Danish: Middle-Box DANE Validation for HTTPS

Andrew McConachie

Image courtesy Wikimedia Commons

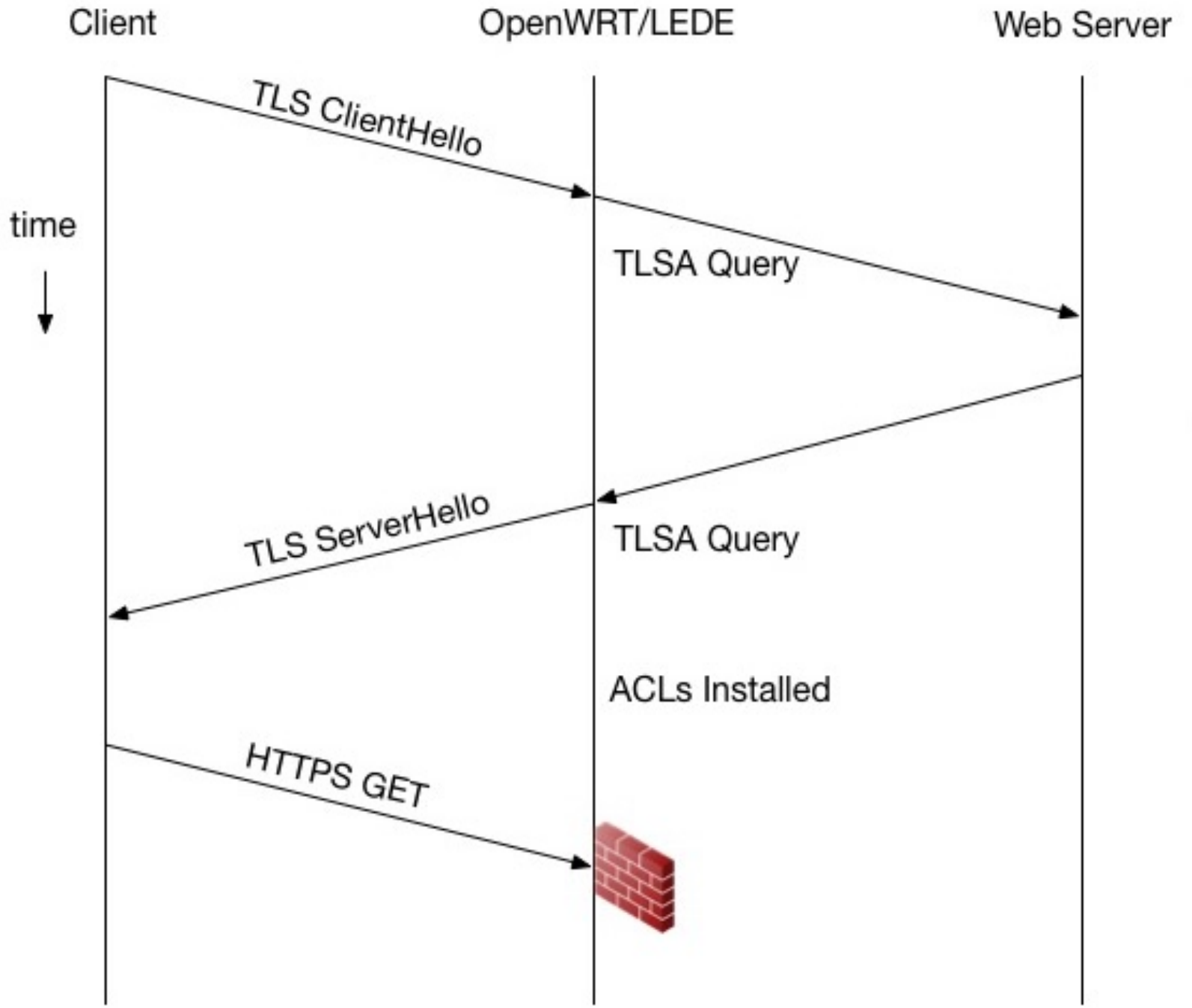
Overview

- Daemon for validating HTTPS DANE (RFC 6698)
- Runs on OpenWRT/LEDE
- Mostly works but still very experimental
- Uses localhost as the DNSSEC validating resolver
  - Will work with any resolver at localhost
  - Developed and tested with dnsmasq
- We usually think of HTTPS DANE as being implemented in web browsers
  - Is that really a requirement?
  - Many HTTPS sessions are not initiated by web browsers

Operation

1. Snoop HTTPS TLS ClientHello and ServerHello messages
   a) Grab Server Name Identifier (SNI) from ClientHello
   b) Grab X.509 Certificate from ServerHello
2. Perform DNS TLSA lookup for comparison
3. If X.509 Certificate and TLSA RR match do nothing
4. Else install ACLs to block client traffic to offending web server
   - 2 ACLs to force TCP timeout
   - 1 ACL to prevent further egressing TLS ClientHellos with matching SNI
     - Installed for both IPv4 and IPv6

DANE Validation Failure



Current Support

- TLS versions 1.0 – 1.2
- IPv4 and IPv6
- RFC 6698 Support
  - TLSA certificate usage 1 and 3 Only
    - Only DANE-EE supported
  - TLSA selector 0 Only
  - TLSA matching types all supported
  - Full RFC 6698 support is dependent on the OpenWRT/LEDE OpenSSL package also supporting DANE

Thank You!

https://www.middlebox-dane.org/