Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 22, 2009

Y. Nir
Check Point

May 21, 2009

A Childless Initiation of the IKE SA
draft-nir-ike-nochild-00

Status of this Memo

Copyright Notice

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

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:

- Checking the liveness status of the peer via liveness checks.
- Quickly setting up child SAs without public key operations, and/or without user interaction.
- 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:

- 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).
- 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.
- 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 exchage without

the piggy-backed child SA negotiation is ultimately up to the reponsder. A supporting resonder 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.

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+]

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

    last request        --> AUTH

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

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

TBA

7. IANA Considerations

There are no IANA considerations for this document.

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

[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.

Author's Address

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

Email: ynir@checkpoint.com