Local and Internet Policy Implications of Encrypted DNS

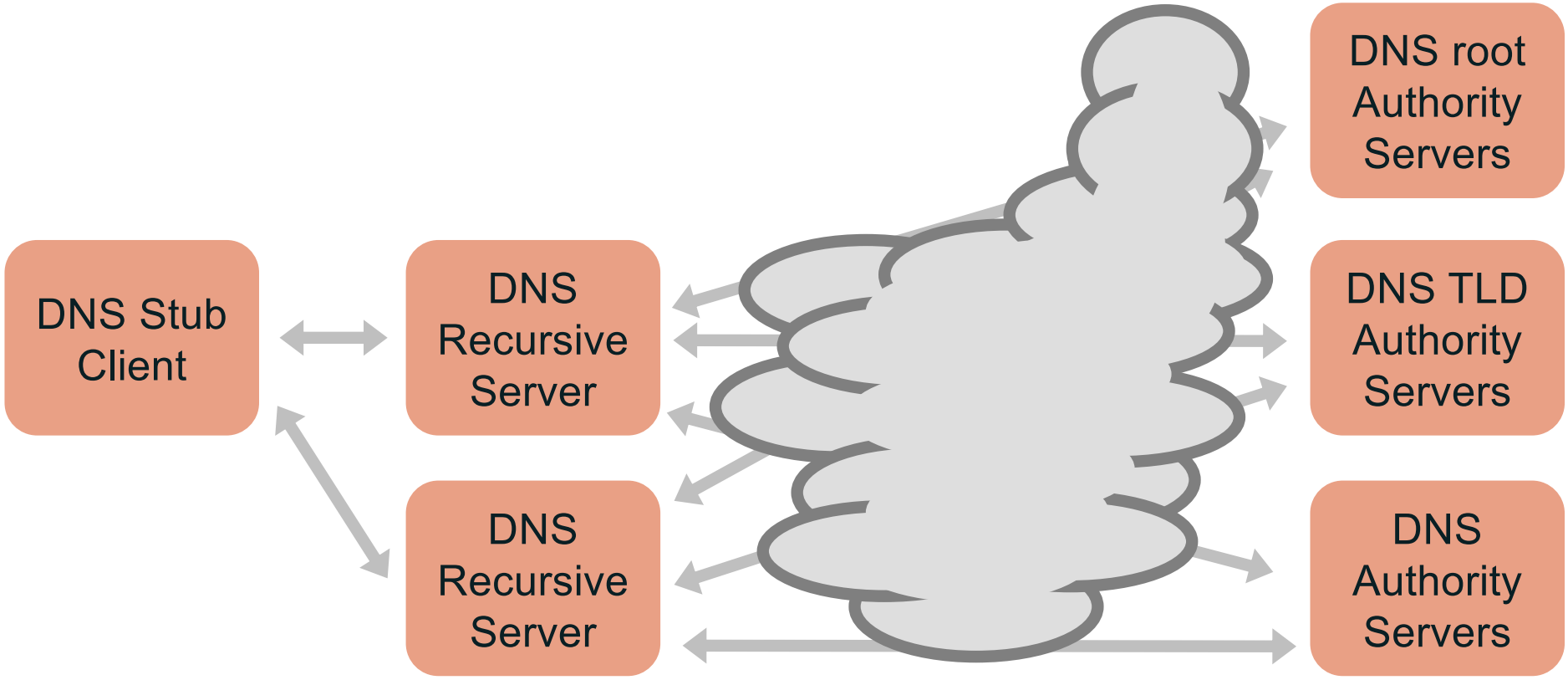
Paul Hoffman

ICANN 67 At-Large Policy Session
10 March 2020

ICANN's document

- *Local and Internet Policy Implications of Encrypted DNS*
- OCTO-003 (from documents produced by OCTO's Office of the CTO
- https://www.icann.org/en/system/files/files/octo-003-en.pdf
- Different focus and different origin from the SSAC document
- Broad topics:
  - Filtering and monitoring in the DNS
  - Policy implications
  - Interested parties
  - ICANN's positions

DNS participants



All those grey arrows are unencrypted communication

“Encrypted DNS” is about the ones on the left, from the stub clients to the recursive servers

DNS encryption: where

- For now, encrypted DNS starts in a stub resolver and ends at the recursive resolver
- 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 resolver
  - Note the “acting” part

DNS encryption: how

- Two standardized protocols:
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)
  - There are other non-standard protocols, but they only have thin deployment
- DoT: https://datatracker.ietf.org/doc/rfc7858/
- DoH: https://datatracker.ietf.org/doc/rfc8484/
- DoT and DoH have a large amount of overlap, but the differences are important to network operators

DNS-over-TLS

- Basically: the stub resolver starts a TLS session with the resolver, and when the session is established, starts sending regular DNS traffic over it
- Authentication of the resolver is optional but needed to prevent on-path attacks
  - Without authentication, the traffic is still unreadable by attackers watching from the outside
- Easy to set up: just need an IP address or domain name for the resolver (the port number is fixed)

DNS-over-HTTPS

- Basically: the stub resolver starts an HTTPS session (like normal web browsing) with the resolver, and when the session is established, starts sending DNS traffic that has been wrapped in HTTP queries over it
- If the HTTP is version 2, the server can also push DNS content to the client, which the client can use or discard
- Authentication of the resolver is mandatory because it is mandatory in HTTPS
- A bit harder to set up than DoT: need a URL
- DoH can re-use existing HTTPS connections because the service is based on the URL

Policy implications

- Increased privacy for users' DNS traffic
- Increased assurance for users' DNS traffic
- Circumvention of DNS filtering for security
- Circumvention of DNS filtering for local policy
- Circumvention of DNS filtering that is mandated by governments
- Unwanted centralization of DNS resolution cannot be detected
- Speed of DNS responses

Increased privacy and assurance

- Privacy is a general good
- Encrypting DNS traffic protects users from observers on the path between the stub and resolver
- Encryption also prevents attackers from changing the traffic in responses
- Using DoT and DoH increases security for the DNS similar to using HTTPS in the web

Circumvention of filtering

- Network operators often filter or monitor DNS for the benefit of their users, or at least for the benefit of the health of their systems
- Middleboxes that filter DNS for security (such as to prevent malware) and/or local policy (such as parental controls), are thwarted by encrypted DNS
- Some filtering is mandated by the governments in some jurisdictions, so encrypted DNS can prevent those who are required to filter from complying with the law

Unwanted centralization

- Clients that implement encrypted DNS can change where the OS or application goes for DNS resolution
  - So can unencrypted DNS, but doing that makes it much more obvious that a change was made
- So far, this has been done only by Firefox in the US
  - Their reasoning is that they only trust certain resolver operators to keep Firefox users' data private
  - They have a list of trusted providers, but that list currently has only two operators
- Concerns about privacy, reduced diversity leading to worse resiliency, ossification, ...

Speed of responses

- Starting a TLS session inherently is slower than just sending a bare DNS query
- Overloaded resolvers might have long TLS startup times
- DoH also requires converting DNS queries to HTTP messages
- However, early data indicates that while 90% of responses are very slightly slower, the last 10% of responses are much faster because TCP is more reliable than UDP

ICANN positions

- 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

Recent updates

- Mozilla is greatly expanding their program in the US (but, so so far, nowhere else)
- Microsoft announced that it will add secure upgrade for resolver connections to Windows using DoH (not DoT)
- More network operators have gotten involved in the discussions of how encrypted DNS should be deployed