Port Control Protocol (PCP) Authentication Mechanism

draft-ietf-pcp-authentication-03

Margaret Wasserman
Sam Hartman
Dacheng Zhang

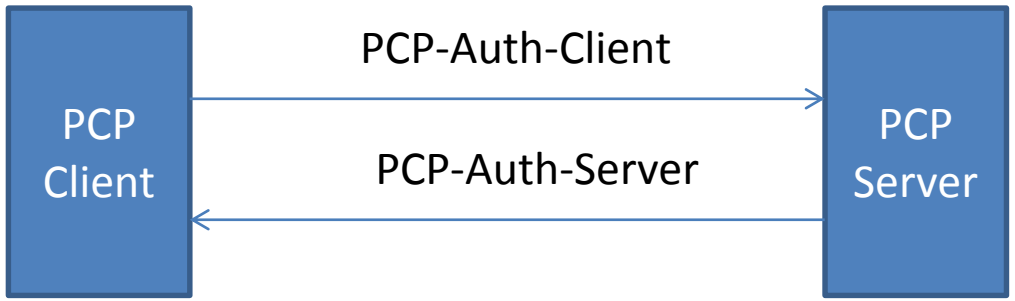
IETF 89 London

Updates Since -02

- Change to ways to name PCP-Auth messages
- Define the Authentication Tag for PCP common messages
- Define the sequence numbers for PCP common messages
- Update the re-transmission polices

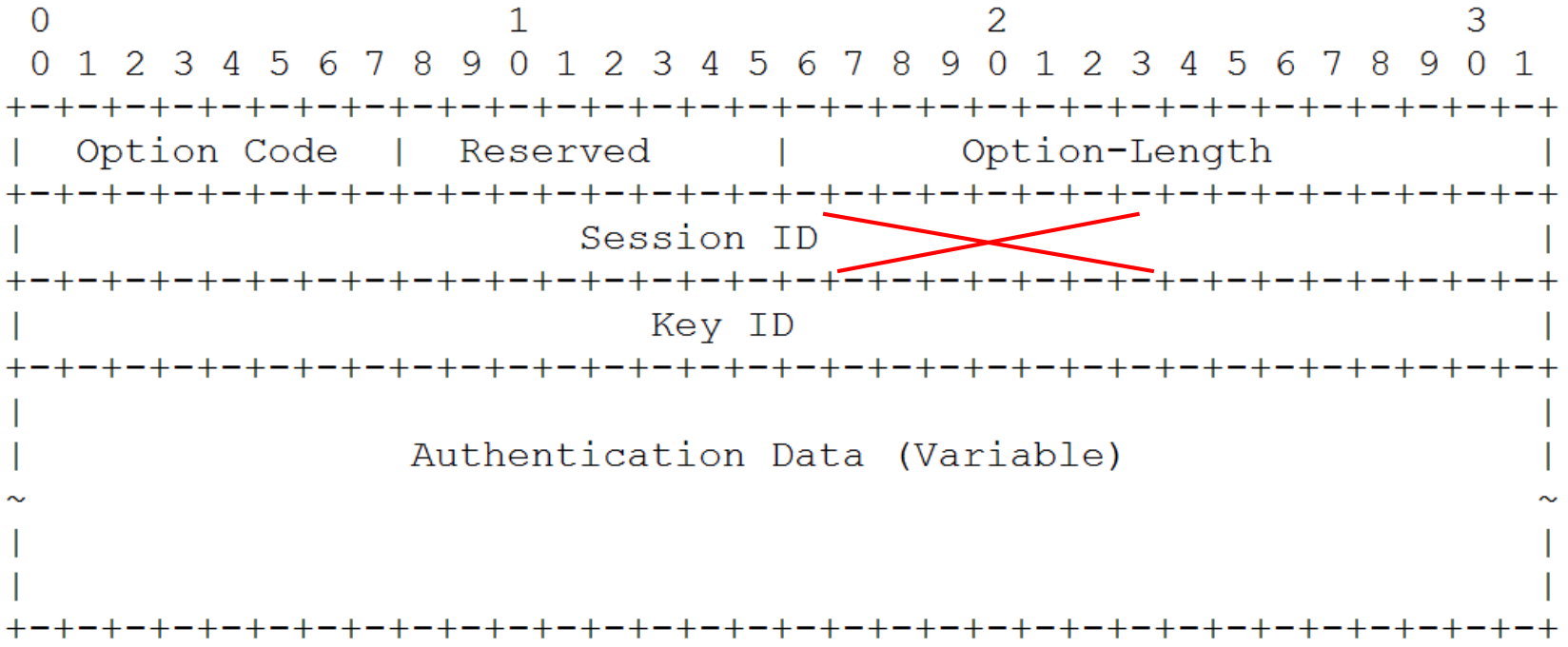
PCP-Auth Messages

- PCP-Auth-Request → PCP-Auth-Server
- PCP-Auth-Answer → PCP-Auth-Client
- In order to address the lost of packets and out-of-order delivery, after sending out a PCP-Auth-Server message, the server cannot send the next one unless it receives a PCP-Auth-Client message with the sequence number exactly matching the incoming sequence number maintained locally, and vice versa.



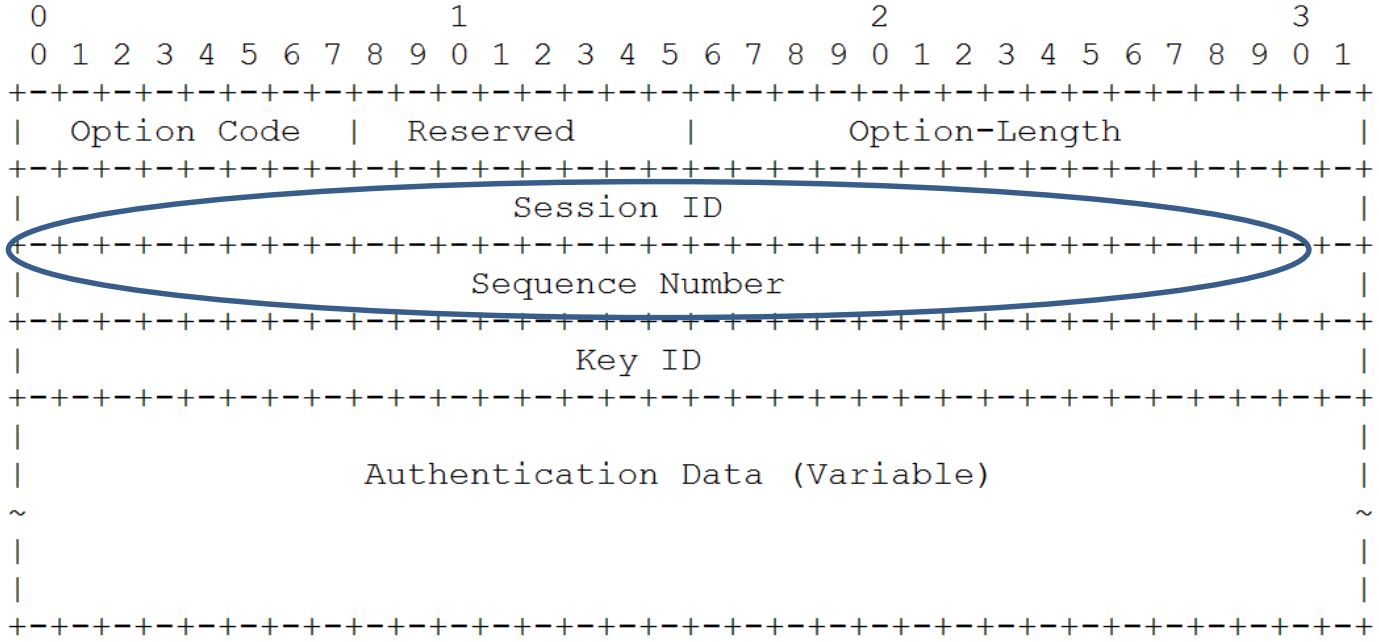
Authentication Tag Option for PCP Auth Messages

- Remove the redundant information



Authentication Tag for Common Packets

- Because there is no Authentication OpCode in a common PCP message, this tag contains the information which is used to transported in the OpCode.



- Also, we discuss how to generate and verify the digests for the common PCP messages.

Add sequence numbers for Common PCP messages (2)

- Two new sequence numbers (for Incoming and outgoing common PCP messages respectively)
- Only used for replay protection, because packet loss is allowed for Common PCP messages
- The sequence number in the incoming packet need not to exactly match the incoming sequence number maintained locally.
- When receiving a PCP packet from its session partner, the PCP device will not accept it if the sequence number carried in the packet is smaller than the incoming sequence number the server maintains.

Add sequence numbers for Common PCP messages (2)

- Exact match of sequence number is not required for common PCP messages
  - A PCP device may stop re-sending a PCP message and send a new one for certain reasons
  - In this case, the sequence numbers in the PCP messages and maintained locally may not match perfectly.

Mandatory PRF and MAC Algorithms

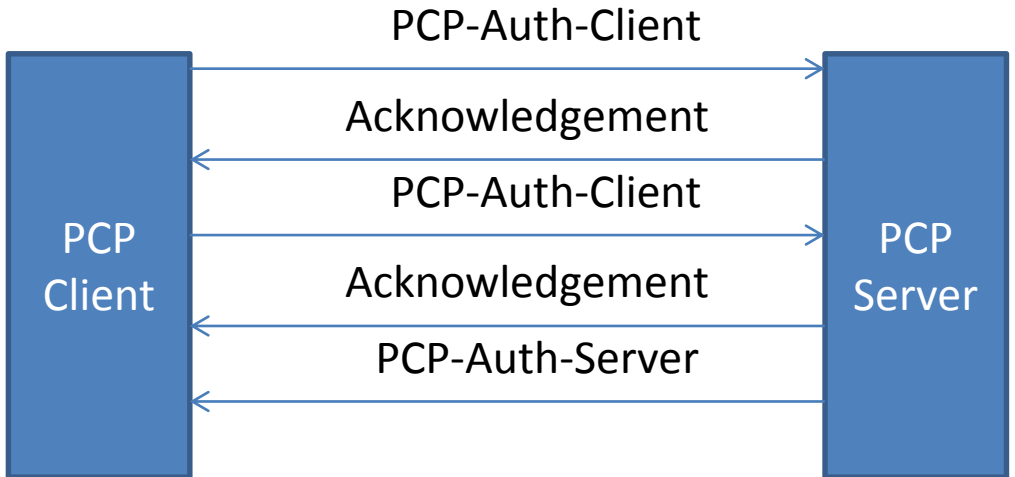
- PCP implementation MUST support PRF_HMAC_SHA2_256.
- A PCP implementation MUST support AUTH_HMAC_SHA2_256_128.

The usage of PCP-Auth-Acknowledgement message (1)

- When an EAP message is too long for a single PCP-Auth message to transport, it will be divided into multiple sections and transport them within different PCP-Auth messages.
- The receiver may not be able to know what to do in the next step until receiving all the sections and constructing the complete EAP message.
- In this case, in order to guarantee reliable message transmission, after receiving a PCP-Auth message, the receiver MUST reply with a PCP- Auth-Acknowledgement message until all the sections have been received.

The usage of PCP-Auth-Acknowledgement message (2)

- Sending and receiving Acknowledge messages will not result in the change of sequence numbers. This approach simplifies the sequence number management in the following case.
  - After a PCP client sends out all the EAP sections to the server, it will wait for the response from the server
  - The server cannot reply in a specified period it will send back an acknowledgement back first.
  - The PCP-Auth-Server is ready and sent out.
  - Because the sequence will not be changed by the acknowledgement, the PCP server don't have to worry whether the acknowledgement has been received or not.



Comments?