Port Control Protocol (PCP) Authentication Mechanism

draft-ietf-pcp-authentication-06

M. Wasserman, S. Hartman
Painless Security
D. Zhang
Huawei
T. Reddy
Cisco

Changes from ietf-pcp-authentication-05 to -06

- Updated Security Considerations section.
- Updated ID Indicator Option.
- Other comments we got from the group

The updates since 06 (1)

- Revise Section 3
  - Having sub-sections for client and server initiated auth sessions respectively
  - Use diagram to make the discussion easier to understand
  - Revise the terms and make sure they are compatible to the terms defined in RFC 6877

The updates since 06 (2)

- Give the definition of "common PCP messages"—The PCP messages without the authentication Opcode.
- AUTHENTICATION-SUCCEED-> AUTHENTICATION-SUCCEEDED
- SESSION- TERMINATION-> SESSION-TERMINATED
- Traffic key -> Transport key
- PCP packets-> PCP messages
- separate out the texts about generation of digests for PA message and common PCP message (Section 6.1)

Current Status

- We have addressed the most of the issues that were raised
- We have updated the issues in the tracker
- There are still some comments from Dave Thaler which need to be discussed and addressed

Issue #1: Mandatory EAP Method

List mandatory-to-implement EAP method(s) for PCP client and server

- EAP-TEAP is newest IETF standard, but not widely implemented
- EAP-TTLS might be better, but would require a down reference because it is not a standard

Next Steps: Talk to EAP experts for advice and add a mandatory-to-implement method

Issue #2: PA-Ack Underspecified

- When is a PA-Acknowledgement sent?

Proposed Resolution: Should be sent when PA response cannot be sent immediately

Issue #3: Detect Downgrade Attack

- Current draft says: The PCP server determines if the set of algorithms conveyed by the client matches the set it had initially sent, to detect an algorithm downgrade attack.
- Doesn't say what to do if they don't match.

- Resolution in Current Draft: Add "If they do not match exactly, the server MAY decide to stop the session according to its local policies (new error code !)." to above text.

Issue #4: When to Trigger ReAuth

- Trigger re-authentication before sequence number reaches the max value.

Proposed Resolution: Trigger reauth when sequence number reaches 2**32 – 2**16

Issue #5: ID Indicator Matching

- ID Indicator field matching rules
  - RFC 6943 : **Definite**/Absolute/Indefinite.

Proposed Solution: Definite

Issue #6: Retrans Policy

- Revise the retransmission policies in Sections 6.3 6.4
  - Discard duplicate PA message with same sequence number but with something different in message.

Issue #7: Rate Limiting

- Rate-limiting is requred for duplicate PA messages
- Should we specify a limit?

Proposed Resolution: No. Other standards do not specify rate limit or method, leave implementation dependent

draft-ietf-pcp-authentication-06

Comments?