The ESP CAST128-CBC Algorithm

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 CAST-128 block cipher algorithm as to be used with the IPSec Encapsulating Security Payload (ESP).
1. Introduction

This document describes how the CAST-128 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 "Security Architecture for the Internet Protocol" [Atkinson95] and "IP Encapsulating Security Payload (ESP)" [Kent97] documents.

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 CAST-128 in CBC mode with a block size of 64 bits as described in [Adams97].

2.1 Rounds

For key sizes up to and including 80 bits (i.e., 40, 48, 56, 64, 72, and 80 bits), the algorithm is exactly as specified but MUST use 12 rounds.
For key sizes greater than 80 bits, the algorithm MUST use the full 16 rounds.

2.2 Background on CAST-128

The CAST design procedure was originally developed by Carlisle Adams and Stafford Travares at Queen’s University, Kingston, Ontario, Canada. Subsequent enhancements have been made over the years by Carlisle Adams and Michael Wiener of Entrust Technologies. CAST-128 is the result of applying the CAST Design Procedure as outlined in [Adams97].

2.3 Performance

CAST-128 runs approximately 3 times faster than a highly optimized DES implementation and runs 5-6 times faster than the DES implementations found in typical applications. This is based on a non optimized C++ implementation of CAST-128. It can therefore be tuned to give even higher performance, if this is required.

The following performance tests were run on a Pentium 90 MHz running the Windows NT operating system using 20 Kbyte buffers and do not include file I/O. The DES-CBC implementation was not optimized for a 32 bit environment.

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAST-128 64 bit key CBC encryption</td>
<td>2,640,000 bytes/sec</td>
</tr>
<tr>
<td>DES CBC encryption</td>
<td>504,000 bytes/sec</td>
</tr>
</tbody>
</table>

3. Key Sizes

The CAST-128 encryption algorithm [Adams97] has been designed to allow a key size which can vary from 40 bits to 128 bits, in 8-bit increments (that is, the allowable key sizes are 40, 48, 56, 64, ..., 112, 120, and 128 bits. To facilitate interoperability, it is recommended that key sizes SHOULD be chosen from the set of 40, 64, 80 and 128.

For key sizes less than 128 bits, the key is padded with zeros in the rightmost, or least significant, positions out to 128 bits since the CAST-128 key schedule assumes an input key of 128 bits. Thus if you had a key with a size of 80 bits ‘3B5D831CFE’, it would be padded to produce a key with a size of 128 bits ‘3B5D831CFE000000’.

In order to avoid confusion, when variable key size operation is used, the name CAST-128 is to be considered synonymous with the name CAST5; this allows a keysize to be appended without ambiguity.
Thus, for example, CAST-128 with a 40 bit key is referred to as CAST5-40; where a 128 bit key is explicitly intended, the name CAST5-128 should be used.

3.1 Weak Keys

CAST-128 no known weak keys.

4. ESP Payload

CAST128-CBC requires an explicit Initialization Vector (IV) of 8 octets (64 bits). Thus the payload is made up of the 8 octet IV followed by raw cipher-text. 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)                  |
+---------------+---------------+---------------+---------------+
```

```
<table>
<thead>
<tr>
<th>Encrypted Payload (variable length)</th>
</tr>
</thead>
</table>
```

```
+---------------------------------------------------------------+
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

The ESP CAST-128 algorithm described in this document MUST use a block size of 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 CAST-128 ESP 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 CAST-128 key is taken from the first \(<x>\) bits of the keying material, where \(<x>\) represents the required key size.

6. Security Considerations

The ESP CAST-128 algorithm described in this document has the same security considerations as in [Adams97].

Care should be taken when using small key sizes. Smaller key sizes of 56 bits and below make brute force type attacks practical regardless of the cipher algorithm used. It is therefore recommended that the ESP CAST-128 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


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


8. Acknowledgments

This document is based on suggestions from Stephen Kent and discussions from the IPSec mailing list as well as other IPSec drafts.

Special thanks for Carlisle Adams and Paul Van Oorschot both of Entrust Technologies who provided input and review with respect to CAST-128.
9. Editors’ Addresses

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

Greg Carter
<carterg@entrust.com>
Entrust Technologies
(613) 763-1358

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