Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2020

V. Smyslov
ELVIS-PLUS

October 17, 2019

An Alternative Approach for Postquantum Preshared Keys in IKEv2
draft-smyslov-ipsecme-ikev2-qr-alt-00

Abstract

An IKEv2 extension defined in [I-D.ietf-ipsecme-qr-ikev2] 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, which allows to extend it on the initial IKEv2 SA.

Table of Contents

1. Introduction 2
2. Terminology and Notation 3
3. Alternative Approach Description 3
4. Computing IKE SA Keys 5
5. Comparison of the Conventional and the Alternative Approaches 6
6. Security Considerations 6
7. IANA Considerations 7
8. References 7
8.1. Normative References 7
8.2. Informative References 7
Author's Address 8

1. Introduction

The Internet Key Exchange Protocol version 2, defined in [RFC7296], is used in the IPsec architecture to perform authenticated key exchange. [I-D.ietf-ipsecme-qr-ikev2] 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.yeung-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.yeung-g-ikev2] specifies how to do it), the needed sequence of actions introduces an additional delay and adds unnecessary complexity to the protocol.

Since [I-D.ietf-ipsecme-qr-ikev2] 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 Post-Quantum Key Exchanges

to be used in IKEv2 (which is another long-term approach to protect against Quantum Computers and is defined in [I-D.tjhai-ipsecme-hybrid-qske-ikev2]), 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 [I-D.ietf-ipsecme-qr-ikev2], 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 [I-D.ietf-ipsecme-qr-ikev2] 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, she 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 to send PPK identity in the IKE_INTERMEDIATE exchange or in the IKE_AUTH exchange, as defined in the [I-D.ietf-ipsecme-qr-ikev2].

If the initiator decides to use alternative approach, he includes one or more PPK_IDENTITY notification containing PPK identities, which the initiator believes can be used for the IKE SA being created, into the IKE_INTERMEDIATE request. If a series of the IKE_INTERMEDIATE exchanges take 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 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.

First, if the responder doesn't support the alternative approach, she will ignore the received PPK_IDENTITY notification(s) and won't include any 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. Depending on his policy, the initiator may abort negotiation or may continue with the IKE_AUTH exchange. In the latter case depending on the policy the initiator may try to negotiate the use of PPK with conventional approach, as described in [I-D.ietf-ipsecme-qr-ikev2], or may proceed with the standard IKE_AUTH exchange, thus giving up using PPK for this IKE SA.

Another situation occurs when the responder supports this extension, but has no PPK with identity equal to any of the identities provided by the initiator. Depending on responder's policy the following scenarios are possible.

If using PPK is mandatory for the responder, then she returns the AUTHENTICATION_FAILED notification, thus informing the initiator that the SA cannot be created. In this case the initiator MUST abort the process of IKE SA establishment.

```
Initiator                       Responder
-------------------------------------------------------------------
                        <---    HDR, SK {N(AUTHENTICATION_FAILED)}
```

If using PPK is optional for the responder, then she returns the empty PPK_IDENTITY notification, thus informing the initiator that the IKE SA can be created only without using PPK.

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

In this case the initiator depending on whether using PPK is mandatory or not in his own policy may continue establishing IKE SA without PPK or abort it.

Finally, if the responder supports this extension and is configured with one of the PPKs which identities were provided by the initiator, then the responder chooses an appropriate PPK and returns back the PPK_IDENTITY notification containing its identity.

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

In this case the IKE_AUTH exchange is performed as defined in the core IKEv2 specification. In particular, neither PPK_IDENTITY nor NO_PPK_AUTH notifications are included, since it's already known which PPK to use. However, the keys for the IKE SA are computed using PPK, as described in Section 4.

Note, that 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.

4. Computing IKE SA Keys

With alternative approach the keys are computed similarly to [I-D.ietf-ipsecme-qr-ikev2], with the difference, that all SK_* (and not only SK_d, SK_pi and SK_pr) keys are calculated using PPK:

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

SK_d  = prf+ (PPK, SK_d')
SK_ai = prf+ (PPK, SK_ai')
SK_ar = prf+ (PPK, SK_ar')
SK_ei = prf+ (PPK, SK_ei')
SK_er = prf+ (PPK, SK_er')
SK_pi = prf+ (PPK, SK_pi')
SK_pr = prf+ (PPK, SK_pr')
```

If the last IKE_INTERMEDIATE exchange performs an update of the IKE SA keys (e.g. as a result of additional key exchange, as described in [I-D.tjhai-ipsecme-hybrid-qske-ikev2]), then applying PPK MUST be performed to the result of this update. In other words, it must be the last action in calculating SK_* keys for the IKE SA being created.

5. Comparison of the Conventional and the Alternative Approaches

This specification isn't intended to be a replacement for [I-D.ietf-ipsecme-qr-ikev2]. 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.yeung-g-ikev2].

2. Using 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 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 Postquantum Preshared Keys in the IKEv2 protocol are discussed in [I-D.ietf-ipsecme-qr-ikev2]. This specification defines an alternative way of exchanging PPK identity information.

7. IANA Considerations

This specification makes no request to IANA.

8. References

8.1. 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>.

[I-D.ietf-ipsecme-qr-ikev2] Fluhrer, S., McGrew, D., Kampanakis, P., and V. Smyslov, "Postquantum Preshared Keys for IKEv2", draft-ietf-ipsecme-qr-ikev2-08 (work in progress), March 2019.

[I-D.ietf-ipsecme-ikev2-intermediate] Smyslov, V., "Intermediate Exchange in the IKEv2 Protocol", draft-ietf-ipsecme-ikev2-intermediate-02 (work in progress), July 2019.

8.2. Informative References

[I-D.yeung-g-ikev2] Weis, B. and V. Smyslov, "Group Key Management using IKEv2", draft-yeung-g-ikev2-16 (work in progress), July 2019.

[I-D.tjhai-ipsecme-hybrid-qske-ikev2] Tjhai, C., Tomlinson, M., grbartle@cisco.com, g., Fluhrer, S., Geest, D., Garcia-Morchon, O., and V. Smyslov, "Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2)", draft-tjhai-ipsecme-hybrid-qske-ikev2-04 (work in progress), July 2019.

Author's Address

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

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