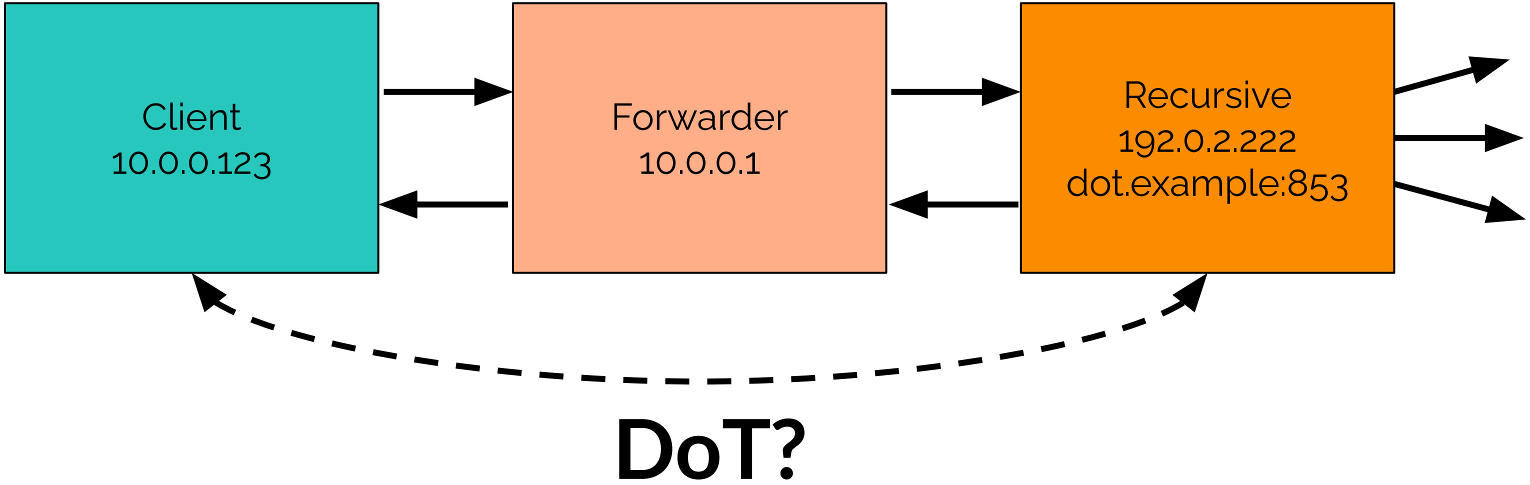
# DDR and Forwarders

Ben Schwartz (Google), Tommy Jensen (Microsoft)

ADD, IETF 111, July 2021
Slides v00

# The Scenario


Client
10.0.0.123

Forwarder
10.0.0.1

Recursive
192.0.2.222
dot.example:853

DoT?

# Or see DDR Requirements Section 5

| | |
|---|---|
| R4.1 | If the local network resolver is a forwarder that does not offer encrypted DNS service, an upstream encrypted resolver SHOULD be retrievable via queries sent to that forwarder. |
| R4.2 | Achieving requirement 4.1 SHOULD NOT require any changes to DNS forwarders hosted on non-upgradable legacy network devices. |

https://datatracker.ietf.org/doc/html/draft-ietf-add-requirements#section-5

# In scope (for this requirement)

- **Legacy forwarders**
  - i.e. forwarders that do not implement DDR, whose DNS filtering behavior (if any) cannot be updated, on networks that cannot implement DNR
- **Reluctant forwarders**
  - i.e. forwarders that would prefer clients to use E2E encrypted DNS directly to the upstream resolver

# Out of scope (not impacted)

- Forwarders that implement DDR
- Forwarders on networks that implement DNR
- Forwarders whose upstream resolver doesn't offer Encrypted DNS
- Forwarders with updatable filtering
  - e.g. age-appropriate content filters, malware control domain filters
  - **They can (and SHOULD) add "resolver.arpa" to the filter list** to disable upgrade, as with Mozilla's "use-application-dns.net".

# The question

- The client has been provided with a DNS server whose **IP address is "private"** (e.g. RFC 1918 space)
- This server forwards queries for "_dns.resolver.arpa" to an upstream resolver, and r**eturns the response unmodified**.
- The upstream resolver **supports Encrypted DNS**, and provides a SVCB response for _dns.resolver.arpa.
- The client has sent this query, and received a response.
- **What should the client do?**

# DDR draft-02: No Upgrade For You

“If the IP address of a Designated Resolver differs from that of an Unencrypted Resolver, clients MUST validate that the IP address of the Unencrypted Resolver is covered by the SubjectAlternativeName of the Encrypted Resolver's TLS certificate”

No Private IPs in certificates -> Validation fails -> No upgrade

# PR #11: You Can Upgrade For Now

“If the client does not have a Validation Identity ... the client SHOULD limit the validity duration of the discovered information (e.g. the SVCB response TTL) to no more than 5 minutes.”

# Security: active vs. passive attack

### DDR-02

This scenario remains unencrypted, **vulnerable to passive attack**.

Connections to DDR-enabled local DNS servers are secure unless **there is an active adversary on the local network**.

### PR #11

This scenario supports encryption, **not vulnerable to passive attack**.

Connections to DDR-enabled local DNS servers are secure unless **there was an active adversary on the local network at the time of the last DDR refresh (≤5 minutes)**.

# Forensics, logs, and active attacks

### DDR-02

**Random sample** of detailed network logs is likely sufficient for manual retrospective detection of an active attack.

User DNS traffic can be hidden from logging during an attack (**while** the attacker is present).

Logging forwarders **can be purely pass-through**.

### PR #11

Logs **must capture a specific packet** (the attacker's DDR designation response) to enable retrospective detection.

User DNS traffic can be hidden from logging during an attack (**potentially after** the attacker was present).

Logging forwarders **must respond for resolver.arpa**.

# Intentional Forwarders (no change)

### DDR-02

“**A DNS forwarder SHOULD NOT forward queries for "resolver.arpa" upstream**. … A DNS forwarder which already acts as a completely blind forwarder MAY choose to forward these queries when ... the operator expects clients of the unencrypted resolver to use the SVCB information opportunistically.

### PR #11

“clients may bypass DNS forwarders that forward queries for "resolver.arpa" upstream. **If this is not the forwarder's intended behavior, it SHOULD NOT forward these queries upstream**.”

# Paths forward

A. Move PR #11 into DDR
B. Move PR #11 into a separate draft
C. Split all local-IP-based discovery into a separate draft
D. Drop R4.1 and R4.2 from the WG requirements
E. Call this a “client policy” matter and reduce use of normative language