Strengthening the DNS service (security & privacy)"

John Crain
ICANN’s Office of the CTO

Sept 2019
DNS Resolution Components at a Glance

- Recursive Name Server
  - Name Server
  - Resolver
  - Cache

- Stub Resolver
  - API call

- Authoritative Name Server
  - DNS queries and responses

- Authoritative Name Server
  - DNS queries and responses

- Authoritative Name Server
  - DNS queries and responses
DNS Resolution’s Traditional Model

Recursive resolvers are typically run by the service provider:
- The ISP
- The University
- The Company

Increasingly, recursive resolvers are operated by public DNS providers:
- Google: 8.8.8.8
- Cloudflare: 1.1.1.1
- TWNIC: 101.101.101.101
- ... and many, many others
But These Resolution Models have 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
- Some VPNs don't include the resolvers the user might have chosen, and in that case the DNS traffic will be exposed in unencrypted channels
- DNS responses from the recursive to the stub are the most vulnerable to being censored or re-written
From the Stub to the Recursive

(Applications Doing DNS - ADD)
DNS Resolution Components at a Glance

- **Recursive Name Server**
- **Name Server**
- **Resolver**
- **Stub Resolver**
- **API call**
- **DNS query and response**
- **Cache**
One Solution is to Encrypt

- Encryption provides 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)

- TLS is Transport Layer Security
- TLS is used by applications like email or mobile apps to keep our data secure
- DoT takes advantage of 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 (making it easy to discover and filter)
DNS-over-HTTPS (DoH)

Protocol Goals (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 user decides who she trusts the most with her DNS traffic, and she 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 connection, making it much harder to discover and filter
But This New Model Prompts Some Concerns

Service providers have a new paradigm to negotiate: No longer able to rely only on DNS to meet regulatory compliance requirements and/or filtering goals

- 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 protect users by denying access to malware sites. DoH/DoT circumvent this protection.

- ISPs often receive court orders to block certain sites. DoH/DoT resolvers may not know about these court orders, and still resolve these sites.
Many Questions

○ Who gets to determine the 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 resolver will be used.

○ Applications are likely to ship with their own chosen Trusted Recursive Resolver (TRR)
  • Firefox ships with Cloudflare 1.1.1.1. as default TRR

○ Will this mean different behaviors dependent on app?
Stepping back from the service provider concerns, ADD introduces all new challenges for broader public policy:

- Where do we discuss these broad public policy issues?
  - ICANN?
  - LACTLD?
  - Network operator forums?
  - IETF?
  - Regulators?

- The answer is probably all of the above. Through community consultation and collaboration we can identify issues and find resolutions.
Applications doing their own DNS with DoH is new, but ADD in general is already being implemented in web browsers and mobile applications.

DNS privacy – especially end user DNS data privacy – is a major regulatory and societal concern.

Encrypting DNS 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 ADD could be implemented in a way that has negative effects for end users, for service providers, and for regulators.
From the Recursive to the Authorative

DNS Private Exchange (DPRIVE)
DNS Resolution Components at a Glance

- Recursive Name Server
  - Name Server
  - Resolver
  - Cache

- Authoritative Name Server

DNS queries and responses
Data Minimization.

- Only send the part of the query that the authoritative server needs to answer

- Query the Root Servers for the TLD only
  - Instead of querying for www.icann.org ask for .org

- Query .org name servers for second level only
  - Instead of querying for www.icann.org ask for icann.org

- And so forth.....
Solutions focus around DoT

853/TCP

But how to discover the keys to use for encryption?

One proposed solution is to use DNS-based Authentication of Named Entities (DANE) to place public keys in the DNS.
Where are we now
ADD or DoT and DoH

- DoT is deployed and works over 853/TCP
  - RFC 7858 – Specification for DNS over Transport Layer Security (TLS)
  - RFC 8310 – Usage Profiles for DNS over TLS and DNS over DTLS

- DoH is being deployed and works over 443/TCP
  - RFC 8484 - DNS Queries over HTTPS (DoH)
Not yet standardized but it is coming

Most likely 853/TCP

Follow the DPRIVE wg at IETF

https://datatracker.ietf.org/wg/dprive/about/
Other good resources

- The DNS Privacy Project
  - [https://dnsprivacy.org](https://dnsprivacy.org)

Very Recent

- The Encrypted DNS Deployment Initiative
  - [https://encrypted-dns.org](https://encrypted-dns.org)
Engage with ICANN – Thank You and Questions

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