AVTCore
Internet-Draft
Intended status: Standards Track
Expires: November 16, 2012

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

May 15, 2012

The ARIA Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP)
draft-ietf-avtcore-aria-srtp-00

Abstract

This document describes the use of the ARIA block cipher algorithm within the Secure Real-time Transport Protocol (SRTP) for providing confidentiality for the Real-time Transport Protocol (RTP) traffic and for the control traffic for RTP, the Real-time Transport Control Protocol (RTCP). It details three modes of operation (CTR, CCM, GCM) and a SRTP Key Derivation Function for ARIA.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on November 16, 2012.

Copyright Notice

Table of Contents

1. Introduction

This document describes the use of the ARIA [RFC5794] block cipher algorithm in the Secure Real-time Transport Protocol (SRTP) [RFC3711] for providing confidentiality for the Real-time Transport Protocol (RTP) [RFC3550] traffic and for the control traffic for RTP, the Real-time Transport Control Protocol (RTCP) [RFC3550].

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. Cryptographic Transforms

Block ciphers ARIA and AES share common characteristics including mode, key size, and block size. ARIA does not have any restrictions for modes of operation that are used with this block cipher. We define three modes of running ARIA within the SRTP protocol, (1) ARIA in Counter Mode, (2) ARIA in Counter with CBC-MAC (CCM) Mode and (3) ARIA in Galois/Counter Mode (GCM).

2.1. ARIA-CTR

Section 4.1.1 of [RFC3711] defines AES-128 counter mode encryption, which it refers to as "AES_CM". Section 2 of [RFC6188] defines "AES_192_CM" and "AES_256_CM" in SRTP. ARIA counter modes are defined in a similar manner, and are denoted by ARIA_128_CTR, ARIA_192_CTR and ARIA_256_CTR respectively, according to the key lengths. The plaintext inputs to the block cipher are formed as in AES-CTR(AES_CM, AES_192_CM, AES_256_CM) and the block cipher outputs are processed as in AES-CTR. The only difference in the processing is that ARIA-CTR uses ARIA as the underlying encryption primitive. When ARIA-CTR is used, it MUST be used only in conjunction with an

authentication function.

The ARIA-CTR ciphersuites with HMAC-SHA1 as an authentication function are listed below. For each ciphersuites, the authentication key size is 20 octets.

Name	Enc. Key Size	Auth. Tag Size
ARIA_128_CTR_HMAC_SHA1_80	16 octets	10 octets
ARIA_128_CTR_HMAC_SHA1_32	16 octets	4 octets
ARIA_192_CTR_HMAC_SHA1_80	24 octets	10 octets
ARIA_192_CTR_HMAC_SHA1_32	24 octets	4 octets
ARIA_256_CTR_HMAC_SHA1_80	32 octets	10 octets
ARIA_256_CTR_HMAC_SHA1_32	32 octets	4 octets

Figure 1: ARIA-CTR algorithms for SRTP/SRTCP

2.2. ARIA-CCM and ARIA-GCM

CCM(Counter with CBC-MAC) [RFC3610] and GCM(Galois Counter Mode) [GCM] are AEAD(authenticated encryption with associated data) block cipher modes. ARIA-CCM and ARIA-GCM are defined similarly as AES-CCM and AES-GCM.

The internet draft [I-D.mcgrew-tls-aes-ccm] describes the use of AES-GCM and AES-CCM with SRTP. The use of ARIA-CCM and ARIA-GCM with SRTP is defined the same as that of AES-CCM and AES-GCM.

The following members of the ARIA-GCM family may be used with SRTP/SRTCP:

Name	Key Size	Auth. Tag Size
AEAD_ARIA_128_GCM	16 octets	16 octets
AEAD_ARIA_256_GCM	32 octets	16 octets
AEAD_ARIA_128_GCM_8	16 octets	8 octets
AEAD_ARIA_256_GCM_8	32 octets	8 octets
AEAD_ARIA_128_GCM_12	16 octets	12 octets
AEAD_ARIA_256_GCM_12	32 octets	12 octets

Figure 2: ARIA-GCM algorithms for SRTP/SRTCP

The following members of the ARIA-CCM family may be used with SRTP/SRTCP:

Name	Key Size	Auth. Tag Size
AEAD_ARIA_128_CCM	16 octets	16 octets
AEAD_ARIA_256_CCM	32 octets	16 octets

Figure 3: ARIA-CCM algorithms for SRTP/SRTCP

3. ARIA-CTR PRF

Section 4.3.3 of [RFC3711] defines the AES-128 counter mode key derivation function, which it refers to as "AES-CM PRF". Section 3 of [RFC6188] defines the AES-192 counter mode key derivation function and the AES-256 counter mode key derivation function, which it refers to as "AES_192_CM_PRF" and "AES_256_CM_PRF" respectively. The ARIA-CTR PRF is defined in a similar manner, but with each invocation of AES replaced with an invocation of ARIA. According to the key lengths of underlying encryption algorithm, ARIA-CTR PRFs are denoted by "ARIA_128_CTR_PRF", "ARIA_192_CTR_PRF" and "ARIA_256_CTR_PRF". The usage requirements of [RFC6188] regarding the AES-CM PRF apply to the ARIA-CTR PRF as well. The PRFs for ARIA ciphersuites with SRTP are defined by ARIA-CTR PRF of the equal key length with the encryption algorithm.

4. Security Considerations

At the time of writing this document no security problem has been found on ARIA (see [TSL]).

The security considerations in [RFC3610] [GCM] [RFC3711] [RFC6188] [I-D.mcgrew-tls-aes-ccm] apply to this document as well.

5. IANA Considerations

[RFC4568] defines SRTP "crypto suites". In order to allow SDP to signal the use of the algorithms defined in this document, IANA is requested to register the following crypto suites into the sub-registry for SRTP crypto suites under the SRTP transport of the SDP Security Descriptions:

```
srtp-crypto-suite-ext = "ARIA_128_CTR_HMAC_SHA1_80"/
                        "ARIA_128_CTR_HMAC_SHA1_32"/
                        "ARIA_192_CTR_HMAC_SHA1_80"/
                        "ARIA_192_CTR_HMAC_SHA1_32"/
                        "ARIA_256_CTR_HMAC_SHA1_80"/
                        "ARIA_256_CTR_HMAC_SHA1_32"/
                        "AEAD_ARIA_128_GCM"        /
                        "AEAD_ARIA_256_GCM"        /
                        "AEAD_ARIA_128_GCM_8"      /
                        "AEAD_ARIA_256_GCM_8"      /
                        "AEAD_ARIA_128_GCM_12"     /
                        "AEAD_ARIA_256_GCM_12"     /
                        "AEAD_ARIA_128_CCM"        /
                        "AEAD_ARIA_256_CCM"        /
                        srtp-crypto-suite-ext
```

DTLS-SRTP[RFC5764] defines a DTLS-SRTP "SRTP Protection Profile". In order to allow the use of the algorithms defined in this document in DTLS-SRTP, IANA will also register the following SRTP Protection Profiles:

```
SRTP_ARIA_128_CTR_HMAC_SHA1_80  = {TBD,TBD};
SRTP_ARIA_128_CTR_HMAC_SHA1_32  = {TBD,TBD};
SRTP_ARIA_192_CTR_HMAC_SHA1_80  = {TBD,TBD};
SRTP_ARIA_192_CTR_HMAC_SHA1_32  = {TBD,TBD};
SRTP_ARIA_256_CTR_HMAC_SHA1_80  = {TBD,TBD};
SRTP_ARIA_256_CTR_HMAC_SHA1_32  = {TBD,TBD};
SRTP_AEAD_ARIA_128_GCM          = {TBD,TBD};
SRTP_AEAD_ARIA_256_GCM          = {TBD,TBD};
SRTP_AEAD_ARIA_128_GCM_8        = {TBD,TBD};
SRTP_AEAD_ARIA_256_GCM_8        = {TBD,TBD};
SRTP_AEAD_ARIA_128_GCM_12       = {TBD,TBD};
SRTP_AEAD_ARIA_256_GCM_12       = {TBD,TBD};
SRTP_AEAD_ARIA_128_CCM          = {TBD,TBD};
SRTP_AEAD_ARIA_256_CCM          = {TBD,TBD};
```

[RFC3830] and [RFC5748] define encryption algorithms and PRFs for the SRTP policy in MIKEY. In order to allow the use of the algorithms defined in this document in MIKEY, IANA is requested to allocate the following numbers in the MIKEY sub-registries.

SRTP Enc. alg	Value
NULL	0
AES-CM	1
AES-F8	2
SEED-CTR	3
SEED-CCM	4
SEED-GCM	5
ARIA-128-CTR	6 (NEW)
ARIA-128-CCM	7 (NEW)
ARIA-128-GCM	8 (NEW)
ARIA-128-GCM-8	9 (NEW)
ARIA-128-GCM-12	10 (NEW)

Figure 4: Figure 1 from RFC 5748 (revised)

SRTP PRF	Value
AES-CM	0
SEED-CTR	1
ARIA-128-CTR	2 (NEW)

Figure 5: Figure 2 from RFC 5748 (revised)

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.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, July 2006.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, May 2010.

[RFC6188] McGrew, D., "The Use of AES-192 and AES-256 in Secure RTP", RFC 6188, March 2011.

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.

[I-D.mcgrew-tls-aes-ccm] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for TLS", draft-mcgrew-tls-aes-ccm-04 (work in progress), May 2012.

[RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.

[RFC5748] Yoon, S., Jeong, J., Kim, H., Jeong, H., and Y. Won, "IANA Registry Update for Support of the SEED Cipher Algorithm in Multimedia Internet KEYing (MIKEY)",

RFC 5748, August 2010.

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

[TSL] Tang, X., Sun, B., Li, R., Li, C., and J. Yin, "A meet-in-the-middle attack on reduced-round ARIA", The Journal of Systems and Software Vol.84(10), pp. 1685-1692, October 2011.

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

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

EMail: dongchan@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