Internet Engineering Task Force (IETF)
Request for Comments: 5748
Category: Informational
ISSN: 2070-1721

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

August 2010

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

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).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5748.

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 firewalls, VPNs, 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 [RFC5669].

2.1. Modified Table 6.10.1.b from RFC 3830

IANA has amended 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 RFC 3830

IANA has amended 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

IANA has amended the indicated sub-registries in Section 2 of the MIKEY [RFC3830] Payload Name registry according to Sections 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

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and 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] Lee, H., Lee, S., Yoon, J., Cheon, D., and J. Lee, "The SEED Encryption Algorithm", RFC 4269, December 2005.

[RFC5669] Yoon, S., Kim, J., Park, H., Jeong, H., and Y. Won, "The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)", RFC 5669, August 2010.

6.2. Informative References

[SEED-EVAL] KISA, "Self Evaluation Report", http://seed.kisa.or.kr/eng/main.jsp

Authors' 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