Network Working Group
Request for Comments: 4312
Category: Standards Track

A. Kato
NTT Software Corporation
S. Moriai
Sony Computer Entertainment Inc.
M. Kanda
Nippon Telegraph and Telephone Corporation

December 2005

The Camellia Cipher Algorithm and Its Use With IPsec

Status of This Memo

Copyright Notice

Abstract

This document describes the use of the Camellia block cipher algorithm in Cipher Block Chaining Mode, with an explicit Initialization Vector, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).

1. Introduction

This document describes the use of the Camellia block cipher algorithm in Cipher Block Chaining Mode, with an explicit Initialization Vector, as a confidentiality mechanism within the context of the IPsec Encapsulating Security Payload (ESP).

Camellia was selected as a recommended cryptographic primitive by the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [NESSIE] and was included in the list of cryptographic techniques for Japanese e-Government systems that was selected by the Japan CRYPTREC (Cryptography Research, Evaluation Committees) [CRYPTREC]. Camellia has been submitted to several other standardization bodies, such as ISO (ISO/IEC 18033) and the IETF S/MIME Mail Security Working Group [Camellia-CMS].

Camellia supports 128-bit block size and 128-, 192-, and 256-bit key lengths, i.e., the same interface specifications as the Advanced Encryption Standard (AES) [AES].

Camellia is a symmetric cipher with a Feistel structure. Camillia was developed jointly by NTT and Mitsubishi Electric Corporation in 2000. It was designed to withstand all known cryptanalytic attacks, and it has been scrutinized by worldwide cryptographic experts. Camellia is suitable for implementation in software and hardware, offering encryption speed in software and hardware implementations that is comparable to AES.

The Camellia homepage [Camellia-Web] contains a wealth of information about camellia, including detailed specification, security analysis, performance figures, reference implementation, test vectors, and intellectual property information.

The remainder of this document specifies the use of Camellia within the context of IPsec ESP. For further information on how the various pieces of ESP fit together to provide security services, please refer to [ARCH], [ESP], and [ROAD].

1.1. Specification of Requirements

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

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 following sections contain descriptions of the relevant characteristics of Camellia.

The algorithm specification and object identifiers are described in [Camellia-Desc].

2.1. Mode

NIST has defined five modes of operation for AES and other FIPS-approved ciphers [SP800-38a]: CBC (Cipher Block Chaining), ECB (Electronic CodeBook), CFB (Cipher FeedBack), OFB (Output FeedBack), and CTR (Counter). The CBC mode is well defined and well understood for symmetric ciphers, and it is currently required for all other ESP ciphers. This document specifies the use of the Camellia cipher in CBC mode within ESP. This mode requires an Initialization Vector

(IV) size that is the same as the block size. Use of a randomly generated IV prevents generation of identical cipher text from packets that have identical data spanning the first block of the cipher algorithm's block size.

The CBC IV is XOR'd with the first plaintext block before it is encrypted. Then, for successive blocks, the previous cipher text block is XOR'd with the current plain text before it is encrypted. More information on CBC mode can be obtained in [SP800-38a, CRYPTO-S].

2.2. Key Size

Camellia supports three key sizes: 128 bits, 192 bits, and 256 bits. The default key size is 128 bits, and all implementations MUST support this key size. Implementations MAY also support key sizes of 192 bits and 256 bits.

Camellia uses a different number of rounds for each of the defined key sizes. When a 128-bit key is used, implementations MUST use 18 rounds. When a 192-bit key is used, implementations MUST use 24 rounds. When a 256-bit key is used, implementations MUST use 24 rounds.

2.3. Weak Keys

At the time of writing this document, there are no known weak keys for Camellia.

2.4. Block Size and Padding

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

Padding is required by the algorithms to maintain a 16-octet (128-bit) block size. Padding MUST be added, as specified in [ESP], such that the data to be encrypted (which includes the ESP Pad Length and Next Header fields) is a multiple of 16 octets.

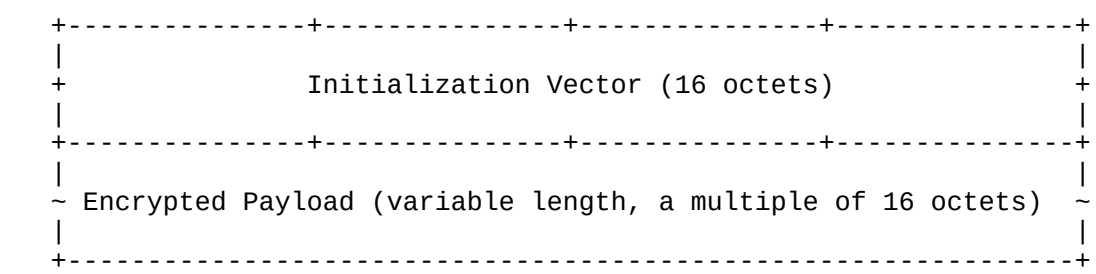
Because of the algorithm-specific padding requirement, no additional padding is required to ensure that the ciphertext terminates on a 4-octet boundary. That is, maintaining a 16-octet block size guarantees that the ESP Pad Length and Next Header fields will be right-aligned within a 4-octet word). Additional padding MAY be included, as specified in [ESP], as long as the 16-octet block size is maintained.

2.5. Performance

Performance figures of Camellia are available at [Camellia-Web]. This web site also includes performance comparison with the AES cipher and other AES finalists. The NESSIE project [NESSIE] has reported performance of Optimized Implementations independently.

3. ESP Payload

The ESP payload is made up of the IV followed by raw cipher-text. Thus, the payload field, as defined in [ESP], is broken down according to the following diagram:



The IV field MUST be the same size as the block size of the cipher algorithm being used. The IV MUST be chosen at random, and MUST be unpredictable.

Including the IV in each datagram ensures that each received datagram can be decrypted, even when some datagrams are dropped or re-ordered in transit.

To avoid CBC encryption of very similar plaintext blocks in different packets, implementations MUST NOT use a counter or other low Hamming-distance source for IVs.

3.1. ESP Algorithmic Interactions

Currently, there are no known issues regarding interactions between the Camellia and other aspects of ESP, such as the use of certain authentication schemes.

3.2. Keying Material

The minimum number of bits sent from the key exchange protocol to the ESP algorithm must be greater than or equal to the key size. The cipher’s encryption and decryption key is taken from the first 128, 192, or 256 bits of the keying material.

4. Interaction with Internet Key Exchange [IKE]

Camellia was designed to follow the same API as the AES cipher. Therefore, this section defines only Phase 1 Identifier and Phase 2 Identifier. Any other consideration related to interaction with IKE is the same as that of the AES cipher. Details can be found in [AES-IPSEC].

4.1. Phase 1 Identifier

For Phase 1 negotiations, IANA has assigned an Encryption Algorithm ID of 8 for CAMELLIA-CBC.

4.2. Phase 2 Identifier

For Phase 2 negotiations, IANA has assigned an ESP Transform Identifier of 22 for ESP_CAMELLIA.

5. Security Considerations

Implementations are encouraged to use the largest key sizes they can, taking into account performance considerations for their particular hardware and software configuration. Note that encryption necessarily affects both sides of a secure channel, so such consideration must take into account not only the client side, but also the server. However, a key size of 128 bits is considered secure for the foreseeable future.

No security problem has been found on Camellia [CRYPTREC][NESSIE].

6. IANA Considerations

IANA has assigned Encryption Algorithm ID = 8 to CAMELLIA-CBC.

IANA has assigned ESP Transform Identifier = 22 to ESP_CAMELLIA.

7. Acknowledgements

Portions of this text were unabashedly borrowed from [AES-IPSEC]. This work was done when the first author worked for NTT.

8. References

8.1. Normative References

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

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

8.2. Informative References

[AES] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001. http://csrc.nist.gov/publications/fips/fips197/ fips-197.{ps,pdf}.

[AES-IPSEC] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use With IPsec," RFC 3602, September 2003.

[ARCH] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[Camellia-CMS] Moriai, S. and A. Kato, "Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)", RFC 3657, January 2004.

[Camellia-Web] Camellia web site: http://info.isl.ntt.co.jp/camellia/.

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

[CRYPTREC] Information-technology Promotion Agency (IPA), Japan, CRYPTREC. http://www.ipa.go.jp/security/enc/CRYPTREC/ index-e.html.

[IKE] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[SP800-38a] Dworkin, M., "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", NIST Special Publication 800-38A, December 2001.

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

[ROAD] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

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

Authors' Addresses

Akihiro Kato
NTT Software Corporation

Phone: +81-45-212-7934
Fax: +81-45-212-7410
EMail: akato@po.ntts.co.jp

Shiho Moriai
Sony Computer Entertainment Inc.

Phone: +81-3-6438-7523
Fax: +81-3-6438-8629
EMail: camellia@isl.ntt.co.jp (Camellia team)
shiho@rd.scei.sony.co.jp (Shiho Moriai)

Masayuki Kanda
Nippon Telegraph and Telephone Corporation

Phone: +81-46-859-2437
Fax: +81-46-859-3365
EMail: kanda@isl.ntt.co.jp

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.