Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 3, 2022

V. Smyslov
ELVIS-PLUS

August 2, 2021

Alternative Approach for Mixing Preshared Keys in IKEv2 for Post-quantum Security

draft-smyslov-ipsecme-ikev2-qr-alt-04

Abstract

An IKEv2 extension defined in [RFC8784] allows IPsec traffic to be protected against someone storing VPN communications today and decrypting it later, when (and if) quantum computers are available. However, this protection doesn't cover an initial IKEv2 SA, which might be unacceptable in some scenarios. This specification defines an alternative way get the same protection against quantum computers, but unlike the [RFC8784] solution it covers the initial IKEv2 SA too.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on February 3, 2022.

Copyright Notice

Copyright (c) 2021 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 (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Internet Key Exchange Protocol version 2, defined in [RFC7296], is used in the IPsec architecture to perform authenticated key exchange. [RFC8784] defines an extension of IKEv2 for protecting today's VPN traffic against future quantum computers. At the time this extension was being developed, it was a consensus in the IPSECME WG that only IPsec traffic needs to have such a protection. It was believed that no sensitive information is transferred over IKE SA and extending the protection to also cover IKE SA traffic would require serious modifications to core IKEv2 protocol, that contradicted to one of the goals to minimize such changes. For the cases when this protection is needed it was suggested to immediately rekey IKE SA once it is created.

In some situations it is desirable to have this protection for IKE SA from the very beginning, when an initial IKE SA is created. An example of such situation is Group Key Management protocol using IKEv2, defined in [I-D.ietf-ipsecme-g-ikev2]. In this protocol session keys are transferred from Group Controller/Key Server (GCKS) to Group Members (GM) immediately once an initial IKE SA is created. While it is possible to postpone transfer of the keys until the IKE SA is rekeyed (and [I-D.ietf-ipsecme-g-ikev2] specifies how to do this), the needed sequence of actions introduces an additional delay and adds unnecessary complexity to the protocol.

Since [RFC8784] was written, a new IKE_INTERMEDIATE exchange for IKEv2 was defined in [I-D.ietf-ipsecme-ikev2-intermediate]. While the primary motivation for developing this exchange was to allow

multiple key exchanges to be used in IKEv2 (which is defined in [I-D.ietf-ipsecme-ikev2-multiple-ke]), the IKE_INTERMEDIATE exchange itself can be used for other purposes too.

This specification makes use of the IKE_INTERMEDIATE exchange to define an alternative approach to [RFC8784], which allows getting protection against quantum computers for initial IKE SA.

2. Terminology and Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

We will use a term Conventional Approach in the content of using PPK to refer to the [RFC8784] and a term Alternative Approach to refer to this specification.

3. Alternative Approach Description

IKE initiator who supports the IKE_INTERMEDIATE exchange and wants to use PPK includes both the INTERMEDIATE_EXCHANGE_SUPPORTED and the USE_PPK notifications in the IKE_SA_INIT request. If responder supports the IKE_INTERMEDIATE exchange and is willing to use PPK, it includes both these notifications in the response.

```
Initiator                       Responder
-------------------------------------------------------------------
HDR, SAi1, KEi, Ni,
N(INTERMEDIATE_EXCHANGE_SUPPORTED),
N(USE_PPK)              --->
                        <---    HDR, SAr1, KEr, Nr, [CERTREQ,]
                                N(INTERMEDIATE_EXCHANGE_SUPPORTED),
                                N(USE_PPK)
```

If the responder returned both these notifications, then the initiator MAY choose to use the IKE_INTERMEDIATE exchange to negotiate PPK identity with the responder. Note, that it is up to the initiator whether to use the alternative or conventional approaches, i.e. whether to send PPK identity in the IKE_INTERMEDIATE exchange or in the IKE_AUTH exchange, as defined in the [RFC8784].

If the initiator decides to use alternative approach, it includes one or more PPK_IDENTITY notification containing PPK identities the initiator believes are appropriate for the IKE SA being created, into

the IKE_INTERMEDIATE request. If a series of the IKE_INTERMEDIATE exchanges takes place, the PPK_IDENTITY notification(s) MUST be sent in the last one, i.e. in the IKE_INTERMEDIATE exchange immediately preceding the IKE_AUTH exchange. If the last IKE_INTERMEDIATE exchange contains other payloads aimed for some other purpose, then the notification(s) MAY be piggybacked with these payloads.

```
Initiator                       Responder
-------------------------------------------------------------------
HDR, SK { ... N(PPK_IDENTITY, PPK_ID_1)
           [, N(PPK_IDENTITY, PPK_ID_2)] ...
           [, N(PPK_IDENTITY, PPK_ID_n)]}   --->
```

Depending on the responder's capabilities and policy the following situations are possible.

If the responder doesn't support the alternative approach, it will ignore the received PPK_IDENTITY notification(s) and won't include any additional notifications in the response. If the responder doesn't have any of the PPKs which IDs were sent by the initiator, then it MUST behave as if it doesn't support the alternative approach, i.e. include no additional notifications in the response.

```
Initiator                       Responder
-------------------------------------------------------------------
                        <---    HDR, SK { ... }
```

In this case the initiator cannot make an initial IKE SA to be a quantum computer resistant, so if this is a requirement for the initiator, then it MUST abort creating IKE SA. Otherwise, the initiator continues with the IKE_AUTH exchange and tries to use PPK as described in [RFC8784].

If the responder supports this extension and is configured with one of the PPKs which IDs were sent by the initiator, then the responder chooses one of these PPKs and returns back its identity in the PPK_IDENTITY notification.

```
Initiator                       Responder
-------------------------------------------------------------------
                  <---    HDR, SK { ... N(PPK_IDENTITY, PPK_ID_i)}
```

In this case the IKE_AUTH exchange is performed as defined in [RFC7296], so that neither PPK_IDENTITY nor NO_PPK_AUTH notifications are sent, since it's already known which PPK to use. The keys for the IKE SA are computed using PPK, as described in Section 4.

If the responder returns PPK identity that was not suggested by the initiator, then the initiator must treat this as a fatal error and MUST abort the IKE SA establishment.

Since the responder selects PPK before it knows identity of the initiator, a situation may occur, when the responder agrees to use some PPK in the IKE_INTERMEDIATE exchange, but later discovers during the IKE_AUTH exchange that this particular PPK is not associated with the initiator's identity in its local policy. Note, that the responder does have this PPK, but it is just not listed among the PPKs for using with this initiator. In this case the responder SHOULD abort negotiation and return back the AUTHENTICATION_FAILED notification to be consistent with its policy. However, if using PPK with this initiator is marked optional in the local policy, then the responder MAY continue creating IKE SA using the negotiated "wrong" PPK.

4. Computing IKE SA Keys

Once the PPK is negotiated in the last IKE_INTERMEDIATE exchange, the IKE SA keys are recalculated. Note that if the IKE SA keys are also recalculated as the result of the other actions performed in the IKE_INTERMEDIATE exchange (for example, as defined in [I-D.ietf-ipsecme-ikev2-multiple-ke], then applying PPK MUST be done after all of them, so that recalculating IKE SA keys with PPK is the last action before they are used in the IKE_AUTH exchange.

The IKE SA keys are computed as follows. A new SKEYSEED' value is computed using the negotiated PPK and the most recently computed SK_d key. Note, that PPK is applied to SK_d exactly how specified in [RFC8784], and the result is used as SKEYSEED'.

```
SKEYSEED' = prf+ (PPK, SK_d)
```

Then the SKEYSEED' is used to recalculate all SK_* keys as defined in Section 2.14 of [RFC7296].

```
{SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr}
                            = prf+ (SKEYSEED', Ni | Nr | SPIi | SPIr )
```

In the formula above Ni and Nr are nonces from the IKE_SA_INIT exchange and SPIi, SPIr - SPIs of the IKE SA being created.

The resulting keys are then used in the IKE_AUTH exchange and in the created IKE SA.

5. Comparison of the Conventional and the Alternative Approaches

This specification isn't intended to be a replacement for [RFC8784]. Instead, it is supposed to be used in situations where the conventional approach has a significant shortcomings. However, if the partners support both approaches, then the alternative approach MAY also be used in situations where convenient approach suffices.

The alternative approach has the following advantages:

1. The main advantage of the alternative approach is that it allows an initial IKE SA to be protected against quantum computers. This is important for those IKE extensions which transfer sensitive information, e.g. cryptographic keys, over initial IKE SA. The prominent example of such extensions is [I-D.ietf-ipsecme-g-ikev2].

2. Using the alternative approach allows the initiator to specify several appropriate PPKs and the responder to choose one of them. This feature could simplify PPK rollover.

3. With the alternative approach there is no need for the initiator to calculate the content of the AUTH payload twice (with and without PPK) to support a situation when using PPK is optional for both sides.

The main disadvantage of the alternative approach is that it requires an additional round trip (the IKE_INTERMEDIATE exchange) to set up IKE SA. However, if the IKE_INTERMEDIATE exchange has to be used for some other purposes in any case, then PPK stuff can be piggybacked with other payloads, thus eliminating this penalty.

6. Security Considerations

Security considerations of using Post-quantum Preshared Keys in the IKEv2 protocol are discussed in [RFC8784]. This specification defines an alternative way of exchanging PPK identity information.

7. IANA Considerations

This specification makes no request to IANA.

8. Acknowledgements

The author would like to thank Paul Wouters for valuable comments.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

[I-D.ietf-ipsecme-ikev2-intermediate] Smyslov, V., "Intermediate Exchange in the IKEv2 Protocol", draft-ietf-ipsecme-ikev2-intermediate-06 (work in progress), March 2021.

9.2. Informative References

[I-D.ietf-ipsecme-g-ikev2] Smyslov, V. and B. Weis, "Group Key Management using IKEv2", draft-ietf-ipsecme-g-ikev2-03 (work in progress), July 2021.

[I-D.ietf-ipsecme-ikev2-multiple-ke] Tjhai, C., Tomlinson, M., Bartlett, G., Fluhrer, S., Geest, D. V., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in IKEv2", draft-ietf-ipsecme-ikev2-multiple-ke-03 (work in progress), July 2021.

Author's Address

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd) 124460
RU

Phone: +7 495 276 0211
Email: svan@elvis.ru