Internet Engineering Task Force
IP Security Working Group
Internet Draft
Expires in six months

R. Pereira
TimeStep Corporation
R. Thayer
Sable Technology Corporation
July 17, 1997

The ESP 3DES-CBC Algorithm Using an Explicit IV

<draft-ietf-ipsec-ciph-3des-expiv-00.txt>

Status of this Memo

Abstract

This document describes the "Triple" DES-EDE3-CBC block cipher algorithm used with the IP Encapsulating Security Payload (ESP). Use of an explicit IV is described.

Table of Contents

1. Introduction

The Encapsulating Security Payload (ESP) [Kent97] provides confidentiality for IP datagrams by encrypting the payload data to be protected. This specification describes the ESP use of 3DES.

It is assumed that the reader is familiar with the terms and concepts described in the "Security Architecture for the Internet Protocol" [Atkinson95], "IP Security Document Roadmap" [Thayer97], and "IP Encapsulating Security Payload (ESP)" [Kent97] documents.

Furthermore, this document is a companion to [Kent97] and MUST be read in its context.

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 [Bradner97].

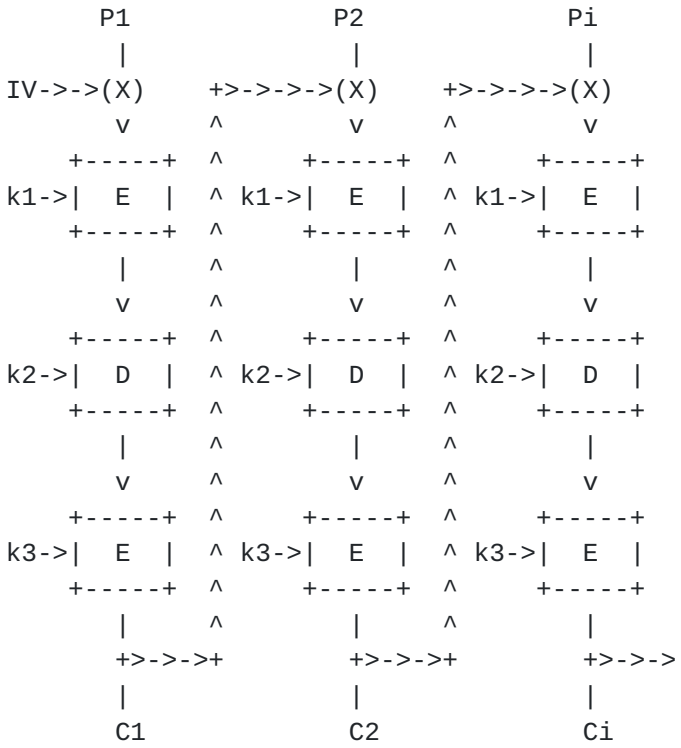
2. Cipher Algorithm

This is a variant of the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46].

This variant, colloquially known as "Triple DES", processes each block three times, each time with a different key. This technique of using more than one DES operation was proposed in [Tuchman79].

For more explanation and implementation information for Triple DES, see [Schneier95].

2.1 Mode



The DES-EDE3-CBC algorithm is a simple variant of the DES-CBC algorithm [RFC-1829x]. The "outer" chaining technique is used.

In DES-EDE3-CBC, an Initialization Vector (IV) is XOR'd with the first 64-bit (8 byte) plaintext block (P1). The keyed DES function is iterated three times, an encryption (Ek1) followed by a decryption (Dk2) followed by an encryption (Ek3), and generates the ciphertext (C1) for the block. Each iteration uses an independant key: k1, k2 and k3.

For successive blocks, the previous ciphertext block is XOR'd with the current plaintext (Pi). The keyed DES-EDE3 encryption function generates the ciphertext (Ci) for that block.

To decrypt, the order of the functions is reversed: decrypt with k3, encrypt with k2, decrypt with k1, and XOR the previous ciphertext block.

Note that when all three keys (k1, k2 and k3) are the same, DES-EDE3-CBC is equivalent to DES-CBC. This property allows the DES-

EDE3 hardware implementations to operate in DES mode without modification.

2.2 Performance

Triple DES is approximately 2.5 times slower than "single" DES (rather than 3 times), because inner permutations may be removed.

Phil Karn has tuned DES-EDE3-CBC software to achieve 6.22 Mbps with a 133 MHz Pentium. Other DES speed estimates may be found at [Schneier95, page 279].

3. Key Sizes

The secret DES-EDE3 key shared between the communicating parties is effectively 168-bits long. This key consists of three independent 56-bit quantities used by the DES algorithm. Each of the three 56-bit sub-keys is stored as a 64-bit (8 byte) quantity, with the least significant bit of each byte used as a parity bit.

Implementations of this transform SHOULD take into consideration the parity bits when initially accepting a new set of keys.

3.1 Weak Keys

DES has 64 known weak keys, including so-called semi-weak keys and possibly-weak keys [Schneier95, pp 280-282]. The likelihood of picking one at random is negligible.

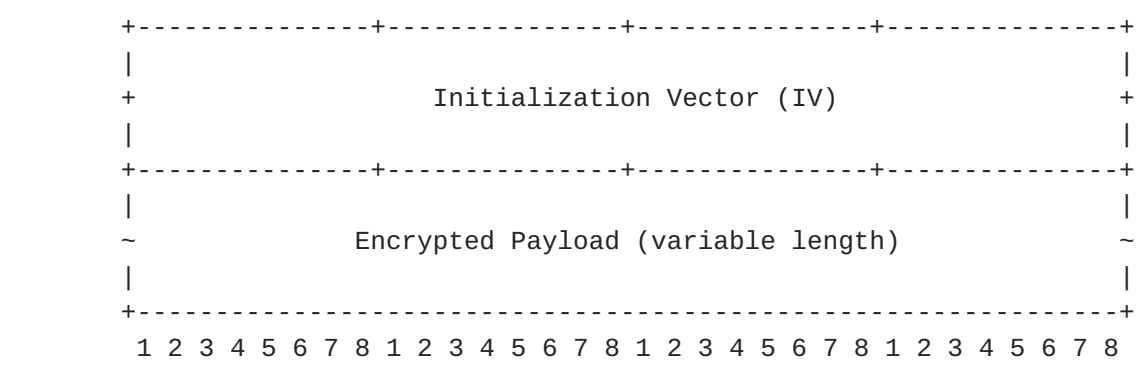
For DES-EDE3, there is no known need to reject weak or complementation keys. Any weakness is obviated by the other keys.

However, if the first two independent 64-bit keys are equal (k1 == k2), then the 3DES operation is simply the same as DES. Implementers MUST reject keys that exhibit this property.

4. ESP Payload

DES-EDE3-CBC requires an explicit Initialization Vector (IV) of 8 octets (64 bits). Thus the payload is made up of the 8 octet IV followed by raw cipher-text. The IV SHOULD be chosen at random. Common practice is to use random data for the first IV and the last 8 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 ESP 3DES-CBC algorithm described in this document MUST use a block size of 8 octets (64 bits).

When padding is required, it MUST be done according to the conventions specified in [Kent97].

4.2 Interaction with Authentication Algorithms

This ESP 3DES-CBC document has no limitations on what authentication algorithm is used in ESP.

5. Keying Material

The number of bits sent from the key exchange protocol to this ESP algorithm must be equal to the key size.

The key is taken from the first 192 bits of the keying material, where the first 64 bits represent the first key, the next 64 bits represent the second key and the last 64 bits represent the third key.

6. Security Considerations

As with other ESP Transforms there are common security considerations, which are not discussed here. The ESP document and the IPsec architecture document should be consulted. Also, as with any other encryption technology, one should examine the current literature for any new attack strategies discovered after this document was published.

A discussion of security considerations specific to DES is also relevant to this cipher, see [RFC-1829x] for this discussion.

Since Triple DES uses three times as much keying material as DES, it places a larger burden on automatic keying systems that use such devices as random number generators and entropy pools. Use of automatic keying should be carefully configured to be aware of this impact.

7. References

[Atkinson95] Atkinson, R., "Security Architecture for the Internet Protocol", draft-ietf-ipsec-arch-sec-01

[Bradner97] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", RFC2119, March 1997

[Kent97] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", draft-ietf-ipsec-new-esp-01

[Thayer97] R. Thayer, N. Doraswamy, R. Glenn, "IP Security Document Roadmap", draft-ietf-ipsec-doc-roadmap-00.txt

[FIPS-46] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 46, January 1977.

[RFC-1829x] Karn, P., Metzger, P., Simpson, W.A., "The ESP DES-CBC Transform", work in progress.

[Schneier95] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1995. ISBN 0-471-12845-7.

[Tuchman79] Tuchman, W, "Hellman Presents No Shortcut Solutions to DES", IEEE Spectrum, v. 16 n. 7, July 1979, pp. 40-41.

8. Acknowledgments

This document is based on the IETF work described in <draft-ietf-ipsec-ciph-3des-00.txt> with he only major differences being an explicit IV instead of a derived one and that padding is done as the default method states in ESP.

Our thanks to all of the editors of the previous ESP 3DES documents; W. Simpson, N. Doraswamy, P. Metzger, and P. Karn.

9. Editors' Addresses

Roy Pereira
rpereira@timestep.com
TimeStep Corporation
(613) 599-3610 x 4808

Rodney Thayer
rodney@sabletech.com
Sable Technology Corporation
(617) 332-7292

The IPSec working group can be contacted via the IPSec working group's mailing list (ipsec@tis.com) or through its chairs:

Robert Moskowitz
rgm@chrysler.com
Chrysler Corporation

Theodore Y. Ts'o
tytso@MIT.EDU
Massachusetts Institute of Technology