

Network Working Group
INTERNET DRAFT
Expires in Six Months

IPsec Working Group
C. Madson
Cisco Systems, Inc.
N. Doraswamy
Bay Networks, Inc.
November 1997

**The ESP DES-CBC Cipher Algorithm
With Explicit IV**
[<draft-ietf-ipsec-ciph-des-expiv-01.txt>](#)

Status of this Memo

This document is a submission to the IETF Internet Protocol Security (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@tis.com) or to the authors.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts draft documents are valid for a maximum of six months and may be updated, replaced, or obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on [ftp.is.co.za](ftp://ftp.is.co.za) (Africa), [nic.nordu.net](ftp://nic.nordu.net) (Europe), [munnari.oz.au](ftp://munnari.oz.au) (Pacific Rim), [ds.internic.net](ftp://ds.internic.net) (US East Coast), or [ftp.isi.edu](ftp://ftp.isi.edu) (US West Coast).

Distribution of this memo is unlimited.

Abstract

This document describes the use of the DES Cipher algorithm in Cipher Block Chaining Mode, with an explicit IV, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).

1. Introduction

This document describes the use of the DES Cipher algorithm in Cipher Block Chaining Mode as a confidentiality mechanism within the context of the Encapsulating Security Payload.

DES is a symmetric block cipher algorithm. The algorithm is described in [[FIPS-46](#)][[FIPS-46-1](#)][[FIPS-74](#)][[FIPS-81](#)]. [[Schneier96](#)] provides a general description of Cipher Block Chaining Mode, a mode which is applicable to several encryption algorithms.

As specified in this draft, DES-CBC is not an authentication mechanism. [Although DES-MAC, described in [[Schneier96](#)] amongst other places, does provide authentication, DES-MAC is not discussed here.]

For further information on how the various pieces of ESP fit together to provide security services, refer to [[ESP](#)] and [[Thayer97](#)].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC-2119](#)].

2. Algorithm and Mode

DES-CBC is a symmetric secret-key block algorithm. It has a block size of 64 bits.

[[FIPS-46](#)][[FIPS-46-1](#)][[FIPS-74](#)] and [[FIPS-81](#)] describe the DES algorithm, while [[Schneier96](#)] provides a good description of CBC mode.

2.1 Performance

Phil Karn has tuned DES-CBC software to achieve 10.45 Mbps with a 90 MHz Pentium, scaling to 15.9 Mbps with a 133 MHz Pentium. Other DES speed estimates may be found in [[Schneier96](#)].

3. ESP Payload

DES-CBC requires an explicit Initialization Vector (IV) of 8 octets (64 bits). This IV immediately precedes the protected (encrypted) payload. The IV SHOULD be chosen at random.

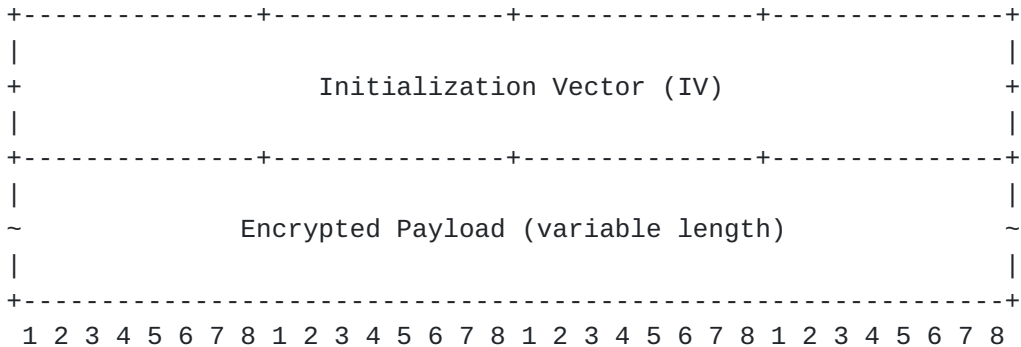
Including the IV in each datagram ensures that decryption of each received datagram can be performed, even when some datagrams are dropped, or datagrams are re-ordered in transit.

Implementation note:

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; this logically extends the CBC across the packets. It also has the advantage of limiting the

leakage of information from the random number generator. No matter which mechanism is used, the receiver MUST NOT assume any meaning for this value, other than that it is an IV.

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



3.1 Block Size and Padding

The DES-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 [ESP].

4. Key Material

DES-CBC is a symmetric secret key algorithm. The key size is 64-bits. [It is commonly known as a 56-bit key as the key has 56 significant bits; these 56 bits are stored in an 8-byte (64-bit) value, where each byte has seven significant bits from the 56-bit value and the least significant bit is used as a parity bit.]

[ESP] describes the general mechanism to derive keying material for the ESP transform. The derivation of the key from some amount of keying material does not differ between the manually- and automatically-keyed security associations.

The mechanism MUST derive a 64-bit key value for use by this cipher. This derived value MUST be adjusted for parity as necessary. Weak key checks will be performed; if a weak key is discovered, the key will be rejected and IPSEC will request a new SA.

4.1 Weak Keys

DES has 64 known weak keys, including so-called semi-weak keys and possibly-weak keys (from [Schneier96] -- corrected version provided by William Allan Simpson -- shown here in hex with parity bits):

0101 0101 0101 0101
1f1f 1f1f 0e0e 0e0e
e0e0 e0e0 f1f1 f1f1
fefe fefe fefe fefe

semi-weak key pairs:

01fe	01fe	01fe	01fe	fe01	fe01	fe01	fe01
1fe0	1fe0	0ef1	0ef1	e0f1	e0f1	f10e	f10e
01e0	01e0	01f1	01f1	e001	e001	f101	f101
1ffe	1ffe	0efe	0efe	fe1f	fe1f	fe0e	fe0e
011f	011f	010e	010e	1f01	1f01	0e01	0e01
e0fe	e0fe	f1fe	f1fe	fee0	fee0	fef1	fef1

possibly-weak keys:

1f1f	0101	0e0e	0101	e001	01e0	f101	01f1
011f	1f01	010e	0e01	fe1f	01e0	fe0e	01f1
1f01	011f	0e01	010e	fe01	1fe0	fe01	0ef1
0101	1f1f	0101	0e0e	e01f	1fe0	f10e	0ef1

e0e0	0101	f1f1	0101	fe01	01fe	fe01	01fe
fefe	0101	fefe	0101	e01f	01fe	f10e	01fe
fee0	1f01	fef1	0e01	e001	1ffe	f101	0efe
e0fe	1f01	f1fe	0e01	fe1f	1ffe	fe0e	0efe

fee0	011f	fef1	010e	1ffe	01e0	0efe	01f1
e0fe	011f	f1fe	010e	01fe	1fe0	01fe	0ef1
e0e0	1f1f	f1f1	0e0e	1fe0	01fe	0ef1	01fe
fefe	1f1f	fefe	0e0e	01e0	1ffe	01f1	0efe

fe1f	e001	fe0e	f101	0101	e0e0	0101	f1f1
e01f	fe01	f10e	fe01	1f1f	e0e0	0e0e	f1f1
fe01	e01f	fe01	f1e0	1f01	fee0	0e01	fef1
e001	fe1f	f101	fe0e	011f	fee0	010e	fef1

01e0	e001	01f1	f101	1f01	e0fe	0e01	f1fe
1ffe	e001	0efe	f101	011f	e0fe	010e	f1fe
1fe0	fe01	0ef1	fe01	0101	fefe	0101	fefe
01fe	fe01	01fe	fe01	1f1f	fefe	0e0e	fefe

1fe0	e01f	0ef1	f10e	fefe	e0e0	fefe	f1f1
01fe	e01f	01fe	f10e	e0fe	fee0	f1fe	fef1
01e0	fe1f	01f1	fe0e	fee0	e0fe	fef1	f1fe
1ffe	fe1f	0efe	fe0e	e0e0	fefe	f1f1	fefe

Implementations SHOULD take care not to select weak keys [CN94], although the likelihood of picking one at random is negligible.

4.2 Key Lifetime

There are no current recommendations for key lifetime.

5. Interaction with Authentication Algorithms

As of this writing, there are no known issues which preclude the use of the DES-CBC algorithm with any specific authentication algorithm.

6. Security Considerations

[Much of this section was originally written by William Allen Simpson and Perry Metzger.]

Users need to understand that the quality of the security provided by this specification depends completely on the strength of the DES algorithm, the correctness of that algorithm's implementation, the security of the Security Association management mechanism and its implementation, the strength of the key [CN94], and upon the correctness of the implementations in all of the participating nodes.

[Bell95] and [Bell96] describe a cut and paste splicing attack which applies to all Cipher Block Chaining algorithms. This attack can be addressed with the use of an authentication mechanism.

The use of the cipher mechanism without any corresponding authentication mechanism is strongly discouraged. This cipher can be used in an ESP transform that also includes authentication; it can also be used in an ESP transform that doesn't include authentication provided there is an companion AH header. Refer to [ESP], [AH], [arch], and [Thayer97] for more details.

When the default ESP padding is used, the padding bytes have a predictable value. They provide a small measure of tamper detection on their own block and the previous block in CBC mode. This makes it somewhat harder to perform splicing attacks, and avoids a possible covert channel. This small amount of known plaintext does not create any problems for modern ciphers.

At the time of writing of this document, [BS93] demonstrated a differential cryptanalysis based chosen-plaintext attack requiring 2^{47} plaintext-ciphertext pairs, where the size of a pair is the size of a DES block (64 bits). [Matsui94] demonstrated a linear cryptanalysis based known-plaintext attack requiring only 2^{43} plaintext-ciphertext pairs. Although these attacks are not considered practical, they must be taken into account.

More disturbingly, [Weiner94] has shown the design of a DES cracking machine costing \$1 Million that can crack one key every 3.5 hours. This is an extremely practical attack.

One or two blocks of known plaintext suffice to recover a DES key. Because IP datagrams typically begin with a block of known and/or guessable header text, frequent key changes will not protect against this attack.

It is suggested that DES is not a good encryption algorithm for the protection of even moderate value information in the face of such

equipment. Triple DES is probably a better choice for such purposes.

However, despite these potential risks, the level of privacy provided by use of ESP DES-CBC in the Internet environment is far greater than sending the datagram as cleartext.

7. References

- [Bell95] Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity", Presentation at the 32nd Internet Engineering Task Force, Danvers Massachusetts, April 1995.
- [Bell96] Bellovin, S., "Problem Areas for the IP Security Protocols", Proceedings of the Sixth Usenix Security Symposium, July 1996.
- [BS93] Biham, E., and Shamir, A., "Differential Cryptanalysis of the Data Encryption Standard", Berlin: Springer-Verlag, 1993.
- [CN94] Carroll, J.M., and Nudiati, S., "On Weak Keys and Weak Data: Foiling the Two Nemeses", Cryptologia, Vol. 18 No. 23 pp. 253-280, July 1994.
- [FIPS-46] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 46, January 1977.
- [FIPS-46-1] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 46-1, January 1988.
- [FIPS-74] US National Bureau of Standards, "Guidelines for Implementing and Using the Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 74, April 1981.
- [FIPS-81] US National Bureau of Standards, "DES Modes of Operation" Federal Information Processing Standard (FIPS) Publication 81, December 1980.
- [Matsui94] Matsui, M., "Linear Cryptanalysis method for DES Cipher," Advances in Cryptology -- Eurocrypt '93 Proceedings, Berlin: Springer-Verlag, 1994.
- [RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC-2119](#)/BCP 14, March, 1997.
- [Schneier96] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1996. ISBN 0-471-12845-7.
- [Weiner94] Wiener, M.J., "Efficient DES Key Search", School of Computer Science, Carleton University, Ottawa, Canada, TR-244, May 1994. Presented at the Rump Session of Crypto '93.
- [ESP] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", [draft-ietf-ipsec-esp-v2-02.txt](#), work in progress, November 1997.

[AH] Kent, S., Atkinson, R., "IP Authentication Header (AH)",
[draft-ietf-ipsec-auth-header-03.txt](#), work in progress, November
1997.

[arch] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", [draft-ietf-ipsec-arch-sec-02.txt](#), work in progress, November 1997.

[Thayer97] Thayer, R., Doraswamy, N., Glenn, R., "IP Security Document Roadmap", [draft-ietf-ipsec-doc-roadmap-02.txt](#), work in progress, November, 1997.

8. Acknowledgments

Much of the information provided here originated with various ESP-DES documents authored by Perry Metzger and William Allen Simpson, including the data entry of the known weak key values, and especially the Security Considerations section.

This document is also derived in part from previous works by Jim Hughes, those people that worked with Jim on the combined DES-CBC+HMAC-MD5 ESP transforms, the ANX bakeoff participants, and the members of the IPsec working group.

Thanks also to Rob Glenn for assisting with the nroff formatting.

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

9. Editors' Addresses

Cheryl Madson
<cmadson@cisco.com>
Cisco Systems, Inc.

Naganand Doraswamy
<naganand@baynetworks.com>
Bay Networks, Inc.

