Domain Name Management & Security Best Practices

AFRALO Webinar Series

Brain Gutterman & Paul Muchene

28 April 2022

ICANN

Agenda

- Introduction
- Responsible Domain Name Registration and Management, Domain Name Management Best Practices
- Protecting your Domain Name
- Security Considerations and Best Practices
- DNSSEC
- DNS Privacy
- Takeaways and Q&A

AFRALO-AFRICANN ICANN73 Statement

DNS Abuse: Capacity Development for End Users

- Calls for increased capacity building and awareness around DNS Abuse as it relates to end-users.

Registants have a role to play in protecting end-users

Always Be Proactive

- Domain name registrants are important players in combating DNS abuse and protecting end-users.
- We encourage Domain Name Holders/Registrants to always be vigilant and proactive in securely and responsibly managing your domain name(s).

Domain Names are Valuable Assets

- For many registrants, domain names (and the services connected to them, like websites and emails) are essential to their professional and personal lives.
- Whether used for online commerce or simply to communicate with family and friends, domain names are valuable assets and should be managed with care.

Domain Name Registrants and the Domain Name Industry

Registries

Organizations that are responsible for maintaining the records of domain names registered under each top-level domain (TLD) e.g., .COM, .BANK.

Registrars

Domain names can be registered through different companies (registrars). The terms of your domain name registration, like fees, transfers, and renewals are governed your registrar.

Resellers

Companies affiliated with or under contract with registrars to register domain names and offer other services like web hosting.

Web Hosting Companies

Provide server storage space and an IP address for your website.

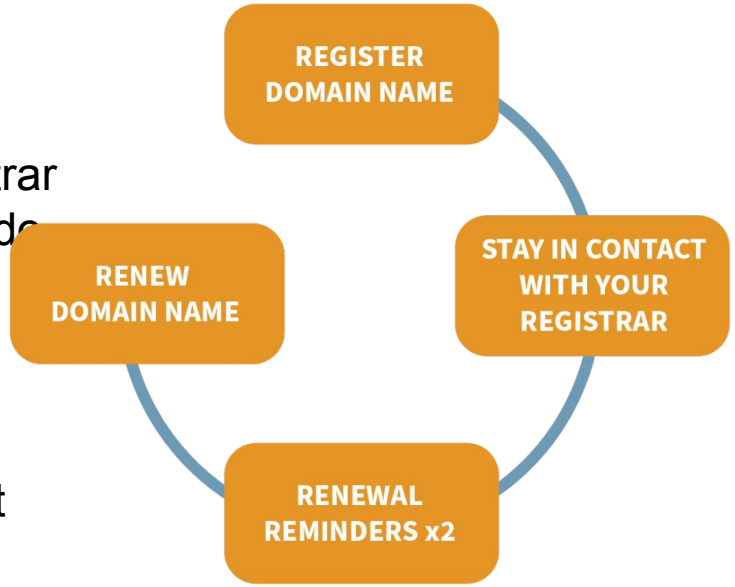
Registrants

Things to Know When Registering a Domain Name

- **Know who you are dealing with**. ICANN has accredited a number of companies for provision of domain-name registration services. We recommend dealing directly with an ICANN-accredited registrar. The full list of accredited registrars is available here.

- **Research the registrar's customer service**. Does the registrar offer the types of services you require? What type of support do they offer for their services? Do they have readily accessible contact information? What is their customer service record?

- **Read and understand the terms and conditions**. When registering a domain name online, you will be asked to accept the terms and conditions of a registration agreement. While it may be tempting to speed through this step and click "I AGREE," taking the time to read this first can save you from unpleasant surprises later.



Domain Name Management Best Practices

- **Keep contact information associated with your domain name registration up-to-date at all times** so you receive important notifications.
- When you register a domain name, you're able to use it for the period you registered it for, which is typically between one to ten years. If you want to keep using the domain name and any of the services associated with it (like a website or email service) you need to **renew the domain name registration prior to its expiration.** If you don't, you risk losing your domain name.
- Keep track of your domain name **expiration date** so you can renew it before it expires.
- **Consider the auto-renew option:** Most registrars offer auto-renewal option for domain name registrations. If you sign up for this service, be sure to keep payment information up-to-date.
- **Keep an eye out for renewal reminders.** Your registrar is required to send you two reminders.
- **Know the terms of your domain name registration**.

Know Who Your Registrar Is!

Registrant Rights

- As a domain registrant, you have certain rights and responsibilities, which include access to information from your registrar regarding processes for registering, managing, transferring, renewing, and restoring your domain name registration.

Contacting your Registrar

- If you run into issues managing your domain name, you can always contact your registrar. If you don't already have a point of contact, you can search for your registrar using ICANN's Lookup Tool: https://lookup.icann.org/

- If your registrar is not providing you with the necessary assistance/information, or is not contactable, you may reach out to ICANN's Global Support team or submit a complaint to ICANN Compliance.

Always remember to receive and save your registrar's contact information when you register a domain name!

Protecting your Domain Name

Protect Your Domain Name

- Remain hypervigilant with your domain name management.
- Be cautious of offers or warnings about renewing your domain name.
- Know your domain name's expiration date. If you are unsure of it, use the Lookup Tool.
- Check the sender's email address and phone number to ensure it is legitimate.
- Look out for suspicious links or language.
- Be suspicious of emails asking you to make immediate payments or requesting banking information.

Protecting your domain name(s)

Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Register with an email address that is not connected to your domain name.** When you register your domain name, you will be asked to provide contact information, including your email address. This information goes into the WHOIS record for your domain name, which might be viewed publicly. It is best to use an email address that is not associated with the domain name you are registering.

- **Here's why.** If your domain name is hijacked by someone who has gained access to your account with the registrar, that person will likely alter the WHOIS information to remove you as the registered holder of the domain name. If you used an email address that is not associated with your domain name in WHOIS, you will be able to provide that email address as evidence to the registrar that you were the registered holder of the domain name before it was altered by unauthorized access to your account.

Protecting your domain name(s)

(Contd.) Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Create a strong, unique password.** Protect your domain name from cybercriminals by creating a unique, strong password. Online services are compromised frequently, making user-names and passwords available to criminals who may attempt to hijack your domain name using the information you provide for other accounts. Avoid this by creating a strong password that you use exclusively for your domain name account.

- **Do not share your password.** You are responsible for the security of your domain name. You should never give anyone the login information to your online account. This includes web hosting providers or web designers as well as friends and colleagues. It is not recommended that you list website designers, hosting providers, or any other third parties as the registrant(s) of your domain name. If you choose to do so, seek legal advice as to contractual obligations that third parties should adhere to with regards to the administration of your domain.

Protecting your domain name(s)

(Contd.) Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Inquire about multistep authentication.** Some registrars offer registrants the ability to implement a multistep authentication when accessing your account. This provides added protection by requiring a unique security code, in addition to your username and password, to access your online accounts. Refer to the terms of your registration agreement to see if multistep authentication is available.

- **Check the email account(s) associated with your domain frequently.** Whatever email address or addresses you provide, you must be sure they are active accounts and that you check them regularly. You want to keep your contact information up to date to be sure you receive WHOIS Data Reminder Policy (WDRP) notifications, renewals, and other important notices from your registrar. This is particularly important for those who use a privacy or proxy service. If you use a privacy service, consider leaving your name as the registrant of record in the WHOIS. This can serve as another evidence to your registrar that you were the registered holder of the domain name.

Protecting your domain name(s)

(Contd.) Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Ask your registrar to put a *transfer lock* on your domain name.** You can request that your registrar put a *transfer lock* on your domain name. Putting this lock on your domain name is not a fail-safe way to guard against unauthorized transfer or hijacking of your domain name, but it could be another layer of security. Each registrar has a different way of implementing the transfer lock. Some require two-factor authentication to remove the lock; some simply require authorization from the registrant. Check with your registrar about their policies regarding transfer lock and decide whether it is a service that's right for you.

- **Be smart about your online behavior.** Be cautious with the links you click in emails, with the attachments you open, and with the websites you visit. These are means that criminals can use to steal your username and password.

Beware of Phishing Scams

- Phishing attacks are a type of fraud that cybercriminals utilize to lure others online, including registrants, into doing what the criminals want them to do. Phishing may result in others voluntarily giving away their username and password or clicking a link that will lead to their devices being infected with malware, which is software that, when installed, performs unwanted or malicious activity.
- If an attacker can gain access to a registrant's private domain name registration information and passwords, they can potentially redirect the domain to wherever they like. As such, it's immensely important that you take note of any suspicious or unsolicited emails.

Beware of Phishing Scams

- Phishing emails may claim that your domain name registration needs to be renewed and that you must pay some sort of fee to get it back. These malicious campaigns typically use deceptive techniques such as forging a trusted sender's address or domain or using a similar or lookalike domain. Phishing messages typically ask for the reader to reply, call a phone number, click a link, or open an attached file, which results in stealing personal information or gaining some other advantage over the victim.
- Sometimes phishing emails aimed at registrants may appear to come from ICANN (even using ICANN's branding and logo or sender email addresses containing the name "ICANN"). It is important to know that ICANN does not send emails directly to registrants about managing their domain names, and never requests payment of fees from registrants.

Protecting yourself from Phishing

- Carefully review every email you receive
- Phishing emails and websites often mirror familiar visuals and language, may include the logos and branding of the organization and appear that the organization is the sender
- Be suspicious of any email or webpage from ICANN that offers domain renewals or registration services.
- ICANN org does not process domain renewals or send WHOIS data privacy notices.

Measures for additional protection

- Be suspicious of any email that offers domain name management services from ICANN. ICANN does not offer domain name management services or process domain registrations and will never collect fees from registrants directly.
- ICANN will never send registrants a WHOIS Data Reminder Policy (WDRP) notice, registration data verification request, domain name expiration reminder, or domain name renewal request message. If you receive an email about your domain that purports to come from ICANN, contact your sponsoring registrar directly to enquire about the validity of that message.
- Contact your sponsoring registrar directly for any concerns about the status of your domain name.

QUIZ

- When registering a domain name and creating a username and password associated with an email address for managing the domain name, what are some best practices to follow?

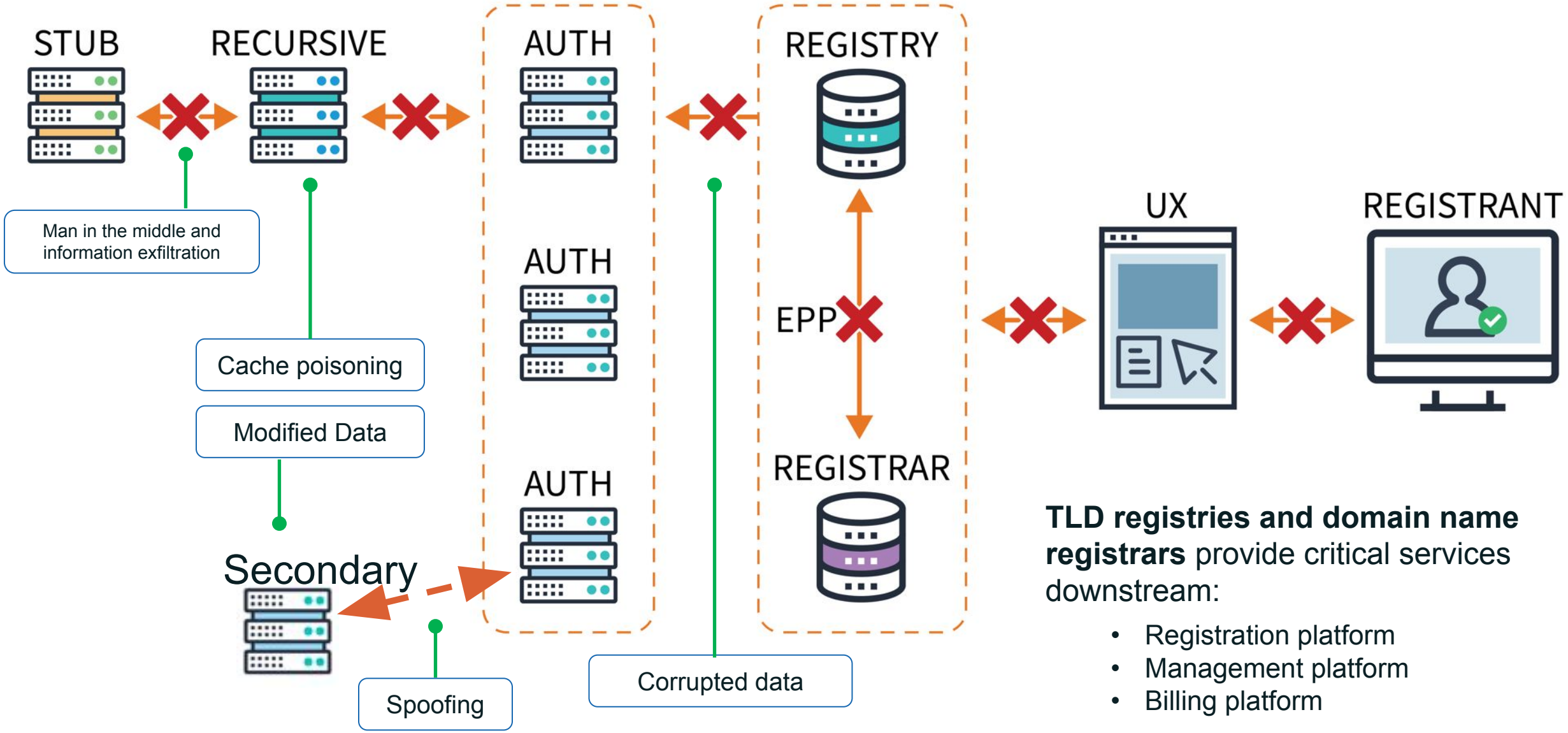
  A) Use the same email address you used to register the domain name and create a short and simple password that is easy to remember.

  B) Use a different email address than you used to register the domain name, and create a password associated with your birthday that you can easily share with others.

  C) Use a different email address than you used to register the domain name and create a strong and unique password (and don't share it with others).

Security Considerations and Best Practices

Some of the Potential Target Points of the DNS Ecosystem



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

Securing Against DNS Attacks

- Recursive Server Protection
  - Access Controls
  - Rate Limiting
- Authoritative Server Protection
  - Redundancy
  - Anycast Servers
  - Switching off Recursion
- DNS Data protection
  - DNSSEC
- DNS Privacy/Confidentiality: DoT & DoH
- 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/

Sanity 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;

Security Hygiene on systems (Continued)

- ✔ 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.

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

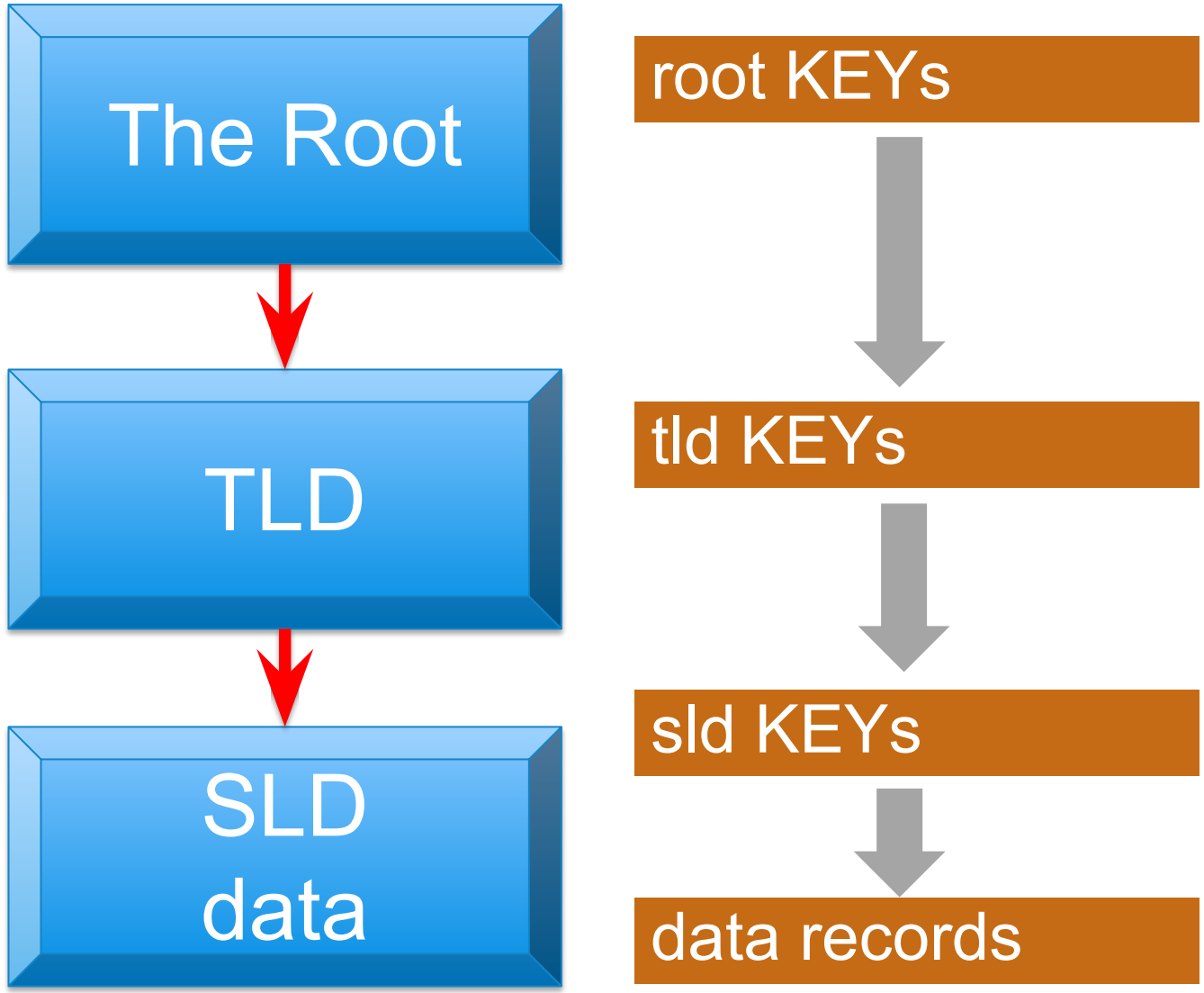
What DNSSEC does & what it doesn't do

- 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

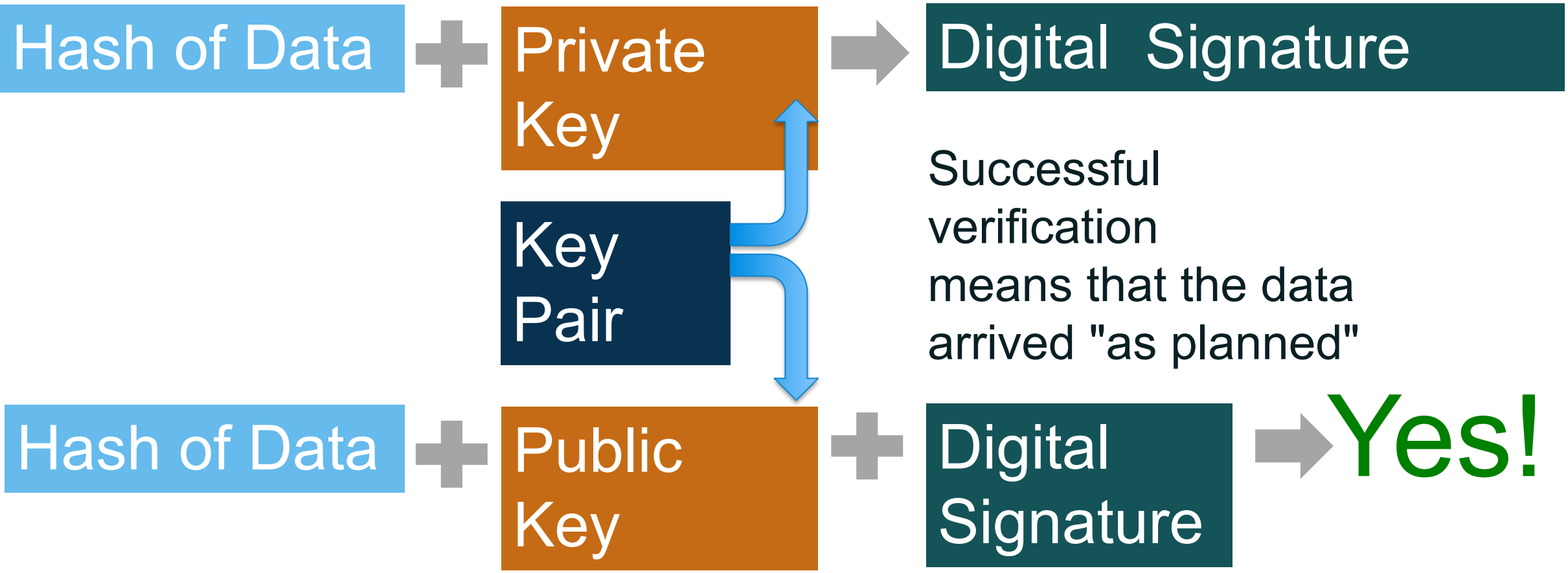
This creates a "chain" used in validation



DNSSEC Validation

- DNSSEC validation is the process of **checking the signatures** on DNSSEC data
- Validation can occur in applications, stub resolvers or recursive resolvers.
- Most validation today occurs in recursive resolvers.
- Trust Anchor: To perform DNSSEC validation, you have to trust somebody (some zone's key). **Root Zone KSK is the most important trust Anchor on the Internet. You can view root key signing ceremony on YouTube.**
- What happens when validation fails?
  - The recursive resolver protects the user by sending a "SERVFAIL" error response.

DNSSEC Validation



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 Can You Do?

- 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 End users
  - Request ISP to turn on validation on their DNS resolvers

DNS Privacy

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

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, encryption of DNS queries prompts some major concerns and implications.
- 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 embedded DoH into the Firefox browser and has partnered with some open public resolver operators to provide DoH.
- Google through their public DNS service (8.8.8.8) supports DoH and users can activate DoH on the Chrome browser.
- Both Brave and Apple’s Safari browser now support DoH

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.

QUIZ

- DNSSEC protects the confidentiality of DNS Data

  A) TRUE

  B) FALSE

Takeaways and Q&As

Takeaways

- Domain Name Holders (Registrants) have a role to play in combating DNS Abuse and protecting end-users.
- Domain Name Holders (Registrants) should be proactive and vigilant in managing their domain names and communicating with their Registrars about issues that may arise.
- The DNS is still evolving and so are the security challenges.
- Security is built into layers and neither DNSSEC nor DoT nor DoH will provide a panacea for security.

ICANN Learn

- Free, online learning platform: https://learn.icann.org
- Set your dashboard to your preferred language.
- 302.1 - Registrant Basics: Essentials for Domain Name Holders.
- 400.1 - Cybersecurity Basics
- 602.1 - DNS Fundamentals

DNSSEC Deployment Guidebook

- OCTO published the document OCTO 029 titled “DNSSEC Deployment Guidebook for ccTLDs”: https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf
- Documents best practice and considerations before deploying DNSSEC
- Other OCTO Publications: https://www.icann.org/octo/publications
- Download and read the publication and feel free to drop an email: octo@icann.org

Ask Questions and Provide Feedback

Questions & Feedback

Connect with us

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