Internet Draft
draft-ietf-ipsec-ui-suites-06.txt
April 14, 2004
Expires in six months
Intended status: Best Common Practice

Paul Hoffman
VPN Consortium

Cryptographic Suites for IPsec

Status of this Memo

Abstract

The IPsec, IKE, and IKEv2 protocols rely on security algorithms to provide privacy and authentication between the initiator and responder. There are many such algorithms available, and two IPsec systems cannot interoperate unless they are using the same algorithms. This document specifies optional suites of algorithms and attributes that can be used to simplify the administration of IPsec when used in manual keying mode, with IKE version 1, or with IKEv2.

1. Introduction

This document is a companion to IPsec [RFC2401] and its two key exchange protocols, IKE [RFC2409] and IKEv2 [IKEv2]. Like most security protocols, IPsec, IKE, and IKEv2 allow users to chose which cryptographic algorithms they want to use to meet their security needs.

Implementation experience with IPsec in manual key mode and with IKE has shown that there are so many choices for typical system administrators to make that it is difficult to achieve interoperability without careful pre-agreement. Because of this, the IPsec Working Group agreed that there should be a small number of named suites that cover typical

security policies. These suites may be presented in the administrative interface of the IPsec system. These suites, often called "UI suites" ("user interface suites"), are optional and do not prevent implementers from allowing individual selection of the security algorithms.

Although the UI suites listed here are optional to implement, this document is intended for Best Common Practice because implementers who call particular suites by the names used here have to conform to the suites listed in this document. These suites should not be considered extensions to IPsec, IKE, and IKEv2, but instead administrative methods for describing sets of configurations.

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in [RFC2119].

2 UI suites

This section lists optional, non-mandatory suites that may be presented to system administrators to ease the burden of choosing among the many options in IPsec systems. These suites cannot cover all of the options that an administrator needs to select. Instead, they give values for a subset of the options.

Note that these UI suites are simply collections of values for some options in IPsec. Use of UI suites does not change the IPsec, IKE, or IKEv2 protocols in any way. Specifically, the transform substructure in IKE and IKEv2 must be used to give the value for each specified option regardless of whether or not UI suites are used.

Implementations that use UI suites SHOULD also provide a management interface for specifying values for individual cryptographic options. That is, it is unlikely that UI suites are a complete solution for matching the security policies of many IPsec users, and therefore an interface that gives a more complete set of options should be used as well.

IPsec implementations that use these UI suites SHOULD use the suite names listed here. IPsec implementations SHOULD NOT use names different than those listed here for the suites that are described, and MUST NOT use the names listed here for suites that do not match these values. These requirements are necessary for interoperability.

Note that the suites listed here are for use of IPsec in virtual private networks. Other uses of IPsec will probably want to define their own suites and give them different names.

Additional suites can be defined by RFCs. The strings used to identify UI suites are registered by IANA.

2.1 Suite "VPN-A"

This suite matches the commonly-used corporate VPN security used in

IKEv1 at the time this document's publication.

IPsec:
Protocol ESP [RFC2406]
ESP encryption TripleDES in CBC mode [RFC2451]
ESP integrity HMAC-SHA1-96 [RFC2404]

IKE and IKEv2:
Encryption TripleDES in CBC mode [RFC2451]
Pseudo-random function HMAC-SHA1 [RFC2104]
Integrity HMAC-SHA1-96 [RFC2404]
Diffie-Hellman group 1024-bit MODP [RFC2409]

Rekeying of Phase 2 (for IKE) or the CREATE_CHILD_SA (for IKEv2) MUST be supported by both parties in this suite. The initiator of this exchange MAY include a new Diffie-Hellman key; if it is included, it MUST be of type 1024-bit MODP. If the initiator of the exchange includes a Diffie-Hellman key, the responder MUST include a Diffie-Hellman key, and it MUST of type 1024-bit MODP.

2.2 Suite "VPN-B"

This suite is what many people expect the commonly-used corporate VPN security that will be used within a few years of the time this document's publication.

IPsec:
Protocol ESP [RFC2406]
ESP encryption AES with 128-bit keys in CBC mode [AES-CBC]
ESP integrity AES-XCBC-MAC-96 [AES-XCBC-MAC]

IKE and IKEv2:
Encryption AES with 128-bit keys in CBC mode [AES-CBC]
Pseudo-random function AES-XCBC-PRF-128 [AES-XCBC-PRF-128]
Integrity AES-XCBC-MAC-96 [AES-XCBC-MAC]
Diffie-Hellman group 2048-bit MODP [RFC3526]

Rekeying of Phase 2 (for IKE) or the CREATE_CHILD_SA (for IKEv2) MUST be supported by both parties in this suite. The initiator of this exchange MAY include a new Diffie-Hellman key; if it is included, it MUST be of type 2048-bit MODP. If the initiator of the exchange includes a Diffie-Hellman key, the responder MUST include a Diffie-Hellman key, and it MUST of type 2048-bit MODP.

2.3 Lifetimes for IKEv1

IKEv1 has two security parameters that do not appear in IKEv2, namely the lifetime of the Phase 1 and Phase 2 SAs. Systems that use IKEv1 with either the VPN-A or VPN-B suites MUST use an SA lifetime of 86400 seconds (1 day) for Phase 1 and an SA lifetime of 28800 seconds (8 hours) for Phase 2.

3. Acknowledgements

Much of the text and ideas in this document came from earlier versions of the IKEv2 document edited by Charlie Kaufman. Other text and ideas were contributed by other members of the IPsec Working Group.

4. Security considerations

This document inherits all of the security considerations of the IPsec, IKE, and IKEv2 documents.

Some of the security options specified in these suites may be found in the future to have properties significantly weaker than those that were believed at the time this document was produced.

5. References

5.1 Normative references

[AES-CBC] "The AES Cipher Algorithm and Its Use With IPsec", draft-ietf-ipsec-ciph-aes-cbc, work in progress.

[AES-XCBC-MAC] "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", draft-ietf-ipsec-ciph-aes-xcbc-mac, work in progress.

[AES-XCBC-PRF-128] "The AES-XCBC-PRF-128 algorithm for IKE", draft-ietf-ipsec-aes-xcbc-prf, work in progress.

[IKEv2] "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2, work in progress.

[RFC2104] "HMAC: Keyed-Hashing for Message Authentication", RFC 2104.

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119.

[RFC2401] "Security Architecture for the Internet Protocol", RFC 2401.

[RFC2404] "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404.

[RFC2406] "IP Encapsulating Security Payload (ESP)", RFC 2406.

[RFC2409] "The Internet Key Exchange (IKE)", RFC 2409.

[RFC2451] "The ESP CBC-Mode Cipher Algorithms", RFC 2451.

[RFC3526] "More MODP Diffie-Hellman groups for IKE", RFC 3526.

6. IANA Considerations

IANA is asked to create and maintain a registry called "Cryptographic Suites for IKEv1, IKEv2, and IPsec". The registry consists of a text string and an RFC number that lists the associated transforms. New entries can be added to the registry only after RFC publication and approval by an expert designated by the IESG.

The initial values for the new registry are:

Identifier	Defined in
VPN-A	RFC [this document]
VPN-B	RFC [this document]

7. Author's address

Paul Hoffman
VPN Consortium
127 Segre Place
Santa Cruz, CA 95060 USA
paul.hoffman@vpnc.org

A. Changes from the -05 draft

[[To be removed when turned into an RFC]]

Changed the IANA considerations to require expert review.