Network Working Group
Request for Comments: 4162
Category: Standards Track

H.J. Lee
J.H. Yoon
J.I. Lee
KISA

August 2005

Addition of SEED Cipher Suites to Transport Layer Security (TLS)

Status of This Memo

Copyright Notice

Abstract

This document proposes the addition of new cipher suites to the Transport Layer Security (TLS) protocol to support the SEED encryption algorithm as a bulk cipher algorithm.

1. Introduction

This document proposes the addition of new cipher suites to the TLS protocol [TLS] to support the SEED encryption algorithm as a bulk cipher algorithm.

1.1. SEED

SEED is a symmetric encryption algorithm that was developed by Korea Information Security Agency (KISA) and a group of experts, beginning in 1998. The input/output block size of SEED is 128-bit and the key length is also 128-bit. SEED has the 16-round Feistel structure. A 128-bit input is divided into two 64-bit blocks and the right 64-bit block is an input to the round function with a 64-bit subkey generated from the key scheduling.

SEED is easily implemented in various software and hardware because it is designed to increase the efficiency of memory storage and the simplicity of generating keys without degrading the security of the algorithm. In particular, it can be effectively adopted in a computing environment that has a restricted resources such as mobile devices, smart cards, and so on.

SEED is a national industrial association standard [TTASSEED] and is widely used in South Korea for electronic commerce and financial services operated on wired & wireless PKI.

The algorithm specification and object identifiers are described in [SEED-ALG]. The SEED homepage, http://www.kisa.or.kr/seed/seed_eng.html, contains a wealth of information about SEED, including detailed specification, evaluation report, test vectors, and so on.

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in [RFC2119].

2. Proposed Cipher Suites

The new cipher suites proposed here have the following definitions:

```
CipherSuite TLS_RSA_WITH_SEED_CBC_SHA      = { 0x00, 0x96};
CipherSuite TLS_DH_DSS_WITH_SEED_CBC_SHA   = { 0x00, 0x97};
CipherSuite TLS_DH_RSA_WITH_SEED_CBC_SHA   = { 0x00, 0x98};
CipherSuite TLS_DHE_DSS_WITH_SEED_CBC_SHA  = { 0x00, 0x99};
CipherSuite TLS_DHE_RSA_WITH_SEED_CBC_SHA  = { 0x00, 0x9A};
CipherSuite TLS_DH_anon_WITH_SEED_CBC_SHA  = { 0x00, 0x9B};
```

3. Cipher Suite Definitions

3.1. Cipher

All the cipher suites described here use SEED in cipher block chaining (CBC) mode as a bulk cipher algorithm. SEED is a 128-bit block cipher with 128-bit key size.

3.2. Hash

All the cipher suites described here use SHA-1 [SHA-1] in an HMAC construction as described in section 5 of [TLS].

3.3. Key Exchange

The cipher suites defined here differ in the type of certificate and key exchange method. They use the following options:

CipherSuite	Key Exchange Algorithm
TLS_RSA_WITH_SEED_CBC_SHA	RSA
TLS_DH_DSS_WITH_SEED_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_SEED_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_SEED_CBC_SHA	DH_anon

For the meanings of the terms RSA, DH_DSS, DH_RSA, DHE_DSS, DHE_RSA, and DH_anon, please refer to sections 7.4.2 and 7.4.3 of [TLS].

4. Security Considerations

It is not believed that the new cipher suites are less secure than the corresponding older ones. No security problem has been found on SEED. SEED is robust against known attacks, including differential cryptanalysis, linear cryptanalysis, and related key attacks, etc. SEED has gone through wide public scrutinizing procedures. Especially, it has been evaluated and also considered cryptographically secure by trustworthy organizations such as ISO/IEC JTC 1/SC 27 and Japan CRYPTREC (Cryptography Research and Evaluation Committees) [ISOSEED] [CRYPTREC]. SEED has been submitted to several other standardization bodies such as ISO (ISO/IEC 18033-3) and IETF S/MIME Mail Security [SEED-SMIME]; and it is under consideration. For further security considerations, the reader is encouraged to read [SEED-EVAL].

For other security considerations, please refer to the security of the corresponding older cipher suites described in [TLS] and [AES-TLS].

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[TTASSEED] Telecommunications Technology Association (TTA), South Korea, "128-bit Symmetric Block Cipher (SEED)", TTAS.KO-12.0004, September 1998, (In Korean) http://www.tta.or.kr/English/new/main/index.htm.

5.2. Informative References

[AES-TLS] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[CRYPTREC] Information-technology Promotion Agency (IPA), Japan, CRYPTREC. "SEED Evaluation Report", February 2002, http://www.kisa.or.kr/seed/seed_eng.html.

[ISOSEED] ISO/IEC JTC 1/SC 27, "National Body contributions on NP 18033 'Encryption Algorithms' in Response to SC 27 N2563 (ATT.3 Korea Contribution)", ISO/IEC JTC 1/SC 27 N2656r1 (n2656_3.zip), October 2000.

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

[SEED-ALG] Park, J., Lee, S., Kim, J., and J. Lee, "The SEED Encryption Algorithm", RFC 4009, February 2005.

[SEED-SMIME] Park, J., Lee, S., Kim, J., and J. Lee, "Use of the SEED Encryption Algorithm in Cryptographic Message Syntax (CMS)", RFC 4010, February 2005.

[SHA-1] FIPS PUB 180-1, "Secure Hash Standard", National Institute of Standards and Technology, U.S. Department of Commerce, April 17, 1995.

Authors' Addresses

Hyangjin Lee
Korea Information Security Agency

Phone: +82-2-405-5446
Fax : +82-2-405-5319
EMail: jiinii@kisa.or.kr

Jaeho Yoon
Korea Information Security Agency

Phone: +82-2-405-5434
Fax : +82-2-405-5219
EMail: jhyoon@kisa.or.kr

Jaeil Lee
Korea Information Security Agency

Phone: +82-2-405-5300
Fax : +82-2-405-5219
EMail: jilee@kisa.or.kr

Full Copyright Statement

Intellectual Property

Acknowledgement

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