Network Working Group
Internet Draft
Intended status: Informational
Expires: May 30, 2011

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

December 1, 2010

Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)
draft-nsri-tls-aria-01.txt

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on May 30, 2011.

Copyright Notice

Abstract

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

1. Introduction

This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) [RFC5246] protocol to support the ARIA [RFC5794] encryption algorithm as a block cipher algorithm. The proposed cipher suites include variants using 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 included.

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 an HMAC-based MAC. Eight out of twenty use elliptic curves.

```
CipherSuite TLS_RSA_WITH_ARIA_128_CBC_SHA256         = { TBD,TBD };
CipherSuite TLS_RSA_WITH_ARIA_256_CBC_SHA384         = { TBD,TBD };
CipherSuite TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256      = { TBD,TBD };
CipherSuite TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384      = { TBD,TBD };
CipherSuite TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256      = { TBD,TBD };
CipherSuite TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384      = { TBD,TBD };
CipherSuite TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
CipherSuite TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
CipherSuite TLS_DH_anon_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DH_anon_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };

CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 = { TBD,TBD };
CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 = { TBD,TBD };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256  = { TBD,TBD };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384  = { TBD,TBD };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256   = { TBD,TBD };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384   = { TBD,TBD };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256    = { TBD,TBD };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384    = { TBD,TBD };
```

2.2. Galois Counter Mode-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         = { TBD,TBD };
CipherSuite TLS_RSA_WITH_ARIA_256_GCM_SHA384         = { TBD,TBD };
CipherSuite TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
CipherSuite TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256      = { TBD,TBD };
CipherSuite TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384      = { TBD,TBD };
CipherSuite TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
CipherSuite TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256      = { TBD,TBD };
CipherSuite TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384      = { TBD,TBD };
CipherSuite TLS_DH_anon_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
CipherSuite TLS_DH_anon_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };

CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 = { TBD,TBD };
CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 = { TBD,TBD };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256  = { TBD,TBD };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384  = { TBD,TBD };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256   = { TBD,TBD };
```

```
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384   = { TBD,TBD };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256    = { TBD,TBD };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384    = { TBD,TBD };
```

2.3. Pre-shared key (PSK) Cipher Suites

The next twelve cipher suites describe pre-shared key cipher suites. The first six cipher suites use HMAC-based MAC and the next six cipher suites use the ARIA Galois Counter Mode.

```
CipherSuite TLS_PSK_WITH_ARIA_128_CBC_SHA256         = { TBD,TBD };
CipherSuite TLS_PSK_WITH_ARIA_256_CBC_SHA384         = { TBD,TBD };
CipherSuite TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
CipherSuite TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
CipherSuite TLS_PSK_WITH_ARIA_128_GCM_SHA256         = { TBD,TBD };
CipherSuite TLS_PSK_WITH_ARIA_256_GCM_SHA384         = { TBD,TBD };
CipherSuite TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
CipherSuite TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
CipherSuite TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
```

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 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]. And 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 as those of AES.

3.3. PRFs

The 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. Pre-shared key (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 problem has been found on ARIA (see [YWL]).

The security considerations in previous RFCs [RFC3711, RFC4279, RFC4785, RFC5116, RFC5288, RFC5289, RFC5487] and [GCM] apply to this document as well.

5. IANA Considerations

IANA is requested to allocate the following numbers in the TLS Cipher Suite Registry:

```
CipherSuite TLS_RSA_WITH_ARIA_128_CBC_SHA256         = { TBD,TBD };
CipherSuite TLS_RSA_WITH_ARIA_256_CBC_SHA384         = { TBD,TBD };
CipherSuite TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256      = { TBD,TBD };
CipherSuite TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384      = { TBD,TBD };
CipherSuite TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256      = { TBD,TBD };
CipherSuite TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384      = { TBD,TBD };
CipherSuite TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
CipherSuite TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
CipherSuite TLS_DH_anon_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
CipherSuite TLS_DH_anon_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };

CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 = { TBD,TBD };
CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 = { TBD,TBD };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256  = { TBD,TBD };
CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384  = { TBD,TBD };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256   = { TBD,TBD };
CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384   = { TBD,TBD };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256    = { TBD,TBD };
CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384    = { TBD,TBD };
```

```
   CipherSuite TLS_RSA_WITH_ARIA_128_GCM_SHA256         = { TBD,TBD };
   CipherSuite TLS_RSA_WITH_ARIA_256_GCM_SHA384         = { TBD,TBD };
   CipherSuite TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
   CipherSuite TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
   CipherSuite TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256      = { TBD,TBD };
   CipherSuite TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384      = { TBD,TBD };
   CipherSuite TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
   CipherSuite TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
   CipherSuite TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256      = { TBD,TBD };
   CipherSuite TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384      = { TBD,TBD };
   CipherSuite TLS_DH_anon_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
   CipherSuite TLS_DH_anon_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };

   CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 = { TBD,TBD };
   CipherSuite TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 = { TBD,TBD };
   CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256  = { TBD,TBD };
   CipherSuite TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384  = { TBD,TBD };
   CipherSuite TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256   = { TBD,TBD };
   CipherSuite TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384   = { TBD,TBD };
   CipherSuite TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256    = { TBD,TBD };
   CipherSuite TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384    = { TBD,TBD };

   CipherSuite TLS_PSK_WITH_ARIA_128_CBC_SHA256         = { TBD,TBD };
   CipherSuite TLS_PSK_WITH_ARIA_256_CBC_SHA384         = { TBD,TBD };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256     = { TBD,TBD };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384     = { TBD,TBD };
   CipherSuite TLS_PSK_WITH_ARIA_128_GCM_SHA256         = { TBD,TBD };
   CipherSuite TLS_PSK_WITH_ARIA_256_GCM_SHA384         = { TBD,TBD };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
   CipherSuite TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256     = { TBD,TBD };
   CipherSuite TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384     = { TBD,TBD };
```

6. References

6.1. Normative References

[GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", National Institute of Standards and Technology 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-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), 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] Barda, M. and Hajjeh, I., ECDHE_PSK Cipher Suites for Transport Layer Security (TLS), RFC 5489, March 2009.

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

6.2. Informative References

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

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

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

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

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