PCP Authentication Requirements

draft-reddy-pcp-auth-req-01

T.Reddy, P.Patil, D.Wing, R.Penno

IETF-86

Requirements

REQ *1*: PCP client and server MUST provide client authentication. PCP Authentication MUST also generate message authentication key for integrity protection of PCP request and response.

REQ 2: PCP Server MUST be able to indicate that a request will not be processed without authentication.

REQ *3,4,5,6,7*: If the original request/response exchange was authenticated

- Client MUST be able to verify integrity and origin of unsolicited server responses
- Server MUST be able to send subsequent authenticated unsolicited responses.
- If previous security association has expired, the server MUST be able to trigger reauthentication with the client.
- If responses do not include integrate related to current security association, those messages MUST NOT be trusted without soliciting an integrity protected version.

REQ *8,9,10,11*: It is important that PCP not leak privacy information between the PCP client and the PCP server(s).

- PCP authentication MUST NOT exchange the PCP clients authentication credentials in clear text.
- Confidentiality of the PCP messages is OPTIONAL
- The authentication mechanism SHOULD be immune to passive dictionary attacks.
- PCP Authentication MUST ensure that an attacker snooping PCP messages cannot guess the SA.

REQ *12*: To ease troubleshooting and ensure fate sharing, PCP authentication and PCP messages MUST be multiplexed over the same port.

REQ *13*: PCP authentication MUST accommodate authentication between administrative domains.

REQ *14*: PCP client MUST be able to ascertain that it is talking to the right PCP server located in a different administrative domain.

REQ *15*: PCP authentication mechanism MUST be functional across address and port translation, including NAPT64 and NAPT44.

REQ *16,17*: A PCP proxy

- MUST validate message integrity of PCP messages from the PCP server and client respectively.
- MUST ensure message integrity after updating PCP requests/responses.

REQ *18*: A single PCP client on the host authenticates with the server. Other PCP clients on the same host SHOULD be able to reuse the previously negotiated key for integrity protection.

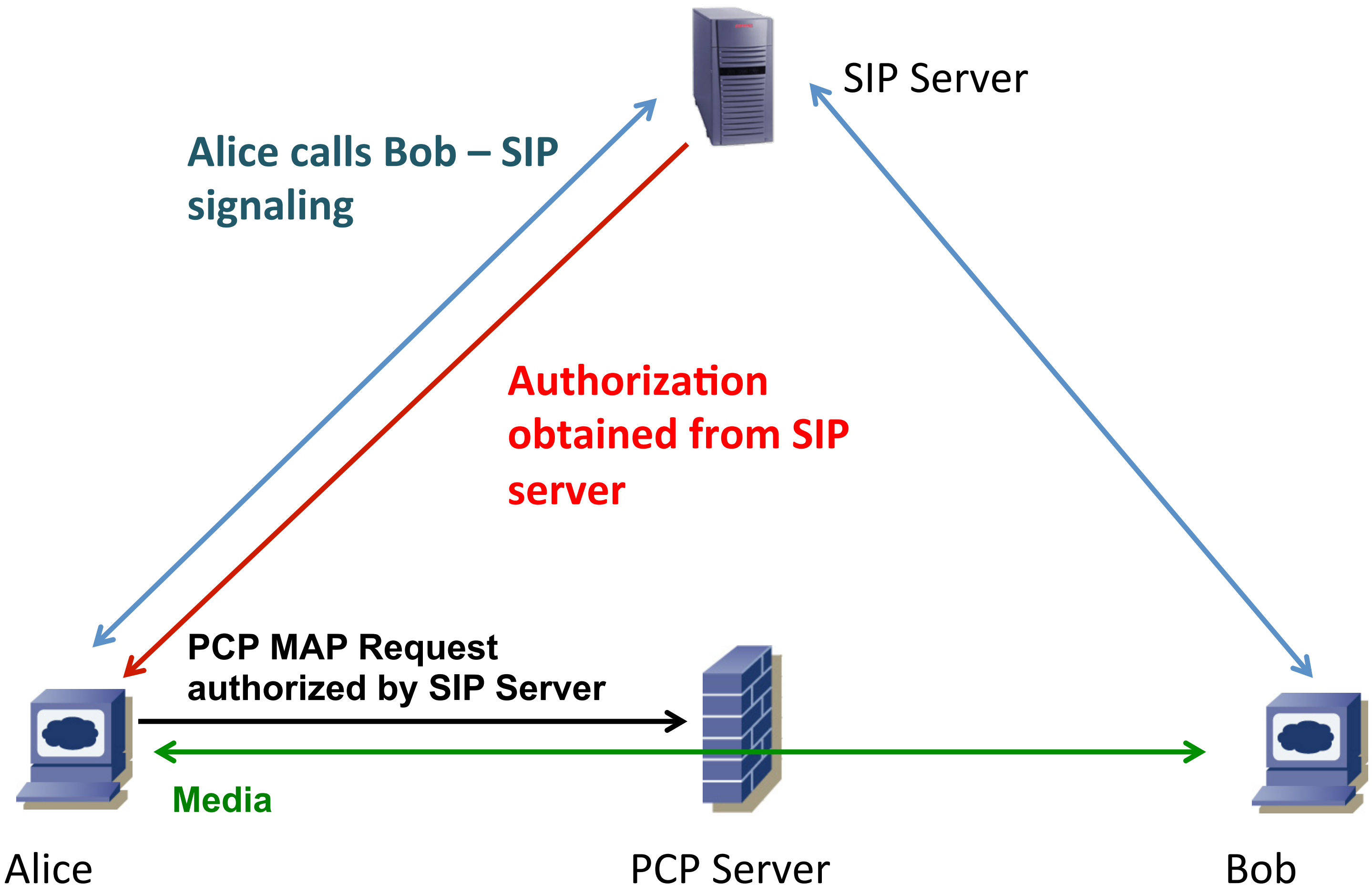
REQ *19*: All else equal, it is RECOMMENDED to choose a widely deployed authentication technique with known security properties rather than inventing a new authentication mechanism.

REQ *20*: Changes in PCP to accommodate authentication SHOULD be minimal so that updates and additions to the authentication mechanism have no bearing on PCP.

Other recommendations:
If a PCP client does not have credentials for a challenge with a certain REALM, it should attempt to use the username GUEST and password GUEST.

Provides integrity protection

Third Party Authorization



SIP Server

Alice calls Bob – SIP signaling

Authorization obtained from SIP server

PCP MAP Request authorized by SIP Server

Media

Alice

PCP Server

Bob

PCP Authentication Requirements

- Next steps