Bootstrapping Procedure to Discover and Authenticate DoT and DoH servers


IETF 104, Prague
March 2019

T. Reddy (McAfee)
D.Wing (Citrix)
M. Richardson(Sandelman Software Works)
M. Boucadair (Orange)
Agenda

• Problem Statement
• Solution overview
• Bootstrapping Phase
• Discovery Phase
• Connection handshake and DNS server certificate validation
• Questions & Comments
Problem statement

- Public DoH/DoT/DNS causes operational problems
  - Breaks split DNS (internal.example.com)
  - Breaks local names (printer.local)
  - Harms CDN localization (modulo RFC7871)
Problem statement

• Network security services cannot act on DoT/DoH traffic to block malware.

• Network security services would want to block public DoT/DoH traffic to
  - Drop traffic to port 853 (DoT)
  - Identifying DoH is far more challenging
    - Identify the domains offering DoH servers and block traffic to these domains. Public DoH servers are categorized as “Proxy / Anonymizer” content category.

• Strict privacy profile
  - No DNS service and No Internet.

• Opportunistic privacy profile
  - Fallback to clear-text or unauthenticated encrypted connection.
Problem statement

• Ramification of successfully blocking DoT/DoH traffic
  ➢ Pervasive monitoring
  ➢ Internal attacker can modify the DNS response to point to malicious servers.

• Ramification of failure to block DoT/DoH traffic
  ➢ Failure to block access to malicious (malware) domains.
  ➢ IoT firewall rules (RFC8520) based on domain names provided by the IoT Manufacturer cannot be enforced.

Both scenarios compromise endpoint security and privacy
Solution overview

- Provide local DoH/DoT/DNS
  - Works with split DNS (internal.example.com)
  - Works with local names (printer.local)
  - Works with CDN localization (without needing RFC7871)

The draft discusses mechanisms to bootstrap endpoints to discover and authenticate local DNS-over-(D)TLS and DNS-over-HTTPS servers.
Bootstrapping Endpoint Devices

- **Endpoint**
- **EST server**

**TLS session with EST server**

- TLS or HTTP authentication using password-based authenticated key exchange (PAKE)

**Fetch CA certificates and End-Entity certificates (DNS server certificate)**

SRV service label "domain-s" to identify the DNS server certificate

---

**RFC5054**: Secure Remote Password (SRP) protocol for TLS authentication

**RFC8120**: Mutual Authentication for HTTPS

**RFC7030**: Enrollment over Secure Transport
Bootstrapping IoT Devices and CPE

Bootstrapping Remote Secure Key Infrastructures (BRSKI)

draft-ietf-anima-bootstrapping-keyinfra provisions credentials to access networks.

- BRSKI provides an automated mechanism for the bootstrap distribution of CA certificates from the EST server.
Discovery Phase

- S-NAPTR lookup to learn DoT and DoH protocols supported by the DNS server and the DNS privacy protocol preferred by the DNS server administrators

  example.net.
  IN NAPTR 100 10 "" DPRIVE:dns.tls "" dns1.example.net.
  IN NAPTR 200 10 "" DPRIVE:dns.dtls "" dns2.example.net.

  dns1.example.net.
  IN NAPTR 100 10 S DPRIVE:dns.tls "" _domain-s._tcp.example.net.

  dns2.example.net.
  IN NAPTR 100 10 S DPRIVE:dns.dtls "" _domain-s._udp.example.net.

  _domain-s._tcp.example.net.
  IN SRV 0 0 853 a.example.net.

  _domain-s._udp.example.net.
  IN SRV 0 0 853 a.example.net.

  a.example.net.
  IN A 192.0.2.1
Discovery Phase

- If DNS-over-HTTPS protocol is supported by the DNS server, discover the URI templates using one of the mechanisms discussed in “Associating a DoH server with a resolver” (draft-ietf-doh-resolver-associated-doh).
Connection handshake and DNS server certificate validation

- Match the certificate in TLS handshake with the DNS server certificate downloaded from EST server.
- Validate the certificate using the Explicit trust anchor database entries.
Privacy considerations

- A new privacy certificate extension that identifies the privacy preserving data policy of the DNS server.
  - The extension will contain a URL that points to the privacy preserving data policy.
Security considerations

• The Explicit trust anchor can be used to perform DNSSEC validation of the responses from local DNS server.
• User can enable the discovery mechanism in trusted networks.
• If the user trusts the network, the user can enable strict privacy profile with the DNS-over-(D)TLS or DNS-over-HTTPS server discovered in the network.
Comments and suggestions are welcome