MSEC Working Group
Internet Draft
Intended Status: Informational
Expires: May 23, 2010

S. Yoon
J. Jeong
H. Kim
H. Jeong
Y. Won
Korea Internet & Security Agency

November 23, 2009

IANA Registry Update for Support of the SEED Cipher Algorithm in the Multimedia Internet KEYing (MIKEY)

draft-seokung-msec-mikey-seed-05

Status of this Memo

Copyright Notice

Abstract

This document updates IANA registries to support the SEED block cipher algorithm for the Secure Real-time Transport Protocol (SRTP) and the secure Real-time Transport Control Protocol (SRTCP) in Multimedia Internet KEYing (MIKEY).

Table of Contents

1. Introduction

This document updates IANA registries to support the SEED [RFC4269] block cipher algorithm for the Secure Real-time Transport Protocol (SRTP) and the Secure Real-time Transport Control Protocol (SRTCP) [RFC3711] in Multimedia Internet KEYing (MIKEY) [RFC3830].

1.1. SEED

SEED is a 128-bit symmetric key block cipher that has been developed by KISA (Korea Information Security Agency) and a group of experts since 1998. The input/output block size of SEED is 128-bit and the key length is also 128-bit. SEED has a 16-round Feistel structure.

SEED is a Korean National Industrial Association standard and is widely used in South Korea for electronic commerce and various security products such as firewall, VPN, and so on.

2. Additions to MIKEY payload

This section specifies new code points for the MIKEY [RFC3830] payload to indicate the use of the SEED cipher algorithm for SRTP and SRTCP. There are three applicable modes of running SEED, SEED in Counter Mode (SEED-CTR), SEED in Counter with CBC-MAC Mode (SEED-CCM) and SEED in Galois/Counter Mode (SEED-GCM) Mode. These are defined in [I-D.ietf-avt-seed-srtp].

2.1. Modified Table 6.10.1.b from RFC3830

IANA is asked to amend the sub-registry derived from Table 6.10.1.b of [RFC3830] as follows:

SRTP encr alg	Value
NULL	0
AES-CM	1
AES-F8	2
SEED-CTR	3 (NEW)
SEED-CCM	4 (NEW)
SEED-GCM	5 (NEW)

Figure 1: Table 6.10.1.b from [RFC3830] (Revised)

2.2. Modified Table 6.10.1.d from RFC3830

IANA is asked to amend the sub-registry derived from Table 6.10.1.d of [RFC3830] as follows:

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

Figure 2: Table 6.10.1.d from [RFC3830] (Revised)

3. Security Considerations

No security problem has been found on SEED. SEED is secure against all known attacks including Differential cryptanalysis, linear cryptanalysis, and related key attacks. The only known attack is an exhaustive search for the key. For further security considerations, the reader is encouraged to read [SEED-EVAL].

4. IANA Considerations

With the adoption of this document for publication IANA has amended the indicated sub-registries in Section 2 of the MIKEY [RFC3830] Payload Name registry according to Section 2.1 and 2.2 above.

5. Acknowledgements

The authors would like to thank David McGrew, Spencer Dawkins, SangHwan Park, Brian Weis, and Tim Polk for their reviews and support.

6. References

6.1. Normative References

[I-D.ietf-avt-seed-srtp]
S. Yoon, J. Kim, H. Park, H. Jeong, Y. Won, "The SEED Cipher Algorithm and Its Use with the Secure Real-time Transport Protocol (SRTP)", draft-ietf-avt-seed-srtp-14 (work in progress), June 2009.

[RFC3711] M. Baugher, D. McGrew, M. Naslund, E.Carrara, 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.

[RFC4269] H. Lee, S. Lee, J. Yoon, D. Cheon, J. Lee, "The SEED Encryption Algorithm", RFC 4269, December 2005.

6.2. Informative References

[SEED-EVAL] KISA, "Self Evaluation Report", http://www.kisa.or.kr/kisa/seed/down/SEED_Evaluation_Report_by_CRYPTREC.pdf

Author's Addresses

Seokung Yoon
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: seokung@kisa.or.kr

Jongil Jeong
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: jijeong@kisa.or.kr

Hwankuk Kim
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: rinyfeel@kisa.or.kr

Hyuncheol Jeong
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: hcjung@kisa.or.kr

Yoojae Won
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa-gu, Seoul, Korea 138-950
Email: yjwon@kisa.or.kr