           Algorithms for Internet Key Exchange version 1 (IKEv1)

Status of This Memo

Copyright Notice

Abstract

   The required and suggested algorithms in the original Internet Key
   Exchange version 1 (IKEv1) specification do not reflect the current
   reality of the IPsec market requirements. The original specification
   allows weak security and suggests algorithms that are thinly
   implemented. This document updates RFC 2409, the original
   specification, and is intended for all IKEv1 implementations deployed
   today.

1. Introduction

   The original IKEv1 definition, [RFC2409], has a set of MUST-level and
   SHOULD-level requirements that do not match the needs of IPsec users.
   This document updates RFC 2409 by changing the algorithm requirements
   defined there.

   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 [RFC2119].

2. Old Algorithm Requirements

   RFC 2409 has the following MUST-level and SHOULD-level requirements:

   o DES for encryption MUST be supported.
   o MD5 and SHA-1 for hashing and HMAC functions MUST be supported.
   o Pre-shared secrets for authentication MUST be supported.
   o Diffie-Hellman MODP group 1 (discrete log 768 bits) MUST be
      supported.
   o TripleDES for encryption SHOULD be supported.
   o Tiger for hashing SHOULD be supported.
   o DSA and RSA for authentication with signatures SHOULD be
      supported.
   o RSA for authentication with encryption SHOULD be supported.
   o Diffie-Hellman MODP group 2 (discrete log 1024 bits) SHOULD be
      supported.

   RFC 2409 gives two conflicting requirement levels for Diffie-Hellman
   MODP groups with elliptic curves. Section 4 of that specification
   says that "IKE implementations ... MAY support ECP and EC2N groups",
   but Sections 6.3 and 6.4 say that MODP groups 3 and 4 for EC2N groups
   SHOULD be supported.

3. New Algorithm Requirements

   The new requirements for IKEv1 are listed here. Note that some of
   the requirements are the same as those in RFC 2409, whereas others
   are changed.

   o TripleDES for encryption MUST be supported.
   o AES-128 in CBC mode [RFC3602] for encryption SHOULD be supported.
   o SHA-1 for hashing and HMAC functions MUST be supported.
   o Pre-shared secrets for authentication MUST be supported.
   o AES-128 in XCBC mode for PRF functions ([RFC3566] and [RFC3664])
      SHOULD be supported.
   o Diffie-Hellman MODP group 2 (discrete log 1024 bits) MUST be
      supported.

   o Diffie-Hellman MODP group 14 (discrete log 2048 bits) [RFC3526]
      SHOULD be supported.
   o RSA for authentication with signatures SHOULD be supported.

   If additional updates are made to IKEv1 in the future, then it is
   very likely that implementation of AES-128 in CBC mode for encryption
   will become mandatory.

   The other algorithms that were listed at MUST-level and SHOULD-level
   in RFC 2409 are now MAY-level. This includes DES for encryption, MD5
   and Tiger for hashing, Diffie-Hellman MODP group 1, Diffie-Hellman
   MODP groups with elliptic curves, DSA for authentication with
   signatures, and RSA for authentication with encryption.

   DES for encryption, MD5 for hashing, and Diffie-Hellman MODP group 1
   are dropped to MAY due to cryptographic weakness.

   Tiger for hashing, Diffie-Hellman MODP groups with elliptic curves,
   DSA for authentication with signatures, and RSA for authentication
   with encryption are dropped due to lack of any significant deployment
   and interoperability.

4. Summary

      Algorithm   RFC 2409   This document

      DES for encryption   MUST   MAY (crypto weakness)
      TripleDES for encryption   SHOULD   MUST
      AES-128 for encryption   N/A   SHOULD
      MD5 for hashing and HMAC   MUST   MAY (crypto weakness)
      SHA1 for hashing and HMAC   MUST   MUST
      Tiger for hashing   SHOULD   MAY (lack of deployment)
      AES-XCBC-MAC-96 for PRF   N/A   SHOULD
      Pre-shared secrets   MUST   MUST
      RSA with signatures   SHOULD   SHOULD
      DSA with signatures   SHOULD   MAY (lack of deployment)
      RSA with encryption   SHOULD   MAY (lack of deployment)
      D-H Group 1 (768)   MUST   MAY (crypto weakness)
      D-H Group 2 (1024)   SHOULD   MUST
      D-H Group 14 (2048)   N/A   SHOULD
      D-H elliptic curves   SHOULD   MAY (lack of deployment)

5. Security Considerations

   This document is all about security. All the algorithms that are
   either MUST-level or SHOULD-level in the "new algorithm requirements"
   section of this document are believed to be robust and secure at the
   time of this writing.

6. Normative References

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

   [RFC2409]   Harkins, D. and D. Carrel, "The Internet Key Exchange
               (IKE)", RFC 2409, November 1998.

   [RFC3526]   Kivinen, T. and M. Kojo, "More Modular Exponential (MODP)
               Diffie-Hellman groups for Internet Key Exchange (IKE)",
               RFC 3526, May 2003.

   [RFC3566]   Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm
               and Its Use With IPsec", RFC 3566, September 2003.

   [RFC3602]   Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher
               Algorithm and Its Use with IPsec", RFC 3602, September
               2003.

   [RFC3664]   Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the
               Internet Key Exchange Protocol (IKE)", RFC 3664, January
               2004.

Author's Address

   Paul Hoffman
   VPN Consortium
   127 Segre Place
   Santa Cruz, CA 95060
   US

   EMail: paul.hoffman@vpnc.org