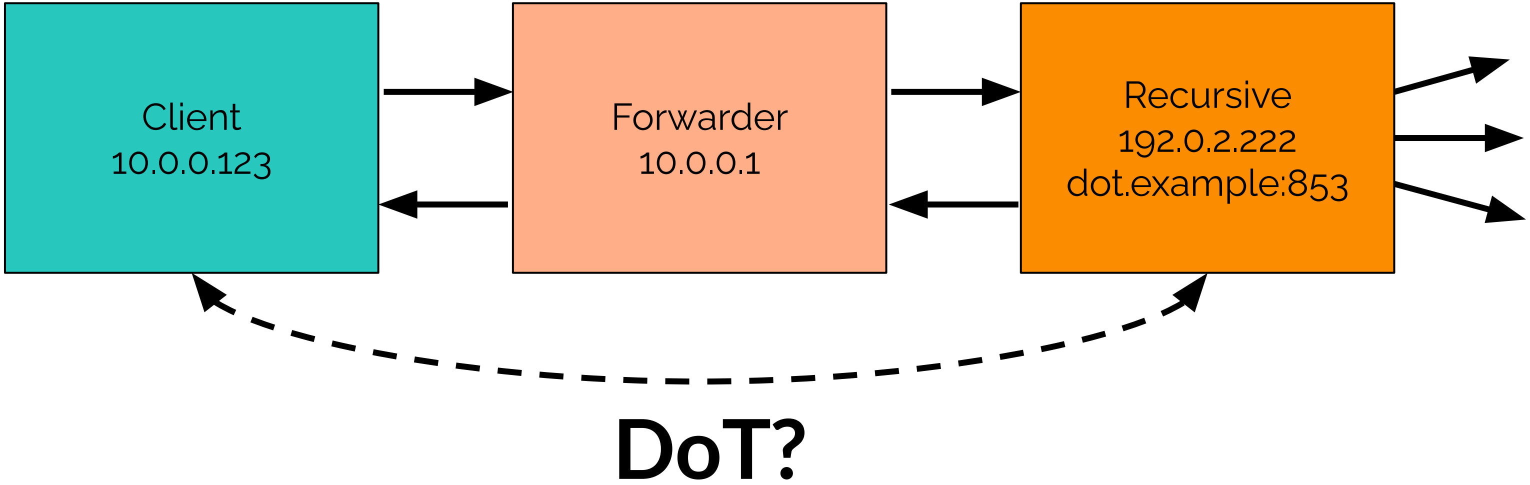
DDR in the Presence of Legacy Forwarders

Intended Status: Informational
Ben Schwartz, Chris Box
ADD, IETF 112, November 2021

The Scenario



Client
10.0.0.123

Forwarder
10.0.0.1

Recursive
192.0.2.222
dot.example:853

DoT?

Background

- This is an “opportunistic encryption” situation.
  - There is no securely sourced validation identity for the DNS server.
  - In DDR active adversaries always win, but we have the opportunity to prevent eavesdropping.
- DDR says:
  - A client MAY use information from the SVCB record for "dns://resolver.arpa" with this "opportunistic" approach (not validating the names presented in the SubjectAlternativeName field of the certificate) as long as the IP address of the Encrypted Resolver does not differ from the IP address of the Unencrypted Resolver.
- This excludes cross-forwarder upgrade.

This draft

- Informational
  - No normative language.
- Describes a “Relaxed Validation client policy”
  - “removes the certificate validation requirement when the Unencrypted Resolver is identified by a private IP address”
- Discusses the compatibility and security issues that this raises
- Mentions various relevant mitigations for these issues.

Compatibility non-issues

- Malware and threat domain filtering and service category restrictions
  - Just add “resolver.arpa” to the list.
- Time of use restrictions
  - Not implemented via DNS
- Upstream resolver services
  - Still using the same upstream resolver

Security concerns

- Makes transient attackers more powerful
  - A transient attacker could inject a long-lived DDR response.
  - Mitigations:
    - TTL limits on DDR
    - Resolver reputation systems, i.e. the client can choose to only connect to authenticated encrypted resolvers with sufficiently good reputation.
- Might bypass forensic logging (e.g. random sampling)
  - Mitigation: Make sure to log any DDR responses

Compatibility concerns

- Split-horizon namespaces
    - Mitigation: NXDOMAIN Fallback
- “Interposable domains” (e.g. SafeSearch CNAMEs)
    - Mitigation: Exemption list
- Caching forwarders (for performance)
    - Mitigation: Stub caches

Closing thoughts

- This draft documents
  - a secure alternative client policy that enables more DDR upgrades,
  - its advantages and disadvantages, and
  - some ways to mitigate known problems (completely or partially).
- No recommendations on policy choices (out of scope)
- Seeking WG adoption
- Please contribute thoughts on other potential issues and mitigations related to cross-forwarder upgrade.