DNS Ecosystem Security

ICAO Asia/Pacific Regional Cybersecurity Webinar

Champika Wijayatunga
Regional Technical Engagement Manager – Asia Pacific

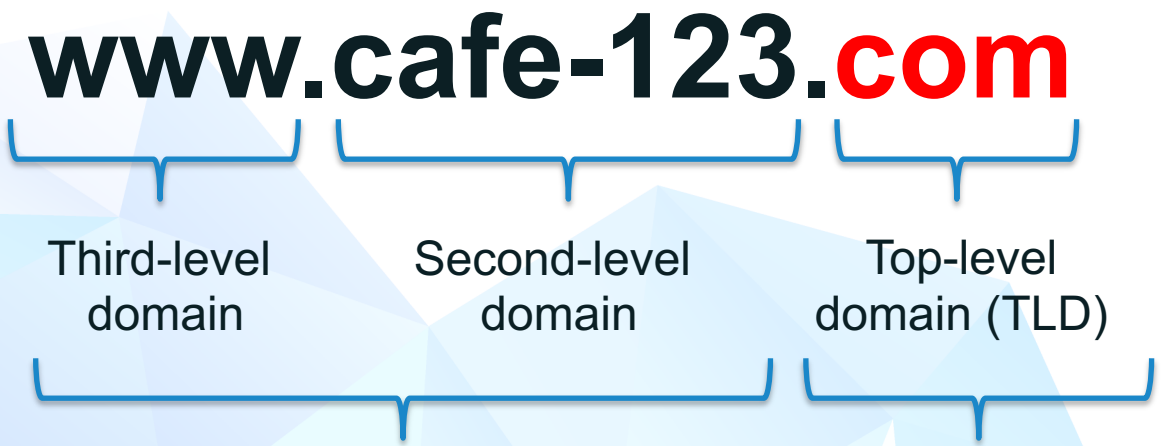
14 June 2021

Agenda

- Overview of the DNS Ecosystem
- DNS Threats and Abuses
- Securing DNS

Overview of the DNS Ecosystem

ASCII Domain Name Labels



② **Forming ASCII Labels**

Use **LDH**

- **L**etters [a-z]
- **D**igits [0-9]
- **H**yphen [H]

Label length = 63

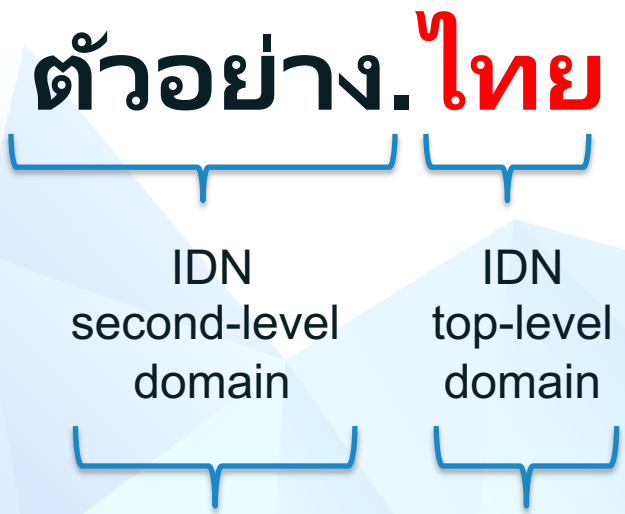
① **Forming ASCII Labels**

Use only Letters

- Letters [a-z]

Label length = 63

Internationalized Domain Name (IDN) Labels



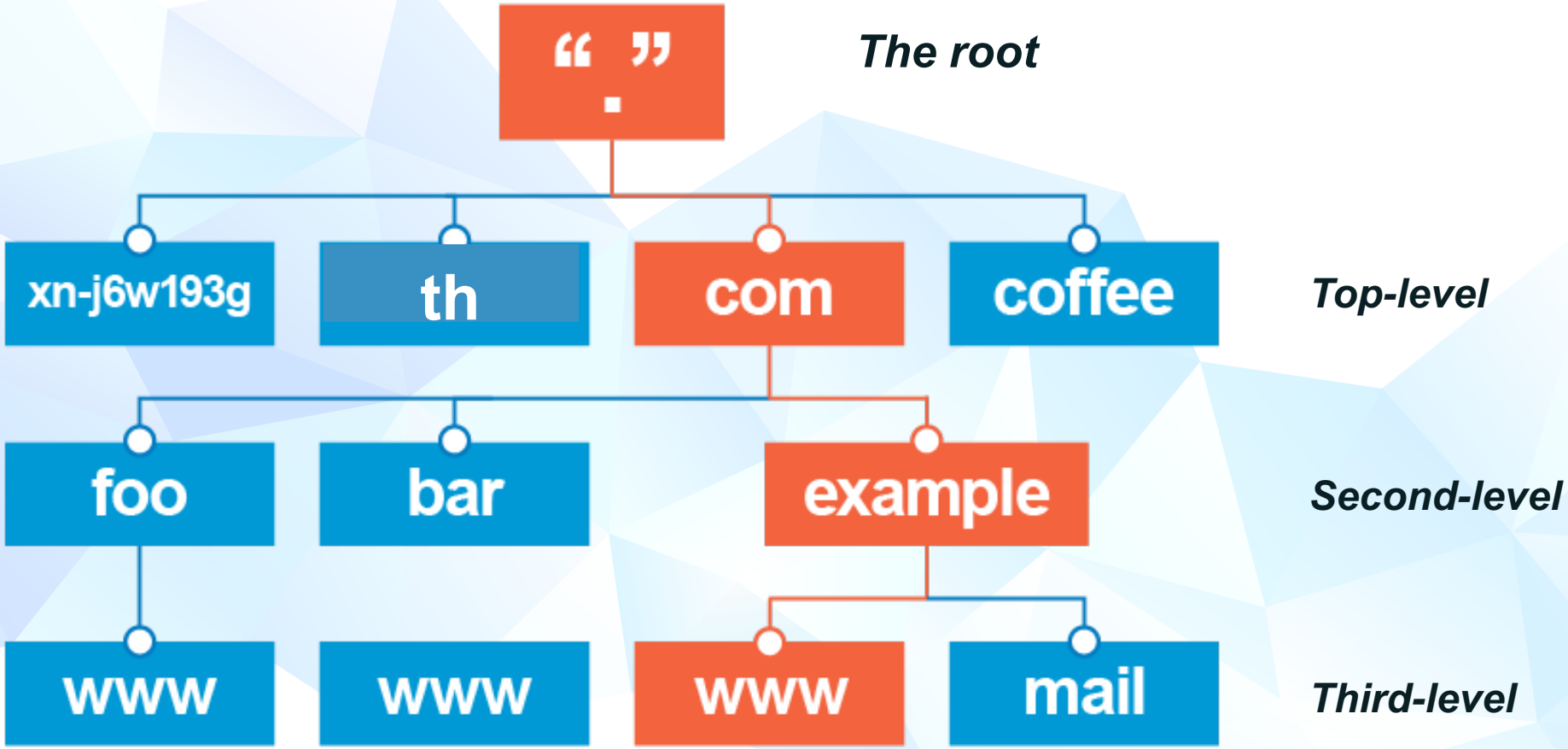
Syntax of IDN Labels
Valid U-Label: Unicode code points as constrained by the "LDH" scheme within IDNA 2008

2

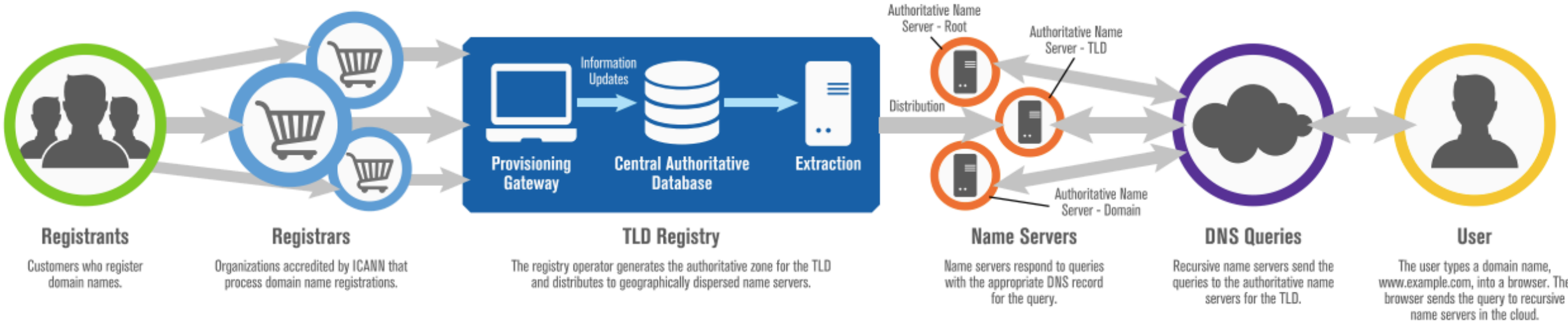
Syntax of IDN Labels
Valid U-label, further constrained by the "letter" principle for TLDs

1

DNS: The Namespace



The DNS Ecosystem



ICANN's Role

Domain Name System

The domain name system provides addressing for the Internet so people can find websites, send email, and other tasks. The ICANN organization also supports the stability of the DNS through its work, and also its contracts and accreditations.

Policy Development

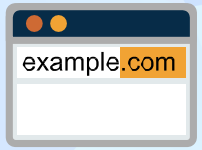
The ICANN organization supports inclusive, open and transparent multi-stakeholder bottom-up consensus based policy development mechanisms.

L-Root

The ICANN organization hosts and supports one of the 13 L-Root infrastructures. At over 160 locations worldwide, L-Root is critical to infrastructure that helps reduce latency and improves performance of the DNS.

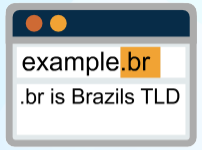
Support and Grow the Community

The ICANN organization engages, nurtures and supports interested stakeholders for active and meaningful participation in ICANN. ICANN connects with stakeholders through outreach and engagement, and meeting & event support.



Generic Top-Level Domains

The ICANN organization manages the domain name system's top-level domains. ICANN helps promotes competition and choice in the gTLD marketplace.



Country Code Top-Level Domains

The ICANN organization delegates top-level domains identified with a country code. Management is done by national ccTLD operators.

Protocol Parameters

The ICANN organization, in coordination with the Internet Engineering Task Force, manages protocol parameters by maintaining many of the codes and numbers used in Internet protocols.

Internet Protocol Addresses

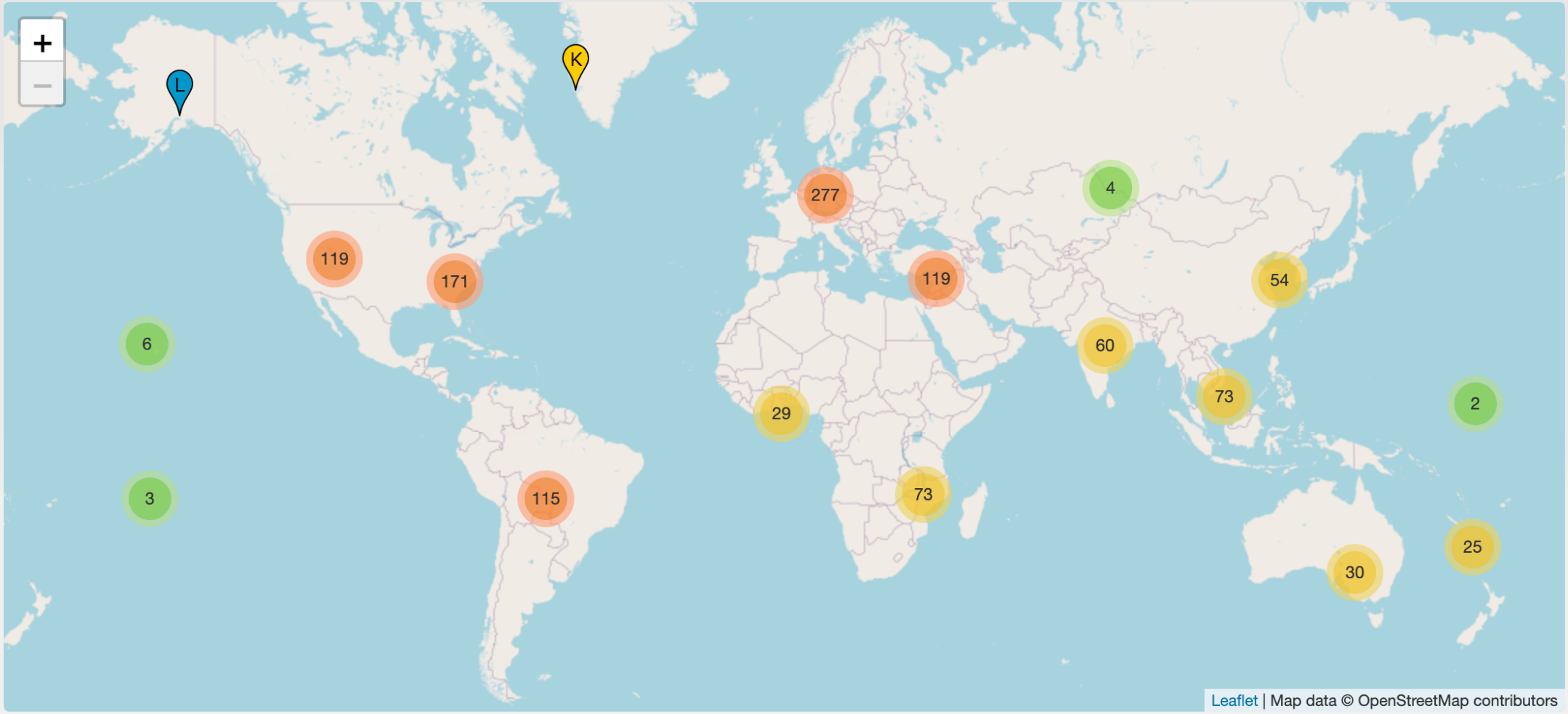
By serving as the central repository for IP addresses, the ICANN organization helps coordinate how IP addresses are supplied – preventing repetition and conflicts.

Root Zone Management

The ICANN organization helps manage the root zone through the IANA functions, which involves assigning the operators of top-level domains, such as .bank and .com, and maintaining the technical and administrative details.

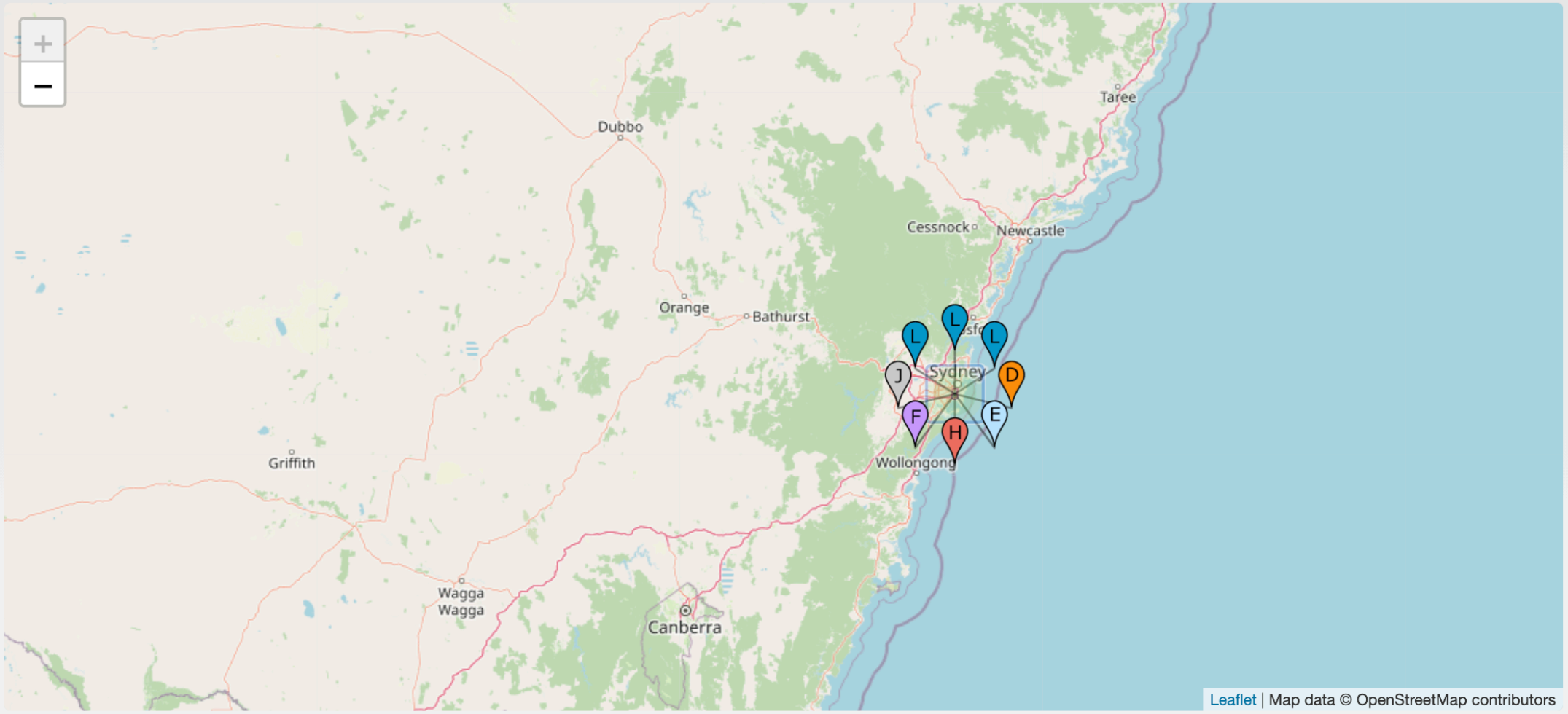
IANA functions

DNS: The Root (Servers)



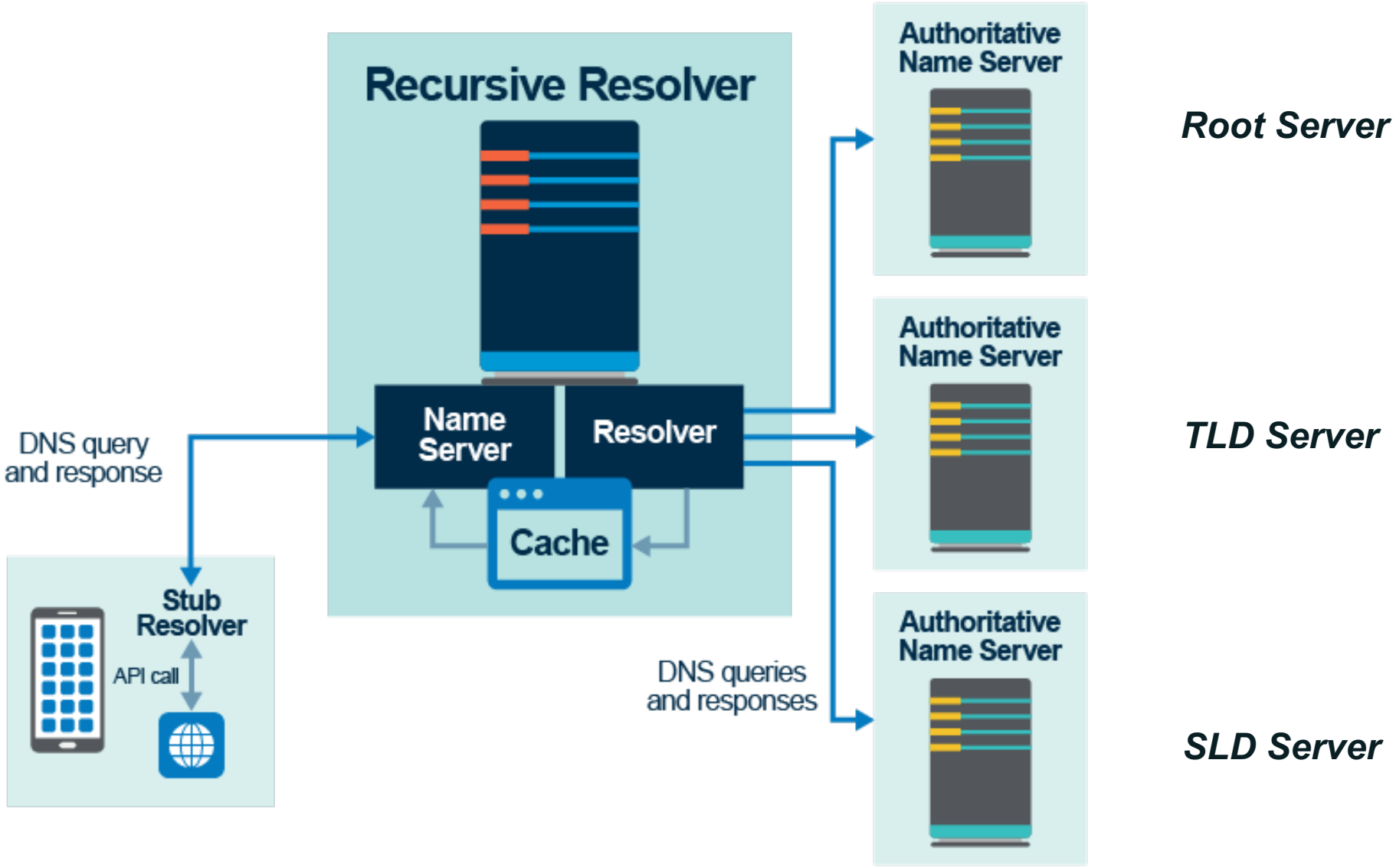
As of 06/08/2021 3:11 a.m., the root server system consists of 1380 instances operated by the 12 independent root server operators.

DNS: The Root (Servers)



As of 06/08/2021 3:11 a.m., the root server system consists of 1380 instances operated by the 12 independent root server operators.

DNS: The Service



DNS Threats and Abuses

DNS contains a wealth of data about your systems

- Your organization's domain names – **example.com**
- Your organization's individual host names – **host.example.com**
- IP addresses
- Mail server data (MX records) – **mail.example.com**
- Database locations – **db0.example.com**
- etc

Domain Registrations are Attractive Targets for Attacks

- Automated processes
- Registrar correspondence with registrants largely via emails
- Registrant is responsible for registration data accuracy
- Inexpensive registrations are plentiful
  - Good for consumers but good for attackers too

Namespace Risks

- Homoglyphs
  - **example.com** vs **examplé.com** (xn--exampl-gva.com)
  - **aero.com** vs **aerο.com** (xn--80agf1b.com)

- Typosquatting
  - **example.com** vs **exmaple.com**

Emojis in Domain Names

Fun, but may be dangerous

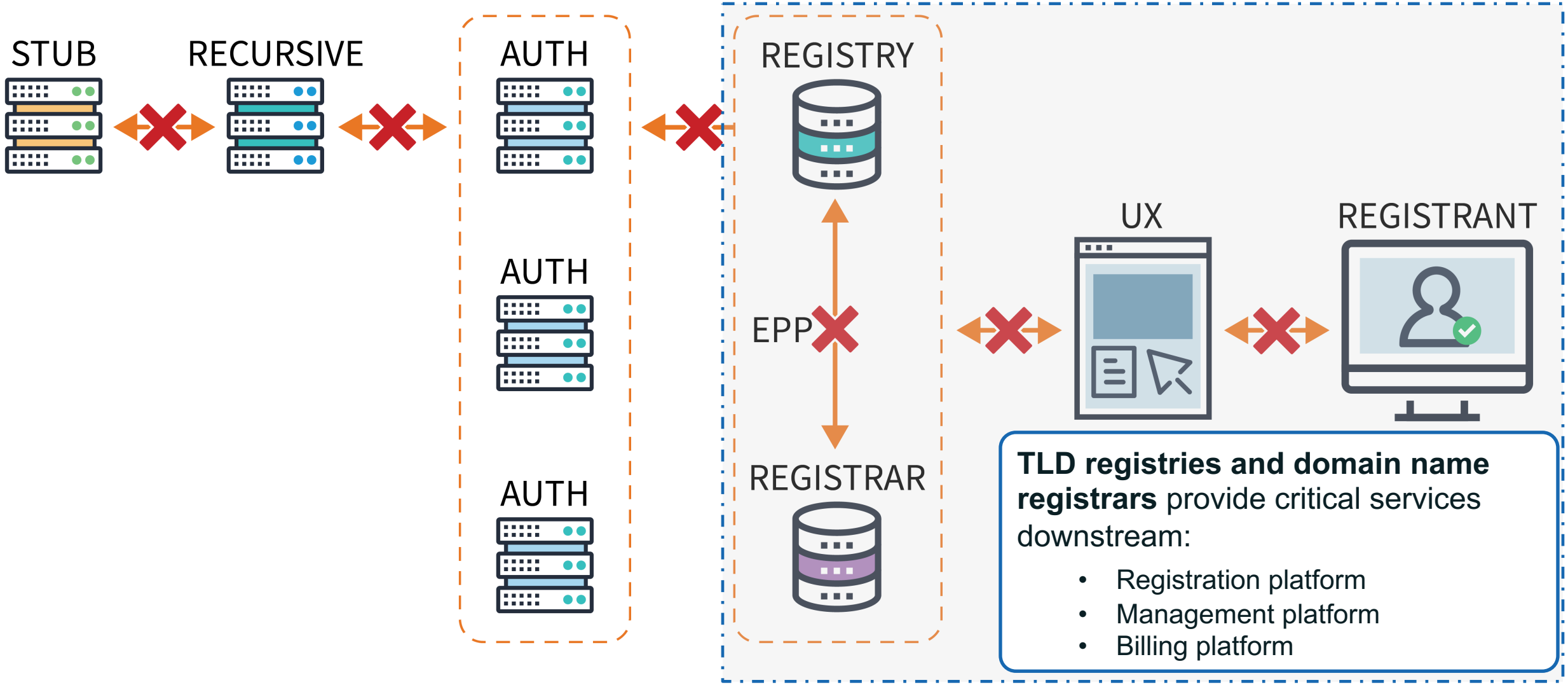
Users could easily confuse the "Grinning face" emoji (left) and "Grinning face with smiling eyes" emoji (right).

⚠ **Emojis can be too visually similar to distinguish especially when displayed in smaller fonts or by different applications** ⚠

Malicious and Misused Domain Registrations

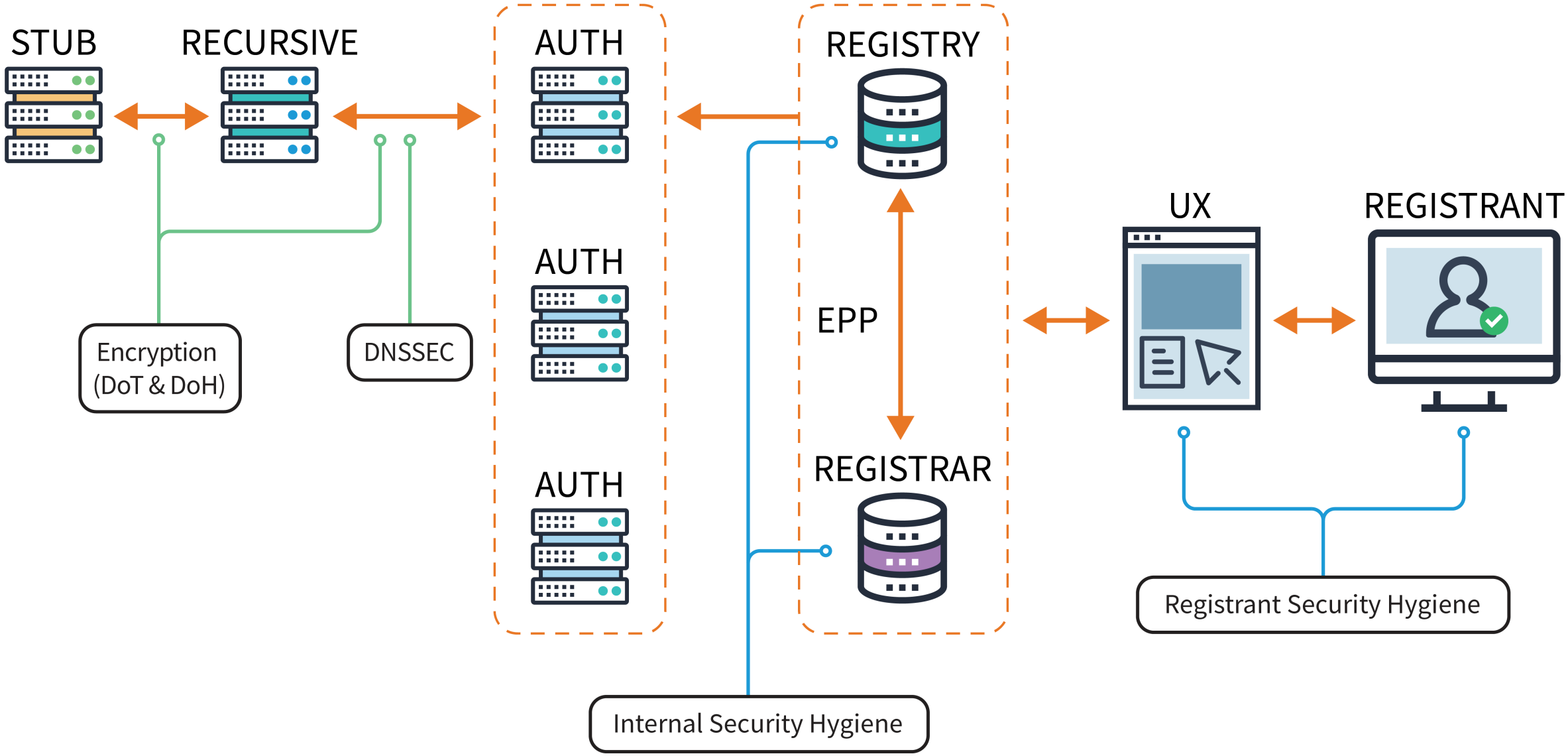
- Phishing
- Business Email Compromises
- Hosting criminal infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism, Exploit attacks
- Malware C&C, Malware distribution
- Cache Poisoning
- Man-in-the-Middle attacks
- etc

Potential Target Points of the DNS Infrastructure/Ecosystem



Securing DNS

A Secure DNS Ecosystem



Best Practices in Securing DNS

- Deployment of DNS Security Extensions (DNSSEC)
- Secure User Interfaces
- Registry/Registrar locks
- Monitoring and diagnostic tools
- Network and Server redundancy
- Secure Zone Transfers (ACLs, TSIG)
- Authoritative Servers must answer authoritatively
- Recursive Servers to provide recursion only to designated clients
- Updated DNS Software
- Support technical standards and compliance
- Know your SLAs
- Have plans in place to deal with attacks and test those regularly
- Good Cyber-hygiene etc.

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann