Network Working Group
Request for Comments: 4132
Category: Standards Track

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

July 2005

Addition of Camellia Cipher Suites to Transport Layer Security (TLS)

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

Abstract

This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) protocol to support the Camellia encryption algorithm as a bulk cipher algorithm.

1. Introduction

This document proposes the addition of new cipher suites to the TLS protocol [TLS] to support the Camellia encryption algorithm as a bulk cipher algorithm. This proposal provides a new option for fast and efficient bulk cipher algorithms.

Note: This work was done when the first author worked for NTT.

1.1. Camellia

Camellia was selected as a recommended cryptographic primitive by the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [NESSIE] and included in the list of cryptographic techniques for Japanese e-Government systems, which were selected by the Japan CRYPTREC (Cryptography Research and Evaluation Committees) [CRYPTREC]. Camellia is also included in specification of the TV-Anytime Forum [TV-ANYTIME]. The TV-Anytime Forum is an association of organizations that seeks to develop

specifications to enable audio-visual and other services based on mass-market high-volume digital storage in consumer platforms. Camellia is specified as Cipher Suite in TLS used by Phase 1 S-7 (Bi-directional Metadata Delivery Protection) specification and S-5 (TV-Anytime Rights Management and Protection Information for Broadcast Applications) specification. Camellia has been submitted to other several standardization bodies such as ISO (ISO/IEC 18033) and IETF S/MIME Mail Security Working Group [Camellia-CMS].

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

Camellia was jointly developed by NTT and Mitsubishi Electric Corporation in 2000 [CamelliaTech]. It was carefully designed to withstand all known cryptanalytic attacks and even to have a sufficiently large security leeway. It has been scrutinized by worldwide cryptographic experts.

Camellia was also designed to be suitable for both software and hardware implementations and to cover all possible encryption applications, from low-cost smart cards to high-speed network systems. Compared to the AES, Camellia offers at least comparable encryption speed in software and hardware. In addition, a distinguishing feature is its small hardware design. Camellia perfectly meets one of the current TLS market requirements, for which low power consumption is mandatory.

The algorithm specification and object identifiers are described in [Camellia-Desc]. The Camellia homepage, http://info.isl.ntt.co.jp/camellia/, contains a wealth of information about camellia, including detailed specification, security analysis, performance figures, reference implementation, and test vectors.

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in [RFC2119].

2. Proposed Cipher Suites

The new cipher suites proposed here have the following definitions:

```
CipherSuite TLS_RSA_WITH_CAMELLIA_128_CBC_SHA      = { 0x00,0x41 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA   = { 0x00,0x42 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA   = { 0x00,0x43 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x44 };
```

```
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x45 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x46 };

CipherSuite TLS_RSA_WITH_CAMELLIA_256_CBC_SHA      = { 0x00,0x84 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA   = { 0x00,0x85 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA   = { 0x00,0x86 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x87 };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x88 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x89 };
```

3. Cipher Suite Definitions

3.1. Cipher

All the cipher suites described here use Camellia in cipher block chaining (CBC) mode as a bulk cipher algorithm. Camellia is a 128-bit block cipher with 128-, 192-, and 256-bit key sizes; i.e., it supports the same block and key sizes as the Advanced Encryption Standard (AES). However, this document only defines cipher suites for 128- and 256-bit keys as well as AES cipher suites for TLS [AES-TLS]. These cipher suites are efficient and practical enough for most uses, including high-security applications.

Cipher	Type	Key Material	Expanded Key Material	Effective Key Bits	IV Size	Block Size
CAMELLIA_128_CBC	Block	16	16	128	16	16
CAMELLIA_256_CBC	Block	32	32	256	16	16

3.2. Hash

All the cipher suites described here use SHA-1 [SHA-1] in a Hashed Message Authentication Code (HMAC) construction, as described in section 5 of [TLS].

3.3. Key Exchange

The cipher suites defined here differ in the type of certificate and key exchange method. They use the following options:

Cipher Suite	Key Exchange Algorithm
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	DH_anon

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	DH_anon

For the meanings of the terms RSA, DH_DSS, DH_RSA, DHE_DSS, DHE_RSA, and DH_anon, please refer to sections 7.4.2 and 7.4.3 of [TLS].

4. Security Considerations

It is not believed that the new cipher suites are ever less secure than the corresponding older ones. Camellia is considered secure, and it has withstood extensive cryptanalytic efforts in several open, worldwide cryptographic evaluation projects [CRYPTREC][NESSIE].

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

For other security considerations, please refer to the security considerations of the corresponding older cipher suites described in [TLS] and [AES-TLS].

5. References

5.1. Normative References

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

[TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

5.2. Informative References

[CamelliaTech] Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T., "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis -", In Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, August 2000, Proceedings, Lecture Notes in Computer Science 2012, pp.39-56, Springer-Verlag, 2001.

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

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

[AES-TLS] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[SHA-1] FIPS PUB 180-1, "Secure Hash Standard", National Institute of Standards and Technology, U.S. Department of Commerce, April 17, 1995.

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

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

[TV-ANYTIME] TV-Anytime Forum, http://www.tv-anytime.org/.

Authors' Addresses

Shiho Moriai
Sony Computer Entertainment Inc.

Phone: +81-3-6438-7523
Fax: +81-3-6438-8629
EMail: shiho@rd.scei.sony.co.jp

Akihiro Kato
NTT Software Corporation

Phone: +81-45-212-7094
Fax: +81-45-212-7506
EMail: akato@po.ntts.co.jp

Masayuki Kanda
Nippon Telegraph and Telephone Corporation

Phone: +81-46-859-2437
Fax: +81-46-859-3365
EMail: kanda.masayuki@lab.ntt.co.jp
camellia@lab.ntt.co.jp (Camellia team)

Full Copyright Statement

Intellectual Property

Acknowledgement

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