Internet Engineering Task Force (IETF)
Request for Comments: 6209
Category: Informational
ISSN: 2070-1721

W. Kim
J. Lee
J. Park
D. Kwon
NSRI

April 2011

Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)

Abstract

This document specifies a set of cipher suites for the Transport Layer Security (TLS) protocol to support the ARIA encryption algorithm as a block cipher.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see 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/rfc6209.

Copyright Notice

Copyright (c) 2011 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 (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document specifies cipher suites for the Transport Layer Security (TLS) [RFC5246] protocol to support the ARIA [RFC5794] encryption algorithm as a block cipher algorithm. The cipher suites include variants using the SHA-2 family of cryptographic hash functions and ARIA Galois counter mode. Elliptic curve cipher suites and pre-shared key (PSK) cipher suites are also defined.

The cipher suites with SHA-1 are not included in this document. Due to recent analytic work on SHA-1 [Wang05], the IETF is gradually moving away from SHA-1 and towards stronger hash algorithms.

1.1. ARIA

ARIA is a general-purpose block cipher algorithm developed by Korean cryptographers in 2003. It is an iterated block cipher with 128-, 192-, and 256-bit keys and encrypts 128-bit blocks in 12, 14, and 16 rounds, depending on the key size. It is secure and suitable for most software and hardware implementations on 32-bit and 8-bit processors. It was established as a Korean standard block cipher algorithm in 2004 [ARIAKS] and has been widely used in Korea, especially for government-to-public services. It was included in PKCS #11 in 2007 [ARIAPKCS]. The algorithm specification and object identifiers are described in [RFC5794].

1.2. 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

2.1. HMAC-Based Cipher Suites

The first twenty cipher suites use ARIA [RFC5794] in Cipher Block Chaining (CBC) mode with a SHA-2 family Hashed Message Authentication Code (HMAC). Eight out of twenty use elliptic curves.

```
CipherSuite TLS_RSA_WITH_ARIA_128_CBC_SHA256         = { 0xC0,0x3C };
CipherSuite TLS_RSA_WITH_ARIA_256_CBC_SHA384         = { 0xC0,0x3D };
CipherSuite TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256      = { 0xC0,0x3E };
CipherSuite TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384      = { 0xC0,0x3F };
CipherSuite TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256      = { 0xC0,0x40 };
CipherSuite TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384      = { 0xC0,0x41 };
CipherSuite TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x42 };
CipherSuite TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x43 };
CipherSuite TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x44 };
CipherSuite TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x45 };
CipherSuite TLS_DH_anon_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x46 };
CipherSuite TLS_DH_anon_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x47 };

CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 = { 0xC0,0x48 };
CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 = { 0xC0,0x49 };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256  = { 0xC0,0x4A };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384  = { 0xC0,0x4B };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256   = { 0xC0,0x4C };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384   = { 0xC0,0x4D };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256    = { 0xC0,0x4E };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384    = { 0xC0,0x4F };
```

2.2. GCM-Based Cipher Suites

The next twenty cipher suites use the same asymmetric algorithms as those in the previous section but use the authenticated encryption modes defined in TLS 1.2 with the ARIA in Galois Counter Mode (GCM) [GCM].

```
   CipherSuite TLS_RSA_WITH_ARIA_128_GCM_SHA256         = { 0xC0,0x50 };
   CipherSuite TLS_RSA_WITH_ARIA_256_GCM_SHA384         = { 0xC0,0x51 };
   CipherSuite TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x52 };
   CipherSuite TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x53 };
   CipherSuite TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256      = { 0xC0,0x54 };
   CipherSuite TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384      = { 0xC0,0x55 };
   CipherSuite TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x56 };
   CipherSuite TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x57 };
   CipherSuite TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256      = { 0xC0,0x58 };
   CipherSuite TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384      = { 0xC0,0x59 };
   CipherSuite TLS_DH_anon_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x5A };
   CipherSuite TLS_DH_anon_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x5B };

   CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 = { 0xC0,0x5C };
   CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 = { 0xC0,0x5D };
   CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256  = { 0xC0,0x5E };
   CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384  = { 0xC0,0x5F };
   CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256   = { 0xC0,0x60 };
   CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384   = { 0xC0,0x61 };
   CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256    = { 0xC0,0x62 };
   CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384    = { 0xC0,0x63 };
```

2.3. PSK Cipher Suites

The next fourteen cipher suites describe PSK cipher suites. Eight cipher suites use an HMAC and six cipher suites use the ARIA Galois Counter Mode.

```
   CipherSuite TLS_PSK_WITH_ARIA_128_CBC_SHA256         = { 0xC0,0x64 };
   CipherSuite TLS_PSK_WITH_ARIA_256_CBC_SHA384         = { 0xC0,0x65 };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x66 };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x67 };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x68 };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x69 };
   CipherSuite TLS_PSK_WITH_ARIA_128_GCM_SHA256         = { 0xC0,0x6A };
   CipherSuite TLS_PSK_WITH_ARIA_256_GCM_SHA384         = { 0xC0,0x6B };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x6C };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x6D };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x6E };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x6F };
   CipherSuite TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256   = { 0xC0,0x70 };
   CipherSuite TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384   = { 0xC0,0x71 };
```

3. Cipher Suite Definitions

3.1. Key Exchange

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

3.2. Cipher

The ARIA_128_CBC cipher suites use ARIA [RFC5794] in CBC mode with a 128-bit key and 128-bit Initialization Vector (IV); the ARIA_256_CBC cipher suites use a 256-bit key and 128-bit IV.

AES-authenticated encryption with additional data algorithms, AEAD_AES_128_GCM, and AEAD_AES_256_GCM are described in [RFC5116]. AES GCM cipher suites for TLS are described in [RFC5288]. AES and ARIA share common characteristics, including key sizes and block length. ARIA_128_GCM and ARIA_256_GCM are defined according to those characteristics of AES.

3.3. PRFs

The pseudorandom functions (PRFs) SHALL be as follows:

a. For cipher suites ending with _SHA256, the PRF is the TLS PRF [RFC5246] using SHA-256 as the hash function.

b. For cipher suites ending with _SHA384, the PRF is the TLS PRF [RFC5246] using SHA-384 as the hash function.

3.4. PSK Cipher Suites

Pre-shared key cipher suites for TLS are described in [RFC4279], [RFC4785], [RFC5487], and [RFC5489].

4. Security Considerations

At the time of writing this document, no security problems have been found on ARIA (see [YWL]).

The security considerations in the following RFCs apply to this document as well: [RFC4279] [RFC4785] [RFC5116] [RFC5288] [RFC5289] [RFC5487] and [GCM].

5. IANA Considerations

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

```
CipherSuite TLS_RSA_WITH_ARIA_128_CBC_SHA256         = { 0xC0,0x3C };
CipherSuite TLS_RSA_WITH_ARIA_256_CBC_SHA384         = { 0xC0,0x3D };
CipherSuite TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256      = { 0xC0,0x3E };
CipherSuite TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384      = { 0xC0,0x3F };
CipherSuite TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256      = { 0xC0,0x40 };
CipherSuite TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384      = { 0xC0,0x41 };
CipherSuite TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x42 };
CipherSuite TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x43 };
CipherSuite TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x44 };
CipherSuite TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x45 };
CipherSuite TLS_DH_anon_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x46 };
CipherSuite TLS_DH_anon_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x47 };

CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 = { 0xC0,0x48 };
CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 = { 0xC0,0x49 };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256  = { 0xC0,0x4A };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384  = { 0xC0,0x4B };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256   = { 0xC0,0x4C };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384   = { 0xC0,0x4D };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256    = { 0xC0,0x4E };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384    = { 0xC0,0x4F };

CipherSuite TLS_RSA_WITH_ARIA_128_GCM_SHA256         = { 0xC0,0x50 };
CipherSuite TLS_RSA_WITH_ARIA_256_GCM_SHA384         = { 0xC0,0x51 };
CipherSuite TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x52 };
CipherSuite TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x53 };
CipherSuite TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256      = { 0xC0,0x54 };
CipherSuite TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384      = { 0xC0,0x55 };
CipherSuite TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x56 };
CipherSuite TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x57 };
CipherSuite TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256      = { 0xC0,0x58 };
CipherSuite TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384      = { 0xC0,0x59 };
CipherSuite TLS_DH_anon_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x5A };
CipherSuite TLS_DH_anon_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x5B };

CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 = { 0xC0,0x5C };
CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 = { 0xC0,0x5D };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256  = { 0xC0,0x5E };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384  = { 0xC0,0x5F };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256   = { 0xC0,0x60 };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384   = { 0xC0,0x61 };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256    = { 0xC0,0x62 };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384    = { 0xC0,0x63 };
```

```
   CipherSuite TLS_PSK_WITH_ARIA_128_CBC_SHA256         = { 0xC0,0x64 };
   CipherSuite TLS_PSK_WITH_ARIA_256_CBC_SHA384         = { 0xC0,0x65 };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x66 };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x67 };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256     = { 0xC0,0x68 };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384     = { 0xC0,0x69 };
   CipherSuite TLS_PSK_WITH_ARIA_128_GCM_SHA256         = { 0xC0,0x6A };
   CipherSuite TLS_PSK_WITH_ARIA_256_GCM_SHA384         = { 0xC0,0x6B };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x6C };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x6D };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256     = { 0xC0,0x6E };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384     = { 0xC0,0x6F };
   CipherSuite TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256   = { 0xC0,0x70 };
   CipherSuite TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384   = { 0xC0,0x71 };
```

6. References

6.1. Normative References

[GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST SP 800-38D, November 2007.

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

[RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, January 2007.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

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

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, August 2008.

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, August 2008.

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009.

[RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5489, March 2009.

[RFC5794] Lee, J., Lee, J., Kim, J., Kwon, D., and C. Kim, "A Description of the ARIA Encryption Algorithm", RFC 5794, March 2010.

6.2. Informative References

[ARIAKS] Korean Agency for Technology and Standards, "128 bit block encryption algorithm ARIA - Part 1: General (in Korean)", KS X 1213-1:2009, December 2009.

[ARIAPKCS] RSA Laboratories, "Additional PKCS #11 Mechanisms", PKCS #11 v2.20 Amendment 3 Revision 1, January 2007.

[Wang05] Wang, X., Yin, Y., and H. Yu, "Finding Collisions in the Full SHA-1", CRYPTO 2005, LNCS vol.3621, pp.17-36, August 2005.

[YWL] Li, Y., Wu, W., and L. Zhang, "Integral attacks on reduced-round ARIA block cipher", ISPEC 2010, LNCS Vol.6047, pp. 19-29, May 2010.

Authors' Addresses

Woo-Hwan Kim
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: whkim5@ensec.re.kr

Jungkeun Lee
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: jklee@ensec.re.kr

Je-Hong Park
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: jhpark@ensec.re.kr

Daesung Kwon
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: ds_kwon@ensec.re.kr