AVTCore Working Group                                        J. Lennox
Internet-Draft                                                   Vidyo
Intended status: Standards Track                        March 27, 2017
Expires: September 28, 2017


           **DTLS/SRTP Protection Profiles for 256-bit AES-CTR Encryption**
                  **draft-lennox-avtcore-dtls-srtp-bigaes-00**

Abstract

   This memo defines Datagram Transport Layer Security (DTLS) Secure
   Real-time Transport Protocol (SRTP) Protection Profiles for 256-bit
   Advanced Encryption Standard (AES) Counter Mode.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF).  Note that other groups may also distribute
   working documents as Internet-Drafts.  The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   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."

   This Internet-Draft will expire on September 28, 2017.

Table of Contents

## 1.  Introduction

This memo defines Datagram Transport Layer Security (DTLS) Secure
Real-time Transport Protocol (SRTP) Protection Profiles for 256-bit
Advanced Encryption Standard (AES) Counter Mode.

DTLS-based key establishment for SRTP is defined in [RFC5764].  The
use of AES-256 counter mode with SRTP is defined in [RFC6188].

The draft document that became [RFC5764] initially defined protection
profiles for AES-256; they were removed because the document that
became [RFC6188] was not yet ready.  However, the definitions of the
protection profiles were not transfered to the [RFC6188] drafts,
apparently as an oversight.  This document restores those codepoints,
with their original values.

## 1.1.  Motivation

The question might arise as to why this is necessary.  [RFC7714]
defines the use of AES-256 with Galois Counter Mode, and current
thought is that Galois Counter Mode is preferable to Counter Mode
plus HMAC-based authentication.

The reason is to minimize the difficulty of moving implementations
away from Security Descriptions-based keying [RFC4568].  Use of
Security Descriptions is strongly discouraged, as its security
properties are much weaker than those of DTLS/SRTP.  However, as
[RFC6188] defines Security Descriptions signaling elements for AES-
256-CTR, existing implementations use them to negotiate the use of
these crypto suites, and many of the these implementations do not
have Galois Counter Mode cryptography implemented (or certified).
Thus, defining AES-256-CTR codepoints for DTLS/SRTP allows these
implementations to continue using their existing SRTP cryptography
while moving to a more secure keying protocol.

## 2.  Conventions, Definitions and Acronyms

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 [RFC2119].

## 3.  SRTP Protection Profiles

A DTLS-SRTP SRTP Protection Profile defines the parameters and
options that are in effect for the SRTP processing.  This document
defines the following SRTP protection profiles.

        SRTPProtectionProfile SRTP_AES256_CM_SHA1_80 = {0x00, 0x03};
        SRTPProtectionProfile SRTP_AES256_CM_SHA1_32 = {0x00, 0x04};

The following list indicates the SRTP transform parameters for each
protection profile.  The parameters cipher_key_length,
cipher_salt_length, auth_key_length, and auth_tag_length express the
number of bits in the values to which they refer.  The
maximum_lifetime parameter indicates the maximum number of packets
that can be protected with each single set of keys when the parameter
profile is in use.  All of these parameters apply to both RTP and
RTCP, unless the RTCP parameters are separately specified.

All of the crypto algorithms in these profiles are from [RFC6188].

    SRTP_AES256_CM_HMAC_SHA1_80
            cipher:  AES_256_CM
            cipher_key_length:  256
            cipher_salt_length:  112
            maximum_lifetime:  2^31
            auth_function:  HMAC-SHA1
            auth_key_length:  160
            auth_tag_length:  80
    SRTP_AES256_CM_HMAC_SHA1_32
            cipher:  AES_256_CM
            cipher_key_length:  256
            cipher_salt_length:  112
            maximum_lifetime:  2^31
            auth_function:  HMAC-SHA1
            auth_key_length:  160
            auth_tag_length:  32
            RTCP auth_tag_length:  80

With both of these SRTP Parameter profiles, the following SRTP
options are in effect:

o  The TLS Key Derivation Function (KDF) is used to generate keys to
   feed into the SRTP KDF.

o  The Key Derivation Rate (KDR) is equal to zero.  Thus, keys are
   not re-derived based on the SRTP sequence number.

o  The key derivation procedures from Section 3 of AES_256_CM_KDF
   [RFC6188] are used.

o  For all other parameters, (in particular, SRTP replay window size
   and FEC order) the default values are used.

If values other than the defaults for these parameters are required,
they can be enabled by writing a separate specification specifying
SDP syntax to signal them.

## 4.  Security Considerations

This document defines security mechanisms.  No additional security
issues beyond those of [RFC5764] and [RFC6188] apply.

## 5.  IANA Considerations

IANA is requested to add the SRTP Protection Profiles defined in
Section 3 to the DTLS SRTPProtectionProfile registry.

## 6.  References

### 6.1.  Normative References

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
           RFC2119, March 1997,
           <http://www.rfc-editor.org/info/rfc2119>.

[RFC3711]  Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K.
           Norrman, "The Secure Real-time Transport Protocol (SRTP)",
           RFC 3711, DOI 10.17487/RFC3711, March 2004,
           <http://www.rfc-editor.org/info/rfc3711>.

[RFC5764]  McGrew, D. and E. Rescorla, "Datagram Transport Layer
           Security (DTLS) Extension to Establish Keys for the Secure
           Real-time Transport Protocol (SRTP)", RFC 5764, DOI
           10.17487/RFC5764, May 2010,
           <http://www.rfc-editor.org/info/rfc5764>.

   [RFC6188]  McGrew, D., "The Use of AES-192 and AES-256 in Secure
              RTP", RFC 6188, DOI 10.17487/RFC6188, March 2011,
              <http://www.rfc-editor.org/info/rfc6188>.

6.2.  Informative References

   [RFC4568]  Andreasen, F., Baugher, M., and D. Wing, "Session
              Description Protocol (SDP) Security Descriptions for Media
              Streams", RFC 4568, DOI 10.17487/RFC4568, July 2006,
              <http://www.rfc-editor.org/info/rfc4568>.

   [RFC7714]  McGrew, D. and K. Igoe, "AES-GCM Authenticated Encryption
              in the Secure Real-time Transport Protocol (SRTP)", RFC
              7714, DOI 10.17487/RFC7714, December 2015,
              <http://www.rfc-editor.org/info/rfc7714>.

Author's Address

   Jonathan Lennox
   Vidyo, Inc.
   433 Hackensack Avenue
   Seventh Floor
   Hackensack, NJ  07601
   US

   Email: jonathan@vidyo.com