JunHyuk Song
Radha Poovendran
University of Washington
Jicheol Lee
Samsung Electronics

INTERNET DRAFT
Expires: August 2, 2006
February 3 2006

The AES-CMAC-96 Algorithm and its use with IPsec
draft-songlee-aes-cmac-96-04.txt

Status of This Memo

Copyright Notice

Abstract

National Institute of Standards and Technology (NIST) has newly specified the Cipher based MAC (CMAC) which is equivalent to the One-Key CBC-MAC1 (OMAC1) algorithm submitted by Iwata and Kurosawa. OMAC1 efficiently reduces the key size of Extended Cipher Block Chaining mode (XCBC). This memo specifies the use of CMAC mode on authentication mechanism of IPsec Encapsulating Security Payload (ESP) and the Authentication Header (AH) protocols. This new algorithm is named AES-CMAC-96.

1. Introduction

National Institute of Standards and Technology (NIST) has newly specified the Cipher-based Message Authentication Code (CMAC). CMAC [NIST-CMAC] is a message authentication code that is based on a symmetric key block cipher such as the Advanced Encryption Standard [NIST-AES]. CMAC is equivalent to the One-Key CBC MAC1 (OMAC1) submitted by Iwata and Kurosawa [OMAC1a, OMAC1b]. OMAC1 is an improvement of the eXtended Cipher Block Chaining mode (XCBC) submitted by Black and Rogaway [XCBCa, XCBCb], which itself is an improvement of the basic CBC-MAC. XCBC efficiently addresses the security deficiencies of CBC-MAC, and OMAC1 efficiently reduces the key size of XCBC.

This memo specifies the usage of CMAC on authentication mechanism of IPsec Encapsulating Security Payload (ESP) [ESP] and the Authentication Header (AH) protocols. This new algorithm is named AES-CMAC-96. For further information on AH and ESP, refer to [AH] and [ROADMAP].

2. Basic definitions

CBC	Cipher Block Chaining mode of operation for message authentication code.
MAC	Message Authentication Code. A bit string of a fixed length, computed by MAC generation algorithm, that is used to established the authority and hence, the integrity of a message.
CMAC	Cipher-based MAC based on an approved symmetric key block cipher, such as the Advanced Encryption Standard.
Key (K)	128-bits (16 octets) long key for AES-128 cipher block. Denoted by K.
Message (M)	Message to be authenticated. Denoted by M.
Length (len)	The length of message M in octets. Denoted by len. Minimum value of the length can be 0. The maximum value of the length is not specified in this document.
truncate(T,l)	Truncate T (MAC) in msb-first order with l octet.
T	The output of AES-CMAC

Truncated T	The truncated output of AES-CMAC-128 in MSB first order.
AES-CMAC	CMAC generation function based on AES block cipher with 128-bits key
AES-CMAC-96	IPsec AH and ESP MAC generation function based on AES-CMAC which truncates MSB 96 bits of 128 bits output

3. AES-CMAC

The core of AES-CMAC-96 is the AES-CMAC [AES-CMAC]. The underlying algorithm for AES-CMAC are Advanced Encryption Standard cipher block [AES] and recently defined CMAC mode of operation [NIST-CMAC]. AES-CMAC provides stronger assurance of data integrity than a checksum or an error detecting code. The verification of a checksum or an error detecting code detects only accidental modifications of the data, while CMAC is designed to detect intentional, unauthorized modifications of the data, as well as accidental modifications. The output of AES-CMAC can validate the input message. Validating the message provide assurance of the integrity and authenticity over the message from the source. According to [NIST-CMAC] at least 64-bits should be used for against guessing attack. AES-CMAC achieves the similar security goal of HMAC [RFC-HMAC]. Since AES-CMAC is based on a symmetric key block cipher, AES, while HMAC is based on a hash function, such as SHA-1, AES-CMAC is appropriate for information systems in which AES is more readily available than a hash function. For detail information about AES-CMAC is available in [AES-CMAC] and [NIST-CMAC].

4. AES-CMAC-96

For use in IPsec message authentication on AH and ESP, AES-CMAC-96 should be used. AES-CMAC-96 is a AES-CMAC with 96-bit-long truncated output in most significant bit first order. The output of 96 bits MAC that will meet the default authenticator length as specified in [AH]. The result of truncation is taken in most significant bits first order. For further information on AES-CMAC, refer to [AES-CMAC] and [NIST-CMAC].

Figure 1 describes AES-CMAC-96 algorithm:

In step 1, AES-CMAC is applied to the message 'M' in length 'len' with key 'K'

In step 2, Truncate output block, T with 12 octets in msb-first-order and return TT.

```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                    Algorithm AES-CMAC-96                          +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                                                                   +
+   Input    : K (128-bit Key described in section 4.1)             +
+            : M    ( message to be authenticated )                 +
+            : len  ( length of message in octets )                 +
+   Output   : Truncated T  (Truncated output with length 12 octets)+
+                                                                   +
+-------------------------------------------------------------------+
+                                                                   +
+   Step 1.  T  := AES-CMAC (K,M,len);                              +
+   Step 2.  TT := truncate (T, 12);                                +
+            return TT;                                             +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 1 Algorithm AES-CMAC-96

5. Test Vectors

These test cases same as defined in [NIST-CMAC] with one exception of 96 bits truncation

```
-------------------------------------------------
K               2b7e1516 28aed2a6 abf71588 09cf4f3c
Subkey Generation
AES_128(key,0) 7df76b0c 1ab899b3 3e42f047 b91b546f
K1              fbeed618 35713366 7c85e08f 7236a8de
K2              f7ddac30 6ae266cc f90bc11e e46d513b

Test Case 1: len = 0
M               <empty string>
AES_CMAC_96     bb1d6929 e9593728 7fa37d12

Test Case 2: len = 16
M               6bc1bee2 2e409f96 e93d7e11 7393172a
AES_CMAC_96     070a16b4 6b4d4144 f79bdd9d

Test Case 3: len = 40
M               6bc1bee2 2e409f96 e93d7e11 7393172a
                ae2d8a57 1e03ac9c 9eb76fac 45af8e51
                30c81c46 a35ce411
AES_CMAC_96     dfa66747 de9ae630 30ca3261

Test Case 4: len = 64
M               6bc1bee2 2e409f96 e93d7e11 7393172a
                ae2d8a57 1e03ac9c 9eb76fac 45af8e51
                30c81c46 a35ce411 e5fbc119 1a0a52ef
                f69f2445 df4f9b17 ad2b417b e66c3710
AES_CMAC_96     51f0bebf 7e3b9d92 fc497417
```

6. Interaction with the ESP Cipher Mechanism

As of this writing, there are no known issues which preclude the use of AES-CMAC-96 with any specific cipher algorithm.

7. Security Considerations

See security consideration of [AES-CMAC].

8. IANA Consideration

IANA should allocate a value for IKEv2 Transform Type 3 (Integrity Algorithm) to the AUTH_AES_CMAC_96 algorithm when this document is published.

9. Acknowledgement

Portions of this text were borrowed from [NIST-CMAC] and [AES-XCBC-MAC]. We would like to thank to Russ Housley for his useful comments.

10. References

10.1. Normative References

[NIST-CMAC] NIST, Special Publication 800-38B Draft,"Recommendation for Block Cipher Modes of Operation: The CMAC Method for Authentication," March 9, 2005

[NIST-AES] NIST, FIPS 197, "Advanced Encryption Standard (AES)," November 2001.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[ESP] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[AES-CMAC] JunHyuk Song, Jicheol Lee, Radha Poovendran, Tetsu Iwata "The AES-CMAC Algorithm" draft-songlee-aes-cmac-02.txt, October 2005 (Work in progress)

10.2. Informative References

[AH] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[ROADMAP] Thayer, R., Doraswamy, N. and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[OMAC1a] Tetsu Iwata and Kaoru Kurosawa, "OMAC: One-Key CBC MAC," Fast Software Encryption, FSE 2003, LNCS 2887, pp. 129-153, Springer-Verlag, 2003.

[RFC-HMAC] Hugo Krawczyk, Mihir Bellare and Ran Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC2104, February 1997.

[OMAC1] "OMAC: One-Key CBC MAC," Tetsu Iwata and Kaoru Kurosawa, Department of Computer and Information Sciences, Ilbaraki University, March 10, 2003.

[OMAC1b] Tetsu Iwata and Kaoru Kurosawa, "OMAC: One-Key CBC MAC," Submission to NIST, December 2002.
Available from the NIST modes of operation web site at http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/omac/omac-spec.pdf

[XCBCa] John Black and Phillip Rogaway, "A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC," NIST Second Modes of Operation Workshop, August 2001.
Available from the NIST modes of operation web site at http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/xcbc-mac/xcbc-mac-spec.pdf

[XCBCb] John Black and Phillip Rogaway, "CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions," Journal of Cryptology, Vol. 18, No. 2, pp. 111-132, Springer-Verlag, Spring 2005.

[XCBC] Black, J. and P. Rogaway, "A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC," NIST Second Modes of Operation Workshop, August 2001.
http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/xcbc-mac/xcbc-mac-spec.pdf

[IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17
(work in progress), September 2004.

11. Author's Address

Junhyuk Song
University of Washington
Samsung Electronics
(206) 853-5843
songlee@ee.washington.edu
junhyuk.song@samsung.com

Jicheol Lee
Samsung Electronics
+82-31-279-3605
jicheol.lee@samsung.com

Radha Poovendran
Network Security Lab (NSL)
Dept. of Electrical Engineering
University of Washington
(206) 221-6512
radha@ee.washington.edu

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.