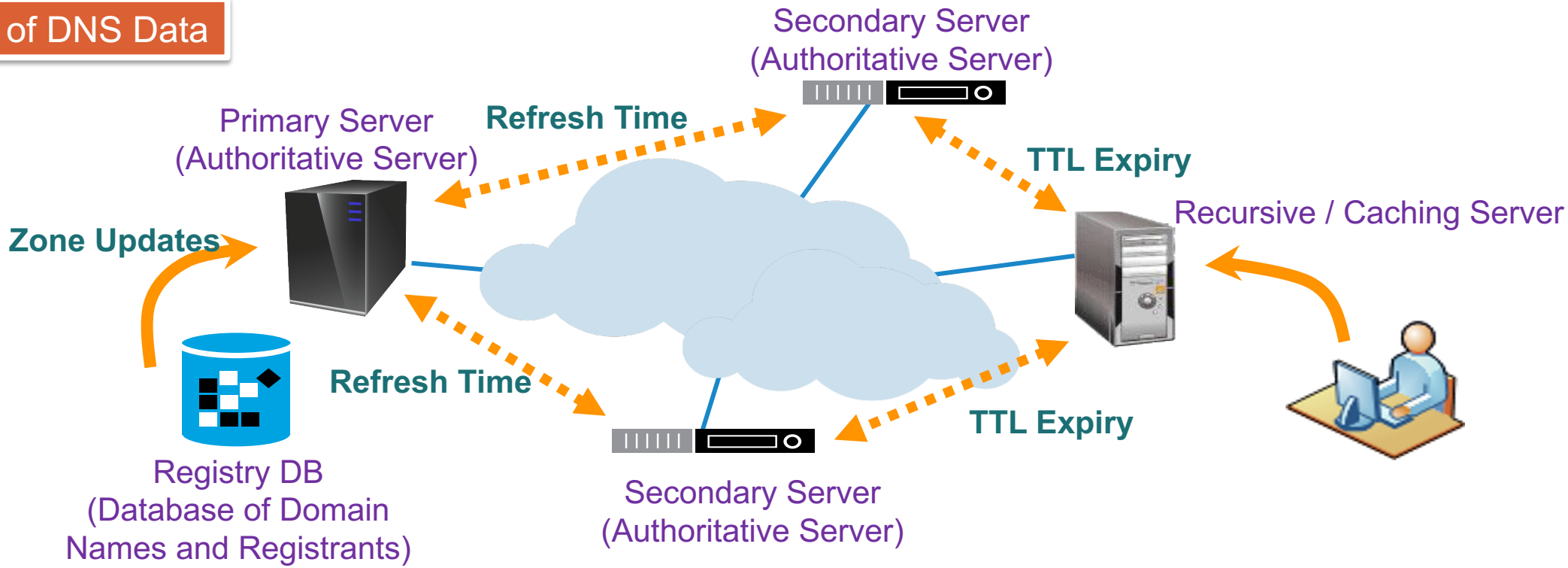
- The name space is divided up to allow **distributed** administration.
- Administrative divisions are called ***zones.***
- An administrator of any zone may delegate the administration of a subtree of its zone, thus creating a new zone.
- ***Delegation*** creates zones.
- **Servers**
  - Authoritative servers.
  - Resolvers (Caching, etc).



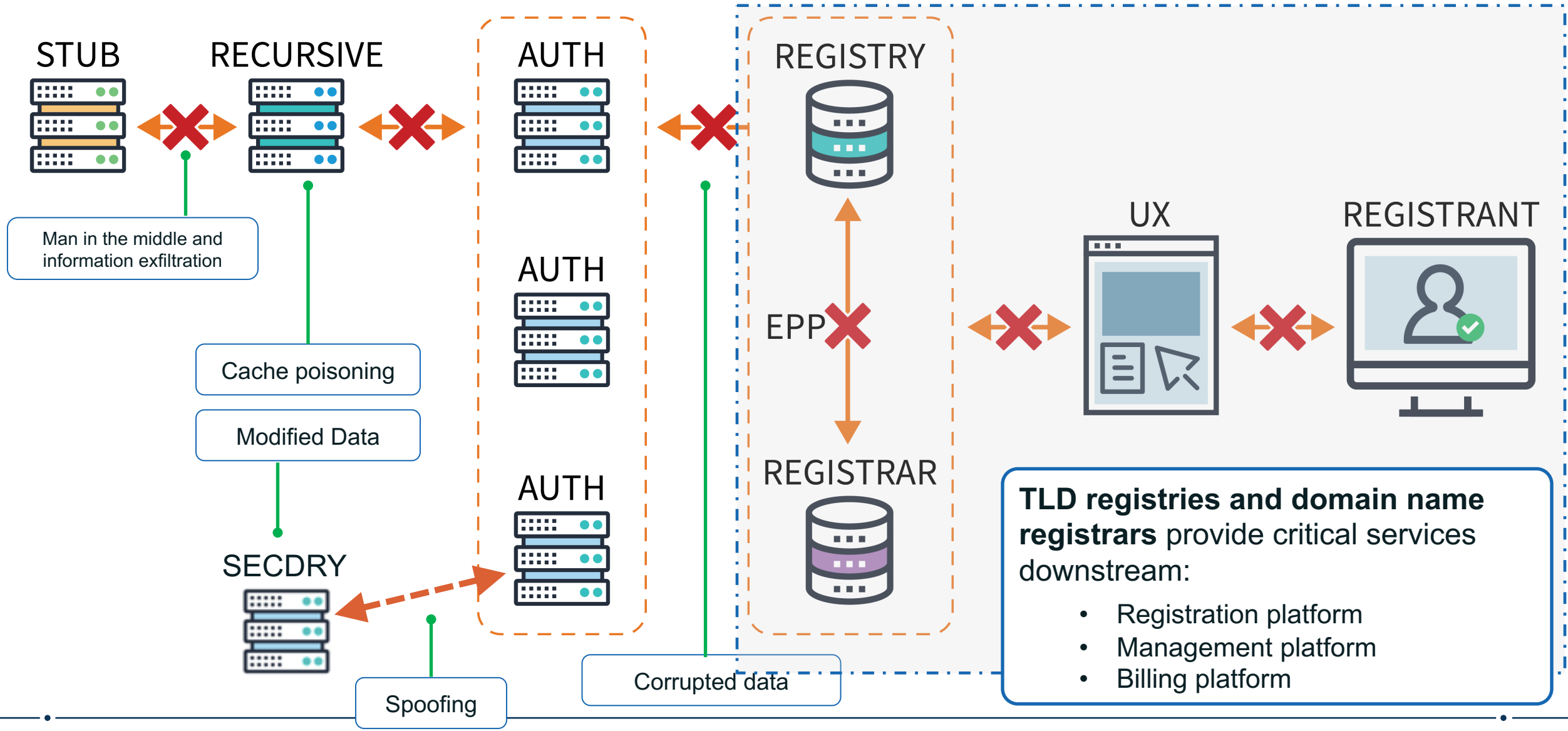
DNS Resolution's Traditional Model

- **Stub <-> Recursive <-> Authoritative**

Propagation of DNS Data



Potential Target Points of the DNS Infrastructure/Ecosystem



DNS Resilience #1

DNS Resilience #1

- Zones may and should have multiple authoritative servers
  - Provides redundancy
  - Spreads the query load

Authoritative Server Synchronization

- How do you keep a zone's data in sync across multiple authoritative servers?
- Fortunately, zone replication is built into the DNS protocol
- A zone's ***primary*** name server has the definitive zone data
  - Changes to the zone are made on the primary
- A zone's ***secondary*** or ***slave*** server retrieves the zone data from another authoritative server via a ***zone transfer***
  - The server it retrieves from is called the ***master server***
- Zone transfer is initiated by the secondary
  - Secondary polls the master periodically to check for changes

Recalling Root Zone Administration

Root Zone Administration Screenshot

- Administration of the root zone is far from a trivial task
- Twelve organizations operate authoritative name servers for the root zone

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)

DNS Resilience #2

About Anycast

Anycast could be defined as a combination of IP addressing and routing scheme, where:

- the same IP address is assigned to many destination devices; and
- the decision of which destination the packet will reach is decided by the network's routing mechanisms and metrics.

Anycast does not require any special configuration at the application level or at any client level. It is a process that is transparent to the client.

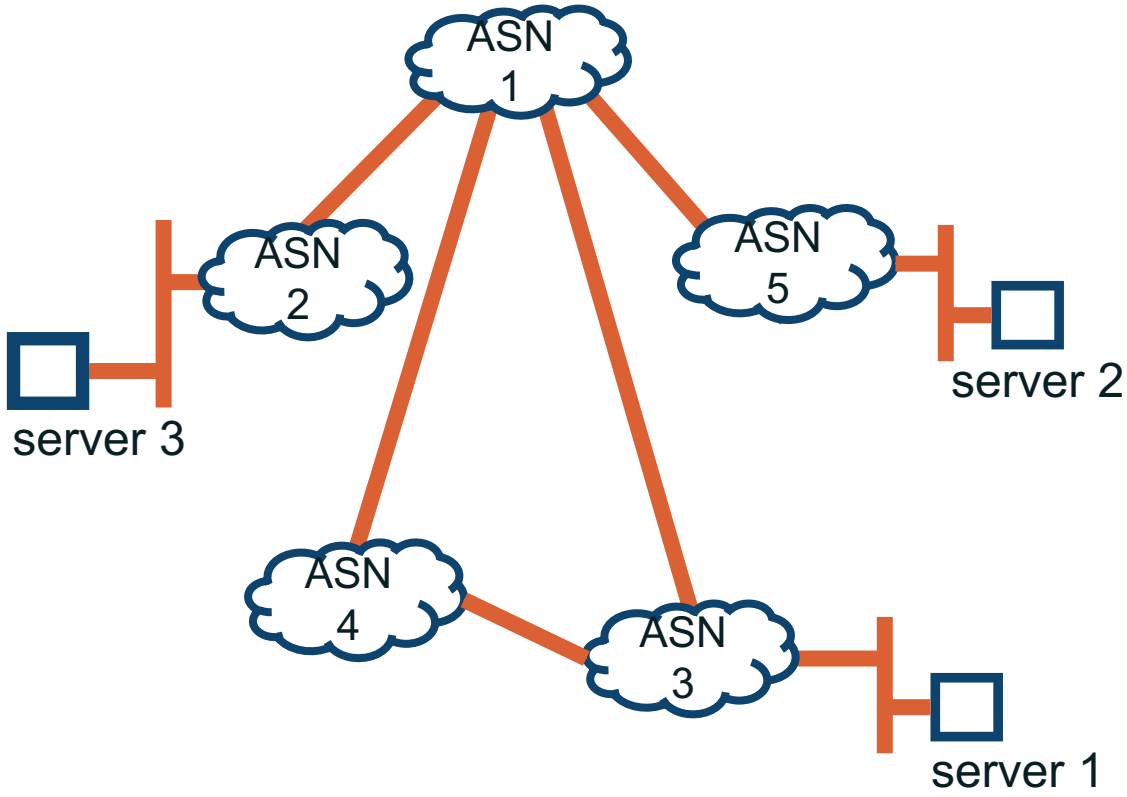
The goal is that packets will reach the *closest* anycast destination according to the routing metrics the network thinks is important (e.g., number of hops).

Anycast Use Cases (Internet)

Implementing anycast at the Internet level

Servers are configured with the same IP address but distributed in different places (different ASes) all over Internet.

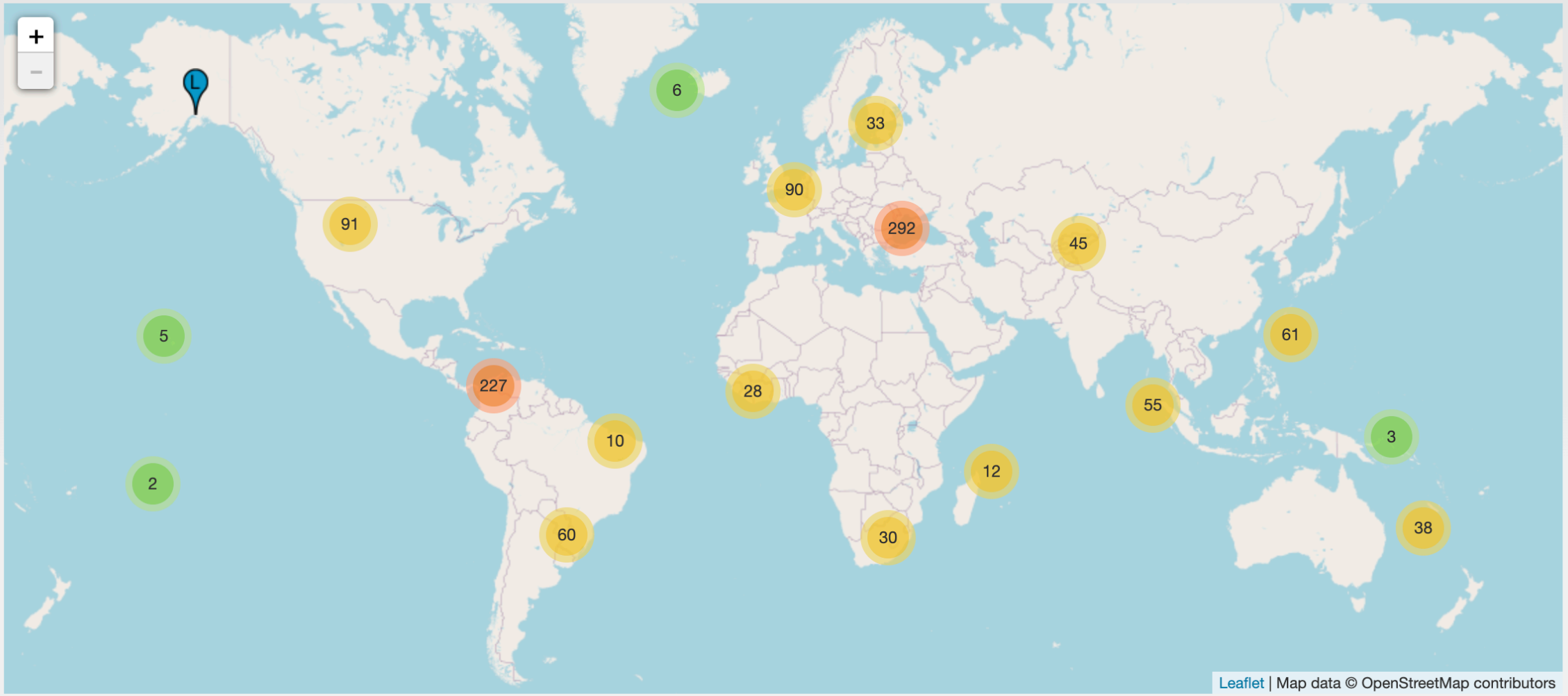
Packets sent by a client will reach one of the servers subject to different AS networking decisions. For instance they'll route packets to the closest server (shortest path to destination).



Anycast for DNS Servers

- Root server operators commonly employ anycast, distributing many **instances** of their root server label to servers all around the world.
- Anycast is also commonly used by recursive resolver operators, distributing many instances of their resolver all around the world.
- Anycast has many benefits for DNS resolvers:
  - Provides redundancy and resiliency to the global DNS infrastructure
  - Spreads the query and response load across many servers
  - Reduces latency by allowing for more instances closer to more clients
  - Provides more robustness, helping to mitigate events like DoS attacks on DNS infrastructure

The *root-servers.org* Web Site



As of 2020-04-28, the root server system consists of 1089 instances operated by the 12 independent root server operators.

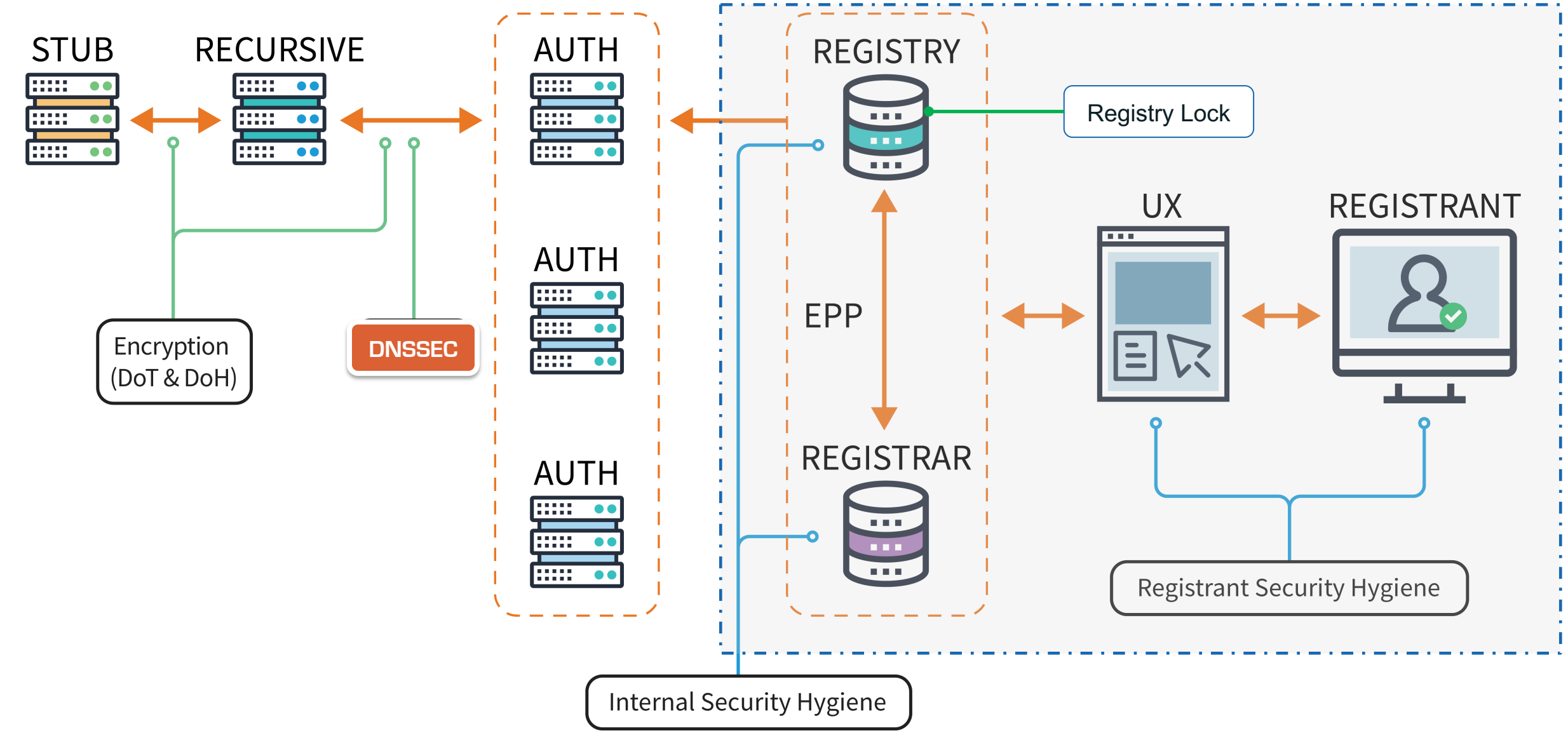
Security and Resiliency of the DNS

Attacks on Services Start by Targeting the DNS Ecosystem

Why attack the DNS?

- Collect data from web traffic to compromised domains
- Chanel to delivery malware
  - DNS is a common method of data exfiltration due to unfiltered port 53
- By meddling with DNS record values, someone can also obtain encryption certificates that is technically “valid” for an organization’s domain names.
  - *Once that is done they can redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.*

Securing the DNS Ecosystem



What is the DNSSEC - Domain Name System Security Extensions

- Helps prevent DNS abuse, DNSSEC introduces cryptography that provides assurances to users that DNS data they are seeing is valid and true
- Allows domain name registrants to **SIGN** their DNS data
- Allows DNS operators **VALIDATE** all DNS data passing through DNS resolvers.

Authenticity: *Are we certain that the entity that publishes the data is authoritative?*
Integrity: *Are the data received the same as what was published?*

DNSSEC does not provide Authorization nor does it provide Confidentiality (privacy)

Benefits of DNSSEC

- **Technical Benefits**
  - Provide Origin authentication/validation
  - Integrity assurance for DNS data
  - *Authenticated denial of existence of DNS data*
- **Impact on players:** *Overall protect the directory lookup*
  - **End User** – Confidence of reaching intended website (complement to https)
  - **Registrant** – Fraud mitigation & greater brand (country code reputation) protection
  - **Registrar** – Comply with industry standards & meet registrant demands for increased security (attract and retain security & reputation-focused registrants)
  - **Registry** – Meet industry best practices & registrar demands for increased domain security

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