Security Working Group D. Frommer
Internet Draft RADGUARD
Expires in six months June 1996

The DES-CBC plus DES-MAC Security Transform
draft-frommer-sec-transform-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 working group mailing list (ipsec@tis.com) or the author.

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 use of DES-CBC for confidentiality plus DES Message Authentication Code (MAC) for integrity, in the IP Encapsulating Security Payload (ESP).

The use of the DES algorithm for both purposes may serve useful in environments where hardware acceleration is available.

1. Introduction

The Encapsulating Security Payload (ESP) [RFC-1827] provides confidentiality for IP datagrams by encrypting the payload data to be protected.

This specification describes the ESP for both confidentiality and integrity. Confidentiality is based on the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46, FIPS-46-1, FIPS-74, FIPS-81]. For integrity calculation the DES MAC (DES-CBC residue) algorithm is used. The MAC value is the last DES CBC block computed over the data using a different key.

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

1.1. Keys

There are two DES keys used by this transform, one used for confidentiality and the other for integrity. The keys are provided by the key management protocol.

DES keys are secret keys shared between the communicating parties and are eight octets (64-bits) in length. The keys consist of a 56-bit quantity stored as a 64-bit quantity, with the least significant bit of each octet used as a parity bit.

For security reasons, it is required that the two keys be different [Kaufman95, p 91].

1.2. Initialization Vectors

The CBC mode of DES requires an Initialization Vector (IV) that is eight octets (64-bits) in length. The IV for confidentiality purposes, denoted in this document as CIV is contained in each datagram. Including the CIV in each datagram ensures that decryption can be performed, even when other datagrams are dropped, or datagrams are re-ordered in transit. The IV for integrity is not included in datagrams and implicitly assumed to have a value of zero.

Implementation Notes:

A common technique for the IV is simply a counter, beginning with a randomly chosen value. This provides an easy method for preventing repetition, and is sufficiently robust for practical use.

Other implementations 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 DES algorithm operates on blocks of eight octets (64-bits). This often requires padding after the end of the unencrypted payload data.

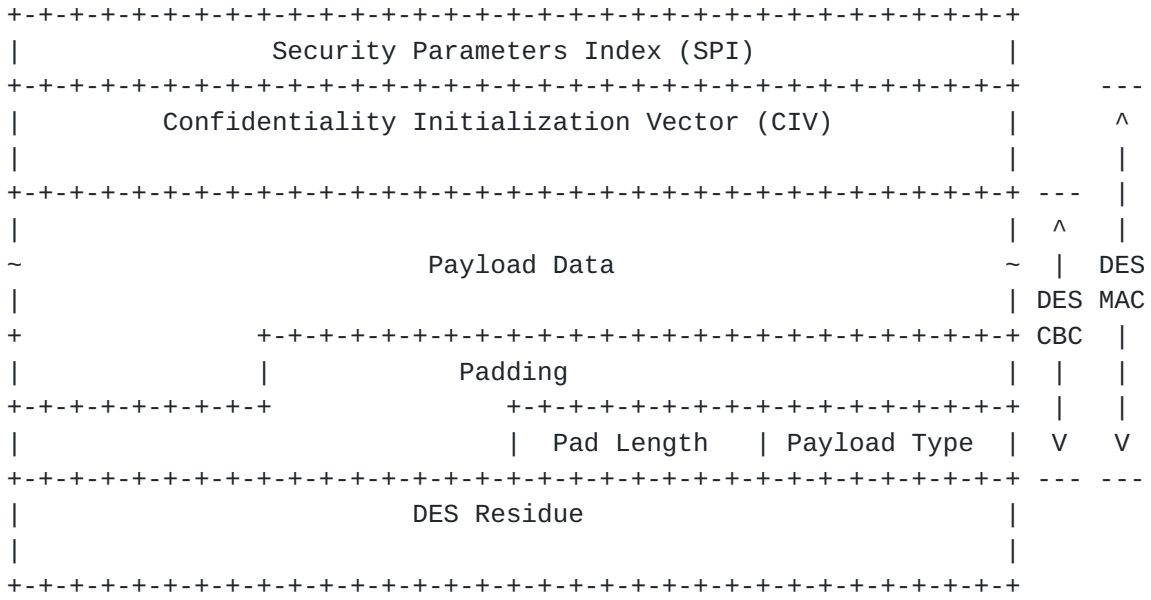
Both input and output result in the same number of octets. This facilitates in-place encryption and decryption.

On receipt, if the length of the data to be decrypted is not an integral multiple of eight octets, then an error is indicated, as described in [RFC-1825].

1.4. Performance

The DES algorithm is designed to perform well using hardware implementations. Commonly available DES hardware is considerably faster than software implementations on popular processors. The use of hardware allows a level of parallelism between the CPU and the DES hardware, especially important in security gateway implementations. In addition, the DES calculation of both integrity and confidentiality may be performed in parallel given the appropriate hardware.

2. Payload Format



Security Parameters Index (SPI)
4 octets. Identifies the Security Parameters for this datagram. The value MUST NOT be zero.

Confidentiality Initialization Vector (CIV)
8 octets. This is the initialization vector used by the DES CBC algorithm for confidentiality purposes.

Payload Data variable.

Prior to encryption and after decryption, this field begins with the IP Protocol/Payload header specified in the Payload Type field. Note that in the case of IP-in-IP encapsulation (Payload Type 4), this will be another IP header.

Padding variable.

Prior to encryption, it is filled with unspecified implementation dependent (preferably random) values, to align the Pad Length and Payload Type fields at an eight octet boundary.

After decryption, it MUST be ignored.

Pad Length — 1 octet. Indicates the size of the Padding field. It does not include the Pad Length and Payload 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.

Payload Type — 1 octet. 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 (Tunnel-Mode), this field will contain the value 4, indicating IP-in-IP encapsulation.

DES Residue — 8 octets. Filled with the result of the DES MAC calculation.

3. Algorithm

DES-CBC is used for both confidentiality and integrity calculations.

For confidentiality, the IV (CIV) is supplied in the packet. Each plaintext block is XOR'd with the previous ciphertext block, and the DES encryption function is applied to yield the ciphertext for the current block. This provides for resynchronization when datagrams are lost.

For integrity, the IV is implicitly assumed to be zero. DES-CBC using a different key than the one used for confidentiality is calculated over the ciphertext. The produced last block is used as the DES MAC.

For more explanation and implementation information for DES, see [Schneier95]. The use of DES for both integrity and confidentiality is discussed in [Kaufman95, p 91].

3.1. Transmission

Append zero or more octets of (preferably random) padding to the plaintext, to make its modulo 8 length equal to 6. For example, if the plaintext length is 41, 5 octets of padding are added.

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

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

Provide a Confidentiality Initialization Vector (CIV), as described earlier.

Encrypt the payload with DES in CBC mode, producing a ciphertext of the same length.

Octets are mapped to DES blocks in network order (most significant octet first) [RFC-1700]. 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.

Add the SPI and IV in front of the Payload Data.

Calculate the 64-bit DES Residue value over the CIV and ciphertext Payload Data, Padding, Pad Length, and Payload Type. Append it to the packet tail.

Construct an appropriate IP datagram for the target Destination. The Total/Payload Length in the encapsulating IP Header reflects the length of the encrypted data, plus the SPI, CIV, Padding, Pad Length, Payload Type, and DES Residue.

3.2. Reception

First, the SPI field is examined. This is used as an index into the local Security Parameter table to find the negotiated parameters and decryption/integrity keys.

The DES Residue is verified by calculating the DES CBC algorithm over the CIV and the encrypted part of the payload.

The SPI and CIV fields are removed.

The encrypted part of the payload is decrypted using DES in the CBC mode. The CIV is used as the initialization vector.

The Payload 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/Payload 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 Payload 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 DES algorithm, the correctness of the 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 nodes.

Among other considerations, applications may wish to take care not to select weak keys, although the odds of picking one at random are low [Schneier95, p 280].

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

Acknowledgements

Significant portions of this specification are derived from earlier work by Phil Karn, Perry Metzger and Bill Simpson.

References

[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.

[Kaufman95] Kaufman, C., Perlman, R. and Speciner, M., "Network Security: Private Communication in a Public World", PTR Prentice Hall, Englewood Cliffs, New Jersey, 1995. ISBN 0-13-061466-1

[RFC-1446] Galvin, J., and McCloghrie, K., "Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC-1446, DDN Network Information Center, April 1993.

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

[RFC-1800] Postel, J., "Internet Official Protocol Standards", STD 1, RFC-1800, USC/Information Sciences Institute, July 1995.

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

[RFC-1826]
Atkinson, R., "IP Authentication Header", RFC-1826, Naval Research Laboratory, July 1995.

[RFC-1827]
Atkinson, R., "IP Encapsulating Security Protocol (ESP)", RFC-1827, Naval Research Laboratory, July 1995.

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

Author's Address

Questions about this memo can be directed to:

Dan Frommer <dan@radguard.com>
RADGUARD, Ltd.
24 Raoul-Wallenberg St.
Tel Aviv 69719
Israel

Telephone: +972-3-645-5396