Port Control Protocol (PCP) Authentication Mechanism

draft-ietf-pcp-authentication

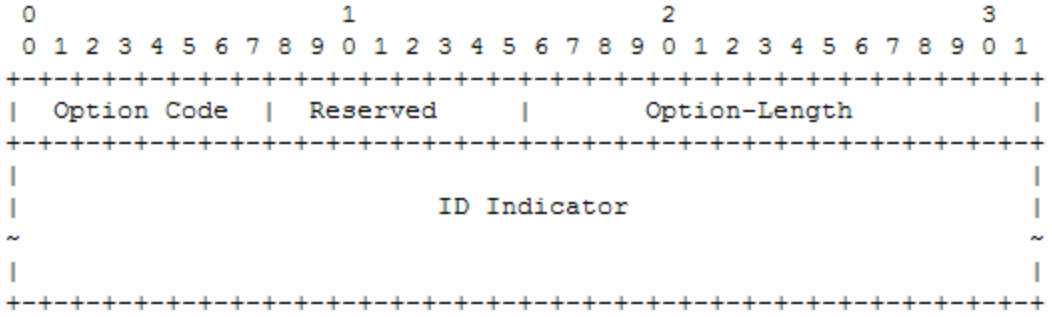
M. Wasserman

S. Hartman

D. Zhang

Updates since -03 (1)

- ID-indicator option:
  - This option provide the an identifier to the PCP client that the client can use to choose which credentials to provide to the PCP server



  - ID Indicator: The value for a PCP client to choose proper credentials for authentication. The method of generating this value is out of scope of this document. Note that this field could be user friendly and may contain the enterprise name and PCP server name in a human-readable format.

Updates since -03 (2)

- More discussions in re-authentication
  - An re-authentication procedure could be triggered by following reasons:
    - The session life period needs to be extended
    - The sequence numbers is going to reach the maximum
  - During re-authentication, the session partners can also exchange common PCP messages in in parallel. The common PCP messages MUST be protected with the current SA until the new SA has been generated.

Updates since -03 (3)

- Clarify the influence of re-authentication on PCP proxies
  - When there is a PCP proxy located between a PCP server and a set of clients, the proxy may need to perform authentication with the PCP server before it generates requests for the clients. In addition, re-authentication will not interrupt the service that the proxy provides to the clients since the proxy is still allowed to send common PCP messages to the server during that period.

Updates since -03 (4)

- Add more discussions in MTU:
  - Particularly, EAP lower layers indicate to EAP methods and AAA servers what the MTU of the lower layer is. EAP methods such as EAP-TLS, TEAP, and others that are likely to exceed reasonable MTUs provide fragmentation and reassembley. Others, such as EAP-GPSK assume they will never send packets larger than the MTU and focus on small EAP packets.

Updates since -03 (5)

- Clarify the influence of re-authentication on PCP proxies
  - When there is a PCP proxy located between a PCP server and a set of clients, the proxy may need to perform authentication with the PCP server before it generates requests for the clients. In addition, re-authentication will not interrupt the service that the proxy provides to the clients since the proxy is still allowed to send common PCP messages to the server during that period.

Updates since -03 (6)

- Discuss why sequence number is also required in PCP responses.
  - Note that in the base EAP specification [RFC6887], a PCP client needs to select a nonce in each MAP or PEER request, the nonce is requested to sent back in the response. However, it is possible for a client to use the same nonce in multiple MAP or PEER request, this may cause potential risk of replay attacks. Under the assistance of the sequence number attached in the PCP responses, this issues can be addressed.

Updates since -03 (7)

- Refine the PA messages retransmission policies.
  - the device needs maintain the last incoming and the associated outgoing packet. When receiving a retransmitted message, if no outgoing PA message has been generated for the received duplicate PA message yet, the device needs to generate a PA-Acknowledgement message and sends it out.
  - If the timer is expired and no expected response is received, the device will terminate the session and discard the current SA.

Updates since -03 (8)

- Change the name "PCP-Auth" to "PA".
- Add IANA considerations.
- Will spend sometime to fix the nits in next few weeks.

- Comments?