DOTS Signal Channel and Data Channel drafts


November 2017

Presenter : Mohamed Boucadair
DOTS Signal Channel and Data Channel drafts

• Addressed most comments received from the WG for both drafts
• Updates to signal channel draft are reflected in data channel draft and vice-versa
• Both drafts uploaded to https://github.com/dotswg and issues are tracked.
• New port for DOTS signal channel
  ▪ Requested IANA for a new port for DOTS signal channel
• Use well-known URI
  ▪ /www.example.com/.wellknown/dots/v1/mitigate
  ▪ URI suffix: dots
• Default mitigation lifetime of 60 minutes.
• client-identifier added by DOTS gateway to uniquely identify mitigation requests, alias-names and filtering rules
  ▪ SHA-256 of the Subject Public Key Info (SPKI) of DOTS client X.509 certificate can be used to compute client-identifier.
-1 value for lifetime parameter in mitigation request to indicate indefinite mitigation lifetime.

- The server MAY refuse indefinite lifetime; the granted lifetime value is returned in the response. DOTS client MUST be prepared not be granted indefinite lifetime.
- SIG-006 requirement

Mitigation is active for active-but-terminating period (120 seconds) after withdrawing the mitigation request.
Recommended default values for message transmission parameters are:

- `ack_timeout`: 2 seconds
- `max-retransmit`: 3
- `ack-random-factor`: 1.5
- `heartbeat-interval`: 30 seconds
- `missing-hb-allowed`: 5
• In peace time, if no response received for 5 consecutive “CoAP ping” confirmable messages then the session is considered disconnected.
  – “CoAP ping” is retransmitted 3 times with exponential back-off (initial timeout set to a random value b/w 2 to 3 seconds).
• In case of DDoS attack saturating the incoming link to the DOTS client:
  - The DOTS client continues the DOTS session even after “missing-hb-allowed” is reached.
  - If the DOTS server does not receive any traffic from the peer DOTS client, then the DOTS server sends heartbeat requests to the DOTS client and after maximum "missing-hb-allowed" threshold is reached, the DOTS server concludes the session is disconnected.
• Overlapped lower number mitigation-id is automatically deleted.
  ▪ Any concerns?
• YANG model aligned with https://tools.ietf.org/html/draft-ietf-netmod-acl-model-14

• Support multiple ACLs from a DOTS client and ordering of ACLs?
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

• Raw public keys

• Mandate DOTS agents to implement all above?
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

• Mandate DOTS agents to support both mechanisms ?
DOTS Signal Channel and Data Channel drafts

- Comments and suggestions are welcome for both drafts.