Network Working Group
Internet-Draft
Updates: 5191 (if approved)
Intended status: Standards Track
Expires: January 04, 2014

Y. Ohba
Y. Tanaka
Toshiba
S. Das
ACS
A. Yegin
Samsung
T. Tsou
Huawei

July 03, 2013

Provisioning Message Authentication Key for PCP using PANA (Side-by-Side Approach)

draft-ohba-pcp-pana-04

Abstract

This document specifies a mechanism for provisioning PCP (Port Control Protocol) message authentication key using PANA (Protocol for carrying Authentication for Network Access).

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 January 04, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

PCP (Port Control Protocol) [I-D.ietf-pcp-base] is used for an IPv6 or IPv4 host to control how incoming IPv6 or IPv4 packets are translated and forwarded by a network address translator (NAT) or by a simple firewall. It also allows a host to optimize its outgoing NAT keepalive messages.

In order to provide integrity protection for PCP messages, a message authentication mechanism for PCP is defined in [I-D.ietf-pcp-authentication]. Three components are defined in [I-D.ietf-pcp-authentication]: (1) PCP options for providing per-packet origin authentication, integrity and replay protection, (2) PCP Security Association (SA) for generating the aforementioned options, and (3) PCP options for generating PCP SA from execution of EAP authentication.

The third component seems to define a new EAP lower-layer within PCP. In this document, PANA (Protocol for carrying Authentication for Network Access) [RFC5191] is proposed instead of defining a new EAP lower-layer. This draft along with other two components described in [I-D.ietf-pcp-authentication] provides a complete solution which otherwise will duplicate the work of transporting EAP over UDP. The proposed solution can run over a single PCP port.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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 RFC 2119 [RFC2119].

2. Establishing a PCP SA

A PCP client should know the authentication capability of the PCP server before deciding to use PANA with it. PCP client can obtain this information either via an out-of band scheme (e.g., manual configuration, DHCP), or via an in-band scheme (e.g., trial-and-error, PCP ANNOUNCE Opcode). In trial-and-error scheme the PCP client tests the PCP server by sending its first request without any authentication. If the PCP server returns AUTHENTICATION_REQUIRED error message, then the PCP client concludes that the PCP server is mandating use of authentication. Otherwise the PCP client concludes that the PCP server is allowing unauthenticated PCP. See Section 3 for the details of ANNOUNCE-based discovery.

A PaC (PANA Client) on a PCP client node initiates PANA authentication over the PCP port number (To be assigned) prior to sending an authenticated PCP message. The initiation may be requested by the PCP client. We assume that a PAA (PANA Authentication Agent) is implemented on each PCP server that supports authenticated PCP messages. Therefore, the PCP server's IP address is used as the address of the PAA. The PANA authentication for establishing a PCP SA is dedicated to the PCP usage only.

In order to distinguish PANA and PCP messages that are multiplexed over the PCP port number (To be assigned), bit 0 of Reserved field of PANA header is used and whose value is 1. In PCP, the corresponding bit is part of Version field and whose value is 0, as shown in Figure 1. For this scheme to work, PCP Version values less than 128 MUST be used.

```
           0
           0 1 2 3 4 5 6 7
          +-+-+-+-+-+-+-+-+
          |    Reserved     ...
          +-+-+-+-+-+-+-+-+
              The first 8 bits of PANA header (bit 0 value is 1)

           0
           0 1 2 3 4 5 6 7
          +-+-+-+-+-+-+-+-+-
          |    Version    | ...
          +-+-+-+-+-+-+-+-+-
               The first 8 bits of PCP header (bit 0 value is 0)
```

Figure 1: The First 8 bits of PANA and PCP Headers

When a PANA message is carried over the PCP port number (To be assigned), the sender MUST set bit 0 of Reserved field. Other Reserved bits and bit 0 when used over port numbers other than the PCP port number (To be assigned) are still governed by [RFC5191].

Upon successful PANA authentication, the message authentication key for PCP message is derived from the EAP MSK as follows:

PCP_AUTH_KEY = prf+(MSK, "IETF PCP" | SID | KID)

where where | denotes concatenation.

o The prf+ function is defined in IKEv2 [RFC5996]. The pseudo-random function to be used for the prf+ function is negotiated using PRF-Algorithm AVP in the initial PANA-Auth-Request and PANA-Auth-Answer exchange with 'S' (Start) bit set, as defined in [RFC5191].

o "IETF PCP" is the ASCII code representation of the non-NULL terminated string (excluding the double quotes around it).

o SID is a four-octet PANA Session Identifier [RFC5191].

o KID is the content of the Key-ID AVP [RFC5191] associated with the MSK.

The same integrity algorithm used for the PANA session MUST be used for PCP message authentication.

The PCP_AUTH_KEY and its associated parameters (i.e., the IP addresses of the PCP client and PCP server, PANA Session ID, Key ID, message authentication algorithm and lifetime) are passed from the

PAA application to the PCP server application on the same PCP server device, and also passed from the PaC application to the PCP client application on the same PCP client node, using an API. The API can be implementation-specific, and therefore is not specified in this document. The PANA Session ID and Key ID are used in the corresponding fields (Session ID, Key ID) of the Authentication Tag Option.

Once a PCP SA is established, any PCP message that does not contain a valid Authentication Tag and a fresh Nonce under the current PCP SA MUST be silently discarded.

The PCP SA MUST be immediately deleted when the corresponding PANA SA is deleted. The PCP SA SHALL remain as long as the corresponding PANA SA exists.

If the PCP server that requires authenticated PCP message receives an unauthenticated PCP request, it returns an "AUTHENTICATION_REQUIRED" result code.

If a PCP SA needs to be updated, the PCP client or the PCP server SHALL initiate PANA re-authentication phase. If a PCP SA needs to be re-established after expiration or loss of the SA for an existing PCP mapping state, the PCP client or the PCP server SHALL initiate PANA authentication and authorization phase.

3. Authentication Capablity Discovery

A PCP client supporting PCP authentication MAY send an ANNOUNCE request with an AUTH_CAPABILITY option prior to initiating PANA in order to know whether a PCP server supports PCP authentication. A PCP server supporting PCP authentication SHALL return an ANNOUNCE response with "SUCCESS" result code and an AUTH_CAPABILITY option.

The AUTH_CAPABILITY Option is formatted in Figure 2.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Option Code=TBA|  Reserved     |         Option Length=0       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: AUTH_CAPABILITY Option Format

The fields are described below:

Option Name: AUTH_CAPABILITY
Number: To be assigned by IANA

Purpose: To indicate the sender's authentication capability
Valid for Opcodes: ANNOUNCE
Length: 0
May appear in: requests, responses
Maximum occurrences: 1

4. Security Considerations

The key provisioning mechanism described in this document provides a cryptographic binding between a PANA session and a PCP SA based on using the PANA session identifier and key identifier in the PCP_AUTH_KEY derivation function.

For EAP channel binding [RFC6677], it is required for a PAA to distinguish whether PANA authentication is conducted for network access authentication or PCP authentication. Such a distinction can be made using the assigned port number over which the PANA authentication is conducted, namely, the PANA authentication is conducted for PCP authentication when the port number is the PCP port number (to be assigned), and it is for network access authentication when the port number is the PANA port number (716). How the corresponding information is conveyed from the PAA to the authentication server is outside the scope of this document.

5. IANA Considerations

A new result code for "AUTHENTICATION_REQUIRED" needs to be allocated. The usage of the "AUTHENTICATION_REQUIRED" result code is described in Section 2.

A new PCP Option for AUTH_CAPABILITY needs to be allocated. The usage of AUTH_CAPABILITY Option is described in Section 3.

6. Acknowledgments

Authors would like to acknowledge Dave Thaler for his suggestion on the use of ANNOUNCE Opcode for capability discovery, and Richard Martija, Pedro Moreno Sanchez and Rafa Marin-Lopez for fully implementing the mechanism described in this document.

7. Normative References

[I-D.ietf-pcp-authentication]
Wasserman, M., Hartman, S., and D. Zhang, "Port Control Protocol (PCP) Authentication Mechanism", draft-ietf-pcp-authentication-01 (work in progress), October 2012.

[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.

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6677] Hartman, S., Clancy, T., and K. Hoeper, "Channel-Binding Support for Extensible Authentication Protocol (EAP) Methods", RFC 6677, July 2012.

Appendix A. Change History

Changes from -00 to -01 :

- Added Alper to authors.
- Changed to use demultiplexing approach from seperate key management.
- Removed PCP server id from key derivation algorithm.
- Added EAP channel binding discussion in Security Considerations section.

Changes from -01 to -02 :

- Added Editor's Note in Section 2.

Changes from -02 to -03 :

- Changed document title
- Added Tina to authors.
- Used Bit 0 instead of Bits 5-6-7 to consider PCP Version 0 used by NAT-PCP.
- Added ANNOUNCE-based authentication capability discovery.

- Moved RFC 2119 to Normative Reference.

Changes from -03 to -04 :

- Added text for SA revnew and re-establishment.

Authors' Addresses

Yoshihiro Ohba
Toshiba Corporate Research and Development Center
1 Komukai-Toshiba-cho
Saiwai-ku, Kawasaki, Kanagawa 212-8582
Japan

Phone: +81 44 549 2127
Email: yoshihiro.ohba@toshiba.co.jp

Yasuyuki Tanaka
Toshiba Corporate Research and Development Center
1 Komukai-Toshiba-cho
Saiwai-ku, Kawasaki, Kanagawa 212-8582
Japan

Phone: +81 44 549 2127
Email: yatch@isl.rdc.toshiba.co.jp

Subir Das
Applied Communication Sciences
1 Telcordia Drive
Piscataway, NJ 08854
USA

Email: sdas@appcomsci.com

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: Tina.Tsou.Zouting@huawei.com
URI: http://tinatsou.weebly.com/contact.html