TLS Working Group
Internet-Draft
Intended status: Informational
Expires: August 17, 2008

P. Eronen, Ed.
Nokia

February 14, 2008

DES and IDEA Cipher Suites for Transport Layer Security (TLS)
draft-ietf-tls-des-idea-00.txt

Status of this Memo

Copyright Notice

Abstract

TLS specification versions 1.0 (RFC 2246) and 1.1 (RFC 4346) included cipher suites based on DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) algorithms. DES (when used in single-DES mode) and IDEA are no longer recommended for general use in TLS, and have been removed from TLS 1.2 main specification (RFC NNNN). This document specifies these cipher suites for completeness, and discusses reasons why their use is no longer recommended.

1. Introduction

TLS specification versions 1.0 [TLS10] and 1.1 [TLS11] included cipher suites based on DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) algorithms. DES (when used in single-DES mode) and IDEA are no longer recommended for general use in TLS, and have been removed from TLS 1.2 main specification [TLS12].

This document specifies these cipher suites for completeness, and discusses reasons why their use is no longer recommended.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [REQ].

2. DES Cipher Suites

DES (Data Encryption Standard) is a block cipher which was originally approved as US federal standard in 1976, and is specified in [DES].

For TLS key generation purposes, DES is treated as having a 64-bit key, but it still provides only 56 bits of protection, as 8 of the 64 bits are not used by the algorithm. DES uses a 64-bit block size.

The following cipher suites have been defined for using DES in CBC mode in TLS:

```
CipherSuite TLS_RSA_WITH_DES_CBC_SHA            = { 0x00,0x09 };
CipherSuite TLS_DH_DSS_WITH_DES_CBC_SHA         = { 0x00,0x0C };
CipherSuite TLS_DH_RSA_WITH_DES_CBC_SHA         = { 0x00,0x0F };
CipherSuite TLS_DHE_DSS_WITH_DES_CBC_SHA        = { 0x00,0x12 };
CipherSuite TLS_DHE_RSA_WITH_DES_CBC_SHA        = { 0x00,0x15 };
CipherSuite TLS_DH_anon_WITH_DES_CBC_SHA        = { 0x00,0x1A };
```

The key exchange algorithms (RSA, DH_DSS, DH_RSA, DHE_DSS, DHE_RSA, and DH_anon) and the MAC algorithm (SHA) are defined in the base TLS specification.

3. IDEA Cipher Suites

IDEA (International Data Encryption Algorithm) is block cipher designed by Xuejia Lai and James Massey [IDEA] [SCH]. IDEA uses a 128-bit key and operates on 64-bit blocks.

The following cipher suite has been defined for using IDEA in CBC mode in TLS:

```
CipherSuite TLS_RSA_WITH_IDEA_CBC_SHA           = { 0x00,0x07 };
```

The key exchange algorithm (RSA) and the MAC algorithm (SHA) are defined in the base TLS specification.

4. Security Considerations

4.1. DES Cipher Suites

DES has an effective key strength of 56 bits, which has been been known to be vulnerable to practical brute force attacks for over 20 years [DH]. A relatively recent 2006 paper by Kumar et al. [COPA] describes a system which performs exhaustive key search in less than nine days on average, and costs less than 10,000 USD to build.

Given these, the single-DES cipher suites SHOULD NOT be implemented by TLS libraries. If a TLS library implements these cipher suites, it SHOULD NOT enable them by default. Experience has also shown that rarely used code is a source of security and interoperability problems, so existing implementations SHOULD consider removing these cipher suites.

4.2. IDEA Cipher Suites

IDEA has a 128-bit key, and thus is not vulnerable to exhaustive key search. However, IDEA cipher suites for TLS have not seen widespread use: most implementations either do not support them, do not enable them by default, or do not negotiate them when other algorithms (such as AES, 3DES, or RC4) are available.

Experience has shown that rarely used code is a source of security and interoperability problems; given this, the IDEA cipher suites

SHOULD NOT be implemented by TLS libraries, and SHOULD be removed from existing implementations.

Several reasons have been suggested to explain why the IDEA cipher suites have been rarely used. These include the existence of IPR disclosures (which can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr); poor performance in software on common CPU architectures; a 64-bit block size which is considered short by modern standards; the existence of weak keys; lack of government approval in many countries; and the availability of other algorithms which addressed at least some of these reasons.

5. IANA Considerations

IANA has already allocated values for the cipher suites described in this document in the TLS Cipher Suite Registry, defined in [TLS11]. IANA is requested to update (has updated) the references of these cipher suites to point to this document:

Value	Description	Reference
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA	[RFCnnnn]
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA	[RFCnnnn]
0x00,0x0C	TLS_DH_DSS_WITH_DES_CBC_SHA	[RFCnnnn]
0x00,0x0F	TLS_DH_RSA_WITH_DES_CBC_SHA	[RFCnnnn]
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA	[RFCnnnn]
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA	[RFCnnnn]
0x00,0x1A	TLS_DH_anon_WITH_DES_CBC_SHA	[RFCnnnn]

This document does not create any new registries to be maintained by IANA, and does not require any new assignments from existing registries.

6. Acknowledgments

The editor would like to thank Steven Bellovin, Uri Blumenthal, Michael D'Errico, Paul Hoffman, Simon Josefsson, Bodo Moeller, Martin Rex, and Len Sassaman for their contributions to preparing this document.

7. References

7.1. Normative References

[DES] National Institute of Standards and Technology, "Data Encryption Standard (DES)", FIPS PUB 46-3, October 1999.

[IDEA] Lai, X., "On the Design and Security of Block Ciphers", ETH Series in Information Processing, v. 1, Konstanz: Hartung-Gorre Verlag, 1992.

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

[SCH] Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd ed., John Wiley & Sons, Inc., 1996.

[TLS10] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[TLS11] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[TLS12] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", draft-ietf-tls-rfc4346-bis-09 (work in progress), February 2008.

7.2. Informative References

[COPA] Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., and M. Schimmler, "Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker", Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006), Yokohama, Japan, October 2006.

[DH] Diffie, W. and M. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard", IEEE Computer, volume 10, issue 6, June 1977.

Author's Address

Pasi Eronen (editor)
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

Email: pasi.eronen@nokia.com

Full Copyright Statement

Intellectual Property

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).