INTERNET DRAFT
draft-nir-ikev2-auth-lt-05.txt
Expires: July 2006
Intended status: Informational
January 9, 2006

Yoav Nir
Check Point

# Repeated Authentication in IKEv2

Status of this Memo

Abstract

This document extends the IKEv2 document [IKEv2]. With some IPsec peers, particularly in the remote access scenario, it is desirable to repeat the mutual authentication periodically. The purpose of this is to limit the time that SAs can be used by a third party who has gained control of the IPsec peer. This document describes a mechanism to perform this function.

## 1. Introduction

In several cases, such as the remote access scenario, policy dictates that the mututal authentication needs to be repeated periodically. Repeated authentication can usually be achieved by simply repeating the Initial exchange by whichever side has a stricter policy.

However, in the remote access scenario it is usually up to a human user to supply the authentication credentials, and often EAP is used for authentication, which makes it unreasonable or impossible for the remote access gateway to initiate the IKEv2 exchange.

This document describes a new notification that the original Responder can send to the original Initiator with the number of seconds before the authentication needs to be repeated.  The Initiator SHOULD repeat the Initial exchange before that time is expired.  If the Initiator fails to do so, the Responder may close all Security Associations.

Repeated authentication is not the same as IKE SA rekeying, and need not be tied to it.The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in [RFC2119].

## 2. Authentication Lifetime

The Responder in an IKEv2 negotiation MAY be configured to limit the time that an IKE SA and the associated IPsec SAs may be used before the peer is required to repeat the authentication, through a new Initial Exchange.

The Responder MUST send this information to the Initiator in an AUTH_LIFETIME notification either in the last message of an IKE_AUTH exchange, or in an INFORMATIONAL request, which may be sent at any time.

When sent as part of the IKE SA setup, the AUTH_LIFETIME notification is used as follows:

```
     Initiator                            Responder
     -------------------------------      -----------------------------
     HDR, SAi1, KEi, Ni              -->
                                     <--  HDR, SAr1, KEr, Nr, [CERTREQ]
     HDR, SK {IDi, [CERT,] [CERTREQ,]
        [IDr,] AUTH, SAi2, TSi, TSr} -->
                                     <--  HDR, SK {IDr, [CERT,] AUTH,
                                                   SAr2, TSi, TSr,
                                                    N(AUTH_LIFETIME)}
```

The separate Informational exchange is formed as follows:

```
                                     <--  HDR, SK {N(AUTH_LIFETIME)}
       HDR  SK {}                    -->
```

The AUTH_LIFETIME notification is described in section 3.

The original Responder that sends the AUTH_LIFETIME notification SHOULD send a DELETE notification soon after the end of the lifetime period, unless the IKE SA is deleted before the lifetime period elapses. If the IKE SA is rekeyed, then the time limit applies to the new SA.

An Initiator that received an AUTH_LIFETIME notification SHOULD repeat the Initial exchange within the time indicated in the notification. The time is measured from the time that the original Initiator receives the notification.

A special case is where the notification is sent in an Informational exchange, and the lifetime is zero. In that case the original responder SHOULD allow a reasonable time for the repeated authentication to occur.

The AUTH_LIFETIME notification MUST be protected and MAY be sent by the original Responder at any time. If the policy changes, the original Responder MAY send it again in a new Informational.

The new Initial exchange is not altered. The initiator SHOULD delete the old IKE SA within a reasonable time of the new Auth exchange.

## 3. AUTH_LIFETIME Notification

The AUTH_LIFETIME message is a notification payload formatted as follows:

```
                           1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      ! Next Payload  !C!  RESERVED   !         Payload Length        !
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      !  Protocol ID  !   SPI Size    !      Notify Message Type      !
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      !                            Lifetime                           !
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Payload Length is 12.
- Protocol ID (1 octet) MUST be 0.
- SPI size is 0 (SPI is in message header).
- Notify Message type is TBA by IANA
- Lifetime is the amount of time in seconds left before the peer should repeat the Initial exchange. A zero value signifies that the Initial exchange should begin immediately.
  It is usually not reasonable to set this value to less than 300 (5 minutes) since that is too cumbersome for a user.
  It is also usually not reasonable to set this value to more than 86400 (1 day) as that would negate the security benefit of repeating the authentication.

## 4. Interoperability with non-supporting IKEv2 implementations

IKEv2 implementations that do not support the AUTH_LIFETIME notification will ignore it and will not repeat the authentication. In that case the original Responder will send a Delete notification for the IKE SA in an Informational exchange.  Such implementations may be configured manually to repeat the authentication periodically.

Non-supporting Responders are not a problem, because they will simply not send these notifications.  In that case, there is no requirement that the original Initiator re-authenticate.

## 5. Security Considerations

The AUTH_LIFETIME notification sent by the Responder does not override any security policy on the Initiator.  In particular, the Initiator may have a different policy regarding re-authentication, requiring more frequent re-authentication.  Such an Initiator can repeat the authentication earlier then is required by the notification.

An Initiator MAY set reasonable limits on the amount of time in the AUTH_LIFETIME notification. For example, an authentication lifetime of less than 300 seconds from SA initiation may be considered unreasonable.

## 6. Normative References

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

[RFC2119]  S. Bradner, "RFC2119 Key words for use in RFCs to Indicate
Requirement Levels.", RFC2119, 1997

## 7. IANA Considerations

IANA is asked to assign a notification payload type for the AUTH_LIFETIME notifications from the IKEv2 Notify Message Types registry. This should be from the STATUS TYPES range.

## 8. Author's address

Yoav Nir
Check Point Software Technologies
ynir@checkpoint.com