Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 8, 2012

R. Cragie
PG&E
P. Duffy
Cisco
Y. Ohba (Ed.)
Toshiba
A. Yegin
Samsung

September 5, 2011

Protocol for Carrying Authentication for Network Access (PANA) Extension for Key Wrap

draft-ohba-pana-keywrap-04

Abstract

This document specifies an extension to PANA (Protocol for carrying Authentication for Network Access) for secure delivery of keys from a PAA (PANA Authentication Agent) to a PaC (PANA Client).

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 8, 2012.

Table of Contents

1. Introduction

PANA [RFC5191] as a UDP-based protocol to perform EAP authentication between a PaC (PANA Client) and a PAA (PANA Authentication Agent).

This document specifies an extension for PANA [RFC5191] to securely distribute keys from a PAA (PANA Authentication Agent) to a PaC (PANA Client) using a key wrap algorithm negotiated between the PAA and PaC. A typical usage for this extension is group key distribution. For example, a ZigBee Network Key is a group key that is shared among members of a ZigBee network and used for bootstrapping IEEE 802.15.4 link-layer ciphering between adjacent ZigBee nodes.

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. Basic Operation

In the Authentication and Authorization phase, a PAA and a PaC negotiate on a key wrap algorithm. A PAA that uses a key wrap AVP MUST include one or more Key-Wrap-Algorithm AVPs in the initial PANA-Auth-Request message with the 'S' (Start) bit set. The PaC, if it supports a key wrap AVP, then selects one key wrap algorithm from these AVPs carried in the initial PANA-Auth-Request, and it responds with the initial PANA-Auth-Answer message carrying one Key-Wrap-Algorithm AVP for the selected algorithm.

Upon successful PANA authentication, a key wrap AVP MAY be placed in the PAR message, which will have the header 'C' (Complete) bit set and contain a Result-Code AVP indicating PANA_SUCCESS. A key wrap AVP MUST be of type OctetString, MUST contain exactly one key of a specific type, and MAY be defined as a standard or vendor-specific AVP. A distinct AVP code MUST be defined for each key type. The key data carried in the key wrap AVP is encrypted by a key encryption key (see Section 3) using the negotiated key wrap algorithm (see Section 4).

When a key needs to be updated in the access phase a PANA ping exchange is used. There are two modes for key update; pull mode and push mode. In the pull mode, the PaC sends a PANA-Notification-Request message with the 'P' (Ping) bit set and the PAA responds with a PANA-Notification-Answer message with the 'P' (Ping) bit set and

carrying a key wrap AVP if there is a new key. In the push mode, the PAA sends a PANA-Notification-Request message with the 'P' (Ping) bit set and carrying a key wrap AVP to the PaC, and the PaC returns a PANA-Notification-Answer message with the 'P' (Ping) bit set to the PAA.

3. Key Encryption Key

PANA_KEY_ENC_KEY is used for encrypting a key to be delivered to the PaC. PANA_KEY_ENC_KEY is derived from MSK as follows.

```
PANA_KEY_ENC_KEY = the first N bits of
      prf+(MSK, "Key Encryption Key" | SID | KID)
      where | denotes concatenation.
```

- The prf+ function is defined in IKEv2 [RFC4306]. The pseudo-random function used for the prf+ function is specified in the PRF-Algorithm AVP carried in a PANA-Auth-Request message with 'S' (Start) bit set.

- N is the bit length of the PANA_KEY_ENC_KEY. The value of N depends on the key wrap algorithm. For AES Key Wrap with Padding algorithm, N=256.

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

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

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

4. Key-Wrap-Algorithm AVP

The Key-Wrap-Algorithm AVP (AVP Code 12 (*needs IANA allocation*)) is used for conveying the identifier of a key wrap algorithm used for encrypting a key carried in a key wrap AVP. The AVP data is of type Unsigned32. The following key wrap algorithm identifiers are defined in this document.

```
AES_KEY_WRAP_WITH_PADDING_256            1
```

AES Key Wrap with Padding algorithm with a 256-bit key encryption key as specified in [RFC5649].

AES_CTR 2

AES-CTR (Counter) key wrap algorithm. A modified version of AES-CCM is used where no MAC block is contained in the output blocks of its encryption processing. The formatting function and counter generation function of AES-CCM as specified in Appendix A of [NIST_SP800_38C] are used, with the following parameters:

n, octet length of nonce, is 12.

q, octet length of message length field, is 3.

The 12-octet nonce consists of a 4-octet Key-Id, a 4-octet Session ID and a 4-octet Sequence Number in that order where each 4-octet value is encoded in network byte order. The Session ID and Sequence Number values must be the same as those in the PANA message carrying the key wrap AVP. The Key-Id value must be the same as the one used for deriving the PANA_KEY_ENC_KEY. The output blocks of the encryption processing of the modified version of AES-CCM are encoded as OctetString data in the Value field of a key wrap AVP. The modified version of AES-CCM is compatible with the CTR mode specified in [NIST_SP800_38A].

In the absence of an application profile specifying otherwise, all implementations MUST support AES_KEY_WRAP_WITH_PADDING_256.

5. ZigBee-Network-Key AVP

The ZigBee-Network-Key AVP (AVP Code 13 (*needs IANA allocation*)) is a key wrap AVP of type OctetString, carrying an encrypted 17-octet key material which consists of a 16-octet Network Key used in the ZigBee IP network over which PANA is operating, followed by a 1-octet Network Key Sequence Number.

6. Security Considerations

Implementations must protect the PANA_KEY_ENC_KEY. Implementations must not use the PANA_KEY_ENC_KEY for other purposes than wrapping keys in key wrap AVPs and must not use wrapped keys for other purposes than their intended usages. Compromise of the PANA_KEY_ENC_KEY may result in the disclosure of all keys that have been wrapped with the PANA_KEY_ENC_KEY, which may lead to the compromise of all traffic protected with those wrapped keys.

According to [RFC5649], the effective security provided to data protected with the wrapped key is determined by the weaker of the

algorithm associated with the key encryption key and the algorithm associated with the wrapped key. In this document, PANA_KEY_ENC_KEY is the key encryption key. For ZigBee Network Key as the wrapped key, the length of the Network Key is 128 bits, therefore, with the PANA_KEY_ENC_KEY of at least 128 bits in length, at most 128 bits protection is provided to any data that depends on the Network Key.

7. IANA Considerations

As described in Section 4, and following the new IANA allocation policy on PANA AVPs [RFC5872], a standard AVP Code of 12 needs to be assigned for Key-Wrap-Algorithm AVP, and a standard AVP Code of 13 needs to be assigned for ZigBee-Network-Key.

Also, the key wrap algorithm identifier namespace for Key-Wrap-Algorithm AVP needs to be managed by IANA. The value of 1 (AES_KEY_WRAP_WITH_PADDING_256) and 2 (AES_CTR) are used in this document. Allocating additional values can be done on IETF Review or IESG Approval [RFC5226].

8. Acknowledgments

The authors would like to thank Michael StJohns, Vlad Gherghisan and Owen Kirby for their valuable comments.

9. References

9.1. Normative References

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

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

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

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226,

May 2008.

[RFC5649] Housley, R. and M. Dworkin, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm", RFC 5649, September 2009.

[RFC5872] Arkko, J. and A. Yegin, "IANA Rules for the Protocol for Carrying Authentication for Network Access (PANA)", RFC 5872, May 2010.

[NIST_SP800_38A] "Recommendation for Block Cipher Modes of Operation: Methods and Techniques", NIST SP800-38A, December 2001.

[NIST_SP800_38C] "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", NIST SP800-38C, May 2004.

9.2. Informative References

[ianaweb] IANA, "Number assignment", http://www.iana.org.

Authors' Addresses

Robert Cragie
Pacific Gas & Electric
Gridmerge Ltd., 89 Greenfield Crescent
Wakefield, WF4 4WA
UK

Email: robert.cragie@gridmerge.com

Paul Duffy
Cisco Systems
200 Beaver Brook Road
Boxborough, MA 01719
USA

Email: paduffy@cisco.com

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

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org