

PCP Working Group

Changes to pcp-base-27

September 21, 2012

PCP Working Group – Interim Meeting

Presented by Dan Wing, dwing@cisco.com

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

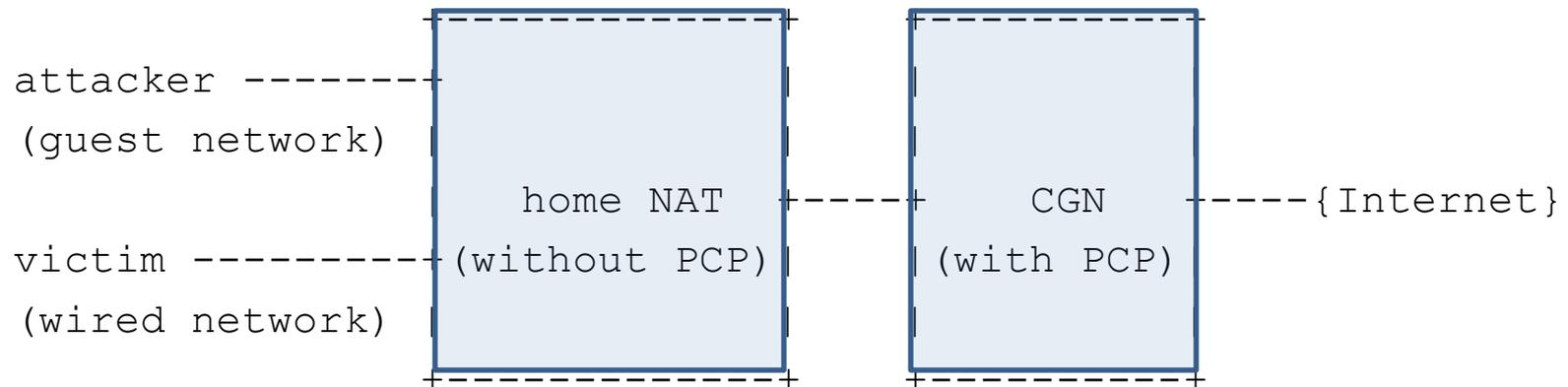
Summary of Major Changes

- Mapping Nonce
 - Prevent off-path attacker from modifying mapping
- Mapping Update is now MUST
 - Feedback from Pete Resnick
- Other changes

Mapping Nonce Change (1/4)

- Previously:
 - MAP and PEER creation and updates can use **any Mapping Nonce value**
- Now:
 - MAP and PEER creation and updates **MUST use same Mapping Nonce value**
- Reason for change:
 - Prevent off-path attacker from modifying mappings

Diagram: Attacker and Victim (2/4)



Mapping Nonce Side Effects (3/4)

- Side effect of change:
 - Cannot delete mappings belonging to a previous host with same IP address (don't know Nonce)
 - Cannot do 'delete all' (even knowing Nonce)
- So, pcp-base-27 encourages:
 - When host joins network, network SHOULD flush PCP mappings and non-PCP mappings. Good hygiene.

Mapping Nonce: Clearing Mappings (4/4)

- Discussion: do we need PCP to clear PCP mappings?
 - E.g., THIRD_PARTY sent by non-subscriber device ignore Mapping Nonce check and delete all

Mapping Update now Required

- Previously:
 - Mapping Update SHOULD
- Now:
 - Mapping Update MUST
- Reason for change:
 - Improve PCP reliability
 - Client can now expect PCP server to inform client of any mapping change, PCP server crash, etc.

Other Changes

- See section B.1, “Changes from draft-ietf-pcp-base-26 to -27”

End