Abstract

This memo describes two new ciphersuites for the Transport Layer Security (TLS) protocol using the Advanced Encryption Standard (AES) in Synthetic IV (SIV) mode. SIV provides authenticated encryption with associated data (AEAD) and, unlike other AEAD cipher modes, provides resistance to nonce misuse.
Table of Contents

1. Introduction .................................................. 3
   1.1. Requirements Language .................................... 3
2. RSA-based AES-SIV Cipher Suites ................................. 3
3. TLS Versions .................................................... 5
4. IANA Considerations ............................................ 5
5. Security Considerations ......................................... 5
6. Acknowledgements ................................................ 6
7. References ....................................................... 6
   7.1. Normative References ....................................... 6
   7.2. Informative References ..................................... 7
Author’s Address .................................................... 7
Intellectual Property and Copyright Statements .................... 8
1. Introduction

This memo describes TLS ciphersuites based on the use of AES [AES] in SIV [SIV-AES] mode. SIV provides nonce-based authenticated encryption with associated data (AEAD) but unlike other cipher modes provides resistance to misuse of the nonce. It is therefore uniquely suited for applications where the supply of nonces is outside the cryptographic engine or where an application developer is responsible for adhering to any guidelines on nonce use.

Other AEAD cipher modes can outperform SIV in raw throughput but they are somewhat fragile because their security depends entirely on their proper use. In many cases it is desirable to build a robust system that will be secure even in the presence of unintentional programming errors, system misconfiguration, or intentional misuse. In these cases SIV is more appropriate to use than other AEAD cipher modes.

The ciphersuites defined here are used with RSA-based key exchange and can be used in both TLS 1.2 [rfc4346bis] and DTLS [RFC4347].

SIV is well-suited for control plane applications. For example CAPWAP, which uses DTLS to protect communications for the provisioning and management of wireless termination points (WTPs) by access controllers (ACs). This traffic will be processed by a control processor on the AC and will therefore have lessened performance requirements and will most likely be handled by an application process written by a programmer who obtains DTLS services through an API.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. RSA-based AES-SIV Cipher Suites

The ciphersuites defined herein are based on the AES-SIV authenticated encryption with associated data (AEAD) algorithms AEAD.SIV_CMAC_256 and AEAD.SIV_SIV_CMAC_512 to be described in [AEAD]. The following ciphersuites are defined:

CipherSuite TLS_RSA_WITH_AES_SIV_CMAC_256_SHA256 = {TBD1, TBD1}
CipherSuite TLS_RSA_WITH_AES_SIV_CMAC_512_SHA384 = {TBD2,TBD2}

CipherSuite TLS_RSA_DHE_WITH_AES_SIV_CMAC_256_SHA256 = {TBD3,TBD3}

CipherSuite TLS_RSA_DHE_WITH_AES_SIV_CMAC_512_SHA384 = {TBD4,TBD4}  

SIV-AES provides both encryption and authentication using [AES] in [CMAC] mode and [CTR] mode. When the underlying AES cipher uses a 128 bit key SIV-AES takes a 256 bit key as input. When the underlying AES cipher uses a 256 bit key AES-SIV takes a 512 bit key.

The nonce used with these cipher suites MUST be 16 octets. It will be carried in the IV field of the GenericAEADCipher structure, therefore for all the algorithms defined in this section SecurityParameters.iv_length=16.

SIV is resistant to nonce misuse and therefore there is no uniqueness requirement placed on its nonce. If a nonce is reused authenticity is not affected and confidentiality is affected only to the extent that an attacker would know that the same plaintext, same associated data, and same nonce were protected twice with the same key. The nonce is chosen by the sender and is included in the (D)TLS packet. It SHOULD be harvested from a pool having at least 128 bits of entropy but a non-random source MAY also be used, such as a timestamp or counter.

The length of plaintext sent to a ciphersuite defined in this section is indicated by the length in the TLSCompressed structure. The ciphertext output will be expanded by the 128 bits.

The RSA and RSA-DHE key exchange are performed as defined in [rfc4346bis].

Cipher modes like SIV that provide authenticated encryption obviate the need for an explicit MAC of the payload. The use of HMAC for data protection has therefore been replaced but a hash function is still used for the TLS PRF. Each cipher suite defined in this section explicitly specifies the hash algorithm to use with the TLS PRF.

The following ciphersuites SHALL use SHA256 as the TLS PRF hash function:

TLS_RSA_WITH_AES_SIV_CMAC_256_SHA256
TLS_RSA_DHE_WITH_AES_SIV_CMAC_256_SHA256

The following ciphersuites SHALL use SHA384 as the TLS PRF hash function:

TLS_RSA_WITH_AES_SIV_CMAC_512_SHA384
TLS_RSA_DHE_WITH_AES_SIV_CMAC_512_SHA384

3. TLS Versions

The ciphersuites defined in this memo make use of features defined in TLS 1.2 [rfc4346bis]. Therefore they MUST NOT be used with earlier versions of TLS. Clients MUST NOT offer these ciphersuites if they do not also offer TLS 1.2 or later and servers MUST NOT select one of these ciphers if they select an earlier version. Because TLS does not provide a way for a client to indicate it supports version 1.2 but not earlier versions a non-compliant server may negotiate an earlier version but select one of these ciphersuites. Therefore clients MUST check the TLS version and generate a fatal "illegal_parameter" alert if they detect an incorrect version.

4. IANA Considerations

IANA will define the following values for ciphersuites defined in this draft:

CipherSuite TLS_RSA_WITH_AES_128_SIV_CMAC_SHA256 = (TBD1,TBD1)
CipherSuite TLS_RSA_WITH_AES_256_SIV_CMAC_SHA384 = (TBD2,TBD2)
CipherSuite TLS_RSA_DHE_WITH_AES_128_SIV_CMAC_SHA256 = (TBD3,TBD3)
CipherSuite TLS_RSA_DHE_WITH_AES_256_SIV_CMAC_SHA384 = (TBD4,TBD4)

5. Security Considerations

SIV performs authenticated encryption with associated data. A proof of the security of SIV is in [DAE]. The nonce passed to a ciphersuite defined in this memo SHOULD be unique but in the event that a nonce is reused security is retained. For a fuller description see [SIV-AES].
6. Acknowledgements

This memo liberally borrows text and format from [gcm-suites] which itself borrows heavily from [tls-ecc-new-mac] and [suiteb-for-tls]. The editor thanks the authors of those drafts for setting a path that has simply been followed.

7. References

7.1. Normative References


[CMAC] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", NIST Special Publication 800-38B.


7.2. Informative References

[gcmsuites]
Internet-Draft: draft-ietf-tls-rsa-aes-gcm-00 (a work in progress).

[suitebfortls]

[tls ECC new mac]
Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode",

Author’s Address

Dan Harkins (editor)
Aruba Networks

Email: dharkins@arubanetworks.com
Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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 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).