DNS Data security

AFRALO Capacity Building

Yazid Akanho & Paul Muchene

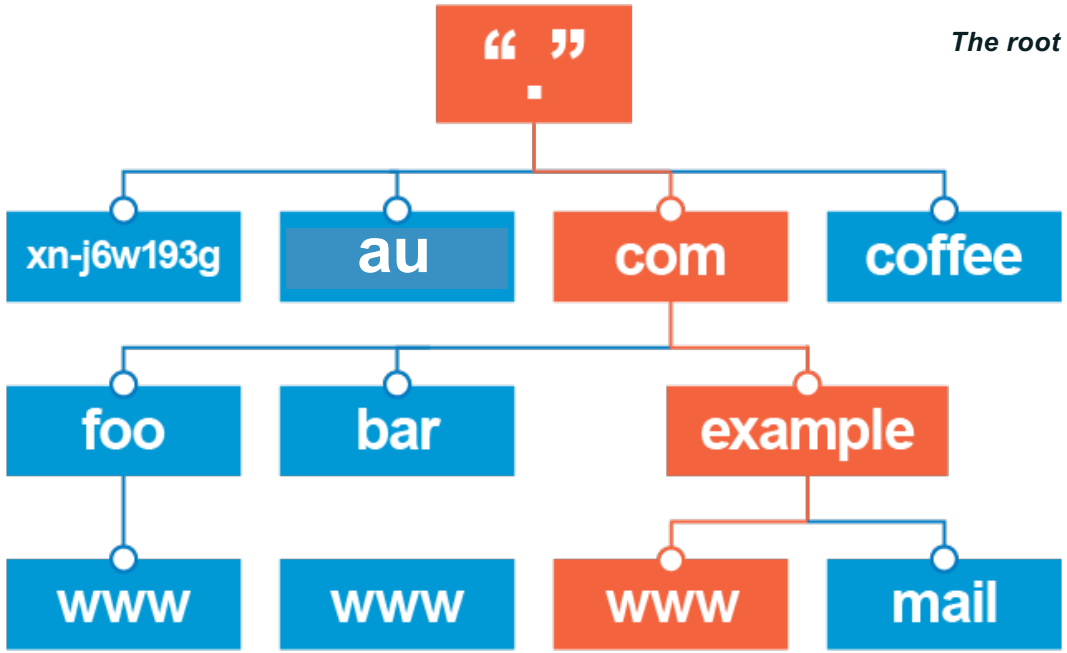
07 Sept. 2021

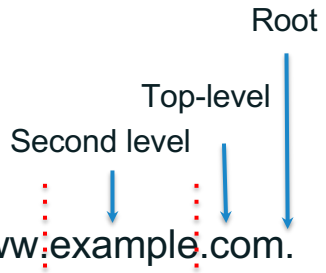
Agenda

- Overview of the DNS
- DNS Data security
- Introduction to DNSSEC
- DNS Privacy
- RDAP
- Some ICANN initiatives to support a secure DNS ecosystem

Overview of the DNS

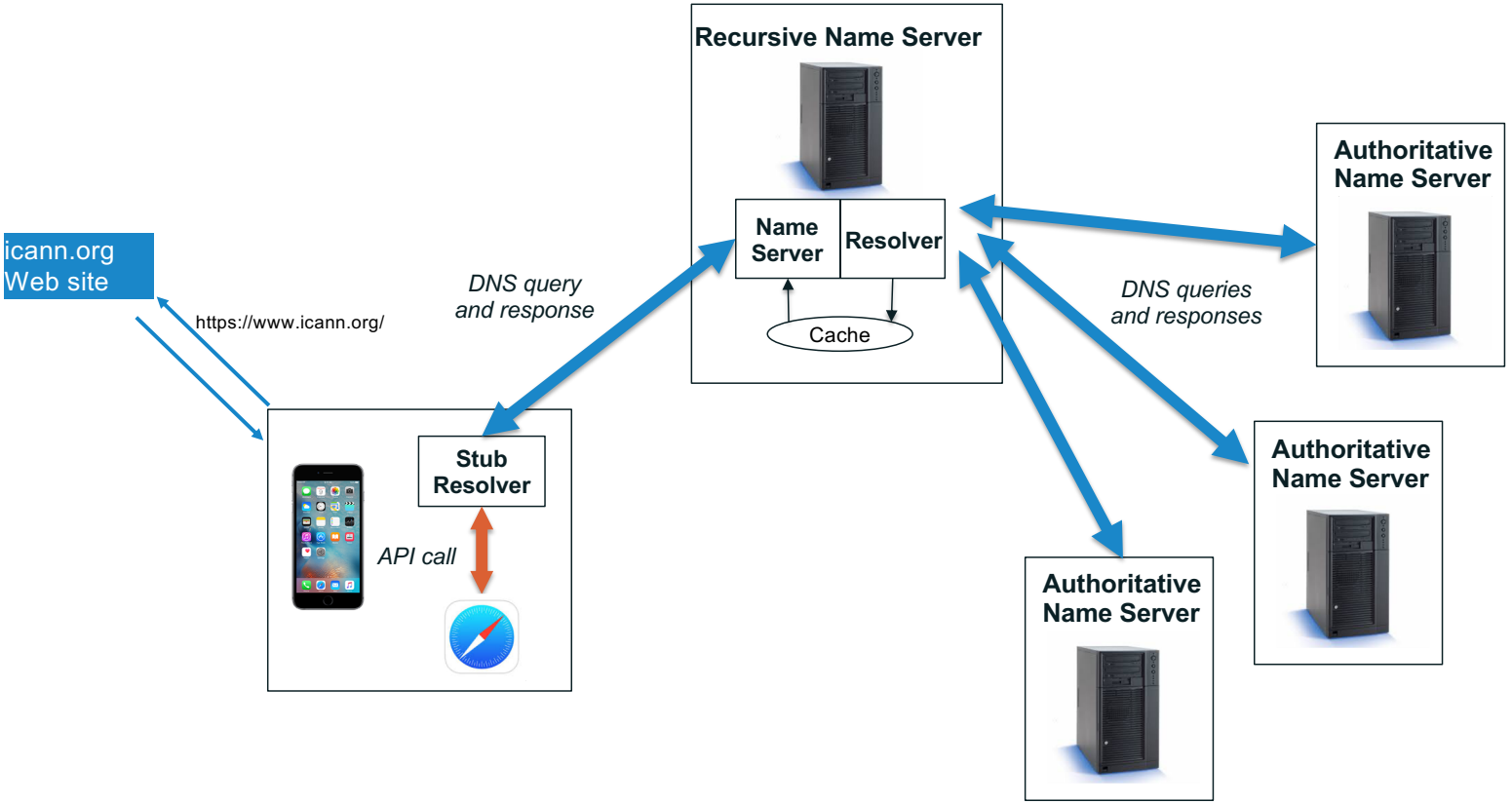
The Domain Name System (DNS)





FQDN = **F**ully **Q**ualified **D**omain **N**ame

DNS Components at a Glance



DNS data security

Goals of Security

SECURITY

CONFIDENTIALITY

prevents unauthorized use or disclosure of information

INTEGRITY

safeguards the accuracy and completeness of information

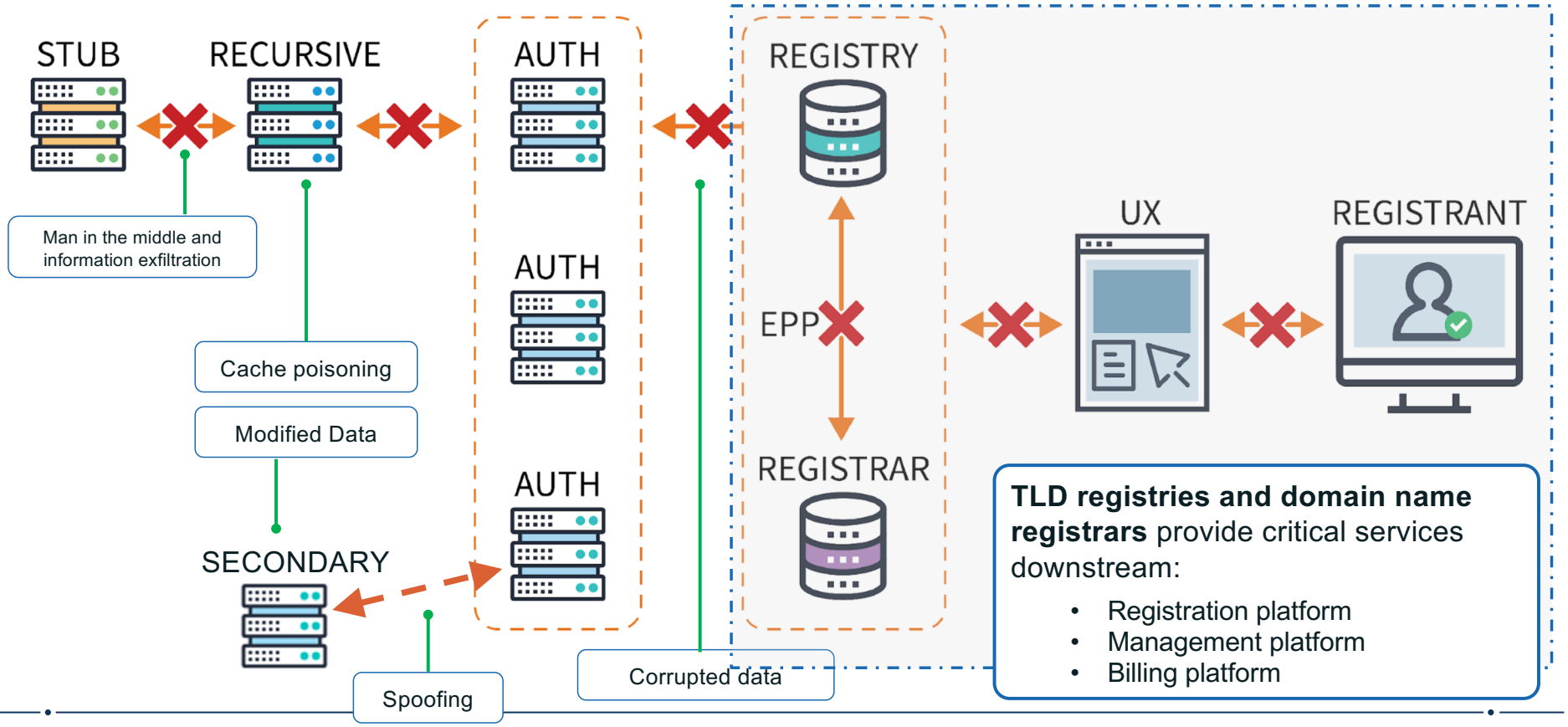
AUTHENTICITY & AVAILABILITY

authorized users have reliable and timely access to information

DNS Attacks

- Large attack surface due to the complexity of the DNS ecosystem
- Cache poisoning
- Guessing Query IDs
- Redirections
  - Change name servers to point to attacker-controlled authoritative servers
- Resolver Hijacking
  - Cause DNS queries to be answered by attacker-controlled resolver
- Man-In-The-Middle attacks etc.

Potential Target Points of the DNS Infrastructure/Ecosystem

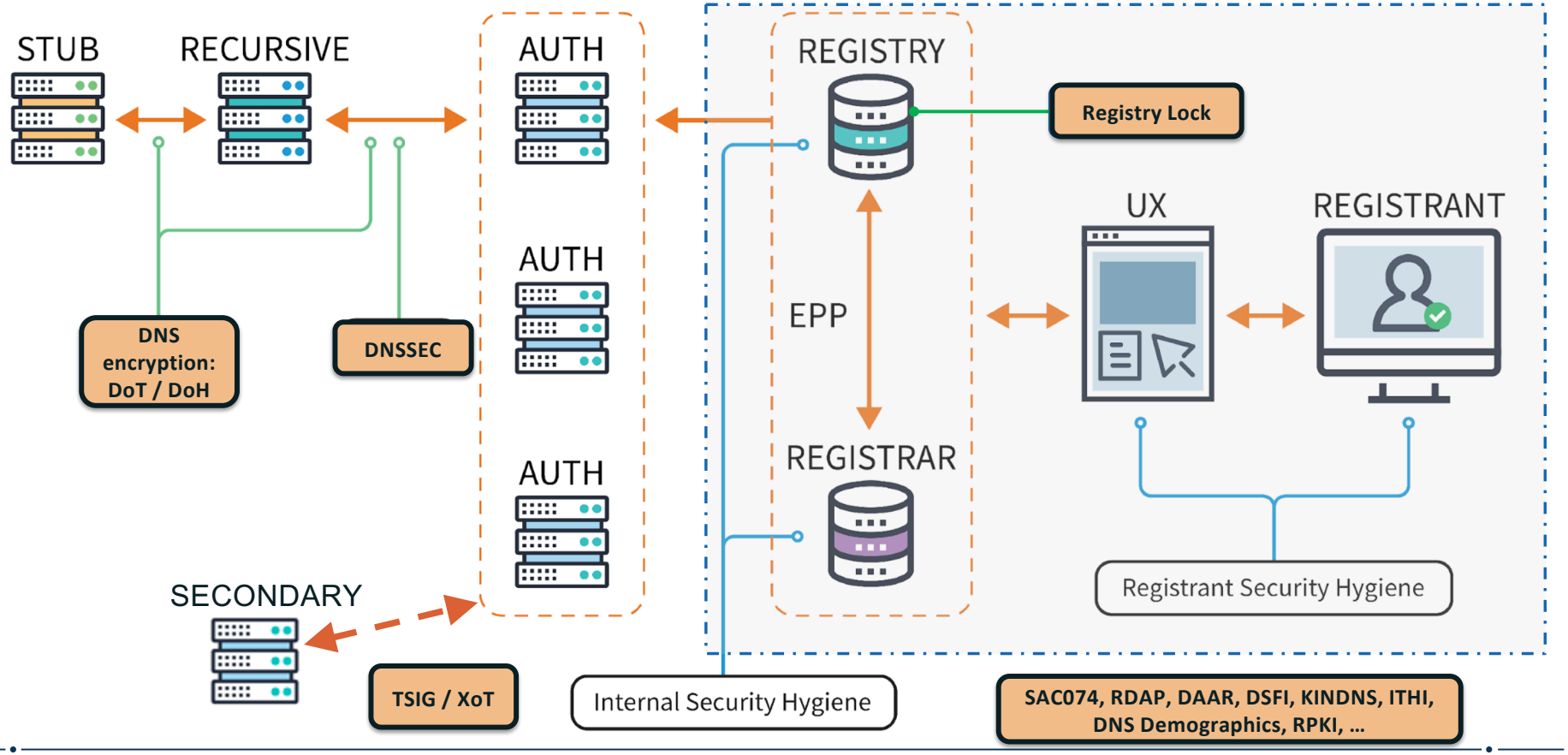


Securing Against DNS Attacks

- Recursive Server Protection
  - Access Controls
  - Rate Limiting
- Authoritative Server Protection
  - Redundancy
  - Anycast Servers
  - Switching off Recursion
- DNS Data protection
  - DNSSEC
- Protecting DNS transactions
  - TSIG (Secret Key Transaction Authentication for DNS) : RFC 8945, https://datatracker.ietf.org/doc/html/rfc8945
  - XoT (XFR over TLS): RFC 9103, https://datatracker.ietf.org/doc/rfc9103/ 

- Privacy/Confidentiality: DoT & DoH

Securing the DNS Ecosystem



DNS mechanisms for protection against SMTP Attacks

- Three DNS TXT records for SMTP security :

  SPF (**Sender Policy Framework**): a DNS record that declares which hosts are, and are not, authorized to use a domain name for the "HELO" and "MAIL FROM" identities. RFC 7208

  DKIM (**DomainKeys Identified Mail**): allows an entity to claim some responsibility for a message through a cryptographic signature. RFC 6376

  DMARC (**Domain-based Message Authentication, Reporting, and Conformance**): a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling. RFC 7489

Sanity Check (security Hygiene) on systems

Ensure all security patches have been reviewed and applied (to you DNS software);

Password/Authentication Hygiene

- *Review log files for unauthorized access, especially administrator access;*
- *Review and limit internal controls over administrator ("root") access;*
- *Enforce sufficient password complexity, especially length of password;*
- *Ensure that passwords are not shared with other users;*
- *Ensure that passwords are **never** stored or transmitted in clear text;*
- *Enforce regular and periodic password changes;*
- *Enforce a password lockout policy;*
- Enable multi-factor authentication on all systems, especially for administrator access;

Verify integrity of every DNS record, and the change history of those records;

Ensure that DNS zone records are DNSSEC signed and your DNS resolvers are performing DNSSEC validation;

Ensure your email domain has a DMARC policy with SPF and/or DKIM and that you enforce such policies provided by other domains on your email system.

Introduction to DNSSEC

What Is DNSSEC?

DNSSEC stands for **Domain Name System (DNS) Security Extensions.**

- DNSSEC is a protocol that is currently being deployed to secure the DNS.
- DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names.
- DNSSEC is the result of over two decade of community-based, open standards development.
- Specified in RFCs 4033, 4034, 4035 and 5155

DNSSEC in summary

- To achieve Authenticity and Integrity of DNS data
- Allows domain name registrants to cryptographically SIGN their DNS data
- Allows DNS operators to VALIDATE all DNS data passing through DNS resolvers
- Provide assurances to users that the DNS data they are seeing is valid and true
- Helps prevent DNS threats and abuses

What DNSSEC Does Vs what it doesn't do

- DNSSEC uses public-key cryptography and digital signatures to provide:

  Data Origin Authenticity : "Did this response really come from the *example.com* zone?"

  Data Integrity: "Did an attacker (e.g., a man in the middle) modify the data in this response since the data was originally signed?"

- DNSSEC offers **protection against spoofing** of DNS data

- DNSSEC **does not provide** any confidentiality for DNS data:

  no encryption

  Man in the middle-attack

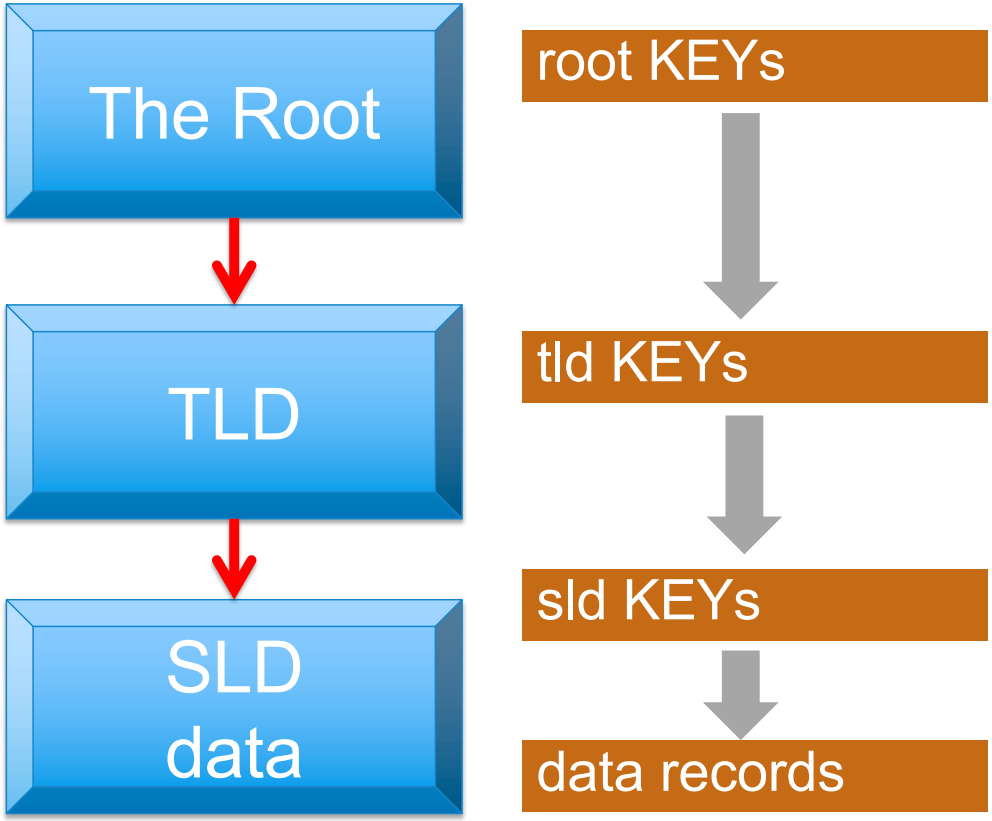
  DNS over HTTPS (DoH- RFC 8484) and DNS over TLS (DoT – RFC 7858) – more suited

- DNSSEC **does not address** attacks against DNS software: DDoS; BCP38

DNSSEC – Chain of Trust

- The root zone signs TLD keys
- A TLD (administrator) signs registrant keys
- A DNS zone administrator (registrant) signs their own data

This creates a "chain" used in validation



DNSSEC - Recommendations

- Registries/Registrars/DNS Operators
  - Offer DNSSEC services to registrants
- For Companies, Financial Institutions etc.
  - Sign your corporate domain names
  - Enable DNSSEC validation on corporate DNS resolvers
- Internet Service Providers (ISPs)
  - Enable DNSSEC validation on ISP resolvers
- Governments, Policy makers
  - Encourage DNSSEC compliance
- For Users
  - Request ISP to turn on validation on their DNS resolvers

Some DNSSEC statistics

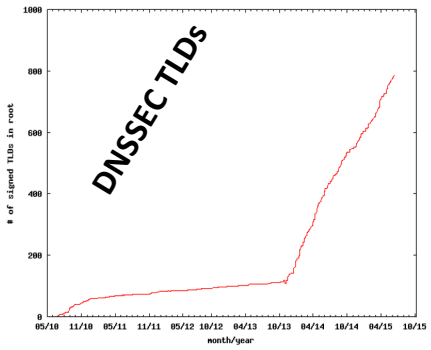
TLD DNSSEC Report (2021-08-25 00:05:37)

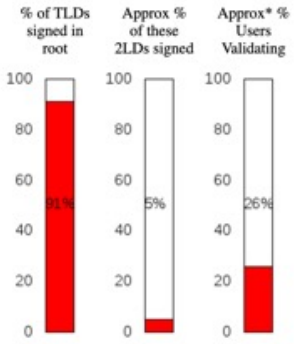
[archive] [latest]

Summary

- 1498 TLDs in the root zone in total
- 1380 TLDs are signed;
- 1372 TLDs have trust anchors published as DS records in the root zone;
- 0 TLDs have trust anchors published in the ISC DLV Repository.

http://stats.research.icann.org/dns/tld_report/





http://rick.eng.br/dnssecstat/

Unsigned ccTLDs : 35
Signed ccTLDs without DS in root zone : 2
Signed ccTLDs with DS in root zone : 21

DNSSEC signing in Africa ccTLDs, Aug. 2021
https://dnssec-africa.org/index.html

Use of DNSSEC Validation for World (XA)

https://stats.labs.apnic.net/dnssec/XA

Code	Region	DNSSEC Validates
XA	World	27.79%
XF	Oceania	37.54%
XE	Europe	34.94%
XC	Americas	31.72%
XD	Asia	25.33%
XB	Africa	23.70%

Discussion: what do you know about DNS privacy?

DNS Privacy

Encrypting DNS Data: Benefits

- Data privacy is good for end users
- Encrypting DNS traffic protects users from observers on the path between the stub resolver and the recursive resolver
- Encryption also prevents attackers from altering responses
- Analogue: using DoT and DoH increases the security of the DNS in a similar way that HTTPS helps secure web traffic
- However, this encryption prompts some major concerns and implications

DNS Encryption: Where?

- Until recently, stub resolvers appear only in operating systems
  - All applications call the OS for DNS service
- In the past few years, browsers (and other browser-like applications) have added their own stub resolvers
- The standards for DNS encryption assume that the client is acting as a stub resolver, and the server is acting as a recursive resolve
  - Note the “acting” part

DNS Encryption: How?

- Two Standardized Protocols:
  - **DNS-over-TLS (DoT) -** RFC 7858 and 8094 - https://datatracker.ietf.org/doc/rfc7858 and https://datatracker.ietf.org/doc/rfc8094
  - **DNS-over-HTTPS (DoH) -** RFC 8484 https://datatracker.ietf.org/doc/rfc8484
  - There are other non-standard protocols e.g. DNSCrypt
- DoT and DoH have a large amount of overlap, but the differences are important to network operators. For example:
  - DoT encrypts DNS traffic between stub resolver and recursive resolver, giving users authentication and confidentiality for their DNS queries; runs on TCP/853
  - DoH runs on TCP/443 and is co-mingled with *web traffic* in a single HTTPS connection, making it much harder to discover and filter

ICANN's Position

- Privacy is good
- Filtering of DNS can be beneficial
- Applications and OSs have insufficient information to make network control decisions, enforcement of legal mandates, and so on…
- DNS data should be protected
- OCTO 003: Local and Internet Policy Implications of Encrypted DNS
  https://www.icann.org/en/system/files/files/octo-003-30apr20-en.pdf

Current Developments

- Mozilla has partnered with Cloudflare to provide DoH and has embedded DoH into their Firefox browser
- Google through their public DNS service (8.8.8.8) supports DoH and can be activated on Chrome

DNS Encryption: What about the root zone ?

- Root Server Operators (RSO) do not feel comfortable being the early adopters of authoritative DNS encryption and have concerns about supporting DNS encryption for serving the root zone :
  - the critical role that root name servers play
  - often targets of DDoS attacks
  - Use of connection-oriented protocols and encryption data reduces performance of the name servers and may raise new types of denial-of-service attacks.
  - RSOs statement on DNS encryption: https://root-servers.org/media/news/Statement_on_DNS_Encryption.pdf
- Meanwhile, RSOs encourage the deployment of QNAME minimization and aggressive DNSSEC caching.

Qname minimization and aggressive DNSSEC caching

- Qname minimization (RFC 7816 - https://datatracker.ietf.org/doc/html/rfc7816):

  a technique that recursive resolvers use to send the shortest possible name to an authoritative server.

  In the context of the root zone, this means that recursive resolvers need only send the TLD portion of a particular name. For example, rather than send 'www.example.com', the recursive resolver can send a query for only 'com'.

- Aggressive DNSSEC caching (RFC 8198 - https://datatracker.ietf.org/doc/html/rfc8198):

  A recursive resolver technique to use DNSSEC data from negative responses to cache the fact that no names exist between a certain range. Avoid sending new queries to an authoritative for non-existent names.

RDAP

Registry Data Access Protocol (RDAP)

- RDAP is a protocol, designed in the Internet Engineering Task Force (IETF), to offer a directory service for the Internet's unique identifiers
- Standardized query (HTTP), response (JSON) and error messages (HTTP error codes + JSON)
- Offers secure access to data when used over HTTPS
- Is fully extensible

  easy to add query and output elements
- RDAP enables differentiated access

  e.g., limited access for anonymous users; full access for authenticated users
- Supports Universal Acceptance (any language/script)

RDAP is the new WHOIS

If you're familiar with Whois based on past decades of attribution work, RDAP is a wholesale replacement for Whois

- Whois is not a very robust protocol. RDAP is.
- Whois is not a secure protocol. RDAP is.
- Whois does not have a standard output format. RDAP does, enabling easy scripting of machine-readable output.
- Whois does not support multiple languages or character sets. RDAP does.
- Check out: https://lookup.icann.org

Some ICANN initiatives to support a Secure DNS Ecosystem

ICANN Org initiatives to Support a Secure DNS Ecosystem

- Though ICANN has no direct day-to-day operational role in the DNS, it has the mission to ensure its secured and scalable operation. It does that through several projects and initiatives such as:
  - Knowledge-sharing and Instantiating Norms for Domain Name Security (KINDNS)
  - DNS Abuse Activity Reporting (**DAAR)**
  - Domain Name Security Threat Identification, Collection, and Reporting (**DNSTICR)**
  - Identifier Technology Health Indicator (**ITHI)**
  - Domain Security Facilitation Initiative (**DSFI)**
  - Revised IMRS Strategy: https://www.icann.org/en/system/files/files/octo-016-26oct20-en.pdf
  - DNS Secured Operation Outreach/Training/Capacity Building programs: **Technical Engagement**

Additional resources

- TE Course Catalogue: https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en
- OCTO publications: https://www.icann.org/resources/pages/octo-publications-2019-05-24-en

  Recent Publication - A Primer in Registration Data Access Protocol (RDAP) Performance - https://www.icann.org/en/system/files/files/octo-024-17may21-en.pdf

  Recent Blog: “How ICANN Strengthened its Technical Engagement Around the World”: https://www.icann.org/en/blogs/details/how-icann-strengthened-its-technical-engagement-around-the-world-23-4-2021-en
- Domain Abuse Activity Reporting (DAAR): https://www.icann.org/octo-ssr/daar
- ITHI - https://ithi.research.icann.org/
- KINDNS - https://community.icann.org/display/KINDNS
- SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle: https://www.icann.org/en/system/files/files/sac-074-en.pdf

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