DOTS Signal Channel and Data Channel drafts

Interim Meeting

https://tools.ietf.org/html/draft-ietf-dots-signal-channel-04

https://tools.ietf.org/html/draft-ietf-dots-data-channel-04

2nd October 2017

Presenter : Tirumaleswar Reddy

DOTS Signal Channel and Data Channel drafts

- Addressed most comments received from the WG for both drafts
- Updated both drafts to use consistent parameter names.

draft-ietf-dots-signal-channel-04

- Added a new parameter to signal the DOTS server to initiate mitigation only after the DOTS server channel session is disconnected.
  - Default value for trigger-mitigation is TRUE

draft-ietf-dots-signal-channel-04

- -1 value for lifetime parameter in mitigation request to indicate indefinite mitigation lifetime.
- Value 0 for target-protocol means “all protocols”.
- FQDN and URI mitigation scopes are a form of scope alias.
  - IP addresses to which FQDN and URI resolve represent the full scope of mitigation.

draft-ietf-dots-signal-channel-04

- Append parameter values in the alias with the other parameters in the mitigation request identifying the target resources.
- 2.02 (Deleted) even if the mitigation request does not exit (align with DELETE method in RFC7252).
- Mitigation is active for active-but-terminating period (30 seconds) after withdrawing the mitigation request.

draft-ietf-dots-signal-channel-04

- If-Match Option in PUT request for efficacy update from DOTS client to make the update conditional on the existence of mitigation request.
  - To handle out-of-order delivery (PUT arrives after DELETE).
- Efficacy update must not change the mitigation scope conveyed in the original mitigation request.

draft-ietf-dots-signal-channel-04

- Recommended default values for message transmission parameters are :
  - ack_timeout (2 seconds)
  - max-retransmit (4)
  - ack-random-factor (1.5)
  - heartbeat-interval (91 seconds)
  - missing-hb-allowed (3)

draft-ietf-dots-signal-channel-04

- If no response received for 3 consecutive “CoAP ping” confirmable messages then the session is considered disconnected.
  - “CoAP ping” retransmitted 4 times with exponential back-off (initial timeout set to a random value b/w 2 to 3 seconds).

draft-ietf-dots-signal-channel-04

- Default port of 5684 ?
  - Request IANA for a new port for DOTS signal channel ?
    - Port can be assigned in the IANA port number registry (just like it was done for DNS-over-(D)TLS after the drafts were adopted by the WG).
  - ALPN [RFC7301] to uniquely identify DOTS signal channel and distinguish from other protocols ?

draft-ietf-dots-signal-channel-04

- CBOR payload for 2.xx and 3.xx response codes.
- Diagnostic payload for 4.xx and 5.xx error response codes.
- New mitigation status parameter, mitigation-start
  - Mitigation start time is represented in seconds relative to 1970-01-01T00:00Z in UTC time

draft-ietf-dots-signal-channel-04

- Overlapped lower number mitigation-id is automatically deleted.
- PUT request to refresh the current mitigation lifetime repeats all other parameters as sent in the original mitigation request.

draft-ietf-dots-signal-channel-04

- Explicit deregister by issuing a GET request with Observe option set to 1 to cancel receiving mitigation status updates.
- GET request without Observe option is allowed for polling.
- Mitigation status parameters (e.g. bytes-dropped) since the attack mitigation is triggered.
  - Counter wraps once it hits the maximum value.

draft-ietf-dots-signal-channel-04

- New CoAP response code (3.00 Alternate server).
- Discovery of configuration parameters conveys current and mix/max values.
- If configuration parameters not acceptable then the client uses GET to learn acceptable values and re-sends PUT with updated attribute values.

draft-ietf-dots-signal-channel-04

- Default mitigation lifetime (60 minutes) ?
- Use well-known URI ?
  - e.g. /.wellknown/dots-signal/signal/v1
  - URI suffix: dots-signal

draft-ietf-dots-data-channel-04

- Updated YANG model to align with https://tools.ietf.org/html/draft-ietf-netmod-acl-model-13

draft-ietf-dots-data-channel-04

- RESTCONF runs on 443 port.
  - ALPN [RFC7301] to uniquely identify DOTS data channel and distinguish from other protocols ?

Mutual authentication

- Certificates
  - DOTS client uses EST to get client certificate from the EST server in the domain operating the DOTS server.
  - Client authenticates to the EST server using certificate or shared credential or HTTP authentication for authorization to get a client certificate.
- TLS-PSK

Mutual authentication

- Subject Public Key Info (SPKI) pinset
  - Backup pin (discussed in public key pinning extension for RFC7469).
- DOTS client directly provisioned with the domain name of the DOTS server.
  - PKIX certificate based validation
  - SubjectAltname extension for the reference identifier

Mutual authentication

- DNSSEC
  - Required when only the domain name of the DOTS server is configured on the DOTS client.
- DANE
- TLS DNSSEC chain extension (full certificate chain).
- All above techniques are used in draft-ietf-dprive-dtls-and-tls-profiles draft

DOTS Signal Channel and Data Channel drafts

- Comments and suggestions are welcome for both drafts.