Internet Engineering Task Force
IP Security Working Group
Internet Draft
Expires in six months

Roy Pereira
TimeStep Corporation
R. W. Baldwin
RSA Data Security, Inc.

July 2, 1997

The ESP RC5-CBC Algorithm

<draft-ietf-ipsec-ciph-rc5-cbc-00.txt>

Status of this Memo

This document is a submission to the IETF Internet Protocol Security (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@tis.com) or to the editor.

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 draft documents are valid for a maximum of six months and may be updated, replaced, or obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "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), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Abstract

This document describes the RC5 block cipher algorithm as to be used with the IPSec Encapsulating Security Payload (ESP).

Table of Contents

1. Introduction..2
   1.1 Specification of Requirements...............................2
2. Cipher Algorithm..2
   2.1 Rounds..3
   2.2 Background on RC5...3
   2.3 Performance...3
3. Key Sizes...3
   3.1 Weak Keys...3
4. ESP Payload...3
   4.1 Block Size and Padding......................................4
   4.2 Interaction with Authentication Algorithms..................4
5. Keying Material...4
6. Security Considerations...4
7. References..5
8. Acknowledgments...5
9. Editors' Addresses..5

1. Introduction

This document describes how the RC5 cipher algorithm may be used with the IPSec ESP protocol.

It is assumed that the reader is familiar with the terms and concepts described in the document "Security Architecture for the Internet Protocol" [Atkinson95] and "IP Encapsulating Security Payload (ESP)" [Kent97].

Furthermore, this document is a companion to [Kent97] and MUST be read in its context.

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 [Bradner97].

2. Cipher Algorithm

The symmetric block cipher algorithm used to secure ESP is RC5 in CBC mode with 16 rounds and a block size of 64 bits as described in [Baldwin96].

2.1 Rounds

RSA Labs recommends that RC5 be used with 16 rounds. Twelve rounds is enough to make RC5 stronger than DES against differential and linear cryptanalysis and sixteen rounds is sufficient to make RC5 secure against both forms of cryptanalysis even at a theoretical level.

Compliant implementations MUST support 16 rounds.

2.2 Background on RC5

The RC5 encryption algorithm was developed by Ron Rivest for RSA Data Security Inc. in order to address the need for a high-performance software and hardware ciphering alternative to DES.

2.3 Performance

Benchmark numbers from RSA Data Security suggest that RC5-CBC runs about twice as fast as Eric Young's DES-CBC implementation from SSLeay on the popular 32-bit CPUs.

3. Key Sizes

RC5's key size MUST be multiple of 8 bits and MUST be from 40 to 2040 bits inclusive. To facilitate interoperability, it is recommended that key sizes SHOULD be chosen from the set of 40, 128 and 160 bits.

If the key size is not negotiated through the key exchange protocol, then a value of 128 bits MUST be used. All compliant implementations MUST support a key size of 128 bits.

3.1 Weak Keys

RC5 has no known weak keys when used with 16 rounds.

4. ESP Payload

RC5-CBC requires an explicit Initialization Vector (IV) of 8 octets (64 bits) that immediately precedes the cipher-text in the payload. The IV SHOULD be chosen at random. Common practice is to use random data for the first IV and the last 8 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:

```
   +---------------+---------------+---------------+---------------+
   |                                                               |
   +                   Initialization Vector (IV)                  +
   |                                                               |
   +---------------+---------------+---------------+---------------+
   |                                                               |
   ~              Encrypted Payload (variable length)              ~
   |                                                               |
   +---------------------------------------------------------------+
    1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8
```

4.1 Block Size and Padding

RC5 has a variably length block size, but for the ESP algorithm described in this document, the block size MUST be 8 octets (64 bits).

When padding is required, it MUST be done according to the conventions specified in [Kent97].

4.2 Interaction with Authentication Algorithms

This ESP RC5 document has no limitations on what authentication algorithm is used in ESP.

5. Keying Material

The minimum number of bits sent from the Key Exchange Protocol to this ESP algorithm must be greater or equal to the key size.

The RC5 key is taken from the first <x> bits of the keying material. Where <x> represents the required key size.

6. Security Considerations

The ESP RC5 algorithm described in this document has the same security considerations as in [Baldwin96].

Care should be taken when using small key sizes. Small key sizes make brute force type attacks practical regardless of the cipher algorithm used. It is therefore recommended that the ESP RC5 key size be at least 80 bits. Use of key sizes less than 80 bits is permitted, but careful considerations should be taken before its use.

7. References

[Atkinson95] Atkinson, R., "Security Architecture for the Internet Protocol", draft-ietf-ipsec-arch-sec-01

[Baldwin96] Baldwin, R.W., Rivest, R., "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", RFC2040, October 1996

[Bradner97] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", RFC2119, March 1997

[Kent97] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", draft-ietf-ipsec-new-esp-01

8. Acknowledgments

This document is based on previous work by B. Howard of TimeStep Corporation, suggestions from Stephen Kent, discussions from the IPSec mailing list as well as the other IPSec drafts.

9. Editors' Addresses

Roy Pereira
<rpereira@timestep.com>
TimeStep Corporation
(613) 599-3610 x 4808

Robert W. Baldwin
<baldwin@rsa.com> or <baldwin@lcs.mit.edu>
RSA Data Security, Inc.
(415)
      595-8782

The IPSec working group can be contacted via the IPSec working group's mailing list (ipsec@tis.com) or through its chairs:

Robert Moskowitz
rgm@chrysler.com
Chrysler Corporation

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