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

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

February 13, 2013

PCP Authentication Requirements
draft-reddy-pcp-auth-req-00

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 17, 2013.

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].

3. Requirements

REQ-1: PCP client and server MUST provide client authentication. The client could be a host running a PCP client or middle box (e.g., NAT) running a PCP Proxy.

* 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 would not be permitted to use MAP opcode, ADMINISTRATOR is only permitted to use THIRD_PARTY option.

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

PCP Authentication MUST also generate message authentication key for integrity protection of PCP request and response.

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

REQ-3: PCP allows a server to send multiple responses. To properly support that model with authentication, a client that sends an authenticated request MUST be able to verify the integrity and origin of an subsequent unsolicited response should it choose to do so.

REQ-4: PCP allows a server to send multiple responses. If the original request/response exchange was authenticated, a server MUST be able to send a subsequent authenticated unsolicited Response.

REQ-5: PCP allows a server to send multiple responses. If the server wants to send an unsolicited message, but the previous security association has expired, the server MUST be able to trigger re-authentication with the client.

REQ-6: Clients that have authenticated with the server MUST verify the integrity of the contents of all unsolicited responses.

REQ-7: If there are circumstances where PCP responses do not include integrity related to a current security association, then those messages MUST NOT be trusted without soliciting an integrity protected version.

REQ-8: It is important that PCP not leak privacy information between the PCP client and the PCP server(s). Thus, the PCP authentication MUST NOT exchange the PCP clients authentication credentials in clear text. For example, exchanging the PCP username in clear text would violate this requirement.

REQ-9: 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 explained in PCP-base [I-D.ietf-pcp-base]. Other PCP drafts MUST evaluate if confidentiality is OPTIONAL or not for new PCP opcodes and options introduced.

REQ-10: The authentication mechanism SHOULD be immune to passive dictionary attacks.

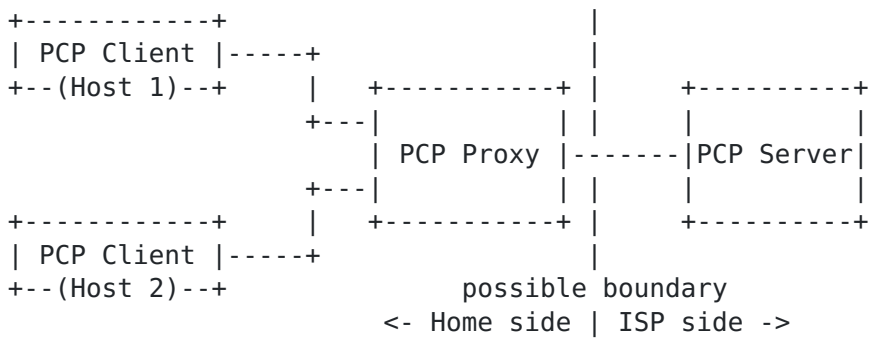
REQ-11: PCP Authentication MUST ensure that an attacker snopping the PCP messages cannot guess the SA.

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

REQ-13: 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-14: For the scenarios described in REQ-13, PCP authentication mechanism MUST be functional across address and port translation, including NAPT64 and NAPT44.

REQ-15: If a PCP client and server desire authentication then a PCP proxy, that modifies PCP request/response before forwarding messages, MUST validate message integrity of PCP messages from the PCP server and client respectively.



REQ-16: PCP Proxy must also ensure message integrity after updating the PCP message for cases described in sections 6 and 7 of [I-D.ietf-pcp-proxy].

REQ-17: PCP authentication SHOULD support a mechanism where only one PCP client on the host will authenticate with the PCP server and any other PCP clients SHOULD 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.

REQ-18: 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-19: Changes in PCP to accommodate authentication SHOULD be minimal so that updates and additions to the authentication mechanism have no bearing on modifying PCP.

4. Other recommendations

- Upon receiving a challenge with a certain REALM, if the PCP client does not have credentials for that REALM, it SHOULD attempt to use the username GUEST and password GUEST. The GUEST credentials are expected to be configured on infrastructure where PCP authentication is not necessary, but such guest users are given some (minimal) authorization to use PCP. This addresses the problem when the client is visiting foreign networks like hotel, hot spot etc where it may gain access to the network but does not know the credentials to authenticate to the ISP's PCP server when the in-home CPE router does not support PCP and the PCP client

needs to directly authenticate with the ISP's PCP server (REQ-14).

5. IANA Considerations

This document does not require any action from IANA.

6. Security Considerations

This document does not define an architecture nor a protocol; as such it does not raise any security concerns.

7. References

7.1. 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.

7.2. 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-05 (work in progress), December 2012.

[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.

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