DTLS and IPsec for DNSE

Eric Rescorla

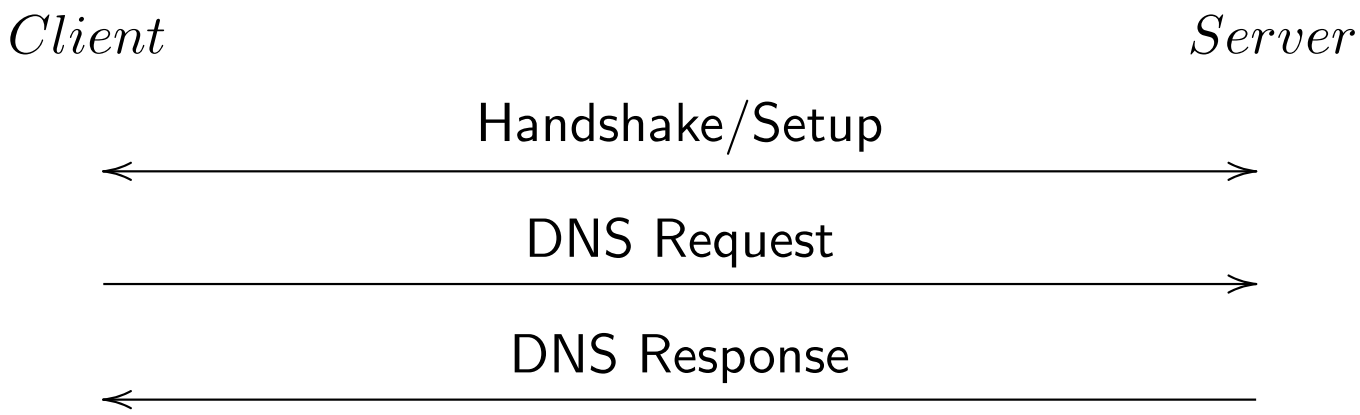
Mozilla

ekr@rtfm.com

Basic assumptions

- We have some other mechanism for identifying the expected server key
  - Manual configuration for configured resolvers
  - DNS records for authoritative servers
- Client is anonymous

General Pattern (current)



- What is this handshake thing?
  - DTLS and IPsec both need a cryptographic handshake to set up the parameters and exchange keys
- Once keys are exchanged, you just send UDP
  - DTLS: DNS Message/DTLS record/UDP/IP
  - IPsec: DNS Message/UDP/IPsec packet

Handshake Issues: NAT/Firewall Penetration

- The handshake needs to get through middleboxes
- Both handshakes are carried over UDP
  - DTLS on the same port
  - IPsec on a separate (defined) port
- We have to worry about these UDP packets being blocked
  - Lots of people block non-53 UDP
    - Though maybe pass IKE
  - But there are also protocol enforcement devices that enforce things look like DNS
- Also need to worry about middleboxes blocking ESP

Handshake Latency

- The handshake isn't free (1-2 RTT)
- Not a big problem for connections to your recursive resolver
  - Just do a setup at bootup and then send requests over it
  - Though requires storing state at the server
- Less good when you are the recursive resolver
  - Need to handshake for each new resolver you see
  - Current option: bear the cost of the handshake each time
  - Future options: TLS WG is currently designing 0-RTT modes for TLS 1.3 which might help

Final Thoughts

- IPsec probably isn't going to work here
- DTLS might work
  - But potential firewall and performance issues need research
- Happy to help if people want to talk more