draft-ietf-pcp-base

Dan Wing, Stuart Cheshire, Mohamed Boucadair, Reinaldo Penno, Paul Selkirk

IETF85, November 2012

pcp-base and behave-lsn-requirements

- pcp-base-26 went through IESG review
- behave-lsn-requirements created new and different restrictions than pcp-base
- Underlying PCP vulnerability occurs with nested NATs
  - Not solely home NAT and CGN
- Decided to fix vulnerability in pcp-base itself

pcp-base Major Change, -26 to -29

- Have to use same Mapping Nonce to change PCP mapping
  - Protects from off-path attackers stealing port mappings (attack described by Sam Hartman)
    - Similar to TCP sequence number validation
  - Side effect: On joining network, PCP client can no longer clear mappings
    - Text suggests address assignment do that clearing
  - Allow PEER to reduce mapping to same as implicit mapping, but not shorter

pcp-base Minor Changes, -26 to -29

- Maximum PCP payload now 1100 bytes
  - Accommodates EAP over PANA over PCP
- Many more; see Changes section or diffs

pcp-base-28 WGLC

- pcp-base-28 had two week WGLC
  - To gather comments on Mapping Nonce change
  - No comments. Silence means consent?
- pcp-base-29 removes one latent paragraph that described PCP client should clear PCP mappings
  - Clearing mappings requires knowing Mapping Nonce
- Ready for IETF LC and ready for IESG

End