Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 7, 2012

A. Yegin
Samsung
R. Cragie
Gridmerge Ltd.

January 4, 2012

Encrypting PANA AVPs
draft-yegin-pana-encr-avp-01

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 will expire on July 7, 2012.

Copyright Notice

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 AVPs. AVPs can be integrity-protected using the AUTH AVP when EAP authentication generates cryptographic keying material. PANA 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

Encr-Encap AVP is used for delivering AVPs in encrypted form.

Each AVP that requires encryption SHALL be encapsulated inside an Encr-Encap AVP. Encr-Encap AVP can encapsulate one or more AVPs. There SHALL be only one Encr-Encap AVP in a PANA message.

Encr-Encap AVP uses the PANA_ENCR_KEY and the encryption algorithm negotiated by the Encr-Algorithm AVP. These AVPs SHALL NOT be used if the EAP method does not generate cryptographic keys (more specifically, MSK).

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.

Encr-Encap AVP MAY be used in any PANA message once the encryption algorithm is successfully negotiated and the PANA_ENCR_KEY is generated. The PRF used for computing the PANA_ENCR_KEY SHALL be

negotiated by the PRF-Algorithm-AVP according to RFC 5191.

3. Encryption Key

PANA_ENCR_KEY is used for encrypting the AVP payload of the Encr-Encap AVP. PANA_ENCR_KEY SHALL be computed according to the following formula.

```
  PANA_ENCR_KEY = prf+(MSK, "IETF PANA Encryption Key" | I_PAR |
                       I_PAN | PaC_nonce | PAA_nonce | Key_ID)
```

where:

- The prf+ function is defined in IKEv2 [RFC4306]. 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.

- MSK is the master session key generated by the EAP method.

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

- 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_ENCR_KEY depends on the integrity algorithm in use.

4. Encryption-Algorithm AVP

The Encryption-Algorithm AVP (AVP Code 12 ** needs IANA allocation **) is used for conveying the encryption algorithm to be used with the Encr-Encap AVP. The AVP data is of type Unsigned32.

Only AES_CTR (code 1) is identified by this document. Algorithm codes other than 1 are reserved for future use. Future specifications are allowed to extend this list.

AES_CTR: 1

AES-CTR (Counter) encryption algorithm as specified in [NIST_SP800_38A]. The formatting function and counter generation function 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.

Note the first counter block used for encryption is Ctr[1].

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 the PANA_ENCR_KEY. The output blocks of the encryption processing are encoded as OctetString data in the Value field of a Encr-Encap AVP.

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

5. Encr-Encap AVP

The Encr-Encap AVP (AVP Code 13 ** needs IANA allocation **) 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 is AES-CTR (code 1), AVP data payload is occupied by the encrypted AVPs.

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 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	X
PRF-Algorithm	N
Result-Code	N
Session-Lifetime	X
Termination-Cause	X

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

7. Security Considerations

PANA_ENCR_KEY is a secret key shared between the PaC and the PAA. It SHALL NOT be used for purposes other than the one specified in this document. Compromise of this key would lead to compromise of the secret information protected by this key.

8. IANA Considerations

The following IANA actions are required by this specification:

- Assignment of a standard AVP code TBD for Encr-Encap AVP

- Assignment of a standard AVP code TBD for Encryption-Algorith AVP.

- Creation of encryption algorithm identifier space for PANA.

- Assignment of an encryption code 1 for AES_CTR.

9. Acknowledgments

The authors would like to thank Yoshihiro Ohba for his 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.

[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.

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