Network Working Group
Internet-Draft
Updates: 5191 (if approved)
Intended status: Standards Track
Expires: March 14, 2013

Y. Ohba
Y. Tanaka
Toshiba
S. Das
ACS
A. Yegin
Samsung

September 10, 2012

Provisioning Message Authentication Key for PCP using PANA
draft-ohba-pcp-pana-01

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 to IETF 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 March 14, 2013.

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 [RFC2119].

2. Establishing a PCP SA

A PaC (PANA Client) on a PCP client node initiates PANA authentication over the PCP port number (To be assigned) prior to send 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), bits 5-6-7 of Reserved field of PANA header is used and whose value is 0b000 In PCP, the

corresponding bits are part of Version field and whose value are no less than 0b010, as shown in Figure 1. Note that "0b" is used as a prefix for expressing binary numbers in most-significant-bit first notation. For this scheme to work, PCP Version values {0, 8, 16, 24, ... 248} MUST NOT be used.

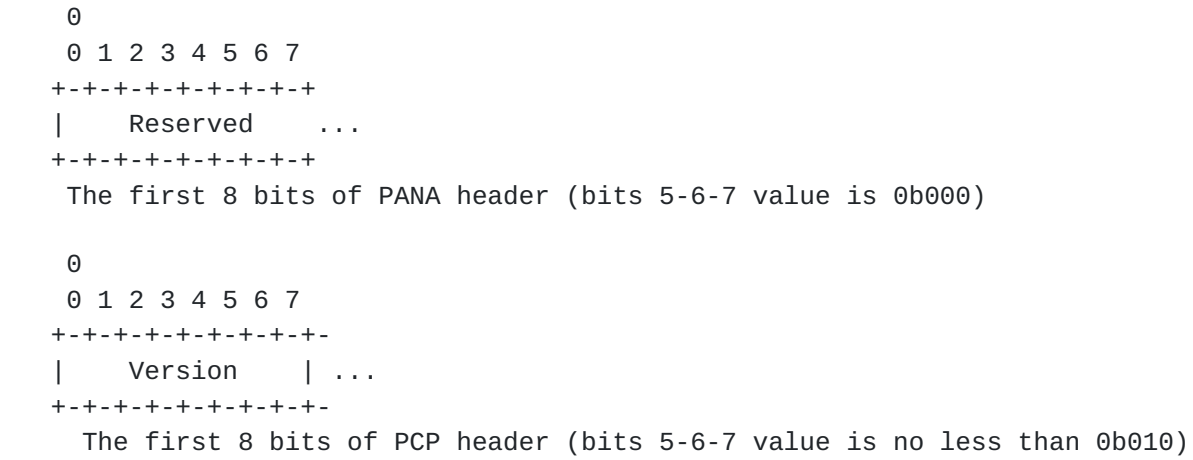

Figure 1: The First 8 bits of PANA and PCP Headers

When a PANA message is carried over the PCP port number (To be assigned), the sender MUST clear bits 5-6-7 of Reserved field and the receiver MUST ignore them. Other Reserved bits and bits 5-6-7 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.

- 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].

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

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

- 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.

3. 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.

4. IANA Considerations

There is no IANA actions required for this document.

5. Acknowledgments

TBD.

6. References

6.1. Normative References

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[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.

[I-D.ietf-pcp-base] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", draft-ietf-pcp-base-26 (work in progress), June 2012.

[I-D.ietf-pcp-authentication] Wasserman, M., Hartman, S., and D. Zhang, "Port Control Protocol (PCP) Authentication Mechanism", draft-ietf-pcp-authentication-00 (work in progress), June 2012.

6.2. Informative References

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

Appendix A. Change History

Changes from -00 to -01 :

o 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.

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