AVTCore
Internet-Draft
Intended status: Standards Track
Expires: November 30, 2015

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

May 29, 2015

The Addition of SRTP crypto suites based on the ARIA algorithms to the SDP Security Descriptions
draft-ietf-avtcore-aria-sdes-00

Abstract

This document defines SRTP crypto suites based on the ARIA block cipher algorithm for use with the Session Description Protocol (SDP) security descriptions.

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 30, 2015.

Copyright Notice

Table of Contents

1. Introduction

This document defines Secure Real-time Transport Protocol (SRTP) [RFC3711] crypto suites based on the the ARIA [RFC5794] block cipher algorithm for use with the SDP Security Descriptions attributes [RFC4568].

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. SRTP Crypto Suites

The transforms based on ARIA and the correspoding SRTP protection profiles for DTLS-SRTP are defined in [I-D.ietf-avtcore-aria-srtp]. The SDP Security Descriptions [RFC4568] crypto suites corresponding to ARIA transforms [I-D.ietf-avtcore-aria-srtp] are sets as shown in Table 1.

Name	Enc. Key Length	Auth. Tag Length
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
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

Table 1: ARIA Crypto Suites for SRTP

1.3. 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. Patameters

The parameters in each crypto suite listed in Table 1 are described for use with the SDP Security Descriptions attributes [RFC4568].

Parameter	Value
Master key length	128 bits
Master salt length	112 bits
Key Derivation Function	ARIA_128_CTR_PRF
Default key lifetime	2^31 packets
Cipher (for SRTP and SRTCP)	ARIA_128_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	80 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 2: The ARIA_128_CTR_HMAC_SHA1_80 Crypto Suite

Parameter	Value
Master key length	128 bits
Master salt length	112 bits
Key Derivation Function	ARIA_128_CTR_PRF
Default key lifetime	2^31 packets
Cipher (for SRTP and SRTCP)	ARIA_128_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	32 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 3: The ARIA_128_CTR_HMAC_SHA1_32 Crypto Suite

Parameter	Value
Master key length	192 bits
Master salt length	112 bits
Key Derivation Function	ARIA_192_CTR_PRF
Default key lifetime	2^31 packets
Cipher (for SRTP and SRTCP)	ARIA_192_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	80 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 4: The ARIA_192_CTR_HMAC_SHA1_80 Crypto Suite

Parameter	Value
Master key length	192 bits
Master salt length	112 bits
Key Derivation Function	ARIA_192_CTR_PRF
Default key lifetime	2^31 packets
Cipher (for SRTP and SRTCP)	ARIA_192_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	32 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 5: The ARIA_192_CTR_HMAC_SHA1_32 Crypto Suite

Parameter	Value
Master key length	256 bits
Master salt length	112 bits
Key Derivation Function	ARIA_256_CTR_PRF
Default key lifetime	2^31 packets
Cipher (for SRTP and SRTCP)	ARIA_256_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	80 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 6: The ARIA_256_CTR_HMAC_SHA1_80 Crypto Suite

Parameter	Value
Master key length	256 bits
Master salt length	112 bits
Key Derivation Function	ARIA_256_CTR_PRF
Default key lifetime	2^31 packets
Cipher (for SRTP and SRTCP)	ARIA_256_CTR
SRTP authentication function	HMAC-SHA1
SRTP authentication key length	160 bits
SRTP authentication tag length	32 bits
SRTCP authentication function	HMAC-SHA1
SRTCP authentication key length	160 bits
SRTCP authentication tag length	80 bits

Table 7: The ARIA_256_CTR_HMAC_SHA1_32 Crypto Suite

Parameter	Value
Master key length	128 bits
Master salt length	96 bits
Key Derivation Function	ARIA_128_CTR_PRF
Default key lifetime (SRTP)	2^48 packets
Default key lifetime (SRTCP)	2^31 packets
Cipher (for SRTP and SRTCP)	AEAD_ARIA_128_GCM
AEAD authentication tag length	128 bits

Table 8: The AEAD_ARIA_128_GCM Crypto Suite

Parameter	Value
Master key length	256 bits
Master salt length	96 bits
Key Derivation Function	ARIA_256_CTR_PRF
Default key lifetime (SRTP)	2^48 packets
Default key lifetime (SRTCP)	2^31 packets
Cipher (for SRTP and SRTCP)	AEAD_ARIA_256_GCM
AEAD authentication tag length	128 bits

Table 9: The AEAD_ARIA_256_GCM Crypto Suite

Parameter	Value
Master key length	128 bits
Master salt length	96 bits
Key Derivation Function	ARIA_128_CTR_PRF
Default key lifetime (SRTP)	2^48 packets
Default key lifetime (SRTCP)	2^31 packets
Cipher (for SRTP and SRTCP)	AEAD_ARIA_128_GCM_8
AEAD authentication tag length	64 bits

Table 10: The AEAD_ARIA_128_GCM_8 Crypto Suite

3. IANA Considerations

SDP Security Descriptions [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 add the below crypto suites to the "SRTP Crypto Suite Registrations" created by [RFC4568], at time of writing located on the following IANA page: http://www.iana.org/assignments/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"      /
                        srtp-crypto-suite-ext
```

4. References

4.1. Normative References

[I-D.ietf-avtcore-aria-srtp]
Kim, W., Lee, J., Kim, D., Park, J., and D. Kwon, "The ARIA Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP)", draft-ietf-avtcore-aria-srtp-07 (work in progress), September 2014.

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

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

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

4.2. 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.

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