INTERNET-DRAFT
TLS Working Group
Expires April 2001

S. Moriai
Nippon Telegraph and Telephone Corporation

October 2000

Addition of the Camellia Encryption Algorithm to TLS

<draft-ietf-tls-camellia-00.txt>

Status of this Memo

Abstract

This document proposes the addition of new cipher suites to the TLS protocol 1.0 to support the Camellia encryption algorithm as a bulk cipher algorithm.

1. Introduction

The demands placed on cryptographic primitives are changing: the required level of security is increasing to match the progress made in computational power and cryptanalytic techniques, and more efficiency on a wide variety of platforms is required as they are being implemented in a wide variety of applications. However, the TLS Protocol Version 1.0 [4] currently does not support cipher suites including 128-bit block ciphers that offer a high level of security and performance.

Camellia is a block cipher with 128-bit block size and 128-, 192-, and 256-bit key sizes, i.e. the same interface specifications as the Advanced Encryption Standard (AES). The algorithm description is in [1] or [3]. Efficiency on both software and hardware platforms is a remarkable characteristic of Camellia in addition to its high level of security. It is confirmed that Camellia provides strong security against differential and linear cryptanalysis. An optimized implementation of Camellia in assembly language can encrypt on a Pentium III (800MHz) at the rate of more than 276 Mbits per second, which is much faster than the speed of an optimized DES implementation. In addition, a distinguishing feature is its small hardware design. The hardware design, which includes the parts for key scheduling, encryption and decryption, occupies approximately 11K gates, which is the smallest among all existing 128-bit block ciphers as far as we know [2].

This document proposes the addition of new cipher suites to the TLS protocol 1.0 [4] to support Camellia as a bulk cipher algorithm. The proposed change is minimal, just the addition of a new option for bulk cipher algorithms.

2. The CipherSuites

We propose the following new cipher suites.

```
CipherSuite TLS_RSA_WITH_CAMELLIA_CBC_128_SHA      = { 0x00,0x2F };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_CBC_128_SHA   = { 0x00,0x30 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_CBC_128_SHA   = { 0x00,0x31 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_CBC_128_SHA  = { 0x00,0x32 };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_CBC_128_SHA  = { 0x00,0x33 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_CBC_128_SHA  = { 0x00,0x34 };

CipherSuite TLS_RSA_WITH_CAMELLIA_CBC_192_SHA      = { 0x00,0x35 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_CBC_192_SHA   = { 0x00,0x36 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_CBC_192_SHA   = { 0x00,0x37 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_CBC_192_SHA  = { 0x00,0x38 };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_CBC_192_SHA  = { 0x00,0x39 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_CBC_192_SHA  = { 0x00,0x3A };

CipherSuite TLS_RSA_WITH_CAMELLIA_CBC_256_SHA      = { 0x00,0x3B };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_CBC_256_SHA   = { 0x00,0x3C };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_CBC_256_SHA   = { 0x00,0x3D };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_CBC_256_SHA  = { 0x00,0x3E };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_CBC_256_SHA  = { 0x00,0x3F };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_CBC_256_SHA  = { 0x00,0x40 };
```

Note: The above numeric definitions for CipherSuites have not yet been registered. The numeric definitions follow the numbers given

in the CipherSuite of TLS standard [4].

3. CipherSuite Definitions

CipherSuite	Is Exportable	Key Exchange	Cipher	Hash
TLS_RSA_WITH_CAMELLIA_CBC_128_SHA		RSA	CAMELLIA_CBC_128	SHA
TLS_DH_DSS_WITH_CAMELLIA_CBC_128_SHA		DH_DSS	CAMELLIA_CBC_128	SHA
TLS_DH_RSA_WITH_CAMELLIA_CBC_128_SHA		DH_RSA	CAMELLIA_CBC_128	SHA
TLS_DHE_DSS_WITH_CAMELLIA_CBC_128_SHA		DHE_DSS	CAMELLIA_CBC_128	SHA
TLS_DHE_RSA_WITH_CAMELLIA_CBC_128_SHA		DHE_RSA	CAMELLIA_CBC_128	SHA
TLS_DH_anon_WITH_CAMELLIA_CBC_128_SHA		DH_anon	CAMELLIA_CBC_128	SHA
TLS_RSA_WITH_CAMELLIA_CBC_192_SHA		RSA	CAMELLIA_CBC_192	SHA
TLS_DH_DSS_WITH_CAMELLIA_CBC_192_SHA		DH_DSS	CAMELLIA_CBC_192	SHA
TLS_DH_RSA_WITH_CAMELLIA_CBC_192_SHA		DH_RSA	CAMELLIA_CBC_192	SHA
TLS_DHE_DSS_WITH_CAMELLIA_CBC_192_SHA		DHE_DSS	CAMELLIA_CBC_192	SHA
TLS_DHE_RSA_WITH_CAMELLIA_CBC_192_SHA		DHE_RSA	CAMELLIA_CBC_192	SHA
TLS_DH_anon_WITH_CAMELLIA_CBC_192_SHA		DH_anon	CAMELLIA_CBC_192	SHA
TLS_RSA_WITH_CAMELLIA_CBC_256_SHA		RSA	CAMELLIA_CBC_256	SHA
TLS_DH_DSS_WITH_CAMELLIA_CBC_256_SHA		DH_DSS	CAMELLIA_CBC_256	SHA
TLS_DH_RSA_WITH_CAMELLIA_CBC_256_SHA		DH_RSA	CAMELLIA_CBC_256	SHA
TLS_DHE_DSS_WITH_CAMELLIA_CBC_256_SHA		DHE_DSS	CAMELLIA_CBC_256	SHA
TLS_DHE_RSA_WITH_CAMELLIA_CBC_256_SHA		DHE_RSA	CAMELLIA_CBC_256	SHA
TLS_DH_anon_WITH_CAMELLIA_CBC_256_SHA		DH_anon	CAMELLIA_CBC_256	SHA

Cipher	Type	Key Material	Expanded Key Material	Effective Key Bits	IV Size	Block Size
CAMELLIA_CBC_128	Block	16	16	128	16	16
CAMELLIA_CBC_192	Block	24	24	192	16	16
CAMELLIA_CBC_256	Block	32	32	256	16	16

Note: Key Exchange Algorithms and Hash Functions are defined in TLS.

4. Security Considerations

The security of Camellia was evaluated by utilizing state-of-the-art cryptanalytic techniques. We confirmed that Camellia has no differential and linear characteristics that hold with probability more than 2^(-128), which means that it is extremely unlikely that differential and linear attacks will succeed against Camellia. Moreover, Camellia was designed to offer security against other advanced cryptanalytic attacks including higher order differential attacks, interpolation attacks, related-key attacks, truncated differential attacks, and so on [3].

5. Intellectual Property Statement

Mitsubishi Electric Corporation (Mitsubishi Electric) and Nippon Telegraph and Telephone Corporation (NTT) have filed patent applications on the techniques used in the block cipher Camellia. For more information, please contact MISTY@isl.melco.co.jp and/or

camellia@isl.ntt.co.jp.

References

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita ``Specification of Camellia --- a 128-bit Block Cipher'', 2000. http://info.isl.ntt.co.jp/camellia/

[2] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita ``Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms'', 2000. http://info.isl.ntt.co.jp/camellia/

[3] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita ``Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms --- Design and Analysis ---'', in Workshop Record of SAC 2000, Seventh Annual Workshop on Selected Areas in Cryptography, pp.41--54, 14-15 August 2000. (to appear in Lecture Notes in Computer Science of Spring-Verlag)

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

Author's Addresses

Shiho Moriai
Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka, 239-0847, Japan
Phone: +81-468-59-2007
FAX: +81-468-59-3858
Email: shiho@isl.ntt.co.jp