Network Working Group P Metzger
Internet Draft P Karn
W A Simpson
expires in six months March 1995

The ESP DES-CBC Transform
draft-ietf-ipsec-esp-des-cbc-03.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 DES-CBC security transform for the IP Encapsulating Security Payload (ESP). |

1. Introduction

The Encapsulating Security Payload (ESP) [A-ESP] provides confidentiality and integrity by encrypting the data to be protected.

This specification describes the ESP use of the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm [FIPS-46, FIPS-46-1, FIPS-74, FIPS-81].

All implementations that claim conformance or compliance with the Encapsulating Security Payload specification MUST implement this 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.

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

1.1. Keys

The secret DES key shared between the communicating parties is eight octets in length. This key consists of a 56-bit quantity used by the DES algorithm. The 56-bit key 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 DES requires an Initialization Vector (IV) that is eight 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 DES algorithm operates on blocks of eight octets. This often requires padding after the end of the unencrypted payload data.

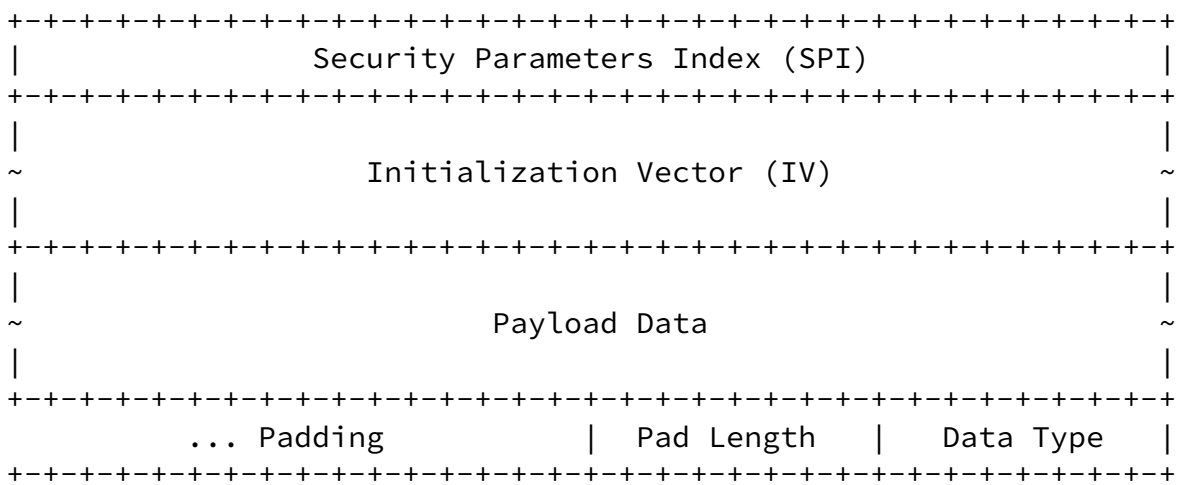
Both input and output result in the same number of octets, which facilitates in-place encryption and decryption.

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 Security Parameters Index (SPI), date/time, Source, Destination, and other identifying information.

1.4. Performance

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 Parameters Index (SPI)

A 32-bit value identifying the Security Parameters for this datagram. The value MUST NOT be zero.

Initialization Vector

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

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

When the size is 32-bits, a 64-bit value is formed from the 32-bit value followed by (concatentated with) the bit-wise complement of the 32-bit value. This field size is most common, as it aligns the Payload Data for both 32-bit and 64-bit processing.

All conformant implementations MUST also correctly process a 64-bit field size. This provides strict compatibility with existing hardware implementations.

> It is the intent that the value not repeat during the lifetime of the encryption session key. Even when a full 64-bit IV is used, the session key SHOULD be changed at least as frequently as 2**32 datagrams.

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 (Tunnel-Mode), or another IP Protocol/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 (preferably random) 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 (Tunnel-Mode), this field will contain the value 4, which indicates IP-in-IP encapsulation.

3. Algorithm

In DES-CBC, the base DES encryption function is applied to the XOR of each plaintext block with the previous ciphertext block to yield the ciphertext for the current block. In formalized notation,


```
DES-CBC:    C[n] = E[k](P[n] XOR C[n-1])
            P[n] = C[n-1] XOR D[k](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 ciphertext block n.

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

For more explanation and implementation information for DES, see [Schneier94].

3.1. Encryption

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 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 size indicated by the SPI.

Encrypt the payload with DES in CBC mode, producing a ciphertext 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 the target Destination, with the indicated SPI, IV, and payload.

The Total/Payload Length in the IP Header reflects the length of the

encrypted data, plus the SPI, IV, padding, pad length, and data type octets.

3.2. Decryption

First, the SPI field is removed and examined. This is used as an |

index into the local Security Parameter table to find the negotiated parameters 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 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/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 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 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 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 [Schneier94, p 233].

At the time of writing of this document, [BS93] demonstrated a differential cryptanalysis based chosen-plaintext attack requiring 2^47 plaintext-ciphertext pairs, and [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. The Unicity distance for DES is only a couple of blocks, and changing the session key frequently will not mitigate the brute force 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.

Acknowledgements

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

The use of DES for confidentiality is closely modeled on the work done for SNMPv2 [RFC-1446].

Steve Bellovin, Steve Deering, Charles Lynn, and Dave Mihelcic provided useful critiques of earlier versions of this draft.

References

[A-SA] Randall Atkinson, "Security Architecture for the Internet Protocol", work in progress.

[A-ESP] Randall Atkinson, "IP 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.

[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 dor DES Cipher," Advances in Cryptology -- Eurocrypt '93 Proceedings, Berlin: Springer-Verlag, 1994.

[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-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

[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.

Author's Address

Questions about this memo can also be directed to:

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