                  Session Description Protocol (SDP) Attributes for
                    Open Mobile Alliance (OMA) Broadcast (BCAST)
                         Service and Content Protection

Status of This Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Abstract

   This document provides descriptions of Session Description Protocol
   (SDP) attributes used by the Open Mobile Alliance's Broadcast Service
   and Content Protection specification.

Table of Contents

1. Introduction

The Open Mobile Alliance (OMA) Broadcast (BCAST) group is specifying
service and content protection mechanisms for broadcast services over
wireless networks. As part of that specification, several new SDP
attributes are necessary to allow the broadcast server to signal the
service and content protection parameters to clients.

Section 8.2.4 of RFC 4566 [1] requires that new SDP attributes are
registered through IANA with name, contact information, and
description (and other similar parameters). A standards track
specification is RECOMMENDED if the new attribute(s) will have
widespread use and interoperability considerations.

OMA BCAST specifications are expected to be used by broadcast
wireless systems that are based on 3rd Generation Partnership Project
(3GPP) Multimedia Broadcast/Multicast Service (MBMS), 3GPP2 Broadcast
and Multicast Services (BCMCS), and Digital Video Broadcasting -
Handheld (DVB-H). Although this would typically be considered a
"widespread" use, in this case IETF chose to use a non-standards-
track RFC to register the SDP attributes because OMA maintains change
control of the documents that specify the interpretation of the
values in the attributes.

This document provides descriptions of the SDP attributes used in the
OMA BCAST Service and Content Protection specification [2].

2. 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 [3].

3. New SDP Attributes

The following new SDP attributes have been specified:

o   a=bcastversion:<major>.<minor>

o   a=stkmstream:<id of the stkm stream>

o   a=SRTPAuthentication:<id for SRTP authentication algorithm value>

o   a=SRTPROCTxRate:<ROC transmission rate>

See Section 5 for details on IANA considerations.

4. Security Considerations

    In addition to the notes in Section 7 of RFC 4566 [1], the following
    considerations may be applicable:

    The bcastversion parameter indicates the version of the broadcast
    system used for distribution of broadcast content. In case future
    versions indicated by this parameter allow for enhanced or additional
    security features, the bcastversion parameter, if unprotected, could
    be utilized for downgrade attacks.

    The stkmstream parameter provides references to relevant key
    management streams so that receivers can map the media streams to key
    streams and retrieve the necessary keys to decrypt media. As such,
    this parameter could be utilized, if unprotected, for denial-of-
    service (DoS) attacks.

5. IANA Considerations

    Per this document, which follows the guidelines of [5], IANA has
    registered a number of SDP attributes.

5.1. Registration of New SDP Attributes

    IANA has registered a number of OMA BCAST only attributes in the
    Session Description Protocol Parameters registry [1]. The
    registration data, according to RFC 4566 [1] follows.

    The registration templates below refer to the OMA-TS-
    BCAST_SvcCntProtection specification [2].

5.1.1. Registration of the Attribute bcastversion:<major>.<minor>

    Contact: Anja Jerichow <anja.jerichow@nsn.com>

    Phone: +49 89 636-45868

    Attribute name: bcastversion

    Long-form attribute name: BCAST version

    Type of attribute: session level

        This attribute is not dependent on charset.

   Purpose: This attribute specifies the OMA BCAST version
      "bcastversion" value in the format x.y.

   Specification of attribute values: This attribute has a mandatory
      value of the form <major>.<minor>, where <major> and <minor> are
      non-negative decimal numbers. The att-value field is of XML data
      type decimal. For details, see OMA-TS-BCAST_SvcCntProtection,
      Section 10.1.1.

5.1.2. Registration of the Attribute stkmstream:<id of the stkm stream>

   Contact: Anja Jerichow <anja.jerichow@nsn.com>

   Phone: +49 89 636-45868

   Attribute name: stkmstream

   Long-form attribute name: Short Term Key Message stream identifier

   Type of attribute: session level or media level

      The attribute can be at session level, in which case it applies to
      all media streams, or it can be at media level, in which case it
      only applies to the specified media and would overwrite possible
      session-level attributes.

      This attribute is not dependent on charset.

   Purpose: The stkmstream attribute specifies the mapping of Short
      Term Key Message streams to media streams in the SDP.

      Each session or media stream can have multiple stkmstream
      attributes. By comparing the value of this attribute with the
      identifier of each STKM stream, the terminal can figure out which
      one to listen to and process. We note that this attribute is
      optional and hence would not be there for unencrypted media
      streams.

   Specification of attribute values: This attribute has a mandatory
      value of the form <id of the stkm stream>, a unique non-zero
      integer identifying a particular key stream. Numbers are unique
      within a particular SDP session, i.e., no global numbering is
      required. The att-value field is of XML data type unsignedShort.
      For details, see OMA-TS-BCAST_SvcCntProtection, Section 10.1.3.

5.1.3. Registration of the Attribute SRTPAuthentication:<id for SRTP
        authentication algorithm value>

   Contact: Anja Jerichow <anja.jerichow@nsn.com>

   Phone: +49 89 636-45868

   Attribute name: SRTPAuthentication

   Long-form attribute name: SRTP authentication algorithm value
      identifier

   Type of attribute: media level

      This attribute is not dependent on charset.

   Purpose: When SRTP is used, the attribute SRTPAuthentication states
      which authentication algorithm to use.

   Specification of attribute values: Based on [4], the identifier is a
      transform-independent parameter of the cryptographic context for
      SRTP in integer format.

      One of the following three integrity transforms registered for the
      three modes MUST be used: value "2" for RCCm1, "3" for RCCm2, and
      "4" for RCCm3. For details, see OMA-TS-BCAST_SvcCntProtection,
      Section 10.4.

5.1.4. Registration of the Attribute SRTPROCTxRate:<ROC transmission
        rate>

   Contact: Anja Jerichow <anja.jerichow@nsn.com>

   Phone: +49 89 636-45868

   Attribute name: SRTPROCTxRate

   Long-form attribute name: ROC transmission rate

   Type of attribute: media level

      This attribute is not dependent on charset.

   Purpose: When SRTP is used, the attribute SRTPROCTxRate defines the
      ROC transmission rate, R.

Specification of attribute values: The attribute value MUST be a
   decimal integer R between 1 and 65535 inclusive, as specified in
   [4]. If the ROC transmission rate is not included in the
   negotiation, the default value of 1 SHALL be used. For details,
   see OMA-TS-BCAST_SvcCntProtection, Section 10.4.

6. Acknowledgments

Many thanks to Hosame Abu-Amara, Francois Ambrosini, David
Castleford, Miguel Garcia, Alfred Hoenes, Charles Lo, and Uwe
Rauschenbach for their help and support.

7. References

7.1. Normative References

   [1] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
        Description Protocol", RFC 4566, July 2006.

   [2] Open Mobile Alliance, "Service and Content Protection for Mobile
        Broadcast Services", OMA OMA-TS-BCAST_SvcCntProtection-V1_0-
        20071218-D, 2007.

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

   [4] Lehtovirta, V., Naslund, M., and K. Norrman, "Integrity
        Transform Carrying Roll-Over Counter for the Secure Real-time
        Transport Protocol (SRTP)", RFC 4771, January 2007.

7.2. Informative References

   [5] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA
        Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Authors' Addresses

    Lakshminath Dondeti (editor)
    QUALCOMM, Inc.
    5775 Morehouse Dr
    San Diego, CA
    USA

    Phone: +1 858-845-1267
    EMail: ldondeti@qualcomm.com

    Anja Jerichow
    Nokia Siemens Networks GmbH and Co.KG
    Martinstr. 76
    81541 Munich
    Germany

    Phone: +49 89 636-45868
    EMail: anja.jerichow@nsn.com

Full Copyright Statement

Intellectual Property