Multiparty Multimedia Session Control
Internet-Draft
Intended status: Standards Track
Expires: September 27, 2012

S. Zhou, Ed.
T. Tian
Z. Xie
ZTE Corporation

March 26, 2012

Security Descriptions Extension for Media Streams
draft-zhou-mmusic-sdes-keymod-01

Abstract

This document provides an extension to the cryptographic attribute (RFC 4568) defined for Session Description Protocol (RFC 4566) to enhance end-to-end communication security, so that some scenarios, e.g., forking and re-targeting can especially benefit from the extension. The usage of the provided extension in Secure Real-time Transport Protocol (SRTP, RFC3711) is also defined in this document.

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 27, 2012.

Table of Contents

1. Introduction

To ensure the media security established by Session Initiation Protocol (SIP), SDP Security Descriptions (SDES) is defined in RFC 4568 [RFC4568], where a cryptographic attribute and application in Secure Real-time Transport Protocol (SRTP,RFC 3711 [RFC3711]) unicast media streams are provided.

SDP Security Descriptions (SDES) is essentially a key transportation scheme in offer/answer model, in which keying material for the direction from offerer to answerer is chosen independently by the offerer and transported in clear text, the keying material for the reverse direction is also chosen independently by the answerer and transported in clear. Later the transported keying materials are provided to SRTP protocol to secure outgoing or incoming media communication. The protection of the transported keying materials obviously relies on the security of the signaling protocol which is beyond the scope of this document.

When SDES is applied in some scenarios,e.g., forking and re-targeting, the intermediate users and devices besides the ultimate answerer also have knowledge of the keying material used for the outgoing media from the offerer, which is a security threat to the content of the end-to-end communication in the affected direction.

To resolve the problem, it is suggested exchanging a new pair of offer/answer with a new key between the offerer and the ultimate answerer,i.e., by using SIP UPDATE message[RFC3311], but it will require more round trip messages. In this document, a resolution is introduced based on the defined SDES extension.

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. Extension to SDES

Following the ABNF format in Security Descriptions, a new session parameter extension "keymod" is defined as follows:

```
srtp-session-extension   =  keymod
keymod                   = "keymod:" <keymod-info>
keymod-info              = <keymod-type> "|"<kdf-func>"|"<keymod-val>
keymod-type              = "rand"/"rand-salt"/keymod-type-ext
keymod-type-ext          = 1*(VCHAR)
kdf-func                 = 1*(ALPHA / DIGIT / "_")
keymod-val               = *(base64);base64 encoded binary string
base64                   = ALPHA/DIGIT/"+"/"/"/"="
```

where base64 encoding follows RFC3548 [RFC3548], ALPHA, DIGIT, and VCHAR are defined in RFC4234 [RFC4234].

The defined "keymod" is a negotiated parameter, which indicates it does not apply to data sent from the answerer to the offerer, as defined in RFC 4568 [RFC4568].

An answer MAY contain keymod value indicating the answerer is asking for the offerer to refresh its keying material using the information following it.

If keymod-type is "rand", then only master key is requested to refresh according to specified function kdf-func;

If keymod-type is "rand-salt", then master key and master salt are both requested to refresh, the master key will be refreshed according to specified function kdf-func and the refresh method of master salt is simply replacement in this document.

The key derivation fumction kdf-func can be as simple as an assignment(defined as "is"), or an XOR between the old master key and the keymod-val value(defined as "xor"), or as complicated as any other key derivation functions based on cryptographic primitives, e.g., RFC 2104 [RFC2104].

In this document, only the two simple functions are defined:"is" and "xor", that is

```
kdf-func =          "is"/"xor"/kdf-func-ext

kdf-func-ext=       1*(ALPHA / DIGIT / "_")
```

And if no kdf-func is indicated in keymod-info, the default kdf-func is "is".

3. Usage of keymod with Offer/Answer

3.1. Generating the Initial Offer - Unicast Streams

The generation of the initial offer for a unicast stream MUST follow that of the crypto attribute RFC4568 [RFC4568], and MAY

also include an additional "keymod" parameter with keymod-val being NULL. It indicates to the ultimate answerer that the offerer wants to employ the mechanism specified in

this document, a key agreement mechanism with a higher security level than the original SDES.

3.2. Generating the Initial Answer - Unicast Streams

The generation of the initial answer for a unicast stream MUST follows that of the crypto attribute RFC4568 [RFC4568], and if the offer message includes a "keymod" parameter, it SHOULD also include an additional "keymod" parameter. That is, when an offered crypto attribute is accepted, the crypto attribute in the answer MUST contain the following:

- The tag and crypto-suite from the accepted crypto attribute in the offer (the same crypto-suite MUST be used in the send and receive direction).

- The key(s) the answerer will be using for media sent to the offerer.

Additionaly the answer MAY contain:

- The keymod parameter for media sent from the offerer to the answerer.

The keymod parameter is constrained by the following limits:

- If keymod type is "rand", the keymod-val value MUST be at the minimum length required by the specified crypto-suite for the master key.

- If keymod type is "rand-salt", the keymod-val value length MUST be no less than the addition of the minimum lengths of master key and master salt required by the specified crypto-suite.

The keymod parameter and the master key retrieved from the offer message MAY be used together to derive a new master key used for the media from the offerer to the answerer.

3.3. Procesing of the Initial Answer - Unicast Streams

When the offerer receives the answer, the offerer MUST do necessary verifications following RFC 4568 [RFC4568].

If the answer includes a "keymod" value in "crypto" attribute, the offerer MUST derive a new master key from the previous master key sent in the offer message and the keymod-info value received in the answer message.

Specifically, if the keymod type retrieved from the answer message is "rand", a new master key will be derived from the previous master key and the keymode-val value according to specified key derivation function kdf-func.

If the keymod type retrieved from the answer message is "rand-salt", a new master key will be derived from the previous master key and the keymode-val value according to specified key derivation function kdf-func, and the master salt will be replaced with the salt value contained in the keymode-val.

The derived new master key and new master salt will be used to protect the media from the offerer to the answerer.

4. Example

This example shows use of the keymod extension described in this document. The "a=crypto" line is actually a one long line, which is shown as two lines due to page formatting.

The following is an offer using crypto attribute indicating deploying keymod, asking the answerer to return a keymod value :

```
v=0
o=alice 2890844730 2890844731 IN IP4 host.example.com
s=
c=IN IP4 192.0.2.1
t=0 0
m=audio 20000 RTP/AVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_80
  inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
  keymod:rand|xor|
```

The following is an answer with the keymod extension where type "rand" is chosen and the refreshment of master key is "xor":

```
v=0
o=Bob 2890844725 2890844725 IN IP4 host.example.org
s=
c=IN IP4 192.0.2.2
t=0 0
m=audio 30000 RTP/AVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
 inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32;
 keymod:rand|xor|WVNfX19zZW1jdGwgKCkgew==
```

The following is an answer with the keymod extension where type "rand-salt" is chosen and the refreshments of master key and master salt are both "is":

```
v=0
o=Bob 2890844725 2890844725 IN IP4 host.example.org
s=
c=IN IP4 192.0.2.2
t=0 0
m=audio 30000 RTP/AVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
 inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32;
 keymod:rand-salt|WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz
```

5. Applicability in Re-targeting Scenarios

In this section, applicability of the defined keymod parameter in re-targeting scenarios is provided.

Re-targeting, or Communications Diversion (CDIV) service is a widely used communication service which enables a served user to divert the communications addressed to the served user's address to another destination according to the specified service type. As define in RFC 4458 [RFC4458] and 3GPP TS 24.604 [TS], there are several conditions that may incur a CDIV service, e.g., when the served user is at the statuses of "Not reachable" , "User busy", "No reply", or the served user has registered with the CDIV Agent Server (AS) to redirect the call unconditionally.The redirected destination may be another call number or a voice mailbox of the same user. CDIV may happen multiple times consecutively till the last destination, see the example below.

5.1. Single CDIV instance

See Figure 1, A initiates a call to B by including a crypto attribute with a key parameter K1 and an empty KEYMOD1 in the SIP message. B has subscribed a CDIV service to divert calls to C. When the

diversion condition is met, the call is re-invited by the Proxy or CDIV AS to C. Proxy sends re-invite SIP message which includes K1, KEYMOD1 and an additional "cause" value to C (the usage and the specification of the CAUSE parameter refers to RFC 4458 [RFC4458] , then C determines it a CVID call and responds with a SIP message with a key parameter K2 and a keymod parameter KEYMOD2. When A receives the SIP message including K2 and KEYMOD2, A will derive a new key parameter K1' from K1 and KEYMOD2 the same way as C. Thus the communication between A and C is protected by K2 and K1', i.e., A uses K1' to protect the media sent from A to C, and C uses K2 to protect the media sent from C to A.

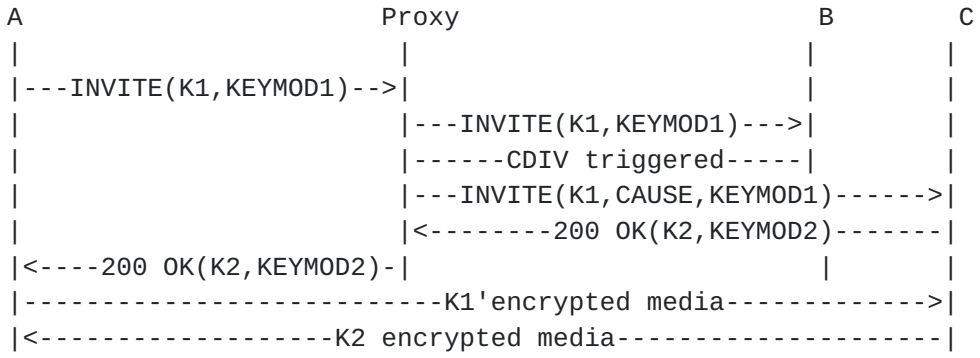

Figure 1

5.2. Multiple CDIV instances

See Figure 2, A initiates a call to B by including a crypto attribute with a key parameter K1 and an empty KEYMOD1 in the SIP message. B has subscribed a CDIV service to divert calls to C. When the diversion condition for B is met, the call is re-invited by the CDIV AS to C. C has also subscribed a CDIV service to divert calls to D. When the diversion condition for C is met, the call is re-invited by the Proxy or CDIV AS to D. Proxy sends re-invite SIP message which includes K1, KEYMOD1 and an additional "cause" value to D (the usage and the specification of the CAUSE parameter refers to RFC 4458 [RFC4458], then D determines it a CVID call and responds with a SIP message with a key parameter K2 and a keymod parameter KEYMOD2. When A receives the SIP message including K2 and KEYMOD2, A will derive a new key parameter K1' from K1 and KEYMOD2 the same way as D. Thus the communication between A and D is protected by K2 and K1', i.e., A uses K1' to protect the media sent from A to D, and D uses K2 to protect the media sent from D to A.

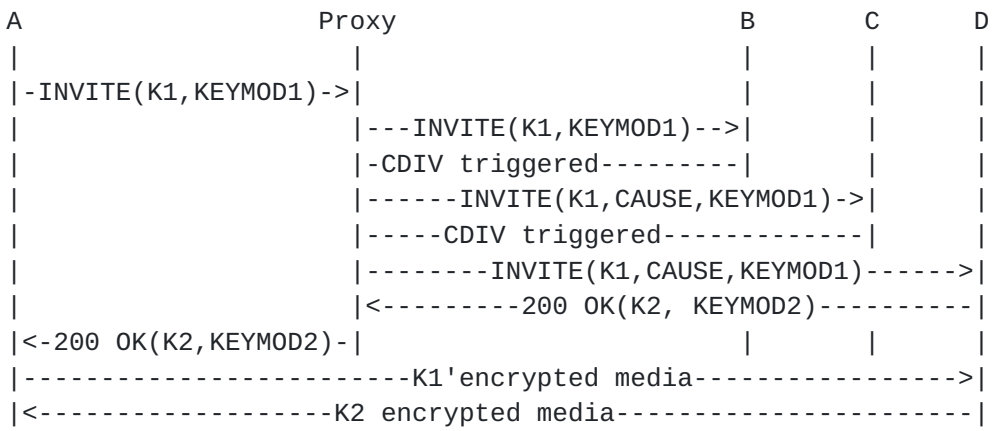

Figure 2

5.3. Computation of K1'

n the above examples, if key method "inline" is used in key parameter. K1 consists of a master key msk1 and a master salt mss1, K2 consists of a master key msk2 and a master salt mss2.

If keymod type is "rand", the keymod-val contained in KEYMOD2 is used to calculate the new master key:

msk1'=kdf-func(keymod-val, msk1)

If keymod type is "rand-salt", the keymod-val contained in KEYMOD2 can be divided into two parts, key and salt, a new master key will be calculated as:

msk1'=kdf-func(keymod-val(key), msk1)

and a new master salt will be:

mss1'=keymod-val(salt).

6. Applicability in Forking Scenarios

In this section, applicability of the defined keymod parameter in forking scenarios is provided, see the example below.

See Figure 3, A initiates a call to a user U by including a crypto attribute with a key parameter K1, an empty KEYMOD1 in the SIP message. And U has multiple devices, e.g., B,C,D, then the call is forked to all the devices till user U answers the call from D. D responds with a SIP message with a key parameter K2 and a keymod parameter KEYMOD2. When A receives the SIP message including K2 and

KEYMOD2, A will derive a new key parameter K1' from K1 and KEYMOD2 the same way as D. Thus the communication between A and D is protected by K2 and K1', i.e., A uses K1' to protect the media sent from A to D, and D uses K2 to protect the media sent from D to A. The computation of K1' is exactly the same as in Section 5.3

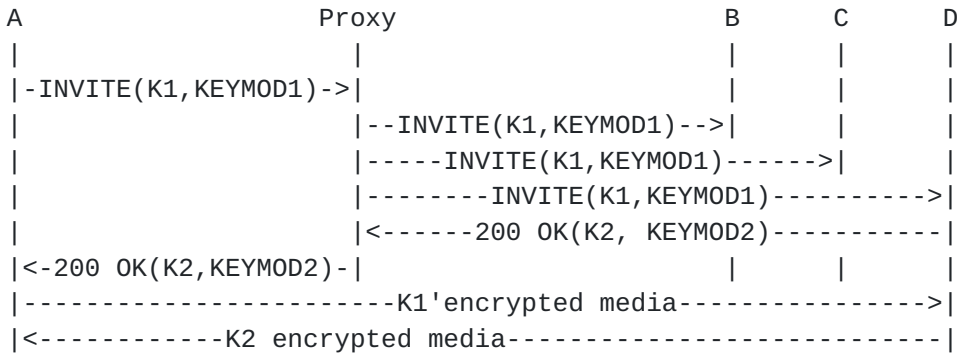

Figure 3

7. IANA Considerations

This document includes no request to IANA.

8. Security Considerations

This document includes an extension to the crypto attribute defined inRFC 4568 [RFC4568], so the security considerations are mostly the same, except that the described solution improves a security drawback when RFC 4568 [RFC4568] is applied in some specific scenarios, i.e., forking and re-targeting.

9. References

9.1. Normative References

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

[RFC3548] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 3548, July 2003.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC4234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, July 2006.

9.2. Informative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[RFC4458] Jennings, C., Audet, F., and J. Elwell, "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)", RFC 4458, April 2006.

[TS] "3GPP TS 24.604 Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

Authors' Addresses

Sujing Zhou (editor)
ZTE Corporation
No.68 Zijinghua Rd. Yuhuatai District
Nanjing, Jiang Su 210012
R.R.China

Email: zhou.sujing@zte.com.cn

Tian Tian
ZTE Corporation
No.68 Zijinghua Rd. Yuhuatai District
Nanjing, Jiang Su 210012
P.R.China

Phone: +86-025-5287-7867
Email: tian.tian1@zte.com.cn

Zhenhua XIe
ZTE Corporation
No.68 Zijinghua Rd. Yuhuatai District
Nanjing, Jiang Su 210012
P.R.China

Phone: +86-25-52871287
Fax: +86-25-52871000
Email: xie.zhenhua@zte.com.cn