Network Working Group
Internet Draft

P Metzger
P Karn
W A Simpson

expires in six months

January 1995

The ESP Triple DES-CBC Transform
draft-metzger-esp-3des-cbc-00.txt

Status of this Memo

This document is a submission to the IP Security Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the ipsec@ans.net mailing list.

Distribution of this memo is unlimited.

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)

Abstract

This document describes the Triple DES-CBC security transform for the Encapsulating Security Payload (ESP).

1. Introduction

The Encapsulating Security Payload (ESP) [AMS-esp] provides confidentiality and integrity by encrypting the data to be protected. This specification describes the ESP use of a variant of 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, known as Triple DES (3DES), encrypts each block of the plaintext three times, each time with a different key [Tuchman79]. A recent book also provides information on 3DES [Schneier94].

All implementations that claim conformance or compliance with the Encapsulating Security Payload specification SHOULD implement this Triple DES-CBC transform.

Implementors should consult the most recent version of the IAB Standards [RFC-1610] for further guidance on the status of this document.

1.1. Keys

The secret 3DES 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 subkeys is stored as a 64-bit (eight octet) quantity, with the least significant bit of each octet used as a parity bit.

1.2. Initialization Vector

This mode of 3DES requires an Initialization Vector (IV) that is 8 octets in length.

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

The method for selection of the IV values is implementation dependent.

Note: A common technique is simply a counter, beginning with a randomly chosen value. Other implementations also exhibit unpredictability, usually through a pseudo-random number generator. Care should be taken that the periodicity of the

number generator is long enough to prevent repetition during the lifetime of the session key.

1.3. Data Size

The 3DES algorithm operates on blocks of 8 octets. This often requires padding after the end of the unencrypted payload data.

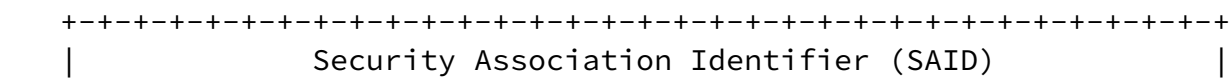
Both input and output result in the same number of octets, which facilitates in-place encryption and decryption.

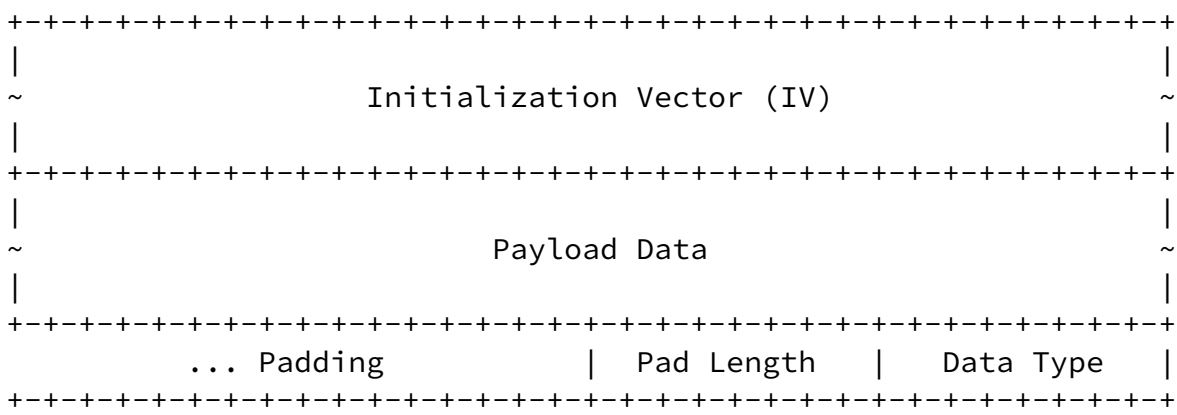
On receipt, if the length of the data to be decrypted is not an integral multiple of 8 octets, then an error is indicated. The datagram is discarded, and an appropriate ICMP message is returned. The failure SHOULD be recorded in the system or audit log, including the cleartext values for the SAID, date/time, Source, Destination, and other identifying information.

1.4. Performance

Three DES-CBC implementations may be pipelined in series to provide parallel computation. At the time of writing, at least one hardware implementation can encrypt or decrypt at about 1 Gbps [Schneier94, p. 231].

2. Payload Format





Security Association Identifier (SAID)

A 32-bit value identifying the Security Association for this datagram. If no Security Association has been established, the value of this field is zero.

Initialization Vector

The size of this field is variable, though for any given Security Association it has a particular known size. Its position and size is constant for all 3DES-CBC datagrams of the same SAID and IP Destination.

The field size MUST be a multiple of 32-bits. Octets are sent in network order.

The field may be longer or shorter than the 64-bits used by 3DES, to allow alignment of the Encrypted Data for convenient in-place decryption by the receiver. However, all conformant implementations MUST correctly process a 64-bit field size.

When the size is negotiated to 0-bits, no IV is used. This is primarily useful for highly random data, such as voice.

When the size is negotiated to 32-bits, a 64-bit value is formed from the 32-bit value followed by (concatentated with) the inverse of the 32-bit value.

When the size is negotiated to 96-bits or greater, the alignment

of the actual 64-bit value within this field is negotiated by an additional parameter. Unused octets are filled with unspecified implementation dependent values, which are ignored on receipt.

It is the intent that the value not repeat during the lifetime of the encryption session key. The session key SHOULD be changed more frequently for shorter IVs.

This field is considered to be transparent, though most users will not be able to make sense of its contents.

Payload Data

The size of this field is variable. This field is opaque.

Prior to encryption and after decryption, the contents of this field begins with an entire IP datagram (IP-Mode), or an IP Payload header (Transport-Mode).

Padding

The size of this field is variable. This field is opaque.

Prior to encryption, it is filled with unspecified implementation dependent values.

After decryption, it MUST be ignored.

Pad Length

This field indicates the size of the Padding field. It does not include the Pad Length and Data Type fields. The value typically ranges from 0 to 7, but may be up to 255 to permit hiding of the actual data length.

This field is opaque. That is, the value is set prior to encryption, and is examined only after decryption.

Data Type

This field indicates the contents of the Payload Data field, using

the IP Protocol/Payload value. Up-to-date values of the IP Protocol/Payload are specified in the most recent "Assigned Numbers" [RFC-1700].

This field is opaque. That is, the value is set prior to encryption, and is examined only after decryption.

For example, when encrypting an entire IP datagram (IP-Mode), this field will contain the value 4, which indicates IP-in-IP encapsulation.

3. Calculation

3.1. Algorithm

The 3DES-CBC algorithm is a simple variant on the DES-CBC algorithm. The DES function is replaced by three rounds of that function, an encryption followed by a decryption followed by an encryption, each with independant keys, k1, k2 and k3. Formally,

```
3DES-CBC:   C[n] = E[k3]( D[k2]( E[k1]( P[n] XOR C[n-1] )))
            P[n] = C[n-1] XOR D[k1]( E[k2]( D[k3]( C[n] )))
```

E[k](X) indicates the DES encryption function with key k performed

upon block X.

D[k](X) indicates the DES decryption function with key k upon block X.

P[n] indicates plaintext block n.

C[n] indicates cyphertext block n.

A XOR B indicates the bitwise exclusive-or of blocks A and B.

Note that when all three keys (k1, k2 and k3) are the same, 3DES-CBC is equivalent to DES-CBC. This property allows the 3DES hardware implementations to operate in DES mode without modification.

3.2. Encryption

Append zero or more octets of padding to the plain text, to make its modulo 8 length equal to 6.

Append a Pad Length octet containing the number of padding octets just added.

Append a Data Type octet containing the IP Protocol/Payload value which identifies the protocol header that begins the payload.

Provide an Initialization Vector (IV) of the form indicated.

Encrypt the payload with Triple DES in CBC mode, producing a cipher text of the same length.

Octets are mapped to DES blocks in network order. Octet 0 (modulo 8) of the payload corresponds to bits 1-8 of the 64-bit DES input block, while octet 7 (modulo 8) corresponds to bits 57-64 of the DES input block.

Contruct a new IP datagram for that Destination, with the indicated SAID, IV, and payload.

The Total Length in the IP Header reflects the length of the encrypted data, plus the SAID, IV, padding, pad length, and data type octets.

3.3. Decryption

First, the SAID field is examined. This is used as an index into the local Security Association table to find the encryption algorithm identifier and decryption key.

The negotiated form of the IV determines the size of the IV field. These octets are removed, and an appropriate 64-bit IV value is

constructed.

The encrypted part of the payload is decrypted using Triple DES in the CBC mode.

The Data Type is removed and examined. If it is unrecognized, the payload is discarded with an appropriate ICMP message.

The Pad Length is removed and examined. The specified number of pad octets are removed from the end of the decrypted payload, and the IP Total Length is adjusted accordingly.

The IP Header(s) and the remaining portion of the decrypted payload are passed to the protocol receive routine specified by the Data Type field.

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 key management mechanism and its implementation, the strength of the key [CN94], and upon the correctness of the implementations in all of the participating systems.

Among other considerations, applications may wish to take care not to select weak keys for any of the three DES rounds, although the odds of picking one at random are low [Schneier94, p. 233].

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, 2DES can be broken with a meet-in-the-middle attack, without significantly more complexity than breaking DES requires [ibid], so 3DES with independant keys is actually needed to provide this level of security. An attack on 3DES using two independent keys that is somewhat (sixteen times) faster than any known for independent keys has been shown [OW91].

Although it is widely believed that 3DES is substantially stronger than DES, as it is less amenable to brute force attack, it should be noted that real cryptanalysis of 3DES 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 cryptography, and especially cryptanalysis, and switch to other transforms should 3DES prove weak.

Acknowledgements

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

References

[AMS-esp] Randall Atkinson, Perry Metzger, William Simpson, "Encapsulating Security Protocol (ESP)", work in progress.

[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.

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

[MH81] Merle, 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-1610]
Postel, J., "Internet Official Protocol Standards", STD 1, RFC 1610, USC/Information Sciences Institute, July 1994.

[RFC-1700]
Reynolds, J., and Postel, J., "Assigned Numbers", STD 2, RFC 1700, USC/Information Sciences Institute, October 1994.

[Schneier94]

Schneier, B., "Applied Cryptography", John Wiley & Sons, New York, NY, 1994. ISBN 0-471-59756-2

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

Author's Address

Questions about this memo can also be directed to:

Randall Atkinson
Information Technology Division
Naval Research Laboratory
Washington,
DC 20375-5320
USA

Telephone: (DSN) 354-8590
Fax: (DSN) 354-7942
<atkinson@itd.nrl.navy.mil>

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

perry@piermont.com

Phil Karn
Qualcomm, Inc.
6455 Lusk Blvd.
San Diego, California 92121-2779

karn@unix.ka9q.ampr.org

William Allen Simpson

Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

Bill.Simpson@um.cc.umich.edu
    bsimpson@MorningStar.com

Table of Contents

1. Introduction 1
1.1 Keys 1
1.2 Initialization Vector 1
1.3 Data Size 2
1.4 Performance 2

2. Payload Format 2

3. Calculation 4
3.1 Algorithm 4
3.2 Encryption 5
3.3 Decryption 6

SECURITY CONSIDERATIONS 6

ACKNOWLEDGEMENTS 7

REFERENCES 7

AUTHOR'S ADDRESS 9