Internet Engineering Task Force (IETF)
Request for Comments: 5932
Obsoletes: 4132
Category: Standards Track
ISSN: 2070-1721

A. Kato
NTT Software Corporation
M. Kanda
NTT
S. Kanno
NTT Software Corporation

June 2010

Camellia Cipher Suites for TLS

Abstract

This document specifies a set of cipher suites for the Transport Security Layer (TLS) protocol to support the Camellia encryption algorithm as a block cipher. It amends the cipher suites originally specified in RFC 4132 by introducing counterparts using the newer cryptographic hash algorithms from the SHA-2 family. This document obsoletes RFC 4132.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5932.

1. Introduction

This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) [RFC5246] protocol to support the Camellia [RFC3713] encryption algorithm as a block cipher algorithm, adding variants using the SHA-2 family of cryptographic hash algorithms [FIPS180-3] to the TLS cipher suite portfolio originally specified in RFC 4132 [RFC4132]. This document obsoletes RFC 4132.

The Camellia algorithm and its properties are described in [RFC3713].

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 [RFC2119].

2. Proposed Cipher Suites

The cipher suites defined here have the following identifiers:

```
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 };
```

```
  CipherSuite TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256      = { 0x00,0xBA };
  CipherSuite TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256   = { 0x00,0xBB };
  CipherSuite TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256   = { 0x00,0xBC };
  CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256  = { 0x00,0xBD };
  CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256  = { 0x00,0xBE };
  CipherSuite TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256  = { 0x00,0xBF };

  CipherSuite TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256      = { 0x00,0xC0 };
  CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256   = { 0x00,0xC1 };
  CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256   = { 0x00,0xC2 };
  CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256  = { 0x00,0xC3 };
  CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256  = { 0x00,0xC4 };
  CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256  = { 0x00,0xC5 };
```

3. Cipher Suite Definitions

3.1. Key Exchange

The RSA, DHE_RSA, DH_RSA, DHE_DSS, DH_DSS, and DH_anon key exchanges are performed as defined in [RFC5246].

3.2. Cipher

The CAMELLIA_128_CBC cipher suites use Camellia [RFC3713] in Cipher Block Chaining (CBC) mode with a 128-bit key and 128-bit IV; the CAMELLIA_256_CBC cipher suites use a 256-bit key and 128-bit IV.

3.3. Hash and Pseudorandom Function

3.3.1. Hash and Pseudorandom Function for TLS 1.1

The cipher suites ending with _SHA use HMAC-SHA1 as the MAC algorithm.

When used with TLS versions prior to 1.2, the pseudorandom function (PRF) is calculated as specified in the appropriate version of the TLS specification.

3.3.2. Hash and Pseudorandom Function for TLS 1.2

The cipher suites ending with _SHA256 use HMAC-SHA-256 as the MAC algorithm. The PRF is the TLS PRF [RFC5246] with SHA-256 as the hash function. These cipher suites MUST NOT be negotiated by TLS 1.1 or earlier versions. Clients MUST NOT offer these cipher suites if they do not offer TLS 1.2 or later. Servers that select an earlier version of TLS MUST NOT select one of these cipher suites.

4. IANA Considerations

IANA has updated the entries for the following numbers that were allocated in RFC 4132 to reference this document:

```
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 };
```

IANA has allocated the following numbers in the TLS Cipher Suite Registry:

```
CipherSuite TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256      = { 0x00,0xBA };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256   = { 0x00,0xBB };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256   = { 0x00,0xBC };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256  = { 0x00,0xBD };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256  = { 0x00,0xBE };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256  = { 0x00,0xBF };

CipherSuite TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256      = { 0x00,0xC0 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256   = { 0x00,0xC1 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256   = { 0x00,0xC2 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256  = { 0x00,0xC3 };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256  = { 0x00,0xC4 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256  = { 0x00,0xC5 };
```

5. Security Considerations

At the time of writing this document, there are no known weak keys for Camellia, and no security problem has been found on Camellia (see [NESSIE], [CRYPTREC], and [LNCS]).

Also, security issues are discussed throughout RFC 5246 [RFC5246], especially in Appendices D, E, and F.

6. References

6.1. Normative References

[FIPS180-3] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180, October 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

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

[RFC3713] Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm", RFC 3713, April 2004.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

6.2. Informative References

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

[LNCS] Mala, H., Shakiba, M., and M. Dakhil-alian, "New Results on Impossible Differential Cryptanalysis of Reduced Round Camellia-128", LNCS 5867, November 2009, <http://www.springerlink.com/content/e55783u422436g77/>.

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

[RFC4132] Moriai, S., Kato, A., and M. Kanda, "Addition of Camellia Cipher Suites to Transport Layer Security (TLS)", RFC 4132, July 2005.

Authors' Addresses

Akihiro Kato
NTT Software Corporation

Phone: +81-45-212-9803
Fax: +81-45-212-9800
EMail: kato.akihiro@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: +81-45-212-9803
Fax: +81-45-212-9800
EMail: kanno.satoru@po.ntts.co.jp