

Advanced Encryption Standard (AES) Ciphersuites for Transport Layer
Security (TLS)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This document proposes several new ciphersuites. At present, the symmetric ciphers supported by Transport Layer Security (TLS) are RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), and triple DES. The protocol would be enhanced by the addition of Advanced Encryption Standard (AES) ciphersuites.

Overview

At present, the symmetric ciphers supported by TLS are RC2, RC4, IDEA, DES, and triple DES. The protocol would be enhanced by the addition of AES [AES] ciphersuites, for the following reasons:

1. RC2, RC4, and IDEA are all subject to intellectual property claims. RSA Security Inc. has trademark rights in the names RC2 and RC4, and claims that the RC4 algorithm itself is a trade secret. Ascom Systec Ltd. owns a patent on the IDEA algorithm.
2. Triple DES is much less efficient than more modern ciphers.
3. Now that the AES process is completed there will be commercial pressure to use the selected cipher. The AES is efficient and has withstood extensive cryptanalytic efforts. The AES is therefore a desirable choice.

4. Currently the DHE ciphersuites only allow triple DES (along with some "export" variants which do not use a satisfactory key length). At the same time the DHE ciphersuites are the only ones to offer forward secrecy.

This document proposes several new ciphersuites, with the aim of overcoming these problems.

Cipher Usage

The new ciphersuites proposed here are very similar to the following, defined in [TLS]:

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
```

All the ciphersuites described here use the AES in cipher block chaining (CBC) mode. Furthermore, they use SHA-1 [SHA-1] in an HMAC construction as described in section 5 of [TLS]. (Although the TLS ciphersuite names include the text "SHA", this actually refers to the modified SHA-1 version of the algorithm.)

The ciphersuites differ in the type of certificate and key exchange method. The ciphersuites defined here use the following options for this part of the protocol:

CipherSuite	Certificate type (if applicable) and key exchange algorithm
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_AES_128_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_AES_128_CBC_SHA	DH_anon
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH_DSS
TLS_DH_RSA_WITH_AES_256_CBC_SHA	DH_RSA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE_DSS
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_DH_anon_WITH_AES_256_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].

The AES supports key lengths of 128, 192 and 256 bits. However, this document only defines ciphersuites for 128- and 256-bit keys. This is to avoid unnecessary proliferation of ciphersuites. Rijndael actually allows for 192- and 256-bit block sizes as well as the 128-bit blocks mandated by the AES process. The ciphersuites defined here all use 128-bit blocks.

The new ciphersuites will have the following definitions:

```
CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA      = { 0x00, 0x2F };
CipherSuite TLS_DH_DSS_WITH_AES_128_CBC_SHA   = { 0x00, 0x30 };
CipherSuite TLS_DH_RSA_WITH_AES_128_CBC_SHA   = { 0x00, 0x31 };
CipherSuite TLS_DHE_DSS_WITH_AES_128_CBC_SHA  = { 0x00, 0x32 };
CipherSuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA  = { 0x00, 0x33 };
CipherSuite TLS_DH_anon_WITH_AES_128_CBC_SHA  = { 0x00, 0x34 };

CipherSuite TLS_RSA_WITH_AES_256_CBC_SHA      = { 0x00, 0x35 };
CipherSuite TLS_DH_DSS_WITH_AES_256_CBC_SHA   = { 0x00, 0x36 };
CipherSuite TLS_DH_RSA_WITH_AES_256_CBC_SHA   = { 0x00, 0x37 };
CipherSuite TLS_DHE_DSS_WITH_AES_256_CBC_SHA  = { 0x00, 0x38 };
CipherSuite TLS_DHE_RSA_WITH_AES_256_CBC_SHA  = { 0x00, 0x39 };
CipherSuite TLS_DH_anon_WITH_AES_256_CBC_SHA  = { 0x00, 0x3A };
```

Security Considerations

It is not believed that the new ciphersuites are ever less secure than the corresponding older ones. The AES is believed to be secure, and it has withstood extensive cryptanalytic attack.

The ephemeral Diffie-Hellman ciphersuites provide forward secrecy without any known reduction in security in other areas. To obtain the maximum benefit from these ciphersuites:

1. The ephemeral keys should only be used once. With the TLS protocol as currently defined there is no significant efficiency gain from reusing ephemeral keys.
2. Ephemeral keys should be destroyed securely when they are no longer required.
3. The random number generator used to create ephemeral keys must not reveal past output even when its internal state is compromised.

[TLS] describes the anonymous Diffie-Hellman (ADH) ciphersuites as deprecated. The ADH ciphersuites defined here are not deprecated. However, when they are used, particular care must be taken:

1. ADH provides confidentiality but not authentication. This means that (if authentication is required) the communicating parties must authenticate to each other by some means other than TLS.
2. ADH is vulnerable to man-in-the-middle attacks, as a consequence of the lack of authentication. The parties must have a way of determining whether they are participating in the same TLS connection. If they are not, they can deduce that they are under attack, and presumably abort the connection.

For example, if the parties share a secret, it is possible to compute a MAC of the TLS Finished message. An attacker would have to negotiate two different TLS connections; one with each communicating party. The Finished messages would be different in each case, because they depend on the parties' public keys (among other things). For this reason, the MACs computed by each party would be different.

It is important to note that authentication techniques which do not use the Finished message do not usually provide protection from this attack. For example, the client could authenticate to the server with a password, but it would still be vulnerable to man-in-the-middle attacks.

Recent research has identified a chosen plaintext attack which applies to all ciphersuites defined in [TLS] which use CBC mode. This weakness does not affect the common use of TLS on the World Wide Web, but may affect the use of TLS in other applications. When TLS is used in an application where this attack is possible, attackers can determine the truth or otherwise of a hypothesis that particular plaintext data was sent earlier in the session. No key material is compromised.

It is likely that the CBC construction will be changed in a future revision of the TLS protocol.

Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of other technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the

IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

During the development of the AES, NIST published the following statement on intellectual property:

SPECIAL NOTE - Intellectual Property

NIST reminds all interested parties that the adoption of AES is being conducted as an open standards-setting activity. Specifically, NIST has requested that all interested parties identify to NIST any patents or inventions that may be required for the use of AES. NIST hereby gives public notice that it may seek redress under the antitrust laws of the United States against any party in the future who might seek to exercise patent rights against any user of AES that have not been disclosed to NIST in response to this request for information.

Acknowledgements

I would like to thank the ietf-tls mailing list contributors who have made helpful suggestions for this document.

References

- [TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.
- [AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)" FIPS 197. November 26, 2001.
- [SHA-1] FIPS PUB 180-1, "Secure Hash Standard," National Institute of Standards and Technology, U.S. Department of Commerce, April 17, 1995.

Author's Address

Pete Chown
Skygate Technology Ltd
8 Lombard Road
London
SW19 3TZ
United Kingdom

Phone: +44 20 8542 7856
EMail: pc@skygate.co.uk

Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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

