Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 18, 2012

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

September 15, 2011

The ARIA Cipher Algorithm and Its Use with IPsec
draft-nsri-ipsecme-aria-ipsec-00

Abstract

This document describes the use of the ARIA block cipher algorithm in conjunction with several different modes of operation within IKE and IPsec. It describes the use of ARIA in CBC, CTR, GCM and CCM modes to encrypt and/or authenticate IKE and ESP traffic. It also describes the use of ARIA in XCBC, CMAC, and GMAC modes to authenticate IKE, ESP and AH traffic. The use of ARIA in XCBC and CMAC modes for pseudorandom functions is also included.

Status of this Memo

Copyright Notice

Table of Contents

*1. Introduction

*1.1. ARIA

*1.2. Modes of Operation

*1.3. Terminology

*2. Encryption and Combined Mode Algorithms

*2.1. ARIA-CBC and ARIA-CTR

*2.2. ARIA-CCM and ARIA-GCM

*3. Integrity-Protection (Authentication) Algorithms

*3.1. ARIA-XCBC and ARIA-CMAC

*3.2. ARIA-GMAC

*4. Pseudo-Random Functions (PRFs)

*5. IKEv2 Conventions

*5.1. Keying Material

*5.2. Transform Type 1

*5.3. Transform Type 2

*5.4. Transform Type 3

*5.5. Key Length Attribute

*6. Security Considerations

*7. IANA Considerations

*8. References

*8.1. Normative References

*8.2. Informative References

*Authors' Addresses

1. Introduction

This document describes how to use ARIA in conjunction with several different modes of operation within IKE *[RFC5996]* and IPsec ([RFC4301] [RFC4302][RFC4303]). Within IKE, it is used either to protect the IKE SA's traffic (encryption and integrity-protection algorithms) or to generate keying material (pseudorandom functions). Within IPsec, it is

used to protect the IPsec/child SA's traffic, and IKE is capable of negotiating its use for that purpose.
For encryption algorithms, the use of ARIA in cipher block chaining (CBC) mode and counter (CTR) mode is described. Both are used to encrypt IKE and/or ESP traffic, providing confidentiality protection to the traffic. For integrity-protection algorithms, the use of ARIA in eXtended CBC (XCBC) mode, CMAC mode and GMAC mode is described. These are used to authenticate IKE and/or IPsec traffic, providing integrity protection to the traffic. For combined mode algorithms, the use of ARIA in counter with CBC-MAC (CCM) mode and Galois/Counter Mode (GCM) is described. Both are used to encrypt and integrity protect IKE and/or ESP traffic, providing both confidentiality and integrity protection to the traffic. For pseudorandom functions, the use of ARIA in XCBC mode and CMAC mode is described. Both are used to generate the secret keys that are used in IKE SAs and IPsec SAs.
This document does not provide an overview of IPsec. However, information about how the various components of IPsec and the way in which they collectively provide security services is available in [RFC4301], [RFC4302], [RFC4303] and [RFC5996].

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. Modes of Operation

Block ciphers ARIA and AES share common characteristics including key size and block length. ARIA does not have any restrictions for modes of operation that are used with this block cipher. So several definitions for ARIA modes of operation such as changes to packet formats, detailed algorithmic computations, and special considerations within relevant protocols can be specified according as those which were previously specified for AES. This document does not describe such definitions appropriate for the specific ARIA mode of operation, but attempts to indicate the reference of the corresponding AES mode of operation. The only difference in the processing is that the underlying encryption primitive is ARIA instead of AES.

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. Encryption and Combined Mode Algorithms

We specify four algorithms within IKE and IPsec ESP, (1) ARIA in CBC Mode (ARIA-CBC), (2) ARIA in CTR Mode (ARIA-CTR), (3) ARIA in CCM Mode (ARIA-CCM) and (4) ARIA in GCM (ARIA-GCM).
ARIA-CBC and ARIA-CTR are used to encrypt IKE and/or ESP traffic. When ARIA-CTR is used to provide confidentiality, the use of integrity protection is strongly recommended. As a single algorithm which can provide both encryption and integrity protection, ARIA-CCM and ARIA-GCM are used for IKE and/or ESP traffic.

2.1. ARIA-CBC and ARIA-CTR

The use of ARIA-CBC and ARIA-CTR within ESP is defined as AES-CBC [RFC3602] and AES-CTR [RFC3686]. [RFC3602] can also be a reference of ARIA-CBC within IKE, while ARIA-CTR within IKE refers to [RFC5930], which extends [RFC3686] to enable the use of AES-CTR to provide confidentiality for IKEv2 traffic.

2.2. ARIA-CCM and ARIA-GCM

The use of ARIA-CCM and ARIA-GCM within ESP is defined as AES-CCM [RFC4309] and AES-GCM [RFC4106]. The use of ARIA-CCM and ARIA-GCM within IKE is defined as AES in [RFC5282]. ARIA-CCM is a block-mode algorithm with a random IV that is sent in the packet along with the encrypted data, a 24-bit salt value; a 128-bit key and ICV sizes of 64, 96 and 128 bits. ARIA-GCM has the same structure with ARIA-CCM, except that a 32-bit salt value is used.

3. Integrity-Protection (Authentication) Algorithms

We specify three algorithms within IKE and IPsec, (1) ARIA in eXtended CBC Mode (ARIA-XCBC), (2) ARIA in CMAC Mode (ARIA-CMAC) and (3) ARIA in GMAC Mode (ARIA-GMAC). These are block cipher modes of operation providing integrity-protection, and can be used as an authentication mechanism within the context of the IKE and/or IPsec AH and ESP protocols. This protection is provided by computing an Integrity Check Value (ICV), which is included in the packet.

3.1. ARIA-XCBC and ARIA-CMAC

XCBC and CMAC are variants of CBC-MAC, which are secure for message of varying lengths (unlike classic CBC-MAC). The use of ARIA-XCBC and ARIA-CMAC is defined as AES-XCBC [RFC3566] and AES-CMAC [RFC4494]. Both

are integrity-protection algorithms with a 128-bit block and 128-bit key and 128-bit ICV. For use within IKE and IPsec, the ICV is truncated to 96 bits.

3.2. ARIA-GMAC

ARIA-GMAC is a variant of ARIA-GCM that provides integrity protection without encryption. It has two versions: an integrity-protection algorithm for use within AH, and a combined mode algorithm with null encryption for use within ESP. It can use key sizes of 128, 192, and 256 bits; the ICV is always 128 bits, and is not truncated. The use ARIA-GMAC within IPsec is defined as AES-GMAC [RFC4543].
ARIA-GMAC cannot be used by IKE to protect its own SAs, since IKE SA traffic requires encryption.

4. Pseudo-Random Functions (PRFs)

IKE uses pseudorandom functions (PRFs) to generate the secret keys that are used in IKE SAs and IPsec SAs. These PRFs are generally the same algorithms used for integrity protection, but their output is not truncated, since all of the generated bits are used for the keys in general.
We specify two algorithms within IKE as PRFs, (1) ARIA-XCBC and (2) ARIA-CMAC. The use of ARIA-XCBC and ARIA-CMAC within IKE is defined as AES-XCBC [RFC4434] and AES-CMAC [RFC4615].

5. IKEv2 Conventions

This section describes the conventions used to generate keying material for use with ARIA modes of operation using the Internet Key Exchange (IKEv2). The identifiers and attributes needed to negotiate a security association that uses ARIA modes of operation are also specified.

5.1. Keying Material

The PRF in IKE is used iteratively to derive keying material of arbitrary size, called KEYMAT. Keying material consisting of the actual ARIA key and the nonce is extracted from the output string without regard to boundaries, but is derived in the same way as AES modes of operation.

5.2. Transform Type 1

For IKEv2 negotiations, IANA is requested to assign IKE Transform Type 1 Identifiers for ARIA-CBC, ARIA-CTR, ARIA-CCM and ARIA-GCM, as recorded in Section 7.

5.3. Transform Type 2

For IKEv2 negotiations, IANA is requested to assign IKE Transform Type 2 Identifiers for ARIA-XCBC, ARIA-CMAC and ARIA-GMAC, as recorded in Section 7.

5.4. Transform Type 3

For IKEv2 negotiations, IANA is requested to assign IKE Transform Type 3 Identifiers for ARIA-XCBC and ARIA-CMAC, as recorded in Section 7.
For the usage of ARIA-GMAC within AH, each key size requires its own IANA value because IKE does not have to negotiate the key size. For the usage of ARIA-GMAC within ESP, there is only one IANA value, because IKE negotiations specify the key size.

5.5. Key Length Attribute

ARIA modes of operation can be used with any of the three ARIA key sizes. The way that the key size is indicated is different for Transform Type 1 and the others.
For Transform Type 1, there is a single encryption identifier. The IKE Key Length attribute MUST be used with each use of this identifier to indicate the key size. The Key Length attribute MUST have a value of 128-, 192-, or 256-bit, and is used in the same way as AES modes of operation.
For Transforms Type 2 and Type 3, the IKE Key Length attribute MUST NOT be used. Like ARIA-GMAC, each key size has its own separate integrity transform identifier and algorithm name.

6. Security Considerations

At the time of writing this document no security problem has been found on ARIA (see [TSL]).
The security considerations in [RFC3566], [RFC3602], [RFC3686], [RFC4106], [RFC4309], [RFC4434], [RFC4494], [RFC4543], [RFC4615] and [RFC5282] apply to this document as well. Within IKE and IPsec, ARIA modes of operation do not create additional security considerations beyond those of AES modes of operation.

7. IANA Considerations

IANA is requested to allocate Transform Type 1 (Encryption Algorithm Transform IDs) Identifiers for ARIA-CBC, ARIA-CTR, ARIA-CCM, and ARIA-GCM with an explicit IV in the "IKEv2 Parameters" registry:

Number	Name
<TBD1>	ENCR_ARIA_CBC;
<TBD2>	ENCR_ARIA_CTR;
<TBD3>	ENCR_ARIA_CCM_8;
<TBD4>	ENCR_ARIA_CCM_12;
<TBD5>	ENCR_ARIA_CCM_16;
<TBD6>	ENCR_ARIA_GCM_8;
<TBD7>	ENCR_ARIA_GCM_12;
<TBD8>	ENCR_ARIA_GCM_16;
<TBD9>	ENCR_NULL_AUTH_ARIA_GMAC;

IANA is also requested to allocate Transform Type 2 (Pseudo-random Function Transform IDs) Identifiers for ARIA-XCBC and ARIA-CMAC with an explicit IV in the "IKEv2 Parameters" registry:

Number	Name
<TBD1>	PRF_ARIA_128_XCBC;
<TBD2>	PRF_ARIA_128_CMAC;

IANA is also requested to allocate Transform Type 3 (Integrity Algorithm Transform IDs) Identifiers for ARIA-XCBC, ARIA-CMAC, and ARIA-GMAC with an explicit IV in the "IKEv2 Parameters" registry:

Number	Name
<TBD1>	AUTH_ARIA_128_XCBC_96;
<TBD2>	AUTH_ARIA_128_CMAC_96;
<TBD3>	AUTH_ARIA_128_GMAC;
<TBD4>	AUTH_ARIA_192_GMAC;
<TBD5>	AUTH_ARIA_256_GMAC;

8. References

8.1. Normative References

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

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC3602] Frankel, S., Glenn, R. and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC3686]

Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[RFC4434] Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4434, February 2006.

[RFC4494] Song, JH., Poovendran, R. and J. Lee, "The AES-CMAC-96 Algorithm and Its Use with IPsec", RFC 4494, June 2006.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC4615] Song, J., Poovendran, R., Lee, J. and T. Iwata, "The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4615, August 2006.

[RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, August 2008.

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

[RFC5930] Shen, S., Mao, Y. and NSS. Murthy, "Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol", RFC 5930, July 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y. and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

8.2. Informative References

[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.

[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.

Authors' Addresses

Woo-Hwan Kim Kim National Security Research Institute P.O.Box 1, Yuseong Daejeon, 305-350 Korea EMail: whkim5@ensec.re.kr

Jungkeun Lee Lee National Security Research Institute P.O.Box 1, Yuseong Daejeon, 305-350 Korea EMail: jklee@ensec.re.kr

Je-Hong Park Park National Security Research Institute P.O.Box 1, Yuseong Daejeon, 305-350 Korea EMail: jhpark@ensec.re.kr

Daesung Kwon Kwon National Security Research Institute P.O.Box 1, Yuseong Daejeon, 305-350 Korea EMail: ds_kwon@ensec.re.kr