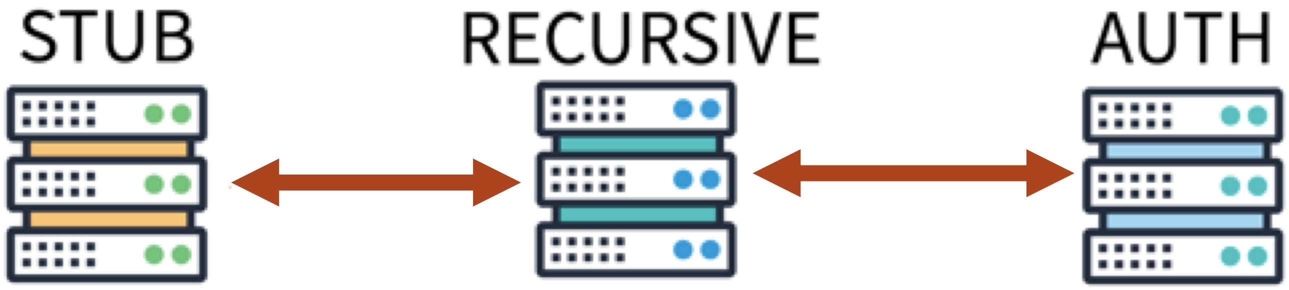
What’s Going On In The World of DNS

SANOG34 – Kolkata - India

Champika Wijayatunga
ICANN

July 2019

DNS Resolution’s Traditional Model



Stub <-> Recursive <-> Authoritative

- Stub resolvers are part of a device’s operating system
- Recursive resolvers are typically run by the service provider (e.g., an ISP, or a university, or a company, etc.)

Because the service provider controls the recursive resolver, many of the *needs* of the service provider are met. For example:

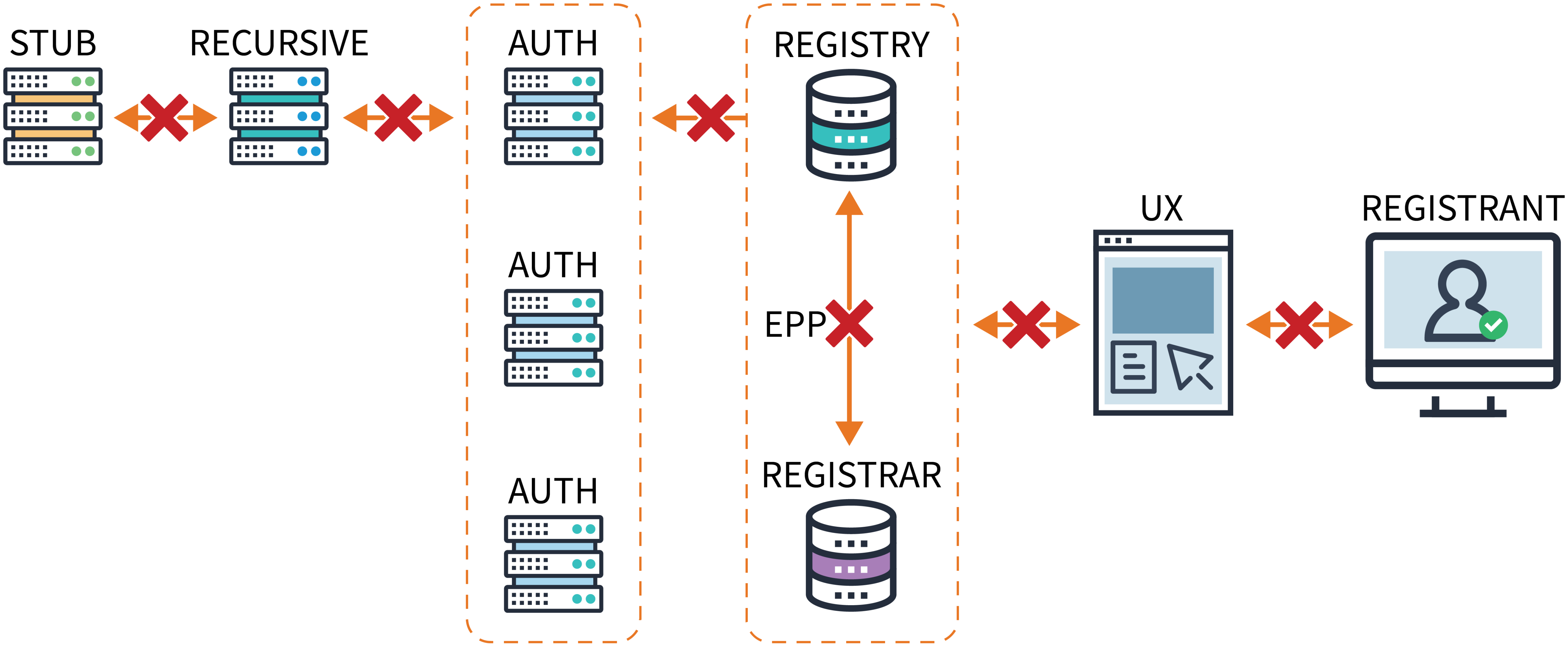
- Regulatory compliance
    - Searches for certain key words that the government requires be logged and/or not responded to
- Malware Protection
    - Service providers know to block access to certain sites that seek to harm the end users

But the Traditional Model has Some Security Concerns

“The DNS is one of the most significant leaks of data about an individual’s activity on the Internet.” – Sara Dickinson, Sinodun

- DNS queries are sent in cleartext (UDP or TCP) which means anyone doing passive monitoring of our DNS learns everything we are asking
- Queries contain the domain names being asked about, but also contain *metadata* about domains for things like the chat services we are using and the domains of our email contacts
- VPNs are not a full solution because some VPNs *leak* DNS data by sending the queries over unencrypted channels
- DNS responses from the recursive to the stub are the most vulnerable to being censored or re-written

Potential Target Points of the DNS Infrastructure/Ecosystem



One Solution is to Encrypt

- **Encryption provides privacy assurances:**
  - Queries cannot be surveilled
  - Eliminates man-in-the-middle attacks

- In 2017 and 2018, the IETF standardized two encryption technologies for DNS:
  - DNS-over-TLS (DoT)
  - DNS-over-HTTP (DoH)

DNS-over-TLS (DoT)

- **DoT (RFC 7858)** takes advantage of Transport Layer Security (TLS) to encrypt DNS traffic between the stub resolver and the recursive resolver, giving users authentication and confidentiality for their DNS queries
    - Runs on TCP/853 instead on UDP/53
    - Useable by any application taking advantage of TLS
        - Email, Mobile apps that use TLS, Popular sites like Facebook
- Does not impact the network operator, ISP, enterprise, or local government's requirements to monitor or enforce local policy.

DNS-over-HTTPS (DoH - RFC 8484)

- Who do you trust?
  - "I trust my bank to give them my money."
  - "I trust my bank enough to do online banking with them."
  - "Maybe my bank is the most trusted vendor I should use for recursive resolver service."
- The Trusted Recursive Resolver (TRR) model
  - The user decides who she trusts the most with her DNS traffic, and configures the DoH application to use a trusted DoH resolver
- Runs on TCP/443 and is co-mingled with *web traffic* in a single HTTPS packet, making it much harder to discover and filter

Public Resolvers

- A recent measurements into resolver centrality has shown that it takes about 8 to 9 resolvers to cover the request of 50% of the internet users.

  - Google Public DNS alone (4.4.4.4 and 8.8.8.8) answered about 33% of the queries
  - Other big global resolvers included China Unicom, China Mobile, DNSpai, Comcast, and OpenDNS (Cisco Umbrella)
  - There are quite a few large public DNS operators these days, including:
    - Cloudflare (1.1.1.1)
    - Quad9 (9.9.9.9)
    - TWNIC (101.101.101.101)

Potential Impacts

But This New Model Prompts Some Concerns

- **Service providers have a new paradigm to negotiate:**
  - *No longer able to use DNS to meet needs like regulatory compliance and malware protection*
  - *What happens if it does not work? The user configures her web browser to use a DoH resolver. For whatever reason, DNS resolution stops working properly. A major concern for service providers is that the user now calls them and asks for help.*
  - *ISPs do significant business working with parents on parental controls. When applications do their own DNS, a lot of these parental controls no longer work.*
  - *ISPs often receive court orders to block certain sites. DoH resolvers do not know about these court orders, and still resolve these sites.*

Public Policy Concerns

- Stepping back from the service provider concerns, **DoH introduces all new challenges for broader public policy:**

  - Which laws apply?
    - In the traditional model, the recursive resolver providing the answers to the end user device is generally found in the same country as the user. Applications doing their own DNS with DoH will sometimes mean that the recursive resolver is in a different country, which means a different legal jurisdiction.
    - Very important when you think about complex topics like content filtering laws and end user data privacy regulations

Taking a Further Step Back

- **Stepping back from the service provider concerns, DoH introduces all new challenges for broader public policy:**
  - Who gets to determine the DoH resolver?
    - The DoH protocol was designed to allow the end user to decide who they trust most for recursive DNS service. But nothing stops the application maker from deciding *for the user* what DoH resolver will be used.
    - What if the application maker is not honest and is purposely using a DoH resolver which steers queries away from their intended sites and instead, provides DNS answers to sites that the application maker can profit from?
    - What if the DoH resolver operator is monetizing DNS data without the user's consent?
    - Bad or dishonest implementations of DoH *disempower* end users, and do so in a context that most end users know nothing about: recursive DNS resolution

Parting Thoughts on Applications Doing DNS (ADD)

- Applications doing their own DNS with DoH is new, but it is already being implemented in web browsers and mobile applications. As an operator or as a policy maker, it’s a good time to pay attention to how vendors are implementing ADD.

- DNS abuse continues to be an issue. Since DNS is a gateway into your systems, it is important to prioritize it in your policy making and security efforts

- DNS privacy – especially end user DNS data privacy – is a major regulatory and societal concern. You need to consider how better end user privacy in the DNS reconciles with certain top-down regulations (e.g. filtering)

- Encrypting data with TLS or HTTPS is good for addressing privacy concerns

- But implementation details matter, and there are a lot of public policy concerns for how DoH could be implemented in a way that has negative effects for end users, for service providers, and for regulators.

Moving Forward

- Where do we discuss these broad issues?
  - ICANN?
  - Network Operator forums?
  - IETF?
  - Regional/Local public policy forums?
  - Etc.
- The answer is probably: all of the above. Which imply that consultation and collaboration will be needed to identify issues and find resolutions.

Get Involved and Informed

Attend an ICANN Public Meeting. Three times a year, ICANN holds free and open public meetings in different regions around the world. Visit **meetings.icann.org** to learn more.

Visit **go.icann.org/journey** to learn how you can attend an ICANN Public Meeting as part of the NextGen@ICANN or ICANN Fellowship programs.

Take a free online course at **learn.icann.org**.

Attend events in your region.

Find and participate in an ICANN community group by visiting **icann.org/community**.

Sign up for ICANN news alerts and regional newsletters.

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