Network Working Group
Request for Comments: 5529
Category: Standards Track
A. Kato
NTT Software Corporation
M. Kanda
NTT
S. Kanno
NTT Software Corporation
April 2009

Modes of Operation for Camellia for Use with IPsec

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document describes the use of the Camellia block cipher algorithm in Cipher Block Chaining (CBC) mode, Counter (CTR) mode, and Counter with CBC-MAC (CCM) mode as additional, optional-to-implement Internet Key Exchange Protocol version 2 (IKEv2) and Encapsulating Security Payload (ESP) mechanisms to provide confidentiality, data origin authentication, and connectionless integrity.

Table of Contents

1. Introduction

This document describes the use of the Camellia block cipher algorithm [1] in Cipher Block Chaining (CBC) mode, Counter (CTR) mode, and Counter with CBC-MAC (CCM) mode as additional, optional-to-implement IKEv2 [2] and Encapsulating Security Payload (ESP) [3] mechanisms to provide confidentiality, data origin authentication, and connectionless integrity.

Since optimized source code is provided under several open source licenses [9], Camellia is also adopted by several open source projects (OpenSSL, FreeBSD, Linux, and Firefox Gran Paradiso).

The algorithm specification and object identifiers are described in [1].

The Camellia web site [10] contains a wealth of information about Camellia, including detailed specification, security analysis, performance figures, reference implementation, optimized implementation, test vectors, and intellectual property information.

The remainder of this document specifies the use of various modes of operation for Camellia within the context of IPsec ESP. For further information on how the various pieces of IPsec in general and ESP in particular fit together to provide security services, please refer to [11] and [3].

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [4].

2. The Camellia Cipher Algorithm

All symmetric block cipher algorithms share common characteristics and variables, including mode, key size, weak keys, block size, and rounds. The relevant characteristics of Camellia are described in [1].

2.1. Block Size and Padding

Camellia uses a block size of 16 octets (128 bits).

Padding requirements are described:

(a) Camellia Padding requirement is specified in [3],
(b) Camellia-CBC Padding requirement is specified in [3],
(c) Camellia-CCM Padding requirement is specified in [5], and
(d) ESP Padding requirement is specified in [3].

2.2. Performance

Performance figures for Camellia are available at [10]. The NESSIE project has reported on the performance of optimized implementations independently [12].

3. Modes

This document describes three modes of operation for the use of Camellia with IPsec: CBC (Cipher Block Chaining), CTR (Counter), and CCM (Counter with CBC-MAC).

3.1. Cipher Block Chaining

Camellia CBC mode is defined in [6].

3.2. Counter and Counter with CBC-MAC

Camellia in CTR and CCM modes is used in IPsec as AES in [7] and [8]. In this specification, CCM is used with the Camellia [13] block cipher.

4. IKEv2 Conventions

This section describes the transform ID and conventions used to generate keying material for use with ENCR_CAMELLIA_CBC, ENCR_CAMELLIA_CTR, and ENCR_CAMELLIA_CCM using the Internet Key Exchange (IKEv2) [2].

4.1. Keying Material

The size of KEYMAT MUST be equal or longer than the associated Camellia key. The keying material is used as follows:

Camellia-CBC with a 128-bit key
: The KEYMAT requested for each Camellia-CBC key is 16 octets. All 16 octets are the 128-bit Camellia key.

Camellia-CBC with a 192-bit key
: The KEYMAT requested for each Camellia-CBC key is 24 octets. All 24 octets are the 192-bit Camellia key.

Camellia-CBC with a 256-bit key
: The KEYMAT requested for each Camellia-CBC key is 32 octets. All 32 octets are the 256-bit Camellia key.

Camellia-CTR with a 128-bit key
: The KEYMAT requested for each Camellia-CTR key is 20 octets. The first 16 octets are the 128-bit Camellia key, and the remaining four octets are used as the nonce value in the counter block.

Camellia-CTR with a 192-bit key
: The KEYMAT requested for each Camellia-CTR key is 28 octets. The first 24 octets are the 192-bit Camellia key, and the remaining four octets are used as the nonce value in the counter block.

Camellia-CTR with a 256-bit key
: The KEYMAT requested for each Camellia-CTR key is 36 octets. The first 32 octets are the 256-bit Camellia key, and the remaining four octets are used as the nonce value in the counter block.

Camellia-CCM with a 128-bit key
: The KEYMAT requested for each Camellia-CCM key is 19 octets. The first 16 octets are the 128-bit Camellia key, and the remaining three octets are used as the salt value in the counter block.

Camellia-CCM with a 192-bit key
: The KEYMAT requested for each Camellia-CCM key is 27 octets. The first 24 octets are the 192-bit Camellia key, and the remaining three octets are used as the salt value in the counter block.

Camellia-CCM with a 256-bit key
The KEYMAT requested for each Camellia-CCM key is 35 octets. The first 32 octets are the 256-bit Camellia key, and the remaining three octets are used as the salt value in the counter block.

4.2. Transform Type 1

For IKEv2 negotiations, IANA has assigned five ESP Transform Identifiers for Camellia-CBC, Camellia-CTR, and Camellia-CCM, as recorded in Section 6.

4.3. Key Length Attribute

Since Camellia supports three key lengths, the Key Length attribute MUST be specified in the IKE exchange [2]. The Key Length attribute MUST have a value of 128, 192, or 256 bits.

5. Security Considerations

For security considerations of CTR and CCM mode, this document refers to Section 9 of [7] and Section 7 of [8].

No security problem has been found for Camellia [14], [12].

6. IANA Considerations

IANA has assigned IKEv2 parameters for use with Camellia-CTR and with Camellia-CCM for Transform Type 1 (Encryption Algorithm):

23 for ENCR_CAMELLIA_CBC;
24 for ENCR_CAMELLIA_CTR;
25 for ENCR_CAMELLIA_CCM with an 8-octet ICV;
26 for ENCR_CAMELLIA_CCM with a 12-octet ICV; and
27 for ENCR_CAMELLIA_CCM with a 16-octet ICV.

7. Acknowledgments

We thank Tim Polk and Tero Kivinen for their initial review of this document. Thanks to Derek Atkins and Rui Hodai for their comments and suggestions. Special thanks to Alfred Hoenes for several very detailed reviews and suggestions.

8. References

8.1. Normative References

[1] Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm", RFC 3713, April 2004.

[2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[3] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality", NIST Special Publication 800-38C, July 2007, <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf>.

[6] Kato, A., Moriai, S., and M. Kanda, "The Camellia Cipher Algorithm and Its Use With IPsec", RFC 4312, December 2005.

[7] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[8] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

8.2. Informative References

[9] "Camellia open source software", <http://info.isl.ntt.co.jp/crypt/eng/camellia/source.html>.

[10] "Camellia web site", <http://info.isl.ntt.co.jp/camellia/>.

[11] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[12] "The NESSIE project (New European Schemes for Signatures, Integrity and Encryption)", <http://www.cosic.esat.kuleuven.be/nessie/>.

[13] Kato, A., Kanda, M., and S. Kanno, "Camellia Counter Mode and Camellia Counter with CBC-MAC Mode Algorithms", RFC 5528, April 2009.

[14] Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees", <http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html>.

Authors' Addresses

Akihiro Kato
NTT Software Corporation

Phone: +81-45-212-7577
Fax: +81-45-212-9800
EMail: akato@po.ntts.co.jp

Masayuki Kanda
NTT

Phone: +81-422-59-3456
Fax: +81-422-59-4015
EMail: kanda.masayuki@lab.ntt.co.jp

Satoru Kanno
NTT Software Corporation

Phone: +81-45-212-7577
Fax: +81-45-212-9800
EMail: kanno-s@po.ntts.co.jp