Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 27, 2008.

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 5246). 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 Suite

IDEA (International Data Encryption Algorithm) is a 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 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 this, 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 Suite

IDEA has a 128-bit key, and thus is not vulnerable to exhaustive key search. However, the IDEA cipher suite for TLS has not seen widespread use: most implementations either do not support it, do not enable it by default, or do not negotiate it 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 suite SHOULD NOT be implemented by TLS libraries, and SHOULD be removed from existing implementations.

### 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.
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, Tom Petch, Martin Rex, and Len Sassaman for their contributions to preparing this document.

7. References

7.1. Normative References


7.2. Informative References


Author’s Address

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

Email: pasi.eronen@nokia.com