Network Working Group
Internet Draft

N Doraswamy
[Bay Networks]
P Metzger
[Piermont]
W A Simpson
[DayDreamer]

expires in six months

July 1997

The ESP Triple DES Transform
draft-ietf-ipsec-ciph-des3-00.txt

Status of this Memo

Follows draft-simpson-esp-des3-x-01.txt.

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 are draft documents valid for a maximum of six months, and may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material, or to cite them other than as a ``working draft'' or ``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 (Africa)
nic.nordu.net (Europe)
ds.internic.net (US East Coast)
ftp.isi.edu (US West Coast)
munnari.oz.au (Pacific Rim)

Distribution of this memo is unlimited.

Astract

This document describes the "Triple" DES-EDE3-CBC block cipher transform interface used with the IP Encapsulating Security Payload (ESP). It provides compatible migration from RFC-1851.

1. Introduction

The Encapsulating Security Payload (ESP) [RFC-1827x] provides confidentiality for IP datagrams by encrypting the payload data to be protected. This specification describes the ESP use of a variant of the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46, FIPS-46-1, FIPS-74, FIPS-81].

This variant, colloquially known as "Triple DES", processes each block three times, each time with a different key [Tuchman79].

For an explanation of the use of CBC mode with this cipher, see [RFC-wwww].

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

This document assumes that the reader is familiar with the related document "Security Architecture for the Internet Protocol" [RFC-1825x], that defines the overall security plan for IP, and provides important background for this specification.

In this document, the key words "MAY", "MUST", "recommended", "required", and "SHOULD", are to be interpreted as described in [RFC-2119].

1.1. Availability

There were a number of US patents (see [Schneier95] for listing). All patents have expired. Several freely available implementations have been published world-wide.

1.2. Performance

As this specification requires "outer" chaining, it is not possible to provide parallel computation for the same data stream. 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]. Your milage may vary.

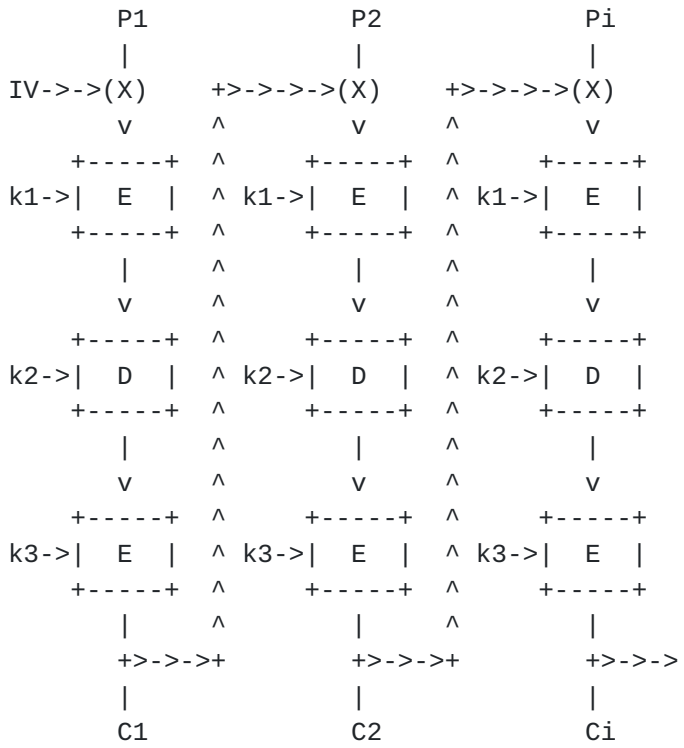
2. Description

2.1. Block Size

The US Data Encryption Standard (DES) algorithm operates on blocks of 64-bits (8 bytes). This often requires padding before encrypting, and subsequent removal of padding after decrypting.

The output is the same number of bytes that are input. This facilitates in-place encryption and decryption.

2.2. Mode



The DES-EDE3-CBC algorithm is a simple variant of the DES-CBC algorithm [RFC-wwww, 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.

2.3. Interaction with Authentication

There is no known interaction of DES with any currently specified Authenticator algorithm. Never-the-less, any Authenticator MUST use a separate and independently generated key.

3. Initialization Vector

DES-EDE3-CBC requires an Initialization Vector (IV) that is 64-bits (8 bytes) in length [RFC-wwww].

By default, the 64-bit IV is generated from the 32-bit ESP Sequence Number field followed by (concatenated with) the bit-wise complement of the same 32-bit value:

```
SN || -SN
```

Alternative IV generation techniques MAY be specified when dynamically configured via a key management protocol.

Security Notes:

Using the Sequence Number provides an easy method for preventing IV repetition, and is sufficiently robust for practical use with the DES algorithm. But, when used alone, cryptanalysis might be aided by the rare serendipitous occurrence when the Sequence Number increments in exactly the same fashion as a corresponding bit position in the first block.

No commonly used IP (Next Header) Protocols exhibit this property. Never-the-less, inclusion of the bit-wise complement ensures that Sequence Number bit changes are reflected twice in the IV.

4. Keys

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.

4.1. 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, since checking for weak keys is quite easy, the configuration mechanisms are expected to incorporate the test.

4.2. Manual Key Management

When configured manually, three independently generated keys are required, in the order used for encryption, and 64-bits (8 bytes) are configured for each individual key.

Keys with incorrect parity SHOULD be rejected by the configuration utility, ensuring that the keys have been correctly configured.

Each key is examined sequentially, in the order used for encryption. A key that is identical to a previous key MAY be rejected. The 64 known weak DES keys [RFC-1829x] SHOULD be rejected.

4.3. Automated Key Management

When configured via a Security Association management protocol, three independently generated keys are required, in the order used for encryption, and 64-bits (8 bytes) are returned for each individual key.

The key manager MAY be required to generate the correct parity. Alternatively, the least significant bit of each key byte is ignored, or locally set to parity by the DES implementation.

Each key is examined sequentially, in the order used for encryption.

A key that is identical to a previous key MUST be rejected. The 64 known weak DES keys [RFC-1829x] MUST be rejected.

4.4. Refresh Rate

To prevent differential and linear cryptanalysis of collisions [RFC-wwww], no more than 2**32 plaintext blocks SHOULD be encrypted with the same key. Depending on the average size of the datagrams, the key SHOULD be changed at least as frequently as 2**30 datagrams.

5. ESP Alterations

5.1. ESP Sequence Number

The Sequence Number is a 32-bit (4 byte) unsigned counter. This field protects against replay attacks, and may also be used for synchronization by stream or block-chaining ciphers.

When configured manually, the first value sent SHOULD be a random number. The limited anti-replay security of the sequence of datagrams depends upon the unpredictability of the values.

When configured via an automated Security Association management protocol, the first value sent is 1, unless otherwise negotiated.

Thereafter, the value is monotonically increased for each datagram sent. A replacement SPI SHOULD be established before the value repeats. That is, no more than 2**32 datagrams SHOULD be sent with any single key.

5.2. ESP Padding

The Padding field may be zero or more bytes in length.

Prior to encryption, this field is filled with a series of integer values to align the Pad Length and Payload Type fields at the end of a 64-bit (8 byte) block boundary (measured from the beginning of the Transform Data).

By default, each byte contains the index of the byte. For example, three pad bytes would contain the values 1, 2, 3.

After decryption, this field MAY be examined for a valid series of integer values. Verification of the sequence of values is at the discretion of the receiver.

Operational Considerations

The specification provides only a few manually configurable parameters:

SPI
: Manually configured SPIs are limited in range to aid operations. Automated SPIs are pseudo-randomly distributed throughout the remaining 2**32 values.

  Default: 0 (none). Range: 256 to 65,535.

SPI LifeTime (SPILT)
: Manually configured LifeTimes are generally measured in days. Automated LifeTimes are specified in seconds.

  Default: 32 days (2,764,800 seconds). Maximum: 182 days (15,724,800 seconds).

Replay Window
: Long term replay prevention requires automated configuration. Also, some earlier implementations used pseudo-random values. This check must only be used with those peers that have implemented this feature.

  Default: 0 (checking off). Range: 32 to 256.

Pad Values
: New implementations use verifiable values. However, some earlier implementations used pseudo-random values. This check must only be used with those peers that have implemented this feature.

  Also, some operations desire additional padding to inhibit traffic analysis.

  Default: 0 (checking off). Range: 7 to 255.

Key
: Three 56-bit keys are configured as a 192-bit quantity, with parity included as appropriate.

Each party configures a list of known SPIs and symmetric secret-keys.

In addition, each party configures local policy that determines what access (if any) is granted to the holder of a particular SPI. For example, a party might allow FTP, but prohibit Telnet. Such considerations are outside the scope of this document.

Security Considerations

Users need to understand that the quality of the security provided by this specification depends completely on the strength of the Triple 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.

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.

It was originally thought that DES might be a group, but it has been demonstrated that it is not [CW92]. Since DES is not a group, composition of multiple rounds of DES is not equivalent to simply using DES with a different key.

Triple DES with independent keys is not, as naively might be expected, as difficult to break by brute force as a cryptosystem with three times the keylength. A space/time tradeoff has been shown which can brute-force break triple block encryptions in the time naively expected for double encryption [MH81].

However, "double" DES (DES-EE2) can be broken with a meet-in-the-middle attack, without significantly more complexity than breaking DES requires [ibid]. DES-EDE3 with three independant keys is actually needed to provide significantly more security than "single" DES.

An attack has been shown on DES-EDE2 (using only two independent keys) [Tuchman79] that is somewhat (sixteen times) faster than exhaustive search [OW91]. Again, DES-EDE3 with three independant keys is actually needed to provide the expected level of security.

Although it is widely believed that DES-EDE3 is substantially stronger than single DES alone, as it is less amenable to brute force attack, it should be noted that real cryptanalysis of DES-EDE3 might not use brute force methods at all. Instead, it might be performed using variants on differential [BS93] or linear [Matsui94] cryptanalysis. It should also be noted that no encryption algorithm is permanently safe from brute force attack, because of the increasing speed of modern computers.

As with all cryptosystems, those responsible for applications with substantial risk when security is breeched should pay close attention to developments in cryptology, and especially cryptanalysis, and

switch to other transforms should DES-EDE3 prove weak.

Changes from RFC-1851:

This specification results in the same default bits-on-the-wire as the 32-bit IV calculation method of RFC-1851. The 32-bit field is semantically identical to a Sequence Number when implemented as a counter (the recommended method).

The 64-bit explicit IV option is deprecated, as no hardware manufacturers were found that required it. It does not meet 64-bit field alignment expectations of IPv6, it is a cryptographically weaker construct than a calculated IV [Bellovin96], and it conflicts with the use of a Sequence Number immediately following the SPI.

Clarified to specify "outer" CBC, as originally intended.

Updated performance estimates. Replaced erroneous text about parallel computation.

Padding is a known series of integers, that may be checked upon receipt.

Many implementation details by Karn were found to be common to all ESP Ciphers, and are awaiting consolidation in the ESP specification.

Added an operational section.

Updated acknowledgements, references, and contacts.

Reorganized according to the new "road map" document.

Acknowledgements

The basic field naming and layout is based on "swIPe" [IBK93, IB93].

Some of the text of this specification was derived from work by Randall Atkinson for the SIP, SIPP, and IPv6 Working Groups.

Perry Metzger provided the original Security Considerations text, some of which is distributed throughout the document.

William Allen Simpson was responsible for the name and semantics of the SPI, the IV calculation technique(s), editing and formatting.

The use of known padding values was suggested in various forms by Robert Baldwin, Phil Karn, and David Wagner. This specification uses Self-Describing-Padding [RFC-1570].

Steve Bellovin, Angelos Keromytis, Holger Kummert, and Rodney Thayer provided useful critiques of earlier versions of this document.

References

[Bellovin96]
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.

[CW92] Campbell, K.W., and Wiener, M.J., "Proof that DES Is Not a Group", Advances in Cryptology -- Crypto '92 Proceedings, Berlin: Springer-Verlag, 1993, pp 518-526.

[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.

[IB93] Ioannidis, J., and Blaze, M., "The Architecture and Implementation of Network-Layer Security Under Unix", Proceedings of the Fourth Usenix Security Symposium, Santa Clara California, October 1993.

[IBK93] Ioannidis, J., Blaze, M., and Karn, P., "swIPe: Network-Layer Security for IP", Presentation at the 26th Internet Engineering Task Force, Columbus Ohio, March 1993.

[Matsui94]
Matsui, M., "Linear Cryptanalysis method for DES Cipher," Advances in Cryptology -- Eurocrypt '93 Proceedings, Berlin: Springer-Verlag, 1994.

[MH81] Merkle, R.C., and Hellman, M., "On the Security of Multiple Encryption", Communications of the ACM, v. 24 n. 7, 1981, pp. 465-467.

[OW91] van Oorschot, P.C., and Weiner, M.J. "A Known-Plaintext Attack on Two-Key Triple Encryption", Advances in Cryptology -- Eurocrypt '90 Proceedings, Berlin: Springer-Verlag, 1991, pp. 318-325.

[RFC-1570]
Simpson, W., "PPP LCP Extensions", DayDreamer, January 1994.

[RFC-1825x]
Atkinson, R., "Security Architecture for the Internet Protocol", Naval Research Laboratory, July 1995.

[RFC-1827x]
Simpson, W., "IP Encapsulating Security Protocol (ESP) for implementors",

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

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

[RFC-wwww]
Simpson, W.A, "ESP with Cipher Block Chaining (CBC)", 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.

Contacts

Comments about this document should be discussed on the ipsec@tis.com mailing list.

Questions about this document can also be directed to:

Naganand Doraswamy
Bay Networks
3 Federal Street #BL3-04
Billerica, Massachusetts 01821

naganand@BayNetworks.Com

Perry Metzger
Piermont Information Systems Inc.
160 Cabrini Blvd., Suite #2
New York, NY 10033

perry@piermont.com

William Allen Simpson
DayDreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

wsimpson@UMich.edu
wsimpson@GreenDragon.com (preferred)
bsimpson@MorningStar.com