Security Issues in PCP Base
draft-pcp-base-24.txt

Presentation By:

Margaret Wasserman

Painless Security

DS-Lite Specific Text

- DS-Lite deployment information is moving to a separate document & DS-Lite specific text in the Security Considerations section will move with it
- Will involve slight reorganization of Security Considerations section (editorial), but no major changes

THIRD_PARTY Option Discuss

- Security Considerations says:
  - Implementations that support the THIRD_PARTY Option (unless they can meet the constraints outlined in Section 17.1.2.2).
- Stephen Farrell (Security AD) has expressed concern about the THIRD_PARTY option
  - How can a client implementation know if its current deployment meets constraints?
  - Not sure THIRD_PARTY should be supported with out mandatory-to-implement crypto protection
  - May want to mandate ability to set further restrains on use of THIRD_PARTY (only for a given address range, etc.)

THIRD_PARTY Proposed Resolution

- Move THIRD_PARTY Option to a separate document
- Add a normative reference to the PCP Auth spec to that document, and indicate that it is mandatory-to-implement (but not to use)
- Consider other ways to limit THIRD_PARTY threats
  - Such as a conceptual list authorized THIRD_PARTY users, including valid address ranges for each

Nonce/Transaction ID

- Mail from Sam Hartman to the PCP list pointed out a potential security hole in the PCP simple threat model that is not present with implicit mappings and STUN
  - New DOS attack
  - Opens inline attacks to offline attackers
- Proposed solution:
  - Use of a per-mapping nonce value to limit vulnerability to inline attackers as in current case
    - One per <client, server, ip address, protocol, port> 5-tuple
  - Use of per-mapping nonce vs. transaction ID can preserve PCP operational model (i.e. section 6)