Security Working Group Ipsec Working Group
INTERNET DRAFT Rob Adams
Cisco Systems Inc.
23 June 1997
Expires in Six Months

The ESP IDEA-CBC Algorithm Using Explicit IV
<draft-ietf-ipsec-ciph-idea-cbc-00.txt>

Status of this Memo

Abstract

This draft describes the use of the IDEA [Schneier] block cipher algorithm in CBC mode with the IPSec Encapsulating Security Payload (ESP) [Kent97].

Table of Contents:

1. Introduction

This draft describes the use of the IDEA cipher algorithm in CBC mode to provide confidentiality in conjunction with the IPsec ESP protocol [Kent97].

This document assumes readers are familiar with the terms and concepts in [RFC-1825] and in [Kent97].

1.1 Specification of Requirements

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", and "MAY" that appear in this document are to be interpreted as described in [RFC-2119].

2. Cipher Algorithm

This document gives implementers specific instructions for using the IDEA block cipher algorithm in CBC mode with a block size of 64 bits as described in [Schneier] to secure ESP.

The IDEA algorithm is patented in Europe and in the United States with patent application pending in Japan. Licenses are required for commercial uses of IDEA.

For patent and licensing information, contact:

Ascom Systec AG,
Dept. CMVV
Gewerbepark, CH-5506
Magenwil, Switzerland
Phone: +41 64 56 59 83
Fax: +41 64 56 59 90
idea@ascom.ch

or see

http://www.ascom.ch/Web/systec/policy/normal/exhibit1.html

2.1 Rounds

Compliant implementations may use either four or eight round IDEA.

The key exchange protocol SHOULD negotiate the number of rounds for IDEA. Only four and eight round IDEA are valid. If the key exchange protocol does not negotiate the number rounds, eight round IDEA is the default.

Although there are no known attacks against four round IDEA, those choosing to use four round IDEA for performance reasons, may wish shorten key lifetimes via site specific policy.

2.2 Background

Xuejia Lai and James Massey developed the IDEA (International Data Encryption Algorithm) algorithm. The algorithm is described in detail in [Lai] and [Schneier].

2.3 Performance

Normal eight round IDEA is approximately twice as fast DES on 386 and 486 processors. However on a Pentium, both eight round IDEA and 56 bit key, 16 round DES require about the same number of clock cycles per byte encrypted.

Four round IDEA is twice as fast as eight round IDEA.

For a comparison table of the speed of IDEA and other cipher algorithms, see [Schneier97].

3. Key Size

IDEA accepts 128 bits of keying material to generate sub-keys. IDEA may also accept keying material of sufficient length to set its sub-keys directly. Eight round IDEA uses 52, 16 bit sub-keys or 832 bits of keying material. Four round IDEA uses 28, 16 bit sub-keys or 448 bits of keying material.

Implementations MAY accept keys shorter or longer than 128 bits. Implementations MUST not accept keying material shorter than 40 bits in length.

3.1 Weak Keys

IDEA has weak keys of the following form:

0000,0000,0x00,0000,0000,000x,xxxx,x000

where "x" can be any hexadecimal number.

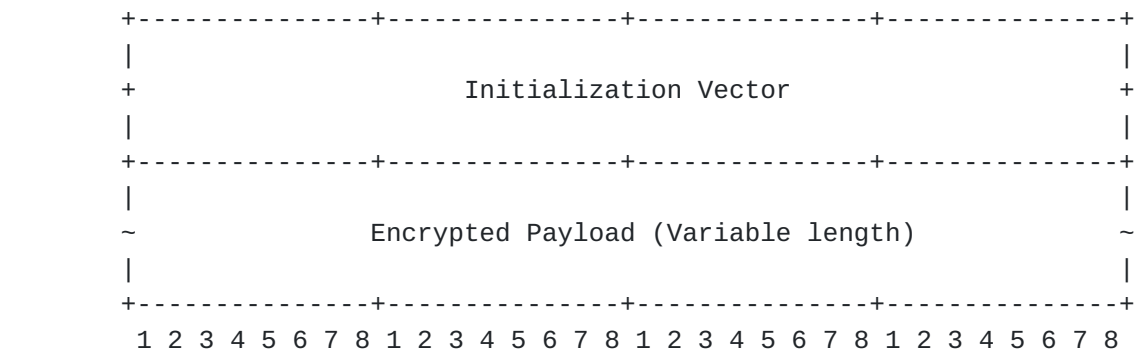
Keys of this form guarantee the value of bit-wise XOR of resultant ciphertext pairs from the bit-wise XOR of certain plaintext pairs. Implementations MUST prohibit weak keys even though the probability of randomly generating such a key is quite small. If the key manager provides the implementation with a weak key, the implementation MUST XOR each of the generated encryption sub-keys with the value 0x0dae before generating the decryption sub-key set [Cryto93]. Implementations may choose to prohibit weak keys by rejecting weak keys altogether and requesting new keying material.

Weak keys cannot be detected if the sub-keys are set directly.

4. ESP Payload

IDEA in CBC mode requires an initialization vector of eight octets for use with ESP [Kent97]. The IV MUST precede the data to be encrypted in the packet and must be eight octets (64 bits) in length. The IV SHOULD be chosen at random. Common practice is to use random data for the first IV and the last eight octets of encrypted data from an encryption process as the IV for the next encryption process.

The payload field, as defined in [Kent97], is broken down according to the following diagram:



4.1 Block Size and Padding

The IDEA-CBC cipher algorithm MUST use a block size of eight octets (64 bits).

Padding is used to align the payload type and pad length octets as specified in [Kent97]. Padding must be sufficient to align the data to be encrypted to an eight octet (64 bit) boundary.

4.2 Interaction with Authentication

This IDEA-CBC ESP document does not limit which authentication algorithm ESP uses.

5. Keying Material

The key exchange protocol MUST provide this ESP algorithm with a number of key material bits greater than or equal to the required key size.

If the key exchange protocol does not negotiate key size, the key MUST be 128 bits in length.

This ESP algorithm will take the IDEA-CBC key from the first <x> bits of keying material, where <x> represents the required key size in bits.

If the required key size is less than 128 bits, the implementation MUST extend the keying material by concatenating it with itself until the concatenated length is greater than or equal to 128 bits. If the concatenated length is greater than 128 bits, implementations MUST truncate the new keying material to 128 bits. Note however that this technique significantly weakens IDEA. It is

suggested that any keys derived in this manner should have short lifetimes.

If the required key size is 128 bits, derive the key schedule normally, according the IDEA specification [Lai].

Two keying material sizes above 128 bits are valid. 448 bits of keying material is valid for four round IDEA. 832 bits of keying material is valid for eight round IDEA.

If the required key size is between 128 bits and the valid size for the number of rounds being used, implementations MUST ignore bits of keying material beyond 128 bits.

If the required key size is greater than 128 bits and valid for the number of rounds being used, implementations MUST set the IDEA encryption key schedule directly from the keying material provided by the key exchange protocol. Set the first IDEA encryption sub-key from the first 16 bits of keying material, and so on. In this case, implementations MUST set the decryption key schedule from the encryption key schedule normally.

Implementations MUST ignore bits of keying material beyond the number of valid bits for the number of rounds being used.

6. Security Considerations

IDEA is thought to be a secure encryption algorithm. Currently there are no known attacks on four or eight round IDEA [Schneier].

7. Reference

[Crypto93] Daeman, J., Govaerts, R., and Vandewalle, J. "Weak Keys for IDEA", Advances in Cryptology, CRYPTO 93 Proceedings, Springer-Verlag, 1994, pp. 224-230.

[Kent97] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", ftp://ietf.org/internet-drafts/draft-ietf-ipsec-new-esp-00.txt, March 1997

[Lai] Lai, X. "On the Design and Security of Block Ciphers", ETH Series in Information Processing, v. 1, Konstanz: Hartung-Gorre Verlag, 1992.

[RFC-1825] Atkinson, R. "Security Architecture for the Internet Protocol", ftp://ds.internic.net/rfc/rfc1825.txt, August 1995.

[RFC-2085] Oehler, M., Glenn, R., "HMAC-MD5 IP Authentication with Replay Prevention," ftp://ds.internic.net/rfc/rfc2085.txt, February 1997.

[RFC-2119] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", ftp://ds.internic.net/rfc/rfc2119.txt, March 1997

[Schneier] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1995. ISBN 0-471-12845-7

[Scheier97] Scheier, B. "Speed Comparisons of Block Ciphers on a Pentium." February 1997, http://www.counterpane.com/speed.html

8. Acknowledgments

This document is based on work done in the IPsec working group and suggestions from Roy Pereira.

The IPSec working group can be contacted through its chairs:

Robert Moskowitz
Rgm3@chrysler.com
Chrysler Corporation

Theodore Y. Tso
Tytso@MIT.EDU
Massachusetts Institute of Technology

or via the IPSec working group's mailing list (ipsec@tis.com).

9. Editors Address

Rob Adams
adams@cisco.com
cisco Systems Inc.
101 Cooper St.
Santa Cruz, CA 95060
United States of America
+1 408 457 5397