102nd IETF, Jul. 2018, Montreal

Mtrace Version 2: Traceroute Facility fo r IP Multicast

draft-ietf-mboned-mtrace-v2-24

Hitoshi Asaeda
Kerry Meyer
WeeSan Lee (Ed.)

IESG Reviews and Draft Revisions

- Start IESG review on Jan. 2018
  - draft-ietf-mboned-mtrace-v2-22
- Revised based on several comments
  - draft-ietf-mboned-mtrace-v2-23
    - Apr. 2018, to address all comments
      - Normative wordings, IANA related things, etc.
    - Except Mirja and Eric, all approved (I believe)
  - draft-ietf-mboned-mtrace-v2-24
    - Jun. 2018, to address Mirja's comments and Eric's com ments
    - Mirja approved but Eric couldn't

C: Forgery of responses and Amplification attacks

- This protocol does not appear to verify that the sender of the query/request actually owns the IP it claims. Because responses are much larger than queries, this allows for an amplification attack, especially if the client is able to send a query/request that elicits multiple replies.
- Because the query ID is so short, an attacker can generally produce a message which has a non trivial chance of corresponding to an extant query. This could be addressed by having a query ID that was large and random.
    - The query ID is not intended as a security protection mechanism; it is just a way of matching responses to queries.

A1: Forgery of responses

- 9.7.4. Delivery of False Information (Forged Reply Messages) (-24, -25)
  - The use of encryption between the source of a Query and the endpoint of the trace would provide a method to protect the values of the Query ID and the dynamically allocated client (source) port (see Section 3.2.1). These are the values needed to create a forged Reply message that would pass validity checks at the querying client. This type of cryptographic protection is not practical, however, …. While it is not practical to provide cryptographic protection between a client and the Mtrace2 endpoints (destinations), it may be possible to prevent forged responses …. The use of encryption protection between nodes is, however, out of the scope of this document.

A2: Configurable packet filtering (aka ACL)

- 9.2. Filtering of Clients and Peers (-24, -25)
  - A router providing Mtrace2 functionality MUST support a configurable packet filtering mechanism to drop Queries from clients and Requests from peer router or client addresses that are unauthorized or that are beyond a specified administrative boundary. This filtering could, for example, be specified via a list of allowed/disallowed client and peer addresses or subnets for a given Mtrace2 message type sent to the Mtrace2 protocol port. If a Query or Request is received from an unauthorized address or one beyond the specified administrative boundary, the Query/Request MUST NOT be processed. The router MAY, however, perform rate limited logging of such events.

A3: Neighbor authentication

- 9.7.2. Amplification Attack
  - (-24) Because an Mtrace2 Query results in Mtrace2 Request and Mtrace2 Reply messages that are larger than the original message, the potential exists for an amplification attack from a malicious sender. This threat is minimized by restricting the set of addresses from which Mtrace2 messages can be received on a given router as specified in Section 9.2.

A3: Neighbor authentication – cont’d

- 9.7.2. Amplification Attack
  - (-25) In addition, for a router running a PIM protocol (PIM-SM, PIM-DM, PIM Source-Specific Multicast, or Bi-Directional PIM), the router SHOULD drop any Mtrace2 Request or Reply message that is received from an IP address that does not correspond to an authenticated PIM neighbor on the interface from which the packet is received. The intent of this text is to prevent non-router endpoints from injecting Request messages. Implementations of non-PIM protocols SHOULD employ some other mechanism to prevent this attack.

A4: Forgery of responses

- 9.7.4. Delivery of False Information (Forged Reply Messages) (-25)
  - The required use of configurable packet filtering (Section 9.2) and recommended use of PIM neighbor authentication (Section 9.7.2) for messages that are only valid when sent by a multicast routing peer (Request and Reply messages) eliminate the possibility of reception of a forged Reply from an authorized host address that does not belong to a multicast peer router.

Next Step

- After Eric’s confirmation and approval (yes, I got it this morningㅆ), we will submit the revision (-25) and ask the final procedure.