DNS Best Practices

In collaboration with PacNOG22

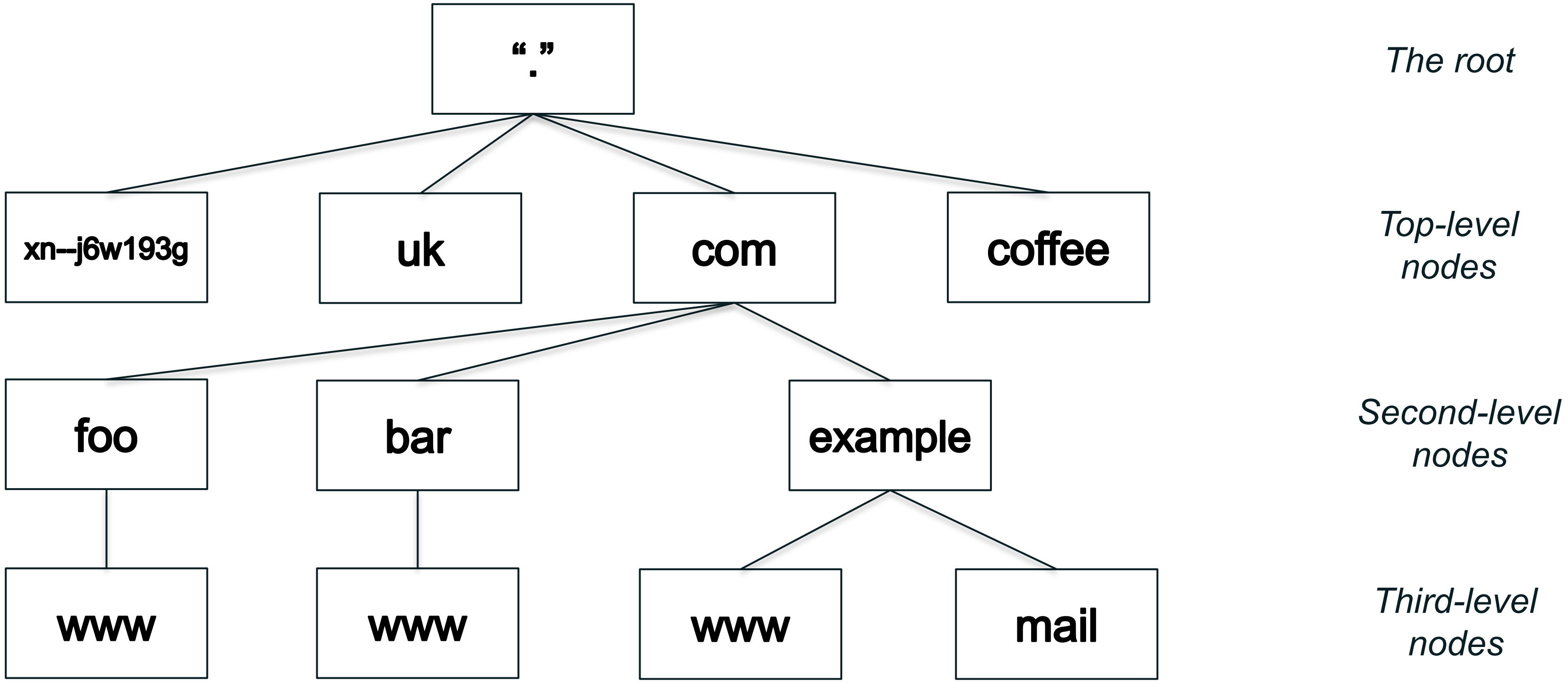
Champika Wijayatunga
Regional Security Engagement Manager – Asia Pacific

25 June 2018

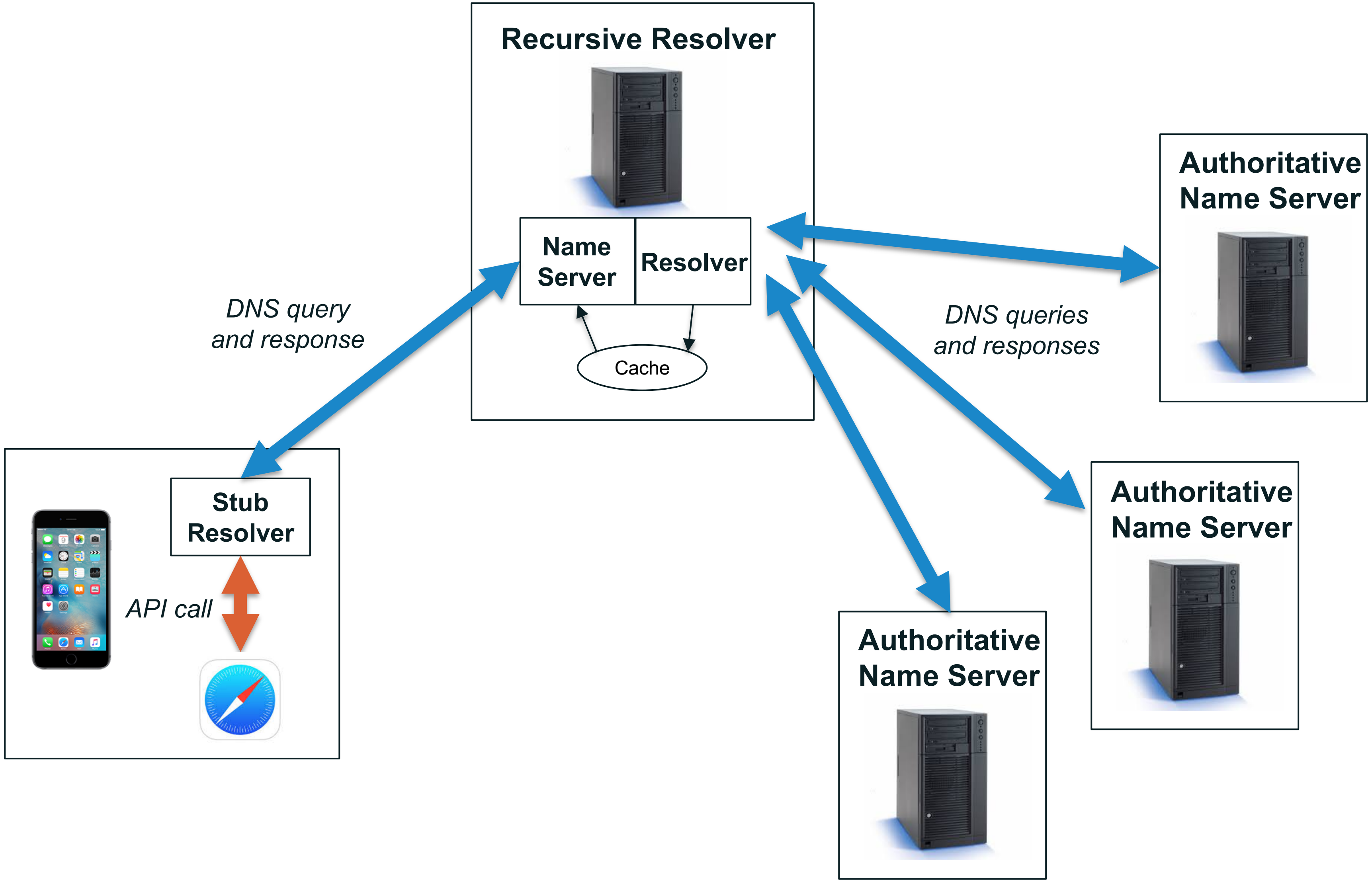
ICANN

Domain Name System (DNS)

- DNS database structure is an inverted tree called the ***name space***
- Each node has a label
- The root node (and only the root node) has a null label



DNS Components at a Glance


Recursive Resolver
Name Server
Resolver
Cache
DNS query and response
DNS queries and responses
Authoritative Name Server
Authoritative Name Server
Authoritative Name Server
Stub Resolver
API call

Authoritative Server Synchronization

- A zone’s ***primary*** name server has the definitive zone data
- 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***
  - Master server is usually the primary but doesn’t have to be
- Zone transfer is initiated by the secondary
  - Secondary polls the master periodically to check for changes
  - The master also notifies the primary of changes
    - RFC 1996, “A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)”

Format of Resource Records

- Resource records have five fields:
    - ***Label:*** Domain name the resource record is associated with
    - ***Time to live (TTL):*** Time (in seconds) the record can be cached
    - ***Class:*** A mechanism for extensibility that is largely unused
    - ***Type:*** The type of data the record stores
    - ***RDATA:*** The data (of the type specified) that the record carries

Start of Authority (SOA)

- One and only one SOA record per zone
- At the zone apex
- Most values control zone transfers

```
example.com.  SOA ns1.example.com. hostmaster.example.com. (
              2016050100 ; serial
              3600       ; refresh (1 hour)
              600        ; retry (10 minutes)
              2592000    ; expire (4 weeks 2 days)
              300        ; minimum (5 minutes)
              )
```

Reverse Mapping

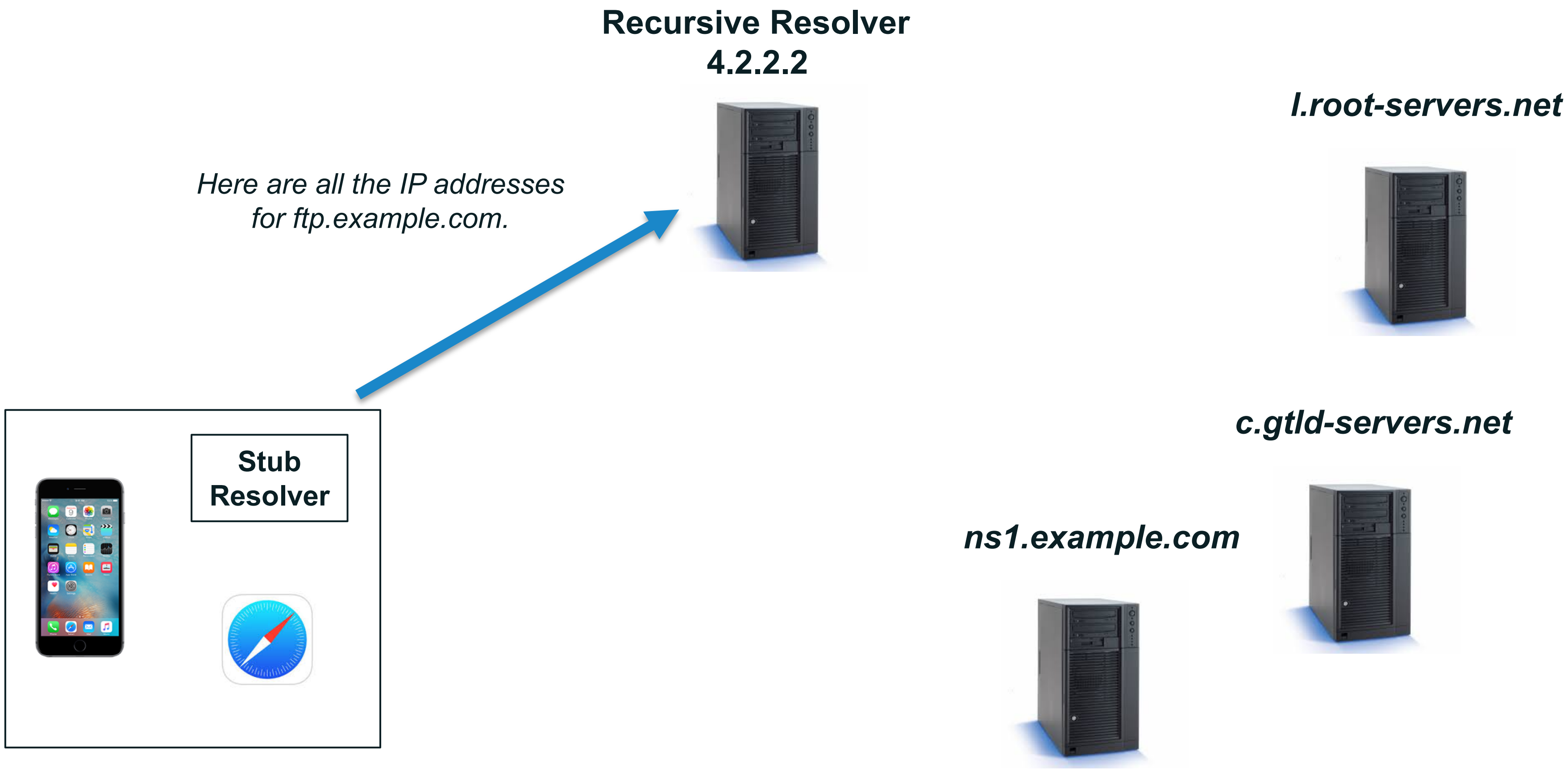
- Name-to-IP is “forward” mapping
- IP-to-name is “reverse” mapping
- Reverse mapping accomplished by mapping IP address space to the DNS name space
  - IPv4 addresses under *in-addr.arpa*
  - IPv6 addresses under *ip6.arpa*
- Uses PTR (pointer) records

```
7.2.0.192.in-addr.arpa.   PTR     example.com.
```

- Corresponds to this A record:

```
example.com.                A      192.0.2.7
```

Resolution Process



Threats in DNS

- Cache Poisoning Attacks
  - Vulnerable resolvers add malicious data to local caches
- DNS Hijacking
  - A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
    - E.g. DNSChanger
  - One of the biggest cybercriminal takedown in history
- And many other DNS hijacks in recent times

Technical Requirements

- Networks and Servers (redundant)
- Back office systems.
- Physical and Electronic Security
- Quality of Service (24/ 7 availability!)
- Name Servers
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol

Name Server Considerations

- Support technical standards
- Handle load multiple times the measured peak
- Diverse bandwidth to support above
- Must answer authoritatively
- Turn off recursion!

Secondary Name Server Choice

Diversity, Diversity and Diversity!

- Don’t place all on the same LAN/building/segment
- Network diversity
- Geographical diversity
- Institutional diversity
- Software and hardware diversity

Security, Stability & Resiliency Considerations

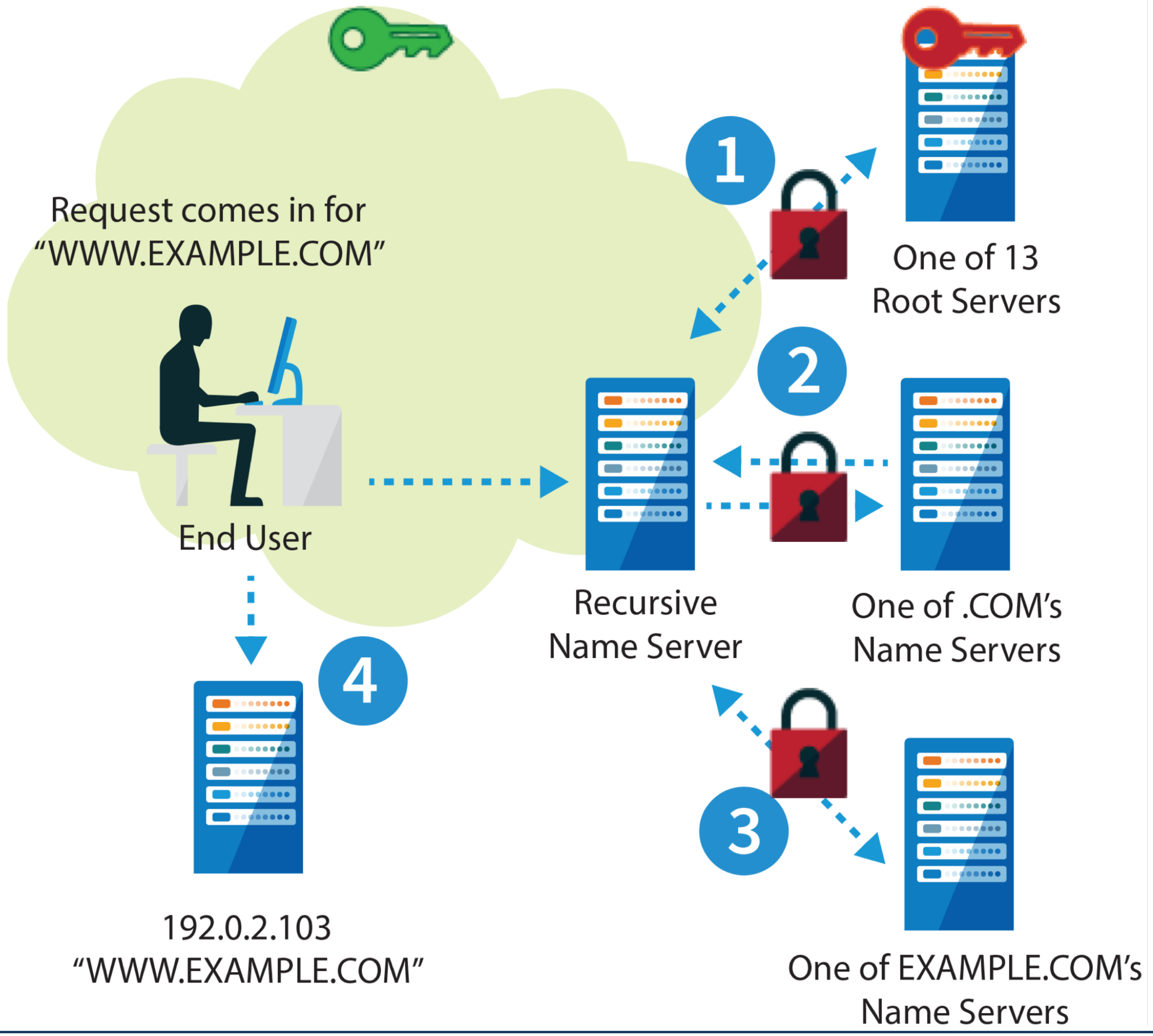
- Physical security
  - Deploy stringent access controls
  - Fire detection and retardation
  - Other environmental sensors (Flood, Humidity etc.)
  - Power continuity for 48 hours (or more)

- Backups
  - Multiple secure copies locally and offsite
  - Test, test and test!!

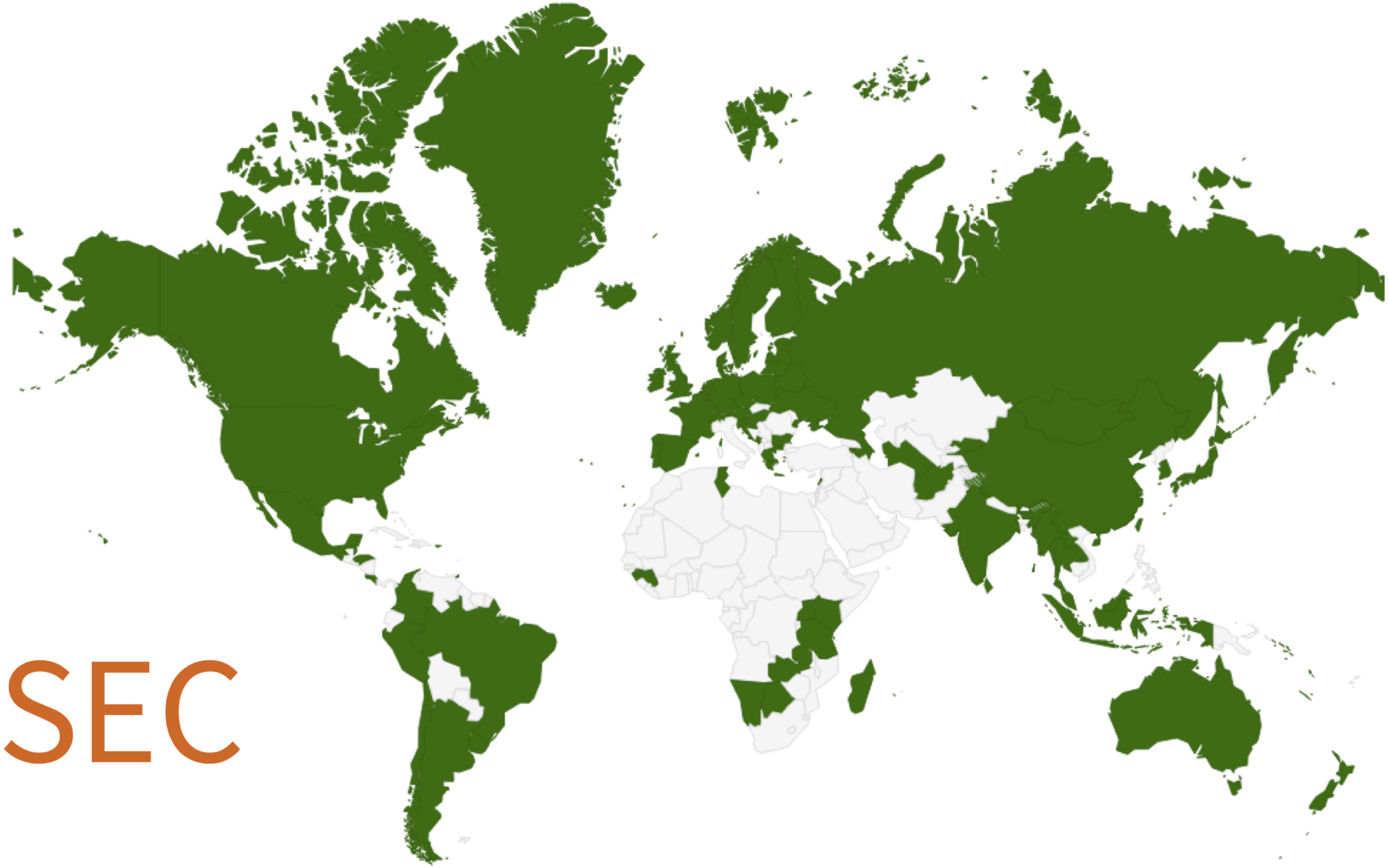
Know Your SLAs

- Functioning name servers are the most critical/visible service
- All other services also need to be considered
  - Billing
  - Whois server, webservers
  - Registrar APIs
- Consider your service level targets and how you will meet them
- DNS servers always on, other systems mostly on?

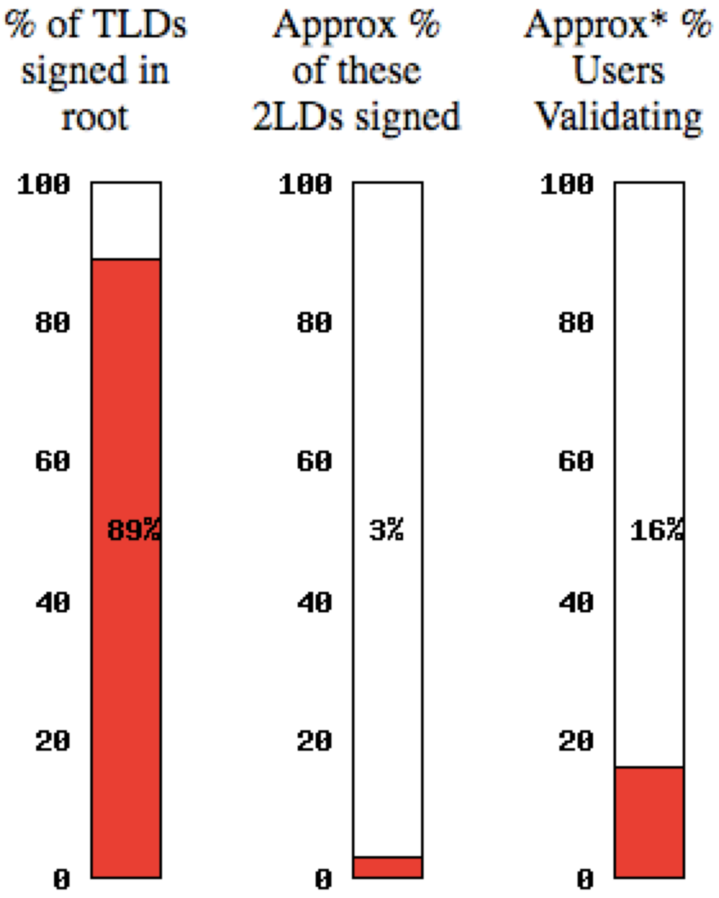
DNSSEC

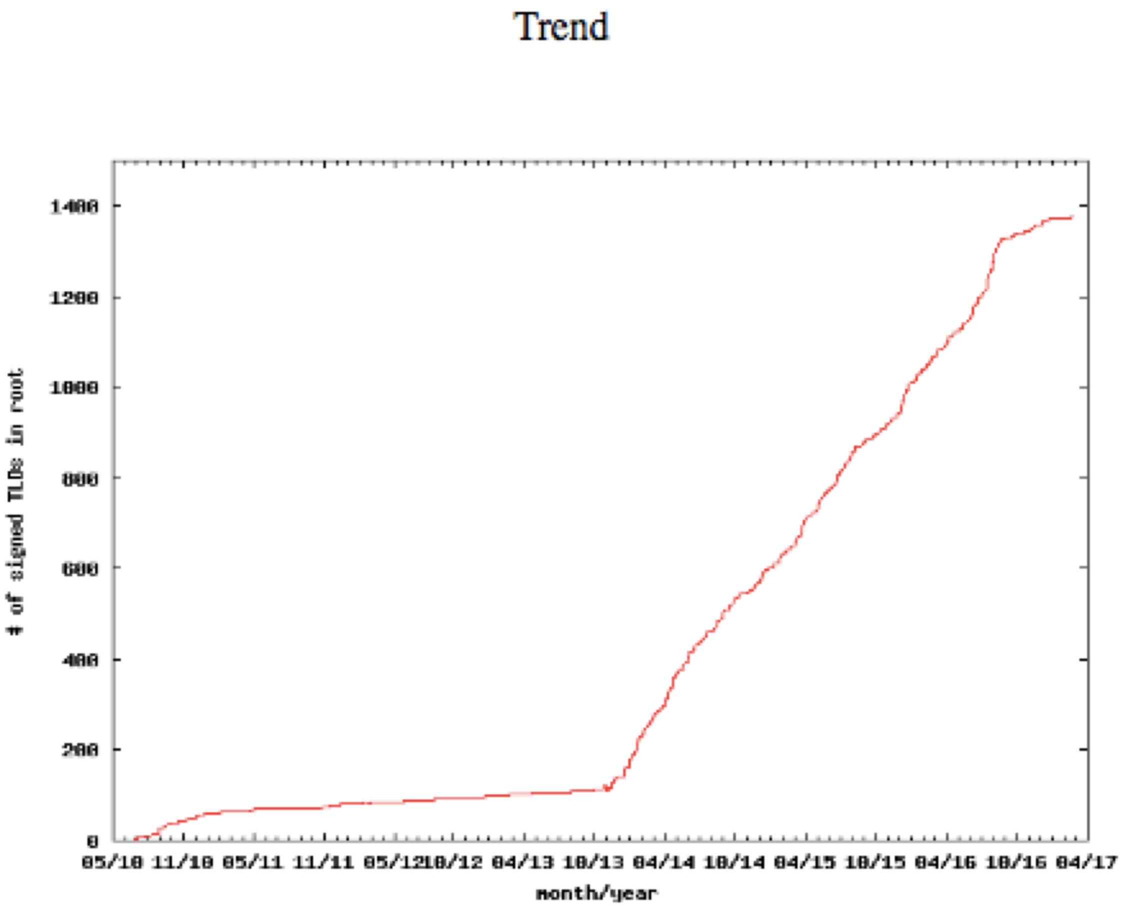

Request comes in for
"WWW.EXAMPLE.COM"
End User
1
One of 13
Root Servers
2
Recursive
Name Server
One of .COM's
Name Servers
3
One of EXAMPLE.COM's
Name Servers
4
192.0.2.103
"WWW.EXAMPLE.COM"

DNSSEC ccTLD Map



DNSSEC Deployment





DNSSEC: So what’s the problem?

- Not enough IT departments know about it or are too busy putting out other security fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars*/DNS providers see no demand leading to “chicken-and-egg” problems.

*but required by new ICANN registrar agreement

What you can do

- For Companies:
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- For Users:
  - Ask ISP to turn on validation on their DNS resolvers
- For All:
  - Take advantage of DNSSEC education and training

Root Zone DNSSEC KSK Rollover

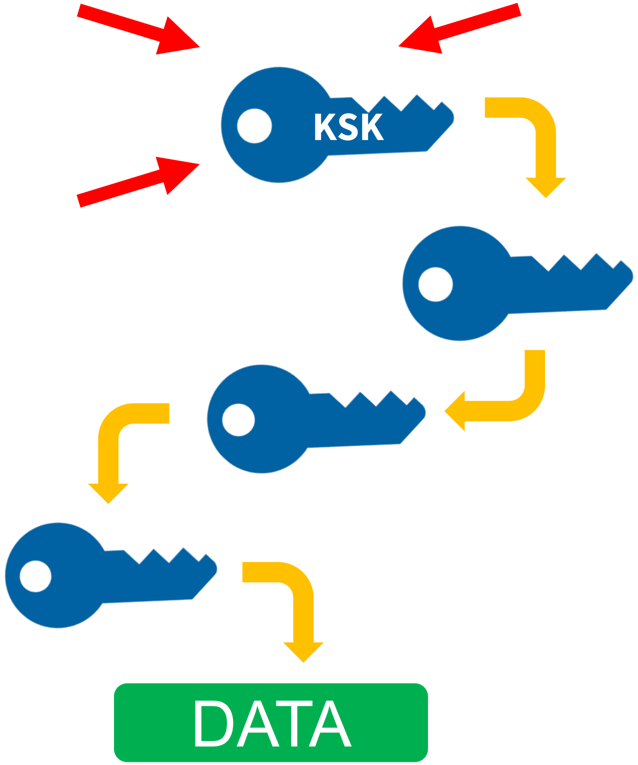
KSK Rollover: An Overview

ICANN is in the process of performing a Root Zone DNS Security Extensions (DNSSEC) Key Signing Key (KSK) rollover

- The Root Zone DNSSEC Key Signing Key "**KSK**" is the topmost cryptographic key in the DNSSEC hierarchy

- The KSK is a cryptographic public-private key pair:
  - Public part: trusted starting point for DNSSEC validation
  - Private part: signs the Zone Signing Key (ZSK)

- Builds a "chain of trust" of successive keys and signatures to validate the authenticity of any DNSSEC signed data



When Does the Rollover Take Place?

- The changing or "rolling" of the KSK Key was originally scheduled to occur on 11 October 2017, but it was delayed because some data obtained in September 2017 showed that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators were not yet ready for the key rollover.

- There may be multiple reasons why operators do not have the new KSK installed in their systems: some may not have their resolver software properly configured.

- After a preliminary consultation with the community, ICANN posted a plan for starting the rollover process again. That plan was open for community comment at https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en.

- The plan calls for ICANN to roll the root KSK on 11 October 2018 while encouraging ISPs and Network operators to use this additional time period to be certain that their systems are ready for the key rollover.

Why You Need to Prepare

⚠ **If you have enabled DNSSEC validation, you must update your systems with the new KSK to help ensure trouble-free Internet access for users**

- Currently, 25 percent of global Internet users, or **750 million people**, use DNSSEC-validating resolvers that could be affected by the KSK rollover
- If these validating resolvers do not have the new key when the KSK is rolled, end users relying on those resolvers will encounter errors and be **unable to access the Internet**

What Do Operators Need to Do?

Be aware whether DNSSEC is enabled in your servers

Be aware of how trust is evaluated in your operations

Test/verify your set ups

Inspect configuration files, are they (also) up to date?

If DNSSEC validation is enabled or planned in your system

- Have a plan for participating in the KSK rollover
- Know the dates, know the symptoms, solutions

For More Information

1 **Visit https://icann.org/kskroll**

2 **Join the conversation online**

- Use the hashtag #KeyRoll
- Sign up to the mailing list https://mm.icann.org/listinfo/ksk-rollover

3 **Ask a question to globalsupport@icann.org**

- Subject line: “KSK Rollover”

4 **Attend an event**

- Visit https://features.icann.org/calendar to find upcoming KSK rollover presentations in your region

Engage with ICANN – Thank You and Questions

ICANN

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