Network Working Group
Internet-Draft
Intended status: Experimental
Expires: January 1, 2011

Y. Nir
Check Point
H. Tschofenig
NSN
H. Deng
China Mobile
R. Singh
Cisco
June 30, 2010

A Childless Initiation of the IKE SA
draft-nir-ipsecme-childless-04

Abstract

This document describes an extension to the IKEv2 protocol that allows an IKE SA to be created and authenticated without generating a Child SA.

Status of this Memo

Copyright Notice

1. Introduction

IKEv2, as specified in [RFC4306], requires that the IKE_AUTH exchange try to create a Child SA along with the IKE SA. This requirement is sometimes inconvenient or superfluous, as some implementations need to use IKE for authentication only, while others would like to set up the IKE SA before there is any actual traffic to protect. The extension described in this document allows the creation of an IKE SA without also attempting to create a Child SA.

An IKE SA without any Child SA is not a fruitless endeavor. Even without Child SAs, an IKE SA allows:

- o Checking the liveness status of the peer via liveness checks.
- o Quickly setting up Child SAs without public key operations, and without user interaction.
- o Authentication of the peer.
- o Detection of NAT boxes between two hosts on the Internet

1.1. Conventions Used in This Document

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. Usage Scenarios

Several scenarios motivated this proposal:

- o Interactive remote access VPN: the user tells the client to "connect", which may involve interactive authentication. There is still no traffic, but some may come later. Since there is no traffic, it is impossible for the gateway to know what selectors to use (how to narrow down the client´s proposal).
- o Location aware security, as in [SecureBeacon]. The user is roaming between trusted and untrusted networks. While in an untrusted network, all traffic should be encrypted, but on the trusted network, only the IKE SA needs to be maintained.
- o An IKE SA may be needed between peers even when there is not IPsec traffic. Such IKE peers use liveness checks, and report to the administrator the status of the "VPN links".
- o IKE may be used on some physically secure links, where authentication is necessary, but traffic protection is not. An example of this in the PON links as described in [3GPP.33.820].

- o Childless IKE can be used for [EAP-IKEv2] where we use IKEv2 as a method for user authentication.
- o A node receiving IPsec traffic with an unrecognized SPI should send an INVALID_SPI notification. If this traffic comes from a peer, which it recognizes based on its IP address, then this node may set up an IKE SA so as to be able to send the notification in a protected IKE_INFORMATIONAL exchange.
- o A future extension may have IKE SAs used for generating keying material for applications, without ever requiring Child SAs. This is similar to what [extractors] is doing in TLS.

In some of these cases it may be possible to create a dummy Child SA and then remove it, but this creates undesirable side effects and race conditions. Moreover, the IKE peer might see the deletion of the Child SA as a reason to delete the IKE SA.

3. Protocol Outline

The decision of whether or not to support an IKE_AUTH exchange without the piggy-backed Child SA negotiation is ultimately up to the responder. A supporting responder MUST include the Notify payload, described in Section 4, within the IKE_SA_INIT response.

A supporting initiator MAY send the modified IKE_AUTH request, described in Section 5, if the Notification was included in the IKE_SA_INIT response. The initiator MUST NOT send the modified IKE_AUTH request if the Notification was not present.

A supporting responder that has advertised support by including the notification in the IKE_SA_INIT response MUST process a modified IKE_AUTH request, and MUST reply with a modified IKE_AUTH response. Such a responder MUST NOT reply with a modified IKE_AUTH response if the initiator did not send a modified IKE_AUTH request.

A supporting responder that has been configured not to support this extension to the protocol MUST behave as the same as if it didn´t support this extension. It MUST NOT advertise the capability with a notification, and it SHOULD reply with an INVALID_SYNTAX Notify payload if the client sends an IKE_AUTH request that is modified as described in Section 5.

4. CHILDLESS_IKE_SUPPORTED Notification

The Notify payload is as described in [RFC4306]

```
                     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    ! Childless Notify Message Type !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        XML2PDFRFC-ENDARTWORK
```

- Protocol ID (1 octet) MUST be 1, as this message is related to an IKE SA.
- SPI Size (1 octet) MUST be zero, in conformance with section 3.10 of [RFC4306].
- Childless Notify Message Type (2 octets) - MUST be xxxxx, the value assigned for CHILDLESS_IKE_SUPPORTED. TBA by IANA.

5. Modified IKE_AUTH Exchange

For brevity, only the EAP version of an AUTH exchange will be presented here. The non-EAP version is very similar. The figures below are based on appendix A.3 of [RFC4718].

```
first request       --> IDi,
                        [N(INITIAL_CONTACT)],
                        [[N(HTTP_CERT_LOOKUP_SUPPORTED)], CERTREQ+],
                        [IDr],
                        [CP(CFG_REQUEST)],
                        [V+]

first response      <-- IDr, [CERT+], AUTH,
                        EAP,
                        [V+]

                  / --> EAP
repeat 1..N times |
                  \ <-- EAP

last request        --> AUTH

last response       <-- AUTH,
                        [CP(CFG_REPLY)],
                        [N(ADDITIONAL_TS_POSSIBLE)],
                        [V+]
           XML2PDFRFC-ENDARTWORK
```

Note what is missing:

- The optional notifications: IPCOMP_SUPPORTED, USE_TRANSPORT_MODE, ESP_TFC_PADDING_NOT_SUPPORTED, and NON_FIRST_FRAGMENTS_ALSO.
- The SA payload.
- The traffic selector payloads.
- Any notification, extension payload or VendorID that has to do with Child SA negotiation.

6. Security Considerations

This protocol variation inherits all the security properties of regular IKEv2 as described in [RFC4306].

The new notification carried in the initial exchange advertises the capability, and cannot be forged or added by an adversary without being detected, because the response to the initial exchange is authenticated with the AUTH payload of the IKE_AUTH exchange. Furthermore, both peers have to be configured to use this variation of the exchange in order for the responder to accept a childless proposal from the initiator.

7. IANA Considerations

IANA is requested to assign a notify message type from the status types range (16418-40959) of the "IKEv2 Notify Message Types" registry with name "CHILDLESS_IKE_SUPPORTED".

8. References

8.1. Normative References

[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.

[RFC4718] Eronen, P. and P. Hoffman, "IKEv2 Clarifications and Implementation Guidelines", RFC 4718, October 2006.

8.2. Informative References

[3GPP.33.820] 3GPP, "Security of H(e)NB", 3GPP TR 33.820 8.0.0, March 2009.

[EAP-IKEv2]
Tschofenig, H., Kroeselberg, D., Pashalidis, A., Ohba, Y., and F. Bersani, "The Extensible Authentication Protocol- Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method", RFC 5106, February 2008.

[SecureBeacon]
Sheffer, Y. and Y. Nir, "Secure Beacon: Securely Detecting a Trusted Network", draft-sheffer-ipsecme-secure-beacon (work in progress), June 2009.

[extractors]
Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", draft-ietf-tls-extractor (work in progress), March 2009.

Authors´ Addresses

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 67897
Israel

Email: ynir@checkpoint.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Hui Deng
China Mobile
53A,Xibianmennei Ave.
Xuanwu District
Beijing 100053
China

Email: denghui02@gmail.com

Rajeshwar Singh Jenwar
Cisco Systems, Inc.
O´Shaugnessy Road
Bangalore, Karnataka 560025
India

Phone: +91 80 4103 3563
Email: rsj@cisco.com