Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2010

V. Cakulev
Alcatel Lucent
A. Lior
Bridgewater Systems
March 8, 2010

Diameter IKEv2 PSK: Pre-Shared Secret-based Support for IKEv2 Server to Diameter Server Interaction

draft-ietf-dime-ikev2-psk-diameter-02.txt

Abstract

The Internet Key Exchange protocol version 2 (IKEv2) is a component of the IPsec architecture and is used to perform mutual authentication as well as to establish and to maintain IPsec security associations (SAs) between the respective parties. IKEv2 supports several different authentication mechanisms, such as the Extensible Authentication Protocol (EAP), certificates, and pre-shared secrets.

With [RFC 5778] the Diameter interworking for Mobile IPv6 between the Home Agent, as a Diameter client, and the Diameter server has been specified. However, that specification focused on the usage of EAP and did not include support for pre-shared secret based authentication available with IKEv2. This document therefore extends the functionality offered by [RFC 5778] with pre-shared key based authentication offered by IKEv2 when no EAP is used.

This Internet-Draft will expire on September 9, 2010.

Copyright Notice

Table of Contents

1. Introduction

[RFC4306] defines Internet Key Exchange v2 as a protocol that performs mutual authentication between two parties and establishes a security association (SA) that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload (ESP) [RFC4303] and/or Authentication Header (AH) [RFC4302], and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry. IKEv2 protocol allows several different mechanisms for authenticating a IKEv2 Peer to be used, such as the Extensible Authentication Protocol, certificates, and pre-shared secrets.

From a service provider perspective it is important to ensure that a user is authorized to use the services. Therefore, the IKEv2 Server must verify that the IKEv2 Peer is authorized for the requested services possibly with the assistance of the operator's Diameter servers. [RFC 5778] defines the home agent as a Diameter client to the Diameter server communication when the mobile node authenticates using the IKEv2 protocol with the Extensible Authentication Protocol or using the Mobile IPv6 Authentication Protocol. This document extends the functionality offered by [RFC 5778] with pre-shared key based authentication offered by IKEv2. This document does not assume that the IKEv2 Server has the pre-shared secrets (PSK) with the IKEv2 Peer. Instead, it allows for PSK to be derived for a specific IKEv2 session and exchanged between IKEv2 Server and HAAA. This is accomplished through the use of a new Diameter application specifically designed for performing IKEv2 authorization decisions.

2. Requirements notation

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].

3. Application Identifier

This specification defines a new Diameter application and its respective Application Identifier:

Diameter IKE PSK (IKEPSK) TBD1 by IANA

The IKEPSK Application Identifier is used when the IKEv2 Peer is to be authenticated and authorized using IKEv2 with PSK-based authentication.

4. Protocol Description

4.1. Support for IKEv2 and Pre-Shared Secrets

When IKEv2 is used with PSK-based initiator authentication, the Diameter commands IKEv2-PSK-Request and IKEv2-PSK-Answer defined in this document are used to authorize the IKEv2 Peer for the services. Upon receiving the IKE_AUTH message from the IKEv2 Peer, the IKEv2 Server uses the information received in IDi to determine if it has the PSK for this IKEv2 Peer. If there is no PSK found associated with this IKEv2 Peer, the IKEv2 Server MUST send an Authorize-Only (Auth-Request-Type set to "Authorize-Only") Diameter IKEv2-PSK message with the IKEv2 Peer's IDi payload to the HAAA to obtain the PSK. The IDi payload extracted from the IKE_AUTH message has to contain an identity that is meaningful for the Diameter infrastructure, such as a Network Access Identifier (NAI), since it is used by the IKEv2 Server to populate the User-Name AVP in the Diameter message. The IKEv2 Server also includes in the IKEv2-Nonces AVP of the same Diameter message the initiator and responder nonces (Ni and Nr) exchanged during initial IKEv2 exchange.

This message is routed to the IKEv2 Peer's HAAA. Upon receiving Diameter IKEv2-PSK-Request message from the IKEv2 Server, the HAAA SHALL use the User-Name AVP to retrieve the associated keying material. The HAAA SHALL use the nonces Ni and Nr received in IKEv2-Nonces AVP to generate the PSK. It is outside of scope of this document how the HAAA obtains or generates the PSK. For example, if the HAAA previously performed EAP based access authentication and authorization of the IKEv2 Peer, it can use the available EMSK to generate the PSK [RFC5295]. The HAAA returns the PSK to the IKEv2 Server using the Key AVP as specified in [I-D.ietf-dime-local-keytran].

Once the IKEv2 Server receives the PSK from the HAAA, the IKEv2 Server verifies the IKE_AUTH message received from the IKEv2 Peer. If the verification of AUTH is successful, the IKEv2 Server sends the IKE message back to the IKEv2 Peer.

4.2. Session Management

The HAAA may maintain state or may be stateless. This is indicated by presence or absence of the Auth-Session-State AVP. The IKEv2 Server MUST support the Authorization Session State Machine defined in [RFC3588].

This specification makes an assumption that each IKE_SA created between the IKEv2 Peer and the IKEv2 Server as a result of a successful IKEv2 negotiation exchange together with CHILD_SAs set up

through that particular IKE_SA correspond to one currently active PSK and one active Diameter session.

4.2.1. Session-Termination-Request/Answer

In the case where session tracking is being used, when the IKEv2 Server terminates the SA it SHALL send a Session-Termination-Request (STR) message [RFC3588] to inform the HAAA that the authorized session has been terminated.

The Session-Termination-Answer (STA) message [RFC3588] is sent by the HAAA to acknowledge the notification that the session has been terminated.

4.2.2. AbortSession-Request/Answer

The Abort-Session-Request (ASR) message [RFC3588] is sent by the HAAA to the IKEv2 Server to terminate the authorized session. When the IKEv2 Server receives the ASR message, it MUST delete the corresponding IKE_SA and all CHILD_SAs set up through it.

The Abort-Session-Answer (ASA) message [RFC3588] is sent by the IKEv2 Server in response to an ASR message.

5. Command Codes for Diameter IKEv2 with PSK

This section defines new Command-Code values that MUST be supported by all Diameter implementations conforming to this specification.

Command-Name	Abbrev.	Code	Reference	Application
IKEv2-PSK-Request	IKEPSKR	TBD2	Section 5.1	IKEPSK
IKEv2-PSK-Answer	IKEPSKA	TBD3	Section 5.2	IKEPSK

Table 1: Command Codes

5.1. IKEv2-PSK-Request (IKEPSKR) Command

The IKEv2-PSK-Request message, indicated with the Command-Code set to TBD2 and the 'R' bit set in the Command Flags field is sent from the IKEv2 Server to the HAAA to initiate IKEv2 with PSK authorization. In this case, the Application-ID field of the Diameter Header MUST be set to the Diameter IKE PSK Application ID (value of TDB1).

Message format

```
<IKEv2-PSK-Request> ::= < Diameter Header: TBD2, REQ, PXY >
                        < Session-Id >
                        { Auth-Application-Id }
                        { Origin-Host }
                        { Origin-Realm }
                        { Destination-Realm }
                        { Auth-Request-Type }
                        [ Destination-Host ]
                        [ NAS-Identifier ]
                        [ NAS-IP-Address ]
                        [ NAS-IPv6-Address ]
                        [ NAS-Port ]
                        [ Origin-State-Id ]
                        { User-Name }
                        [ Auth-Session-State ]
                        { IKEv2-Nonces }
                      * [ Proxy-Info ]
                      * [ Route-Record ]
                        ...
                      * [ AVP ]
```

IKEv2-PSK-Request message MUST include a IKEv2-Nonces AVP containing

Ni and Nr nonces exchanged during initial IKEv2 exchange.

5.2. IKEv2-PSK-Answer (IKEPSKA) Command

The IKEv2-PSK-Answer (IKEPSKA) message, indicated by the Command-Code field set to TBD3 and the 'R' bit cleared in the Command Flags field, is sent by the HAAA to the IKEv2 Server in response to the IKEPSKR command. In this case, the Application-ID field of the Diameter Header MUST be set to the Diameter IKE PSK Application ID (value of TDB1).

Message format

```
<IKEv2-PSK-Answer> ::= < Diameter Header: TBD3, PXY >
                       < Session-Id >
                       { Auth-Application-Id }
                       { Auth-Request-Type }
                       { Result-Code }
                       { Origin-Host }
                       { Origin-Realm }
                       [ User-Name ]
                       [ Key ]
                       [ Error-Message ]
                       [ Error-Reporting-Host ]
                     * [ Failed-AVP ]
                       [ Origin-State-Id ]
                     * [ Redirect-Host ]
                       [ Redirect-Host-Usage ]
                       [ Redirect-Max-Cache-Time ]
                     * [ Proxy-Info ]
                     * [ Route-Record ]
                       ...
                     * [ AVP ]
```

If the authorization procedure was successful then the IKEv2-PSK-Answer message SHALL include the Key AVP as specified in [I-D.ietf-dime-local-keytran]. The value of the Key-Type AVP SHALL be set to TBD4. The Keying-Material AVP SHALL contain the PSK. Exactly how the PSK is derived is beyond the scope of this document. The Key-Lifetime AVP may be included and if it is included then the associated key shall not be used if the lifetime has expired.

6. Attribute Value Pair Definitions

This section defines new AVPs for the IKEv2 with PSK.

6.1. IKEv2-Nonces

The IKEv2-Nonces AVP (Code TBD5) is of type Grouped and contains the nonces exchanged between the IKEv2 Peer and the IKEv2 Server during IKEv2 initial exchange. The nonces are used for PSK generation.

```
IKEv2-Nonces ::= < AVP Header: TBD5>
                 {Ni}
                 {Nr}
                *[AVP]
```

6.1.1. Ni

The Ni AVP (AVP Code TBD6) is of type Unsigned32 and contains the IKEv2 initiator nonce.

6.1.2. Nr

The Nr AVP (AVP Code TBD7) is of type Unsigned32 and contains the IKEv2 responder nonce.

7. AVP Occurrence Tables

The following tables present the AVPs defined or used in this document and their occurrences in Diameter messages. Note that AVPs that can only be present within a Grouped AVP are not represented in this table.

The table uses the following symbols:

0:

The AVP MUST NOT be present in the message.

0+:

Zero or more instances of the AVP MAY be present in the message.

0-1:

Zero or one instance of the AVP MAY be present in the message.

1:

One instance of the AVP MUST be present in the message.

	Command-Code	
AVP Name	IKEPSKR	IKEPSKA
Key	0-1	0-1
IKEv2-Nonces	0-1	0

IKEPSKR and IKEPSKA Commands AVP Table

8. AVP Flag Rules

The following table describes the Diameter AVPs, their AVP Code values, types, possible flag values, and whether the AVP MAY be encrypted. The Diameter base [RFC3588] specifies the AVP Flag rules for AVPs in Section 4.5.

				AVP Flag rules				
Attribute Name	AVP Code	Defined in	Value Type	MUST	MAY	SHOULD NOT	MUST NOT	MAY Encr
Key	TBD	Note 1	Grouped	M	P		V	Y
Keying-Material	TBD	Note 1	OctetString	M	P		V	Y
Key-Lifetime	TBD	Note 1	Integer64	M	P		V	Y
Key-SPI	TBD	Note 1	Unsigned32	M	P		V	Y
Key-Type	TBD	Note 1	Enumerated	M	P		V	Y
Key-Name	TBD	Note 1	OctetString	M	P		V	Y
IKEv2-Nonces	TBD5	6.2	Grouped	M	P		V	Y
Ni	TBD6	6.2.1	Unsigned32	M	P		V	Y
Nr	TBD7	6.2.2	Unsigned32	M	P		V	Y

AVP Flag Rules Table

Note 1: Key, Keying-Material, Key-Type, Key-SPI, Key-Name and Key-Lifetime AVPs are defined in [I-D.ietf-dime-local-keytran].

9. IANA Considerations

This section contains the namespaces that have either been created in this specification or had their values assigned to existing namespaces managed by IANA.

9.1. Command Codes

IANA is requested to allocate a command code value for the IKEv2-PSK-Request message (IKEPSKR) and for the IKEv2-PSK-Answer message (IKEPSKA) from the Command Code namespace defined in [RFC3588]. See Section 5 for the assignment of the namespace in this specification.

9.2. AVP Codes

This specification requires IANA to register the following new AVPs from the AVP Code namespace defined in [RFC3588].

- IKEv2-Nonces
- Ni
- Nr

The AVPs are defined in Section 6.

9.3. AVP Values

IANA is requested to create a new value for the Key-Type AVP. The new value TBD4 signifies that IKEv2 PSK is being sent.

9.4. Application Identifier

This specification requires IANA to allocate one new value "Diameter IKE PSK" from the Application Identifier namespace defined in [RFC3588].

Application Identifier	Value
Diameter IKE PSK (IKEPSK)	TBD1

10. Security Considerations

The security considerations of the Diameter Base protocol [RFC3588] are applicable to this document.

The Diameter messages between the IKEv2 Server and the HAAA may be transported via one or more AAA brokers or Diameter agents. In this case, the HA to the Diameter server AAA communication relies on the security properties of the intermediating AAA inter-connection networks, AAA brokers, and Diameter agents. Furthermore, any agents that process IKEv2-PSK-Answer messages can see the contents of the Master-Security-Association AVP. For this reason, this specification strongly recommends avoiding Diameter agents when they cannot be trusted to keep the keys secret.

This specification expects that the HAAA derives and returns the associated session key to the IKEv2 Server. For the key derivation this specification recommends the use of a short lived secrets, possibly based on a previous network access authentication run if such secrets are available. To ensure key freshness, limit the key scope etc., this specification also recommends the use of nonces, if nonces are included in IKEv2-PSK-Request. However, this specification does not define how the Diameter server actually derives required keys. The details of the key derivation depends on the deployment where this specification is used and therefore the security properties of the system depend on how this is done.

11. References

11.1. Normative References

[I-D.ietf-dime-local-keytran]
Wu, W. and G. Zorn, "Diameter Attribute-Value Pairs for Cryptographic Key Transport", draft-ietf-dime-local-keytran-01 (work in progress), January 2010.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

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

11.2. Informative References

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

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

[RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.

Authors' Addresses

Violeta Cakulev
Alcatel Lucent
600 Mountain Ave.
3D-517
Murray Hill, NJ 07974
US

Phone: +1 908 582 3207
Email: violeta.cakulev@alcatel-lucent.com

Avi Lior
Bridgewater Systems
303 Terry Fox Drive
Otawa, Ontario K2K 3J1
Canada

Phone: +1 613-591-6655
Email: avi@bridgewatersystems.com