Transport Layer Security Working Group
INTERNET-DRAFT
Expires October, 1999

John Banes
Richard Harrington
Microsoft Corporation
April 13, 1999

56-bit Export Cipher Suites For TLS

draft-ietf-tls-56-bit-ciphersuites-00.txt

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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.

2. Introduction

This document describes several new cipher suites to be used with the Transport Layer Security (TLS) protocol. Recent changes in US export regulations permit the export of software programs using 56-bit data encryption and 1024-bit key exchange. The cipher suites described in this document take full advantage of these new regulations.

3. The CipherSuites

The following values define the CipherSuite codes used in the client hello and server hello messages.

The following CipherSuite definitions require that the server provide an RSA certificate that can be used for key exchange. The server may request either an RSA or a DSS signature-capable certificate in the certificate request message.

```
CipherSuite TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA     = { 0x00,0x62 };
CipherSuite TLS_RSA_EXPORT1024_WITH_RC4_56_SHA      = { 0x00,0x64 };
```

The following CipherSuite definitions are used for server-authenticated (and optionally client-authenticated) Diffie-Hellman. DHE denotes ephemeral Diffie-Hellman, where the Diffie-Hellman parameters are signed by a DSS certificate, which has been signed by the CA.

```
CipherSuite TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA = { 0x00,0x63 };
CipherSuite TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA  = { 0x00,0x65 };
CipherSuite TLS_DHE_DSS_WITH_RC4_128_SHA            = { 0x00,0x66 };
```

4. CipherSuite definitions

CipherSuite	Is Exportable	Key Exchange	Cipher	Hash
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	*	RSA_EXPORT1024	DES_CBC	SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	*	RSA_EXPORT1024	RC4_56	SHA
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	*	DHE_DSS_EXPORT1024	DES_CBC	SHA
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA	*	DHE_DSS_EXPORT1024	RC4_56	SHA
TLS_DHE_DSS_WITH_RC4_128_SHA		DHE_DSS	RC4_128	SHA

* Indicates IsExportable is True

Key Exchange Algorithm	Description	Key size limit
RSA_EXPORT1024	RSA key exchange	RSA = 1024 bits
DHE_DSS_EXPORT1024	Ephemeral DH with DSS signatures	DH = 1024 bits

Key size limit
The key size limit gives the size of the largest public key that can be legally used for encryption in cipher suites that are exportable.

Cipher	Type	Key Material	Expanded Key Material	Effective Key Bits	IV Size	Block Size
RC4_56	Stream	7	16	56	0	N/A
DES_CBC	Block	8	8	56	8	8

5. Implementation Notes

When an RSA_EXPORT1024 cipher suite is used, and the server's RSA Key is larger than 1024 bits in length, then the server must send a server key exchange message to the client. This message is to contain a temporary RSA key, signed by the server. This temporary

RSA key should be the maximum allowable length (i.e., 1024 bits).

Servers with a large RSA key will often maintain two temporary RSA keys: a 512-bit key used to support the RSA_EXPORT cipher suites, and a 1024-bit key used to support the RSA_EXPORT1024 cipher suites.

When 56-bit DES keys are derived for an export cipher suite, the additional export key derivation step must be performed. That is, the final read and write DES keys (and the IV) are not taken directly from the key_block.

6. References

[TLS] T. Dierks, C. Allen, The TLS Protocol, <draft-ietf-tls-protocol-06.txt>, November 1998.

7. Authors

John Banes
Microsoft Corp.
jbanes@microsoft.com

Richard Harrington
Microsoft Corp.
richha@microsoft.com