Denial-of-Service Open Threat Signaling (DOTS) Server Discovery


IETF 104, Prague
March 2018

M. Boucadair (Orange)
T. Reddy (McAfee)
P. Patil (Cisco)
Status

• A Call for adoption was issued
  – Fair support
  – Still waiting for the official chairs’ conclusion

• Points for further discussion:
  – Do we need all the four discovery methods?
  – Clarify the overall model
Point#1: Remove Some Discovery Mechanisms

• We went there in the past:
  • A rationale is discussed in (Why Multiple Discovery Mechanisms?) draft-boucadair-dots-server-discovery-05#section-4
    – A unified discovery mechanism to prioritize the 4 mechanisms is specified
    – Still...this comment is a fair one

• Candidate methods to be abandoned
  – Anycast: given the complications that may arise in the multi-homing scenario, in particular
  – mDNS
Point#2: Clarify the Model

- The I-D separates server’s discovery vs. credential provisioning & authentication
  - Credentials provisioning is done before discovering where to find the DOTS servers
  - Some text is needed to further clarify the rationale

- Triggers for running the discovery procedure are missing?
  - Some are inherent to the protocol (e.g., DHCP)
  - Others will require NEW text to clarify the behavior:
How To Progress?

• Wait for the conclusion of the WG CFA
• Then, start updating the I-D to record the WG consensus on the various points:
  – Shortened list of discovery mechanisms
  – Elaborate/re-structure authentication considerations
  – Triggers for executing the discovery procedure
• Address any further comments from the WG, as usual