PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 17, 2013

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

May 16, 2013

PCP Authentication Requirements
draft-reddy-pcp-auth-req-03

Abstract

In an attempt to reach consensus on a PCP authentication mechanism, this document describes requirements for PCP authentication. It is hoped this can serve as the basis for a comparison of PCP authentication mechanisms.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document derives requirements for PCP Authentication from PCP deployment scenarios and scope described in PCP-base [I-D.ietf-pcp-base] and other PCP drafts. The document focuses on requirements and does not make a suggestion on the authentication mechanism to be used to satisfy requirements.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This note uses terminologies defined in [RFC4949] such as realm, security association, identity, credential etc.

3. Requirements

REQ-1: PCP MUST provide client authentication. PCP client and server MUST also be able to mutually authenticate. Mutual

authentication is especially necessary 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.

* The identity details of the client could be used by the PCP server to grant access to certain PCP opcodes or PCP options. For example GUESTS might not be permitted to use the MAP opcode and only ADMINISTRATOR might be permitted to use the THIRD_PARTY option.

* The identity details of the client could be used for auditing.

REQ-2: PCP Authentication MUST generate security association for integrity protection of PCP request and response. This and all subsequent requirements are not applicable to multicast PCP responses like ANNOUNCE.

REQ-3: A PCP server MUST be able to indicate that a request will not be processed without authentication.

REQ-4: If a PCP client authenticates with a PCP server,

a. The client MUST be able to verify the integrity and origin of responses from the server.

b. The server MUST be able to send authenticated unsolicited responses.

c. If a PCP response does not include integrity related to a current security association, then those messages MUST NOT be trusted without soliciting an integrity protected version.

d. If the server wants to send an unsolicited message, but the previous security association association for the mapping identified in the original PCP request 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 MUST be able to optionally trigger re-authentication with the client.

REQ-5: 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 the client and server.

b. Confidentiality of the PCP messages is OPTIONAL for PCP request and response of opcodes MAP, PEER, ANNOUNCE and options THIRD_PARTY, PREFER_FAILURE and FILTER as explained in PCP-base [I-D.ietf-pcp-base]. Other PCP drafts MUST evaluate if confidentiality is OPTIONAL for new PCP opcodes and options introduced.

c. PCP authentication SHOULD be immune to passive dictionary attacks.

d. PCP Authentication MUST ensure that an attacker snooping PCP messages cannot guess the SA.

REQ-6: To ease troubleshooting and ensure fate sharing, PCP authentication and PCP messages MUST be multiplexed over the same port.

REQ-7: PCP authentication MUST accommodate authentication between administrative domains. For example, a PCP client may wish to communicate directly to an ISP's PCP server, even though the in-home CPE router does not support PCP. In this scenario the PCP client needs to directly authenticate with the ISP's PCP server.

REQ-8: For the scenarios described in REQ-7, the PCP authentication mechanism MUST be functional across address and port translation, including NAPT64 and NAPT44.

REQ-9: A PCP proxy that modifies PCP requests and/or responses before forwarding messages:

```
      +------------+                       |
      | PCP Client |-----+                 |
      +--(Host 1)--+     |   +-----------+ |     +----------+
                         +---|           | |     |          |
                             | PCP Proxy |-------|PCP Server|
```

```
                         +---|           | |     |          |
      +------------+     |   +-----------+ |     +----------+
      | PCP Client |-----+                 |
      +--(Host 2)--+               possible boundary
                              <- Home side | ISP side ->
```

a. MUST be able to validate message integrity of PCP messages from the PCP server and client respectively.

b. MUST be able to 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 authentication on one port MUST be usable on other ports without requiring another authentication exchange for other ports. For example, there could 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.

REQ-11: It is RECOMMENDED to choose a widely deployed authentication technique with known security properties rather than inventing a new authentication mechanism.

REQ-12: Changes in PCP to accommodate authentication SHOULD be minimal so that updates and additions to the authentication mechanism have minimal bearing on modifying PCP.

4. Third Party Authorization

REQ-13: In addition to a two party authentication that has been discussed in this draft, a mechanism for third party authorization MUST also be supported. This is applicable in cases where a third party authorizes the use of a resource on a PCP server for a desired PCP client. For example, as depicted in Figure 1 , a PCP request to a PCP capable firewall authorized by a SIP proxy rather than by virtue of the end user making the PCP request. The PCP server is to permit a PCP MAP request from the PCP client if the user is making a SIP call with the Enterprise or a trusted SIP server in 3rd party network, otherwise do not allow MAP request from that particular user. In this scenario the first party is the user, second party is the PCP server (which is also the firewall) and the third party is

the SIP server, where the user is authorized to use MAP request only when making a call using the trusted SIP Server.

```
                  =========================
                  |  SIP Server        |
                  =========================
                            |  3rd Party Network
                            |
                            |
                    ==================
                    |    WAN         |-----+-+----+---+----+-+---
                    ==================                       |
                              |                              |
                              |                              |
                              |                              |
                      +-------+-------+                      |
                      | Firewall  -   |                      |
                      | PCP Server    |                      |
                      +-------+-------+                      |
                              |                              |
                              |                              |
      Network A               |                              | Network B
   -+-+-----+-----------+-+-----+--------         -----+-+-------+------
                              |                              |
                           +-+------+                 +--------+
                           | Alice  |                 | Bob    |
                           +--------+                 +--------+


   Users : Alice, Bob
```

Figure 1: WebRTC server in a different administrative domain

5. Other recommendations

REQ-14: There SHOULD be support for a means to provide integrity protection without user authentication, i.e., integrity protection for PCP messages exchanged between a PCP server and anonymous PCP clients. For example, a client visiting foreign networks such as a hotel, hot spot etc where the client may gain access to the network but does not know the credentials to authenticate with the PCP server.

a. An SA MUST be made available to the client and server, which will be used for integrity protection of PCP messages. The negotiation of SA should be secure such that the SA is only known to the anonymous client and PCP server.

b. A PCP client MUST be able to validate that it is communicating with the designated PCP server and not an attacker posing as a PCP server.

6. IANA Considerations

This document does not require any action from IANA.

7. Security Considerations

This entire document is about security considerations for PCP.

8. References

8.1. Normative References

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", draft-ietf-pcp-base-29 (work in progress), November 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

8.2. Informative References

[BitTorrent]
, "Cohen, B., "The BitTorrent Protocol Specification Version 11031", February 2008.", September 2012.

[I-D.ietf-pcp-proxy]
Boucadair, M., Penno, R., and D. Wing, "Port Control Protocol (PCP) Proxy Function", draft-ietf-pcp-proxy-02 (work in progress), February 2013.

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-06 (work in progress), February 2013.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

Appendix A. Change History

A.1. Change from -01 to -02

- Requirements reorganized based on commonality

- New requirement 3(c(2)) added.

A.2. Change from -02 to -03

- Merged REQ-1 and REQ-7

- Updated Section 5 "Other recommendations"

Authors' Addresses

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tireddy@cisco.com

Prashanth Patil
Cisco Systems, Inc.
Bangalore
India

Email: praspati@cisco.com

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: dwing@cisco.com

Reinaldo Penno
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: repenno@cisco.com