PCP Authentication Requirements

draft-reddy-pcp-auth-req

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

PCP Interim Meeting – April 2013

Agenda

- Draft updates based on the comments received from the WG.
- Finalize the requirement of using “Expired SA”

REQ-3: If the original PCP request/response was authenticated,

c. If a server wants to send an unsolicited message, but the previous security association has expired

1. The server can continue to use the same SA to protect messages pertaining to that mapping, even if the SA is technically expired.

   - Such server notifications will not change state in the PCP client.
   - The notification could be a trigger for the client to re-authenticate. For example, if the server indicates that external IP address/port has changed, the PCP client can then re-authenticate with the server to confirm if the external IP address/port for the mapping has indeed changed.

2. The server can optionally trigger re-authentication with the client.

REQ-4: It is important that PCP not leak privacy information between the PCP client and PCP server,

a. The authentication mechanism MUST be able to keep credentials hidden from eavesdroppers on path between client and server.

Why ?

• Exchanging username in clear text, could be considered privacy leakage; An adversary snooping the PCP messages can identify the IP address associated with the user “CEO of the company” and then continues to snoop the traffic identifying the user activity.

REQ-7: PCP client and server MUST be able mutually authenticate, especially when the PCP server is located in a different administrative domain from the PCP client. Credentials to gain access to the network could be different from the credentials used to authenticate with the PCP server.

REQ-9: A PCP proxy, that modifies PCP request/response before forwarding messages,

a. MUST validate message integrity of PCP messages from the PCP server and client respectively.
b. MUST ensure message integrity after updating the PCP message for cases described in sections 6 and 7 of [I-D.ietf-pcp-proxy].

REQ-10: It is RECOMMENDED that PCP authentication support a mechanism where only one PCP client on the host authenticates with the PCP server and other PCP clients be able to reuse the previously negotiated key for integrity protection. For example, multiple applications on the host like BitTorrent [BitTorrent], WebRTC[I-D.ietf-rtcweb-overview]/SIP [RFC3261] using PCP. Multiple authentication exchanges increase load on the PCP server and chatter on the network.

For example, if 'N' messages are to be exchanged for PCP authentication and 'M' independent applications implement their own PCP client, a total of N*M messages have to be exchanged and 'M' number of SAs maintained for each host.

Other recommendations :

It is recommended that there be support for a means to provide integrity protection without user authentication. For example, upon receiving a challenge with a certain REALM, if the PCP client does not have credentials for that REALM, the client will attempt to use a default username and password.

Next Steps