                        A Childless Initiation of
 the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)

Abstract

   This document describes an extension to the Internet Key Exchange
   version 2 (IKEv2) protocol that allows an IKEv2 Security Association
   (SA) to be created and authenticated without generating a Child SA.

1. Introduction

   IKEv2, as specified in [RFC5996], requires that the IKE_AUTH exchange
   try to create a Child SA along with the IKEv2 SA. This requirement
   is sometimes inconvenient or superfluous, as some implementations
   need to use IKEv2 for authentication only, while others would like to
   set up the IKEv2 SA before there is any actual traffic to protect.
   The extension described in this document allows the creation of an
   IKEv2 SA without also attempting to create a Child SA. The terms
   IKEv2, IKEv2 SA, and Child SA and the various IKEv2 exchanges are
   defined in [RFC5996]

   An IKEv2 SA without any Child SA is not a fruitless endeavor. Even
   without Child SAs, an IKEv2 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 IKEv2 SA needs to be maintained.

   o An IKEv2 SA may be needed between peers even when there is not
      IPsec traffic. Such IKEv2 peers use liveness checks, and report
      to the administrator the status of the "VPN links".

   o IKEv2 may be used on some physically secure links, where
      authentication is necessary but traffic protection is not. An
      example of this is the Passive Optical Network (PON) links as
      described in [3GPP.33.820].

   o Childless IKEv2 can be used for [RFC5106] where we use IKEv2 as a
      method for user authentication.

   o A node receiving IPsec traffic with an unrecognized Security
      Parameter Index (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 IKEv2 SA so as to be able
      to send the notification in a protected INFORMATIONAL exchange.

   o A future extension may have IKEv2 SAs used for generating keying
      material for applications, without ever requiring Child SAs. This
      is similar to what [RFC5705] is doing in Transport Layer Security
      (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 IKEv2 peer might see the deletion of
   the Child SA as a reason to delete the IKEv2 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_IKEV2_SUPPORTED Notification

   The Notify payload is as described in [RFC5996]

```
                        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 !
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   o Protocol ID (1 octet) MUST be 1, as this message is related to an
      IKEv2 SA.

   o SPI Size (1 octet) MUST be zero, in conformance with section 3.10
      of [RFC5996].

   o Childless Notify Message Type (2 octets) - MUST be 16418, the
      value assigned for CHILDLESS_IKEV2_SUPPORTED.

5. Modified IKE_AUTH Exchange

   For brevity, only the Extensible Authentication Protocol (EAP)
   version of an AUTH exchange will be presented here. The non-EAP
   version is very similar. The figures below are based on Appendix C.3
   of [RFC5996].

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

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

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

 last request          --> AUTH

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

   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

   This protocol variation inherits all the security properties of
   regular IKEv2 as described in [RFC5996].

   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 has assigned a notify message type from the "IKEv2 Notify
   Message Types" registry with the name "CHILDLESS_IKEV2_SUPPORTED" and
   the value "16418".

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.

   [RFC5996]   Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen,
                   "Internet Key Exchange Protocol Version 2 (IKEv2)",
                   RFC 5996, September 2010.

8.2. Informative References

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

   [RFC5106]   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.

   [RFC5705]   Rescorla, E., "Keying Material Exporters for
                   Transport Layer Security (TLS)", RFC 5705,
                   March 2010.

   [SecureBeacon] Sheffer, Y. and Y. Nir, "Secure Beacon: Securely
                   Detecting a Trusted Network", Work in Progress,
                   June 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