

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 19, 2009

Y. Nir
Check Point
H. Tschofenig
NSN
H. Deng
China Mobile
June 17, 2009

A Childless Initiation of the IKE SA
draft-nir-ike-nochild-02

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 19, 2009.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft

IKE WITHOUT CHILD

June 2009

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.

Table of Contents

1.	Introduction	3
1.1.	Conventions Used in This Document	3
2.	Usage Scenarios	3
3.	Protocol Outline	4
4.	VID Payload	4
5.	Modified IKE_AUTH Exchange	5
6.	Security Considerations	5
7.	IANA Considerations	5
8.	References	6
8.1.	Normative References	6
8.2.	Informative References	6
	Authors' Addresses	6

1. Introduction

IKEv2, as specified in [[RFC4306](#)] requires that in an IKE_AUTH exchange, a child SA is created along with the IKE SA. This requirement is sometimes inconvenient, as some implementations need to use IKE for authentication only, while other implementations would like to set up the IKE SA before there is any actual traffic to protect.

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/or without user interaction.
- o Authentication of the peer.

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 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 VID payload, described in [Section 4](#), within the IKE_INIT response.

A supporting initiator MAY send the modified IKE_AUTH request, described in [Section 5](#), if the VID payload was included in the IKE_INIT response. The initiator MUST NOT send the modified IKE_AUTH request if the VID was not present.

A supporting responder that advertised the VID payload in the IKE_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 VID payload, 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](#). VID Payload

The VID payload is as described in [[RFC4306](#)] with the data as follows:

73da4b423dd9f75563b15b9f918650fc

This value was obtained by hashing the string "Will do IKE_AUTH without child SA payloads"

[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+]

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

last request       --> AUTH
```

```
last response      <-- AUTH,
                    [CP(CFG_REPLY)],
                    [V+]
```

Note what is missing:

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

[6.](#) Security Considerations

TBA

[7.](#) IANA Considerations

There are no IANA considerations for this document.

[8.](#) References

Nir, et al. Expires December 19, 2009 [Page 5]

Internet-Draft IKE WITHOUT CHILD June 2009

[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.

[SecureBeacon]

Sheffer, Y. and Y. Nir, "Secure Beacon: Securely Detecting a Trusted Network", [draft-sheffer-ipsec-secure-beacon](#) (work in progress), January 2008.

[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

Nir, et al.

Expires December 19, 2009

[Page 6]

Internet-Draft

IKE WITHOUT CHILD

June 2009

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