Security Working Group
INTERNET DRAFT

Ipsec Working Group
Rob Adams
Cisco Systems Inc.
23 June 1997

Expires in Six Months

The ESP Blowfish-CBC Algorithm Using an Explicit IV

<draft-ietf-ipsec-ciph-blowfish-cbc-00.txt>

Status of this Memo

Abstract

This draft describes the use of the Blowfish [Schneier] block cipher algorithm to be used with the IPSec Encapsulating Security Payload (ESP) [Kent97].

Table of Contents

1. Introduction

This draft describes the use of the Blowfish cipher algorithm in CBC mode to provide confidentiality in conjunction with the IPsec ESP protocol [Kent97].

This document assumes readers are familiar with the terms and concepts in [RFC-1825] and in [Kent97].

Blowfish is described in detail in [Schneier] and [Schneier93].

1.1 Specification of Requirements

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", and "MAY" that appear in this document are to be interpreted as described in [RFC-2119].

2. Cipher Algorithm

This document gives implementers specific instructions for using the Blowfish block cipher algorithm in CBC mode with a block size of 64 bits as described in [Schneier93] to secure ESP.

2.1 Rounds

Compliant implementations MUST use only 16 round Blowfish. Fewer rounds are open to several different sorts of attacks outlined in [Schneier95].

2.2 Background

Bruce Schneier of Counterpane Systems developed the Blowfish block cipher algorithm. The algorithm is described in detail in [Schneier93].

2.3 Performance

Blowfish is designed to encrypt data very efficiently on 32 bit processors. Although setting up the keys for Blowfish is complex and time consuming, actual encryption is efficient. Sixteen round Blowfish uses only 18 clock cycles per byte encrypted on a Pentium versus 45 clock cycles for 16 round DES with a 56 bit key, and 108 for 48 round Triple-DES.

For a comparison table of the speed of Blowfish and other cipher algorithms, see [Schneier97].

3. Key Size

Blowfish accepts keying material of varying lengths up to 448 bits inclusive. Implementations MUST prohibit the use of a zero length key for this transform. Implementations SHOULD prohibit the use of a key of length less than 40 bits. Implementations SHOULD support keys longer than 128 bits up to 448 bits. Implementations MUST only allow key sizes in 8 bit increments for interoperability purposes. For example, implementations should allow 40, 48, 56, 64, ? 440, and 448 bit keys. The number of bits of keying material required for Blowfish is a host specific policy issue.

3.1 Weak Keys

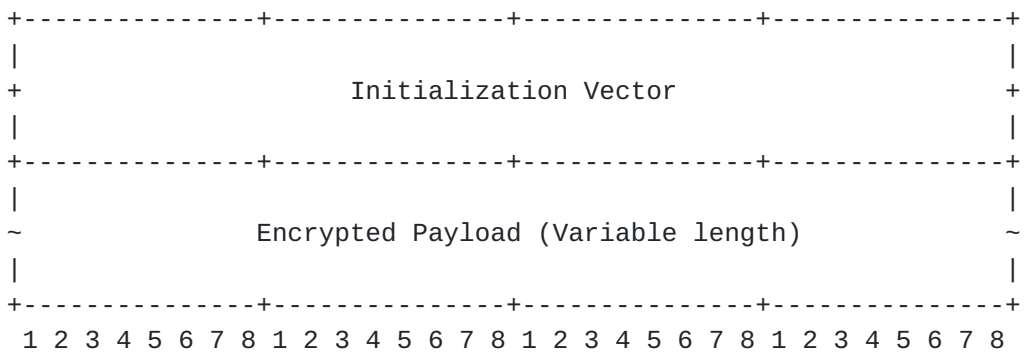
Weak keys for Blowfish have been discovered. Weak keys are keys that produce the identical entries in a given S-box. Unfortunately, there is no way to test for weak keys before the S-box values are generated. However, the chances of randomly generating such a key are small.

4. ESP Payload

Blowfish in CBC mode requires an initialization vector of eight octet for use with ESP [Kent97]. The IV MUST precede the data to be encrypted in the packet and must be eight octets (64 bits) in length. The IV SHOULD be chosen at random. Common practice is to use random data for the first IV and the last eight octets of

encrypted data from an encryption process as the IV for the next encryption process.

The payload field, as defined in [Kent97], is broken down according to the following diagram:



4.1 Block Size and Padding

The Blowfish-CBC cipher algorithm MUST use a block size of eight octets (64 bits).

Padding is used to align the payload type and pad length octets as specified in [Kent97]. Padding must be sufficient to align the data to be encrypted to an eight octet (64 bit) boundary.

4.2 Interaction with Authentication

This Blowfish-CBC ESP document does not limit which authentication algorithm ESP uses.

5. Keying Material

The key exchange protocol MUST provide this ESP algorithm with a number of key material bits greater than or equal to the required key size.

If the key exchange protocol does not negotiate key size, the key must be 128 bits in length.

This ESP algorithm will take the Blowfish-CBC key from the first <x> bits of keying material, where <x> represents the required key size in bits.

6. Security Considerations

Blowfish is thought to be a secure encryption algorithm. Currently there are no known attacks on 16 round Blowfish [Schneier].

7. References

[Kent97] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", ftp://ietf.org/internet-drafts/draft-ietf-ipsec-new-esp-00.txt, March 1997

[RFC-1825] Atkinson, R. "Security Architecture for the Internet Protocol", ftp://ds.internic.net/rfc/rfc1825.txt, August 1995.

[RFC-2085] Oehler, M., Glenn, R., "HMAC-MD5 IP Authentication with Replay Prevention," ftp://ds.internic.net/rfc/rfc2085.txt, February 1997.

[RFC-2119] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", ftp://ds.internic.net/rfc/rfc2119.txt, March 1997

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

[Schneier93] Schneier, B., "Description of a New Variable-Length Key, 64-Bit Block Cipher", from "Fast Software Encryption, Cambridge Security Workshop Proceedings", Springer-Verlag, 1994, pp. 191-204. http://www.counterpane.com/bfsverlag.html

[Schneier95] Schneier, B., "THE BLOWFISH ENCRYPTION ALGORITHM--ONE YEAR LATER", Dr. Dobb's Journal, September 1995, http://www.counterpane.com/bfdobsoyl.html

[Scheier97] Scheier, B. "Speed Comparisons of Block Ciphers on a Pentium." February 1997, http://www.counterpane.com/speed.html

8. Acknowledgements

This document is based on work done in the IPsec working group and suggestions from Roy Pereira and Stephen Kent.

The IPSec working group can be contacted through its chairs:

Robert Moskowitz
Rgm3@chrysler.com
Chrysler Corporation

Theodore Y. Ts'o
Tytso@MIT.EDU
Massachusetts Institute of Technology

or via the IPSec working group's mailing list (ipsec@tis.com).

9. Editor's Address

Rob Adams
adams@cisco.com
cisco Systems Inc.
101 Cooper St.
Santa Cruz, CA 95060
United States of America

+1 408 457 5397