IPSECME Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 09, 2014

J. Song
T. Tsou
Huawei Technologies
V. Manral
Hewlett-Packard Company

July 08, 2013

IPsec sequence number integrity check value
draft-song-ipsecme-seq-icv-01

Abstract

This document specifies an IPsec AH and ESP sequence number validation scheme, which is complementary to the existing ICV mechanism and anti-replay mechanism of AH and ESP in defense against DOS attack. It is an optional feature negotiable through IKE, for this feature to be negotiated, both sender and receiver must implement it. If any party doesn't support it, then this feature should be excluded from negotiation. The rationale for such a scheme is discussed first; then requirements and guidelines for design of the scheme are laid out. There can be various ways to implement the scheme, some reference designs are discussed to set the base for effort of identifying best practice and eventually establishing a standard on the subject.

Status of This Memo

Copyright Notice

1. Introduction

As defense against replay attack, IPsec, both AH and ESP, uses anti-replay window to keep track of the sequence numbers of received packets, and reject packets with sequence number that is either too old (below anti-replay window) or duplicate (within anti-replay window, but marked as received). Anti-replay window is not effective against DOS attack by packets with sequence number that are above anti-replay window, in which case the sequence number is neither considered too old, nor duplicate. Attack packets with sequence number above anti-replay window would penetrate anti-replay check and only be rejected after failing ICV check. The issue is that ICV check, which involves hashing operation, is rather expensive in terms of resource and time consumption. In case of ESP, when hardware crypto acceleration engine is used, ICV check and decryption often need to be performed together to optimize bandwidth efficiency, which makes the operation even more expensive. Large number of such packets would cause recevier's service degradation or interruption because significant amount of receiver's resource and time would be consumed by performing expensive ICV check on these packets.

An inexpensive mechanism to check sequence number would allow rejecting such packets without causing service degradation or interruption. This check can be performed either before or after anti-replay check depending on policy and situation, but must be performed before ICV check. Such check doesn't have to be 100% accurate as long as it doesn't yield false positive result, i.e. mistaking correct sequence number as incorrect sequence number, since the packet with false negative result, i.e. incorrect sequence number passing the check, will be caught by ICV check eventually. But it must be significantly more resource and time efficient than ICV check to be beneficial.

This check will increase packet length slightly, and incur slight computation overhead per packet, but greatly improve IPsec's capability to withstand DOS attack. This check would not be effective if attacker can prevent original packets from reaching destination, since in such case the attacker doesn't need to change sequence number, instead he or she can change payload, then the packet would pass both anti-replay check and this proposed sequence number check. But in order to shoot down original packets, attacker must compromise intermediate router. The proposed sequence number check is not designed to defend against attacks that involves compromised intermediate router, instead it is designed against attacks where attacker does not control intermediate router, but is able to obtain copy of original packets and launch attack by changing sequence number of the original packets to values that are greater so that anti-replay check would pass and ICV check is required. The latter is simpler attack and easier to carry out therefore is a more serious threat.

This check is not designed for systems that are capable of line rate ICV check; instead it is designed for systems that are not capable of line rate ICV check. This check makes it possible for systems that are not capable of line rate ICV check to continue with normal function when under attacks, as long as the original packets are still being delivered, or in another words, as long as the network in between is not compromised. Systems that are capable of line rate ICV check should decline SEQ-ICV in negotiation.

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 RFC 2119 [RFC2119].

2. SEQ-ICV

SEQ-ICV is a 4 byte value generated by sender for each IPsec packet based on 4 byte packet sequence number, 12 byte ICV value, and 16 byte secret key known and only known to sender and receiver. The value is appended to immediately follow ICV and transmitted together with the packet to receiver, which generates its own value locally the same way as sender, then compares with the transmitted value. If the value is the same, then the sequence number is considered to be good, otherwise the sequence number is considered to be bad.

Following figure illustrates AH header format with SEQ-ICV,

```
        0                   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 Header   |  Payload Len  |          RESERVED             |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                 Security Parameters Index (SPI)               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                    Sequence Number Field                      |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                                                               |
      +                Integrity Check Value-ICV (variable)           |
      |                                                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |        Sequence Number Integrity Check Value-SEQ-ICV          |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Following figure illustrates ESP packet format with SEQ-ICV,

```
    0                   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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ----
   |               Security Parameters Index (SPI)                 | ^Int.
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
   |                      Sequence Number                          | |ered
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
   |                    Payload Data* (variable)                   | |   ^
   ~                                                               ~ |   |
   |                                                               | |Conf.
   +               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
   |               |     Padding (0-255 bytes)                     | |ered*
   +-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
   |                               |  Pad Length   | Next Header   | v   v
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
   |         Integrity Check Value-ICV   (variable)                |
   ~                                                               ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Sequence Number Integrity Check Value-SEQ-ICV          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SEQ-ICV is generated as the following,

SEQ - sequence number, 4 bytes
ICV - Integrity Check Value, 12 bytes
K - secret key, 12 bytes

```
SEQ-ICV = (SEQ + ICV[0-3]) ^ K[0-3] +
          (SEQ + ICV[4-7]) ^ K[4-7] +
          (SEQ + ICV[8-11]) ^ K[8-11]
```

3. Outbound processing

AH transport/tunnel mode

1. generate ICV

2. generate SEQ-ICV

3. adjust packet length in IP header

Packet length field can only be adjusted after generating ICV, since ICV must be based on the packet length without SEQ-ICV

ESP transport/tunnel mode

1. encrypt packet payload

2. generate ICV

3. generate SEQ-ICV

4. adjust packet length in IP header

4. Inbound processing

AH transport/tunnel mode

1. reject if failed anti-replay check

2. generate SEQ-ICV

3. Compare locally generated SEQ-ICV with received SEQ-ICV

4. Reject packet if not same, otherwise adjust packet length field of IP header proceed to AH processing

Packet length field must be adjusted before AH processing

ESP transport/tunnel mode

1. reject if failed anti-replay check

2. generate SEQ-ICV

3. Compare locally generated SEQ-ICV with received SEQ-ICV

4. Reject packet if not same, otherwise proceed to ESP processing

In calculating ESP payload length, SEQ-ICV must be excluded.

Enable SEQ-ICV dynamically

If too many packets passed anti-replay but failed ICV check, then notify sender to enable SEQ-ICV, and receiver begins SEQ-ICV check but would not reject packets that failed SEQ-ICV check, once receiver no longer observes packets passing ICV check but failing SEQ-ICV check, then receiver considers SEQ-ICV has been enabled, and begins to reject packet that failed SEQ-ICV check.

Disable SEQ-ICV dynamically

If no packets passed anti-replay but failed SEQ-ICV, then notify sender to disable SEQ-ICV, and receiver stops rejecting packets that failed SEQ-ICV check, once receiver no longer observes packets passing both SEQ-ICV and ICV check, but only packets passing ICV check, then receiver considers SEQ-ICV has been disabled, and stops checking SEQ-ICV

Following is summary of conditions that could occur throughout the whole process of dynamically enabling and disabling SEQ-ICV with assumption that original packets are delivered,

id	condition	packet	anti-replay	SEQ-ICV	icv	action
1	normal, SEQ-ICV disabled	original	pass	skip	pass	accept
2	under attack, SEQ-ICV disabled	original	pass	skip	pass	accept
	under attack, SEQ-ICV disabled	with fake seq	pass	skip	fail	reject
	under	original	pass	fail	pass	accept

3	attack, enabling SEQ-ICV					
	under attack, enabling SEQ-ICV	with fake seq	pass	fail	fail	reject
4	under attack, enabling SEQ-ICV ready	original	pass	pass	pass	accept
	under attack, enabling SEQ-ICV ready	with fake seq	pass	fail	fail	reject
5	under attack, SEQ-ICV enabled	original	pass	pass	pass	accept
	under attack, SEQ-ICV enabled	with fake seq	pass	fail	skip	reject
6	normal, SEQ-ICV enabled	original	pass	pass	pass	accept
7	normal, disabling SEQ-ICV	original	pass	fail	pass	accept

1 - normal, SEQ-ICV disabled

2 - under attack, SEQ-ICV disabled

3 - under attack, enabling SEQ-ICV

4 - under attack, enabling SEQ-ICV ready

5 - under attack, SEQ-ICV enabled

6 - normal, SEQ-ICV enabled

7 - normal, disabling SEQ-ICV

SEQ-ICV enabling process is 1 through 5

SEQ-ICV disabling process is 6 -> 7 -> 1

5. IKE negotiation

SEQ-ICV will be a type of transform used in AH/ESP.

Following is list of transform IDs that will be defined for transform type of SEQ-ICV

Name	Number
No SEQ-ICV	0
Static SEQ-ICV	1
Dynamic SEQ-ICV	2

Note that an initiator who supports SEQ-ICV will usually construct two proposal, one with SEQ-ICV transform, another without SEQ-ICV transform. It allows implementation that doesn't support SEQ-ICV to choose proposal without SEQ-ICV. In the proposal containing SEQ-ICV transform, an initiator will usually include at least two SEQ-ICV transforms, one with value "0", one with value "1" or "2". A proposal containing a single SEQ-ICV transform with value "1" or "2" means that SEQ-ICV must be used.

A Notify payload with Notify Message Type of SEQ-ICV_ENABLE in an Informational Exchange will be used to notify sender of SEQ-ICV enabling when receiver is under attack by packets with modified sequence number.

6. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

7. Security Considerations

8. Acknowledgments

Robert Moskowitz reminded us of importance of grammatical integrity.

Tero Kivinen pointed out issue with original sample SEQ-ICV-4 generation algorithm and provided insightful feedback on issues like compatibility with existing standard and usage scenario of SEQ-ICV.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

9.2. Informative References

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

Appendix A. Encapsulation Mode

Appendix B. Justification

Authors' Addresses

Jifei Song
Huawei Technologies

Email: jifei.song@huawei.com

Tina Tsou
Huawei Technologies
2330 Central Expressway
Santa Clara
USA

Phone: +1-408-330-4424
Email: tina.tsou.zouting@huawei.com

Vishwas Manral
Hewlett-Packard Company
3000 Hanover St.
Palo Alto
USA

Email: vishwas.manral@hp.com