Network Working Group L. Schmertmann
Internet-Draft C. Bormann, Ed.
Intended status: Informational Universitaet Bremen TZI
Expires: August 18, 2014 February 14, 2014

ECDHE-PSK AES-CCM Cipher Suites with Forward Secrecy for Transport Layer Security (TLS)
draft-schmertmann-dice-ccm-psk-pfs-00

Abstract

RFC 6655 describes the use of the Advanced Encryption Standard (AES) in the Counter with Cipher Block Chaining - Message Authentication Code (CBC-MAC) Mode (CCM) of operation within Transport Layer Security (TLS) and Datagram TLS (DTLS) to provide confidentiality and data origin authentication. The AES-CCM algorithm is amenable to compact implementations, making it suitable for constrained environments. It has been chosen as one of the preferred cipher suites for use with DTLS in the Constrained Application Protocol, CoAP.

The present document defines additional cipher suites that provide forward secrecy. It also discusses an option to replace the Hash-based PRF in RFC 6655 by CMAC, reducing the number of cryptographic primitives required for implementation. (The intention is that the option is either chosen or not chosen before this document is agreed, not that both options are defined.)

This document is initially addressed at the DICE working group in order to build consensus that there is an actual gap to be filled and about the technical parameters of a solution for that gap. Once this is agreed, the usual path for agreeing a cipher suite will need to be taken.

Status of This Memo

Table of Contents

1. Introduction 2
   1.1. Terminology 3
2. AES-CCM Cipher Suites with Forward Secrecy 3
3. Option: Replacing the SHA-256 PRF with a CMAC-based PRF 3
4. IANA Considerations 4
5. Security Considerations 4
6. Acknowledgements 4
7. References 5
   7.1. Normative References 5
   7.2. Informative References 6
Appendix A. Recommended Curves and Algorithms 6
Authors' Addresses 7

1. Introduction

[RFC6655] describes the use of Advanced Encryption Standard (AES) [AES] in Counter with CBC-MAC Mode (CCM) [CCM] in several TLS cipher suites. AES-CCM provides both authentication and confidentiality and uses as its only primitive the AES encrypt operation (the AES decrypt operation is not needed). This makes it amenable to compact implementations, which is advantageous in constrained environments. For instance, the use of AES-CCM has been specified for IPsec Encapsulating Security Payload (ESP) [RFC4309] and 802.15.4 wireless networks [IEEE802154].

One of the cipher suites defined in RFC 6655, TLS_PSK_WITH_AES_128_CCM_8, has been made one of the preferred cipher suites for use with DTLS in CoAP, [I-D.ietf-core-coap].

The cipher suites defined in RFC 6655 do not provide forward secrecy (see [RFC4949] for a definition).

The cipher suites defined in this document use Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) as their key establishment mechanism; these cipher suites can be used with DTLS [RFC6347].

Similar to the way [RFC5489] defines ECDHE_PSK cipher suites for RC4, 3DES, and AES, the present document defines equivalents of the cipher suites defined in RFC 6655 (Table 1).

RFC 6655	Forward Secrecy (new)
TLS_PSK_WITH_AES_128_CCM	TLS_ECDHE_PSK_WITH_AES_128_CCM
TLS_PSK_WITH_AES_128_CCM_8	TLS_ECDHE_PSK_WITH_AES_128_CCM_8

Table 1: new ECDHE_PSK ciphersuites using AES-CCM

These cipher suites are only defined for use with TLS version 1.2 and above. They are DTLS-OK.

1.1. Terminology

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. AES-CCM Cipher Suites with Forward Secrecy

The cipher suites defined in this document operate exactly like the equivalent cipher suites defined in [RFC6655], except that the ECDHE_PSK Key Exchange Algorithm from [RFC5489] is used for forming the premaster secret.

3. Option: Replacing the SHA-256 PRF with a CMAC-based PRF

For both the cipher suites defined in RFC 6655 and the ones defined in the previous section, the PRF is the TLS PRF [RFC5246] with SHA-256 as the hash function.

This means that, besides AES encryption and ECDHE, implementations have to provide SHA-256. The option discussed in this section would, if taken, replace the SHA-256-based hash function with an AES-based PRF.

In this section, we propose examining the use of AES-CMAC [RFC4493] as the function underlying the TLS PRF, based on the recommendations in [NISTKDF]. One way to do this (patterned somewhat after [RFC4615], but with a counter that attempts to preserve more of the entropy) is shown in Figure 1.

```
PRF(secret, label, seed) = P_CMAC(secret, label || seed)

P_CMAC(secret, seed) = STEP(0, 0, secret, A(1) || seed) ||
                       STEP(0, 1, secret, A(2) || seed) ||
                       STEP(0, 2, secret, A(3) || seed) || ...
A(0) = seed
A(i) = STEP(1, i, secret, A(i-1))

STEP(v, i, secret, seed) = AES-CMAC(K(v, i, secret), seed)

K(v, i, secret) = AES-CMAC((v || 0^127) + i, secret)
(note that the + is addition)
```

Figure 1: CMAC-based PRF for TLS

P_CMAC can be iterated as many times as necessary to produce the required quantity of data.

Defining such an alternative PRF requires security analysis that is not provided in the present version of this document.

4. IANA Considerations

IANA is requested to assign values for the new ciphersuites defined in Table 1 from the "TLS Cipher Suite" registry.

5. Security Considerations

The security considerations of [RFC5489] and [RFC6655] apply.

If the option to define a CMAC-based PRF is chosen, this section will need to discuss its security considerations.

6. Acknowledgements

This document borrows heavily from RFC 6655.

7. References

7.1. Normative References

[AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001.

[CCM] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", SP 800-38C, May 2004.

[NISTKDF] Chen, L., "Recommendation for Key Derivation Using Pseudorandom Functions", NIST Special Publication 800-108, n.d..

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", RFC 4493, June 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5489, March 2009.

[RFC5639] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, July 2012.

7.2. Informative References

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., and C. Bormann, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18 (work in progress), June 2013.

[IEEE802154]
Institute of Electrical and Electronics Engineers, "Wireless Personal Area Networks", IEEE Standard 802.15.4-2006, 2006.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[RFC4615] Song, J., Poovendran, R., Lee, J., and T. Iwata, "The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4615, August 2006.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

Appendix A. Recommended Curves and Algorithms

This memo does not mandate any particular elliptic curves or cryptographic algorithms, for the sake of flexibility. However, since the main motivation for the AES-CCM-ECC cipher suites is their suitability for constrained environments, it is valuable to identify a particular suitable set of curves and algorithms.

This appendix identifies a set of elliptic curves and cryptographic algorithms that meet the requirements of this note, which are widely supported and believed to be secure.

Where the following recommendations mention a hash function, the hash function does not apply if the option to use CMAC as a PRF is chosen.

The curves and hash algorithms recommended for each cipher suite are:

An implementation that includes either TLS_ECDHE_PSK_WITH_AES_128_CCM or TLS_ECDHE_PSK_WITH_AES_128_CCM_8 SHOULD support the secp256r1 curve and the SHA-256 hash function.

More information about the secp256r1, secp384r1, and secp521r1 curves is available in Appendix A of [RFC4492].

It is not necessary to implement the above curves and hash functions in order to conform to this specification. Other elliptic curves, such as the Brainpool curves [RFC5639] for example, meet the criteria laid out in this memo.

Authors' Addresses

Lars Schmertmann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Email: lars@tzi.de

Carsten Bormann (editor)
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org