Using the SEED Cipher Algorithm with MIKEY

Seokung Yoon (KISA)

Goal / Motivation

- Motivation
  - In Korea, the VoIP service becomes more popular and we predict the VoIP market could grow to as much as $10 billion by the year 2009.
  - Our agency developed a VoIP phone to support secure communications for confidentiality, integrity and user privacy, and adopted SRTP and MIKEY/SDES as key management protocol.
  - We add two algorithms for multimedia data encryption
    - AES and SEED

- Goal : Addition of new values to use the SEED cipher algorithm for SRTP in MIKEY

The SEED Cipher Algorithm

- developed by KISA in 1999

- Standard status

  - IETF Standard

    ✓ RFC 4269, The SEED Encryption Algorithm

    ✓ RFC 4010, Use of the SEED Encryption Algorithm in CMS

    ✓ RFC 4162, Addition of SEED Cipher Suites to TLS

    ✓ RFC 4196, The SEED Cipher Algorithm and Its Use with IPSec

  - ISO/IEC Standard

    ✓ JTC 1/SC 27 N3979, “IT Security technique – Encryption Algorithm – Part3 : Block ciphers

The SEED with SRTP

- AVT WG Item since 69th meeting

- SEED-SRTP defines three modes of running SEED
  - SEED in Counter Mode (SEED-CTR)
  - SEED in Counter with CBC-MAC (SEED-CCM)
  - SEED in Galois/Counter Mode (SEED-GCM)

- Current Status
  - AD Last Call by 2009-3-27

The SEED with MIKEY

- To use the SEED cipher algorithm in MIKEY, new values should add to Security Policy (SP) payload.
- For the Encryption algorithm, the currently define possible values are :

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

- For the SRTP pseudo-random function, the currently define possible values are :

SRTP PRF	Value
AES-CM	1
SEED-CTR	2 (NEW) ♪

Next Steps

- Comments or Questions ??

- Working Group Item ??