Authentication and (D)TLS Profiles for DNS-over-TLS and DNS-over-DTLS

draft-ietf-dprive-dtls-and-tls-profiles-01

S. Dickinson  Sinodun
D. Gillmor   ACLU
T. Reddy   Cisco

BUENOS AIRES    D-PRIVÉ WG    IETF 95
Recap

- DNS-over-TLS is now approved as RFC
- DNS-over-DLTS is at version -06

- DNS-over-TLS RFC still contains
  - Strict Authentication using SPKI pinsets
  - Opportunistic security

Originally both described authentication

A standard authentication mechanism enables deployment
Recap

- IETF 94: WG agreed to create a ‘combined’ document for other authentication mechanism

- Authentication removed from DNS-over-DTLS

- Also agreed a combined (D)TLS profile should move to this draft (from I-D: “DPRIVE TLS/DTLS Message Flows”)

- Adopted by WG January 2016 (revved to -01)
What is in the draft?

- Scope is
  - Both DNS-over-TLS and DNS-over-DTLS
  - Authentication of Recursive DNS Server by client
    - Not client authentication, not Authoritative
  - Domain name based authentication
    - Normative ref to DNS-over-TLS RFC
  - “Privacy Enabled DNS Server”
Terminology

• “Usage Profiles”
  • Describe security properties, without reference to a specific authentication mechanism
• Strict
• Opportunistic
• No Privacy

• Comment: Unclear/confusing?
• Slightly different to DNS-over-TLS draft…
• Both will be clarified!
Usage Profile: No Privacy

- Usage Profiles
  - Strict
  - Opportunistic
- No Privacy

Clear text 😠
Usage Profile: Opportunistic

- Usage Profiles
- Strict
- Opportunistic
- No Privacy

[ RFC7435 ]
"... the use of cleartext as the baseline communication security policy, with encryption and authentication negotiated and applied to the communication when available. "

D-PRIVÉ WG  IETF 95
# Detecting attacks

<table>
<thead>
<tr>
<th>Usage Profile</th>
<th>Passive Attacker</th>
<th>Active Attacker</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strict</strong></td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td><strong>Opportunistic</strong></td>
<td>Auth + Enc</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>Enc</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>N (D)</td>
<td>N (D)</td>
</tr>
<tr>
<td><strong>Clear text</strong></td>
<td>N (D)</td>
<td>N (D)</td>
</tr>
<tr>
<td><strong>No Privacy</strong></td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
Usage Profile: Strict

- Usage Profiles:
  - **Strict**
  - Opportunistic
  - No Privacy

Authenticate or die

**BUT...**
- meta queries can be Opportunistic but
- MUST be DNSSEC validated
Super Strict?

- Usage Profiles
  - Strict
  - Opportunistic
  - No Privacy

Q: What about requiring ALL queries (including meta queries) to be private?
Relaxed?

• Usage Profiles
  • Strict
  • Opportunistic
  • No Privacy

Q: What about requiring encryption but no authentication?
Auth mechanisms

- Out-of-band SPKI
- Server Credentials
- Strict/Oppportunistic

Trusted Relationship
Auth mechanisms

Strict/Oppportunistic

Config of domain name + IP address

SRV

Config of domain name
Auth mechanisms

Strict/Oppportunistic

Config of domain name + IP address

Config of domain name

X.509

SRV
Auth mechanisms

Strict/Oppportunistic

Config of domain name + IP address

Config of domain name

X.509

SRV

TLSA...

DANE

Server Credentials
Auth mechanisms

Strict/Oppportunistic

Config of domain name + IP address
SRV
TLSA...
X.509
DANE
Server Credentials

Config of domain name

TLS DNSSEC Extension:
Server provides DANE records + Server Credentials
Auth mechanisms

Strict/Oppportunistic

Config of domain name + IP address

SRV

Config of domain name

TLS DNSSEC Extension: Server provides DANE records (EE + SPKI) + SPKI
DHCP

- To securely auto configure IP address **and** domain name would require a new options
  - and secure, trusted connection to DHCP server

Q: Should we pursue this option?
(D)TLS profile

- BCP 195
- Session resumption
- (False start)

- Expect to address TLS 1.3 in future version
Implementation Status

- **Client**: getdns
  - Strict and Opportunistic
  - SPKI pinset
  - Hostname validation of cert
  - (WIP) DANE mechanisms

- **Servers**
  - Unbound
  - Knot (as of Hackathon!)
Feedback and review please!