Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 11, 2013

A. Yegin
Samsung
R. Cragie
Gridmerge Ltd.

September 7, 2012

Encrypting PANA AVPs
draft-yegin-pana-encr-avp-10

Abstract

This document specifies a mechanism for delivering PANA (Protocol for Carrying Authentication for Network Access) AVPs (Attribute-Value Pairs) in encrypted form.

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 March 11, 2013.

Copyright Notice

Copyright (c) 2012 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

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

Various types of payloads are exchanged as part of the network access authentication and authorization. These payloads are carried in PANA Attribute-Value Pairs (AVPs). AVPs can be integrity-protected using the AUTH AVP when EAP authentication generates cryptographic keying material. AVPs are transmitted in the clear (i.e., not encrypted).

There are certain types of payloads that need to be delivered privately (e.g., network keys, private identifiers, etc.). This document defines a mechanism for applying encryption to selected AVPs.

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. Details

This document extends the AVP set defined in Section 8 of [RFC5191] by defining two new AVPs: the Encryption-Algorithm AVP (see Section 4) and the Encr-Encap AVP (see Section 5). Two new encryption keys, PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY, are defined to encrypt AVPs from the PaC to the PAA and AVPs from the PAA to the PaC respectively (see Section 3).

When encryption needs to be used, the required algorithm is negotiated as follows: the PAA SHALL send the initial PANA-Auth-Request carrying one or more Encryption-Algorithm AVPs supported by it. The PaC SHALL select one of the algorithms from this AVP, and it SHALL respond with the initial PANA-Auth-Answer carrying one Encryption-Algorithm AVP for the selected algorithm. Once PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY have been generated, a PANA message MAY contain an Encr-Encap AVP.

3. Encryption Keys

PANA_PAC_ENCR_KEY is used for encrypting the AVP payload of the Encr-Encap AVP sent in a PANA message from the PaC to the PAA.

PANA_PAC_ENCR_KEY SHALL be computed according to the following formula:

```
PANA_PAC_ENCR_KEY = prf+(MSK, "IETF PANA PaC Encr" | I_PAR |
                         I_PAN | PaC_nonce | PAA_nonce | Key_ID)
```

PANA_PAA_ENCR_KEY is used for encrypting the AVP payload of the Encr-Encap AVP sent in a PANA message from the PAA to the PaC. PANA_PAA_ENCR_KEY SHALL be computed according to the following formula:

```
PANA_PAA_ENCR_KEY = prf+(MSK, "IETF PANA PAA Encr" | I_PAR |
                         I_PAN | PaC_nonce | PAA_nonce | Key_ID)
```

In both cases:

- The prf+ function is defined in IKEv2 [RFC5996].

- The pseudo-random function (PRF) to be used for the prf+ function SHALL be negotiated using PRF-Algorithm AVP in the initial PANA-Auth-Request and PANA-Auth-Answer exchange with 'S' (Start) bit set as described in Section 4.1 of [RFC5191]

- MSK is the master session key generated by the EAP method [RFC3748]. PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY MUST be recalculated whenever a new MSK is generated by the EAP method.

- "IETF PANA PaC Encr" and "IETF PANA PAA Encr" are the ASCII code representations of the respective non-NULL terminated strings (excluding the double quotes around them).

- I_PAR and I_PAN are the initial PANA-Auth-Request and PANA-Auth-Answer messages (the PANA header and the following PANA AVPs) with 'S' (Start) bit set, respectively.

- PaC_nonce and PAA_nonce are values of the Nonce AVP carried in the first non-initial PANA-Auth-Answer and PANA-Auth-Request messages in the authentication and authorization phase or the first PANA-Auth-Answer and PANA-Auth-Request messages in the re-authentication phase, respectively.

- Key_ID is the value of the Key-Id AVP.

The length of PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY depends on the

encryption algorithm in use.

4. Encryption-Algorithm AVP

The Encryption-Algorithm AVP (AVP code TBD1) is used for conveying the encryption algorithm to be used with the Encr-Encap AVP. The AVP value data is of type Unsigned32.

Only one encryption algorithm identifier AES128_CTR (code 1) is identified by this document. Encryption algorithm identifier values other than 1 are reserved for future use. Future specifications are allowed to extend this list.

AES128_CTR: 1

In the absence of an application profile specifying otherwise, all implementations SHALL support AES128_CTR.

4.1. AES128_CTR Encryption Algorithm

The AES128_CTR encryption algorithm uses the AES-CTR (Counter) mode of operation as specified in [NIST_SP800_38A] using the AES-128 block cipher. The formatting function and counter generation function as specified in Appendix A of [NIST_SP800_38C] are used, with the following parameters:

n = 12,
q = 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 SHALL be the same as those in the PANA message carrying the key Encr-Encap AVP. The Key-Id value SHALL be the same as the one used for deriving PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY. The output blocks of the encryption processing are encoded as OctetString data in the Value field of a Encr-Encap AVP.

Note the first counter block used for encryption is Ctr_1, where "_1" denotes "subscript 1" as described in section A.3 of [NIST_SP800_38C]. For example, given the following:

Key-Id = 0x55667788,
Session ID = 0xaabbccdd,
Sequence Number = 0x11223344

The first counter block used for encryption will be:

0x0255667788aabbccdd11223344000001

where the initial 0x02 represents the Flags Field of the counter block.

The nonce meets the requirement of uniqueness per key usage providing the sequence number does not wrap. Therefore, for the purpose of generating new keys:

- If Encr-Encap AVPs are being sent from the PaC to the PAA and the sequence number is about to wrap, the PaC SHALL initiate PANA re-authentication as described in Section 4.3 of [RFC5191].

- If Encr-Encap AVPs are being sent from the PAA to the PaC and the sequence number is about to wrap, the PAA SHALL initiate PANA re-authentication as described in Section 4.3 of [RFC5191].

Re-authentication ensures the generation of a new MSK [RFC3748] and thus a new PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY.

5. Encr-Encap AVP

The Encr-Encap AVP (AVP code TBD2) is used to encrypt one or more PANA AVPs. Format of the Encr-Encap AVP depends on the negotiated encryption algorithm.

When the negotiated encryption algorithm identifier is AES128_CTR (code 1), AVP data payload is occupied by the encrypted AVPs.

There SHALL be only one Encr-Encap AVP in a PANA message. All AVPs that require encryption SHALL be encapsulated within the Encr-Encap AVP.

The Encr-Encap AVP uses either PANA_PAC_ENCR_KEY or PANA_PAA_ENCR_KEY and the encryption algorithm negotiated by the Encryption-Algorithm AVP. The Encr-Encap AVP SHALL only be used if the EAP method generates cryptographic keys (specifically the MSK [RFC3748]).

The Encr-Encap AVP MAY be used in a PANA message from the PaC to the PAA when the encryption algorithm has been successfully negotiated and once PANA_PAC_ENCR_KEY has been generated.

The Encr-Encap AVP MAY be used in a PANA message from the PAA to the PaC when the encryption algorithm has been successfully negotiated and once PANA_PAA_ENCR_KEY has been generated.

The Encr-Encap AVP MAY be used in the very first PANA message carrying the Result-Code AVP set to PANA_Success value, and any subsequent message within the same PANA session.

6. Encryption Policy

The specification of any AVP SHOULD state that the AVP either shall or shall not be encrypted using Encr-Encap AVP. The specification of an AVP MAY state that the AVP may (or may not) be encrypted using Encr-Encap AVP. The specification SHOULD use a table in the format specified in Section 6.1. If the specification of an AVP is silent about whether the AVP shall or shall not be encrypted using Encr-Encap AVP, this implies that the AVP MAY be encrypted using Encr-Encap AVP.

6.1. Encryption Policy Specification

This section defines a table format for the specification of whether an AVP shall or shall not be encrypted using Encr-Encap AVP.

The table uses the following symbols:

Y: The AVP SHALL be encrypted using Encr-Encap AVP. If the AVP is encountered not encrypted using Encr-Encap AVP, it SHALL be considered invalid and the message containing the AVP SHALL be discarded.

N: The AVP SHALL NOT be encrypted using Encr-Encap AVP. If the AVP is encountered encrypted using Encr-Encap AVP, it SHALL be considered invalid and the message containing the AVP SHALL be discarded.

X: The AVP MAY be encrypted using Encr-Encap AVP. If the AVP is encountered either encrypted or not encrypted using Encr-Encap AVP, it SHALL be considered valid.

The legitimate occurrence of unencrypted AVPs and AVPs after decryption and unencapsulation SHALL be subject to the AVP Occurrence Table (Figure 4 in [RFC5191]).

The following table shows the encryption requirements for the existing AVPs defined in [RFC5191]:

Attribute Name	Enc
AUTH	N
EAP-Payload	X
Integrity-Algorithm	N
Key-Id	N
Nonce	N
PRF-Algorithm	N
Result-Code	N
Session-Lifetime	X
Termination-Cause	X

The following table shows the encryption requirements for the AVPs defined in [RFC6345]:

Attribute Name	Enc
PaC-Information	N
Relayed-Message	N

The following table shows the encryption requirements for the AVPs defined in this document:

Attribute Name	Enc
Encr-Algorithm	N
Encr-Encap	N

The following table is an example of showing the encryption requirements for a newly-defined AVP, Example-AVP:

Attribute Name	Enc
Example-AVP	Y

The guidance for specifying the encryption requirements for a newly-defined AVP is as follows:

Y: If the payload needs privacy against eavesdroppers (e.g., carrying a secret key).

N: If the payload may need to be observed by on-path network elements (i.e., subject to deep packet inspection).

X: If neither concern applies.

7. Security Considerations

PANA_PAC_ENCR_KEY and PANA_PAA_ENCR_KEY are secret keys shared between the PaC and the PAA. They SHALL NOT be used for purposes other than those specified in this document. Compromise of these keys would lead to compromise of the secret information protected by these keys.

7.1. AES-CTR Security Considerations

The use of AES-CTR encryption has its own security considerations, which are detailed in the Security Considerations section of [RFC3686]. Specifically:

- The nonce specified in Section 4.1 meets the requirement of uniqueness per key usage.

- Section 4.1 of [RFC5191] states that if the EAP method generates cryptographic keys, an AUTH AVP will always be present in every PANA message after key generation. Therefore, an Encr-Encap AVP will always be sent in conjunction with an AUTH AVP. This meets the requirement of a companion authentication function.

8. IANA Considerations

As described in Section 4 and Section 5, and following the new IANA allocation policy on PANA messages [RFC5872], two PANA AVP codes and one set of AVP values are requested. An additional encryption policy for AVP codes is also requested.

8.1. PANA AVP codes

The following AVP codes are requested in the PANA Parameters - AVP Codes registry:

o A standard AVP code of TBD1 (suggested value 12) for Encr-Encap AVP.

- A standard AVP code of TBD2 (suggested value 13) for Encryption-Algorithm AVP.

8.2. PANA Encryption-Algorithm AVP values

The following AVP values representing the encryption algorithm identifier for the Encryption-Algorithm AVP code are requested as a sub-registry under the PANA Parameters - AVP Codes registry:

- An AVP value of 1 for AES128_CTR.

- All other AVP values (0, 2-4294967295) are unassigned

The registration procedures are IETF Review or IESG Approval in accordance with [RFC5872].

8.3. PANA AVP codes encryption policy

The additional encryption policy defined in Section 6.1 is requested to be assigned as an additional column labeled "Enc" to the PANA AVP Codes parameter, applied to all existing AVP codes and those defined in this specification.

9. Acknowledgments

The authors would like to thank Yoshihiro Ohba, Yasuyuki Tanaka, Adrian Farrel, Brian Carpenter, Yaron Sheffer, Ralph Droms, Stephen Farrell, Barry Leiba and Sean Turner for their valuable comments.

10. Normative References

[NIST_SP800_38A]
Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Methods and Techniques", December 2001.

[NIST_SP800_38C]
Dworkin, M., "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", May 2004.

[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.

[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.

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

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

[RFC6345] Duffy, P., Chakrabarti, S., Cragie, R., Ohba, Y., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Relay Element", RFC 6345, August 2011.

Authors' Addresses

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org

Robert Cragie
Gridmerge Ltd.
89 Greenfield Crescent
Wakefield, WF4 4WA
UK

Email: robert.cragie@gridmerge.com