JunHyuk Song

Radha Poovendran

University of Washington

Jicheol Lee

Samsung Electronics

Tetsu Iwata

Ibaraki University

INTERNET DRAFT

Expires: August 2, 2006

February 3 2006

The AES-CMAC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)

draft-songlee-aes-cmac-prf-128-03.txt

Status of This Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

Some implementations of IP Security (IPsec) may want to use a pseudo-random function derived from the Advanced Encryption Standard (AES). This memo describes such an algorithm, called AES-CMAC-PRF-128.

1. Introduction

[AES-CMAC] describes a method to use the Advanced Encryption Standard (AES) as a message authentication code (MAC) whose output is 128 bits long. 128 bits output is useful as a long-lived pseudo-random function (PRF) in either IKE version 1 or version 2. This document specifies PRF that support fixed and variable key sizes for IKEv2 [IKEv2] Key Derivation Function (KDF) and authentication.

2. Basic definitions

VK	Variable length key for AES-CMAC-PRF-128, Denoted by VK.
0^n	The string that consists of n zero-bits. 0^3 means that 000 in binary format. 10^4 means that 10000 in binary format. 10^i means that 1 followed by i-times repeated zero's.
AES-CMAC	AES-CMAC algorithm with 128 bits long key described in section 2.4 of [AES-CMAC].

3. The AES-CMAC-PRF-128 Algorithm

The AES-CMAC-PRF-128 algorithm is identical to AES-CMAC defined

in [AES-CMAC] except that the 128 bits key length restriction is removed.

IKEv2 [IKEv2] uses PRFs for multiple purposes, most notably for generating keying material and authentication of the the IKE_SA. The IKEv2 specification differentiates between PRFs with fixed key sizes and those with variable key sizes

When using the PRF described in this document with IKEv2, the PRF is considered to be fixed-length for generating keying material but variable-length for authentication.

```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                        AES-CMAC-PRF-128                               +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                                                                       +
+ Input  : VK ( Variable length key )                                   +
+        : M ( Message to be authenticated )                            +
+        : VKlen ( length of VK )                                       +
+        : len ( length of message in octets )                          +
+ Output : PRV ( 128 bits Pseudo Random Variable )                      +
+                                                                       +
+-----------------------------------------------------------------------+
+ Variables: K ( 128-bits fixed key )                                   +
+                                                                       +
+ Step 1.                                                               +
+           If VKlen is equal to 16 octets then                         +
+ Step 1a.      K := VK;                                                +
+           Else                                                        +
+ Step 1b.      K := AES-CMAC (0^128, VK, VKlen);                       +
+                                                                       +
+ Step 2.                                                               +
+           PRV := AES-CMAC (K,M,len);                                  +
+           return PRV;                                                 +
+                                                                       +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 1. AES-CMAC-PRF-128 Algorithm

In step 1, the key for AES-CMAC-PRF-128 is created as follows:

o If the key is exactly 128 bits long, use it as-is.

o If the key is longer or shorter than 128 bits long, then we derive new key K by performing AES-CMAC algorithm using 128 bits all zero key and VK as the message. This step is described in step 1b.

In step 2, we perform AES-CMAC algorithm using K as the key and M as the message. The output of this algorithm is returned.

5. Test Vectors

```
-------------------------------------------------------------

Test Case AES-CMAC-PRF-128 with 20-octet input
Key        : 00010203 04050607 08090a0b 0c0d0e0f edcb
Key Length : 18
Message    : 00010203 04050607 08090a0b 0c0d0e0f 10111213
PRF Output : 84a348a4 a45d235b abfffc0d 2b4da09a

Test Case AES-CMAC-PRF-128 with 20-octet input
Key        : 00010203 04050607 08090a0b 0c0d0e0f
Key Length : 16
Message    : 00010203 04050607 08090a0b 0c0d0e0f 10111213
PRF Output : 980ae87b 5f4c9c52 14f5b6a8 455e4c2d

Test Case AES-CMAC-PRF-128 with 20-octet input
Key        : 00010203 04050607 0809
Key Length : 10
Message    : 00010203 04050607 08090a0b 0c0d0e0f 10111213
PRF Output : 290d9e11 2edb09ee 141fcf64 c0b72f3d

-------------------------------------------------------------
```

6. Security Considerations

The security provided by AES-CMAC-PRF-128 is based upon the strength of AES and AES-CMAC. At the time of this writing, there are no known practical cryptographic attacks against AES or AES-CMAC.

However as is true with any cryptographic algorithm, part of its strength lies in the secret key, 'K' and the correctness of the implementation in all of the participating systems.

Keys need to be chosen at random based on RFC 4086 [RFC4086] and should be kept in safe and periodically refreshed.

Whenever keys larger than 128 bits are reduced to meet AES-128 key input size, some entropy might be lost. However, if using collision-resistant hash function such as AES-CMAC when generating new key for pseudo-random function, it preserves sufficient entropy as long as the pseudo-random function to be used requires 128 bits long input key.

7. IANA Consideration

IANA should allocate a value for IKEv2 Transform Type 2 (Pseudo-Random Function) to the PRF_AES128_CMAC algorithm when this document is published.

8. Acknowledgement

Portions of this text were borrowed from [AES-XCBC-PRF] and [AES-XCBC-PRF_bis], and many thanks to Russ Housley and Paul Hoffman for suggestions and guidance.

9. Reference

9.1 Normative References

[AES-CMAC] JunHyuk Song, Jicheol Lee, Radha Poovendran and Tetsu Iwata, "The AES-CMAC Algorithm," draft-songlee-aes-cmac-03.txt, (work in progress) December 2005.

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

[RFC4086] Eastlake 3rd, D., Crocker, S., and J. Schiller, "Randomness Requirements for Security", RFC 4086 June 2005

9.2. 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.

[AES-XCBC-PRF] P. Hoffman, "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)," RFC3664, Jan 2004.

[AES-XCBC-PRF-bis] P. Hoffman, "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)," draft-hoffman-rfc3664bis-05.txt (work in progress), October 2005.

Author's Address

Junhyuk Song

Samsung Electronics

University of Washington

(206) 853-5843

songlee@u.washington.edu

junhyuk.song@samsung.com

Jicheol Lee

Samsung Electronics

+82-31-279-3605

jicheol.lee@samsung.com

Radha Poovendran

Network Security Lab

University of Washington

(206) 221-6512

radha@ee.washington.edu

Tetsu Iwata

Ibaraki University

iwata@cis.ibaraki.ac.jp

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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