Authentication Mechanism for Port Control Protocol (PCP)

draft-wasserman-pcp-authentication-02.txt

IETF 83 Paris
Margaret Wasserman
Sam Hartman
Painless Security
Dacheng Zhang
Huawei

PCP Authentication Overview

- PCP Authentication relies on EAP for authentication and key derivation
  - Use of EAP is consistent with widely deployed enterprise security systems
  - Can also scale down to simple shared keys for a single proxy/PCP server combination
- Mechanism allows for both client-initiated and server-initiated security
  - Clients can choose to make secure requests
  - Servers can force authentication when needed

Changes from -01 to -02

- Added MTU/fragment handling
  - To support large credentials (certificates, etc.)
- Added a nonce to prevent offline attacks
- Add the key ID field so that a MSK can generate multiple traffic keys
  - For long-lived associations

Open Issue

- Suggestion to use PANA instead of in-band EAP-based approach
- Following slides attempt to summarize on-list discussion

PANA Proposal

- From Alper Yegin's mail to WG list
- First, we run PANA between the end-points. That yields a PANA session -- with a session-id and a PANA SA.
- Now that security association can be used with the PCP and the Authentication Tag Option from this draft.

PANA vs. In-Line Tradeoffs

- From Sam Hartman's response to Alper Yegin (on the list)
- Advantages of PANA include:
  - PANA exists as a published RFC
  - Some implementations available
  - Possibility of shared code when PANA and PCP used on the same host
- Disadvantages of PANA
  - PANA is more complex, as needed to handle network access use case
    - No need for liveness detection, reauthentication or IP address reconfiguration
  - Current PANA implementation do not support PANA applications other than network access
  - PANA protocol does not support specification of which application the PANA client is being used to authenticate
    - Difficult to separate network access authentication vs. authentication for PCP
  - May create need for PANA-to-PCP interface to confirm authentication

Thoughts on PANA vs. In-Line

- Both solutions rely on IETF standard security technologies
  - EAP over PANA vs. EAP over PCP
  - EAP is widely deployed, and existing implementations support multiple applications
  - PANA is less widely implemented/deployed
  - EAP over PCP is considerably simpler than having PCP use PANA over EAP
- Whatever the WG decides, we are willing to document

Discussion of PANA vs. In-Line?

Any Other Questions/Comments?

Adopt as a WG Draft?