                 Extended Sequence Number (ESN) Addendum to
                   IPsec Domain of Interpretation (DOI)
                     for Internet Security Association
                  and Key Management Protocol (ISAKMP)

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

   The IP Security Authentication Header (AH) and Encapsulating Security
   Payload (ESP) protocols use a sequence number to detect replay. This
   document describes extensions to the Internet IP Security Domain of
   Interpretation (DOI) for the Internet Security Association and Key
   Management Protocol (ISAKMP). These extensions support negotiation
   of the use of traditional 32-bit sequence numbers or extended (64-
   bit) sequence numbers (ESNs) for a particular AH or ESP security
   association.

1. Introduction

   The specifications for the IP Authentication Header (AH) [AH] and the
   IP Encapsulating Security Payload (ESP) [ESP] describe an option for
   use of extended (64-bit) sequence numbers. This option permits
   transmission of very large volumes of data at high speeds over an
   IPsec Security Association, without rekeying to avoid sequence number
   space exhaustion. This document describes the additions to the IPsec
   DOI for ISAKMP [DOI] that are needed to support negotiation of the
   extended sequence number (ESN) option.

   The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD,
   SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this
   document, are to be interpreted as described in RFC 2119 [Bra97].

2. IPsec Security Association Attribute

   The following SA attribute definition is used in Phase II of an
   Internet Key Exchange Protocol (IKE) negotiation. The attribute type
   is Basic (B). Encoding of this attribute is defined in the base
   ISAKMP specification [ISAKMP]. Attributes described as basic MUST
   NOT be encoded as variable. See [IKE] for further information on
   attribute encoding in the IPsec DOI. All restrictions listed in
   [IKE] also apply to the IPsec DOI and to this addendum.

   Attribute Type

class	value	type
Extended (64-bit) Sequence Number	11	B

   Class Values

      This class specifies that the Security Association will be using
      64-bit sequence numbers. (See [AH] and [ESP] for a description
      of extended (64-bit) sequence numbers.)

      RESERVED   0
      64-bit Sequence Number   1

3. Attribute Negotiation

If an implementation receives a defined IPsec DOI attribute (or attribute value) that it does not support, an ATTRIBUTES-NOT-SUPPORT SHOULD be sent and the security association setup MUST be aborted.

If an implementation receives any attribute value but the value for 64-bit sequence numbers, the security association setup MUST be aborted.

4. Security Considerations

This memo pertains to the Internet Key Exchange protocol [IKE], which combines ISAKMP [ISAKMP] and Oakley [OAKLEY] to provide for the derivation of cryptographic keying material in a secure and authenticated manner. Specific discussion of the various security protocols and transforms identified in this document can be found in the associated base documents and in the cipher references.

The addition of the ESN attribute does not change the underlying security characteristics of IKE. In using ESNs with ESP, it is important to employ an encryption mode that is secure when very large volumes of data are encrypted under a single key. Thus, for example, Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode would NOT be suitable for use with the ESN, because no more than 2^{32} blocks should be encrypted under a single DES key in that mode. Similarly, the integrity algorithm used with ESP or AH should be secure relative to the number of packets being protected. To avoid potential security problems imposed by algorithm limitations, the SA lifetime may be set to limit the volume of data protected with a single key, prior to reaching the 2^{64} packet limit imposed by the ESN.

5. IANA Considerations

This document contains a "magic" number to be maintained by the IANA. No additional class values will be assigned for this attribute. The IANA has allocated an IPsec Security Attribute value for "Attribute Type". This value is listed under the heading "value" in the table in Section 2.

Acknowledgements

The author would like to thank the members of the IPsec working group. The author would also like to acknowledge the contributions of Karen Seo for her help in the editing of this specification.

Normative References

   [Bra97]   Bradner, S., "Key words for use in RFCs to Indicate
             Requirement Level", BCP 14, RFC 2119, March 1997.

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

   [DOI]   Piper, D., "The Internet IP Security Domain of
             Interpretation for ISAKMP", RFC 2407, November 1998.

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

   [IKE]   Harkins, D. and D. Carrel, "The Internet Key Exchange
             (IKE)", RFC 2409, November 1998.

   [ISAKMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner,
             "Internet Security Association and Key Management Protocol
             (ISAKMP)", RFC 2408, November 1998.

Informative References

   [OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC
             2412, November 1998.

Author's Address

   Stephen Kent
   BBN Technologies
   10 Moulton Street
   Cambridge, MA 02138
   USA

   Phone: +1 (617) 873-3988
   EMail: kent@bbn.com