

AES Ciphersuites for TLS

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>>

Distribution of this document is unlimited. Please send comments to the author (pc@skygate.co.uk) or to the Transport Layer Security Working Group's discussion list (ietf-tls@lists.certicom.com).

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 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 offer reduced key lengths). At the same time the DHE ciphersuites are the only ones to offer forward secrecy.

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

Rationale

Certain of the TLS ciphersuites use an ephemeral Diffie-Hellman key exchange. These ciphersuites provide forward secrecy. The other ciphersuites do not; if either party's key is ever compromised, all the sessions which it secured can be decrypted.

The additional overhead associated with ephemeral Diffie-Hellman is not believed to be significant, and forward secrecy is an extremely desirable property for a system like TLS. For this reason, both the new ciphersuites employ an ephemeral Diffie-Hellman key exchange.

Cipher Usage

The new ciphersuites proposed here are very similar to the following, defined in [\[TLS\]](#).

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

and

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA

Both the ciphersuites proposed in this document use either RSA or DSS certificates. They use the AES in cipher block chaining (CBC) mode. Furthermore, they use 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 AES supports key lengths of 128, 192 and 256 bits. At the present time, all of these are believed to be secure against even the best equipped attackers. The overall strength of TLS is such that there is no gain from using a key length longer than 128 bits. Accordingly the AES will use 128 bit keys.

The new ciphersuites will have the following definitions:


```
CipherSuite TLS_DHE_DSS_WITH_AES_128_CBC_SHA = { 0x00, 0x2F };  
CipherSuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA = { 0x00, 0x30 };
```

TLS implementations SHOULD implement the AES ciphersuites.

Security Considerations

It is not believed that adding these ciphersuites will ever reduce security. The AES is believed to be secure, and it has withstood extensive cryptanalytic attack. The ephemeral Diffie-Hellman ciphersuites provide forward secrecy without any reduction in security in other areas.

Copyright

Copyright (C) The Internet Society 2000. 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 assignees.

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.

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.

One of the authors of Rijndael signed the following disclaimer when submitting the algorithm to NIST for consideration in the AES process:

I, Joan Daemen, do hereby declare that to the best of my knowledge the practice of the algorithm, reference implementation, and mathematically optimized implementations, I have submitted, known as Rijndael may be covered by the following U.S. and/or foreign patents:

none

I do hereby declare that I am aware of no patent applications which may cover the practice of my submitted algorithm, reference implementation or mathematically optimized implementations.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Advanced Encryption Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for inclusion in the Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES). I further understand that I will not receive financial compensation from the government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the AES or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for inclusion in the AES, I hereby agree not to place any restrictions on the use of the algorithm intending it to be available on a worldwide, non-exclusive, royalty-free basis.

I do hereby agree to provide the statements for any patent or patent application identified to cover practice of my algorithm, reference implementation or mathematically optimized implementations and the right to use such implementations for the purposes of the AES evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for inclusion in the FIPS (including those not selected for second round of public evaluation), I understand that all rights, including use rights of the reference and mathematically optimized implementations, revert back to the submitter (and other owner[s] as appropriate). Additionally, should the U.S. Government not select my algorithm for inclusion in the AES after a period of four years from the close of the submission date for candidate algorithms, all rights revert to the submitter (and other owner[s] as appropriate).

[signed]

Title: Cryptographer

Dated: 10-6-98

Place: Brussels

The following disclaimer was signed at the start of the second "round" of the AES process:

Dear Mr Foti [of NIST],

Hereby we confirm that the original patent and patent application information, as provided to NIST with our original submission in June 1998, has not changed. To the best of our knowledge, there are no patents or patent applications covering the practice of the algorithm, reference implementation or the mathematically optimized implementations.

[signed]

Joan Daemen, Vincent Rijmen

Acknowledgements

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

References

[TLS] T. Dierks, C. Allen, "The TLS Protocol Version 1.0" [RFC-2246](#). January, 1999.

[AES] J. Daemen, V. Rijmen, "The Rijndael Block Cipher" <http://csrc.nist.gov/encryption/aes/round2/AESAlgs/Rijndael/Rijndael.pdf> 3rd September 1999.

Author's Address

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

Phone: +44 20 8542 0176
Email: pc@skygate.co.uk

