MSDES: More SDES Key Agreement for SRTP

S. Puangpronpitag and P. Kasabai

***Abstract*—SRTP has been designed to provide confidentiality, message authentication and replay protection to the RTP traffic. It is very useful for protecting against voice and video stream eavesdropping. However, a good key management protocol is needed to support SRTP. SDES, ZRTP, and DTLS-SRTP have been proposed as keying protocols. Yet, from the literature, all of them have some drawbacks. So, in this paper, we propose a technique to enhance the SDES protocol to be more secure.**

***Index Terms*—VoIP keying protocol, SDES, SRTP, VoIP security**

I. Introduction

Session Initiation Protocol (SIP)[1]is a signalingprotocol, widelyused for controllingmultimediacommunication sessions such as Voice over InternetProtocol (VoIP). The protocolcanbeused for creating, modifying and terminating sessions with one or more participants. The SIP protocol is an applicationlayer protocol designed for independent transports.It can work on both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Similar to the Hypertext Transfer Protocol (HTTP), it is a text-based protocol. Media communications in SIP applications are carried over another application protocol, namelyReal-time Transport Protocol (RTP). For these media streams, parameters including port numbers, protocols and CODECs are defined and negotiated usingSession Description Protocol (SDP), which is transported in the SIP packet body.

Any voice and video stream communication involves risks, such as voice/video eavesdropping, as shown in [2]-[4].The risk results from that RTP exchanges packets in clear-text.For this reason, a Secure RTP (SRTP [5]) has been designed to provide confidentiality, message authentication and replay protection to the RTP traffic.

However,keys provided by some key management protocols such as SDES[6], ZRTP[7], DTLS-SRTP[8] raises some major issues concerning the key protection. In this regard, this paper discusses the way in which the SDES used for keying protection can be enhanced.

The paper comprises five sections. Following this section (Introduction), Section II reviews related work. Section III then outlines motivations underpinning this work. After that, Section IV presents our design to enhance SDES. Section V discusses the experimentalevaluation, and section VI concludes the paper respectively.

II. Related Work

Thekey disadvantages of VoIP concerns the security protocols.VoIP sessions can be attacked where the information transported could be interceptedby the third party using a technique known as a Man in the Middle (MitM).Thetechnique is popular among hackers, and the tools required are available on the Internet. These tools include Cain and Abel [9] and Backtrack [10].

The voice and video stream communication over the RTP can be MitM attacked and cause further problems, such as voice/video eavesdropping, RTP payload spoofing and RTP tampering. Concerning the problems, SRTP has been designed to protect the RTP traffic.

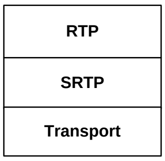

Fig. 1. SRTP “bump in the stack”.

SRTP is seen as a “bump in the stack” (see Fig. 1) functioning as the implementedactionbetween the RTP layer and the transport layer.The protocol provides an extension to the RTP packet format to encrypt the RTP payload. Bydoing so, itgives confidentiality, a message authentication, and a replay protection to the RTP traffic. In order to do so,SRTP uses two types of keys, namely a session key and a master key. These keys are provided by a key management protocol. The master key, salts, and other parameters in the cryptographic context are also provided by the key management protocol, such asSDES, ZRTP, or DTLS-SRTP. As reviewed in the literature, these key management protocols remain as the major issues requiring further work to improve their keying protection.

```
INVITE sip:600@202.28.33.51 SIP/2.0
Via: SIP/2.0/UDP
10.115.0.84:17312;branch=z9hG4bK-d8754z-e90fd842af615f4f-1---d8754
z-;rport
Contact: <sip:1001@10.115.0.84:17312>
To: “600”<sip:600@202.28.33.51>
From:”1001”<sip:1001@202.28.33.51>;tag=ab007
Call-ID:OGI4YmFiNWQwYTJkZWEwMGYwODgwZTIzNzc.
CSeq: 1 INVITE
Content-Type: application/sdp

v=0
o=- 9 2 IN IP4 10.115.0.84
c=IN IP4 10.115.0.84
t=0 0
m=audio 8638 RTP/SAVP 107 0 8 18 101
a=crypto:1
AES_CM_128_HMAC_SHA1_80inline:kNprFcrbtufQT3U+mWrMVSId
FYbRLi0lijM8ARi|2^20
```

Fig. 2. SIP/SDP.

Session Description Protocol Security Descriptions for

Manuscript received June 20, 2012; revised August 5, 2012.

S. Puangpronpitag is with the Department of Computer Science, Faculty of Informatics, Maharakham University (e-mail: somnukp@isan.msu.ac.th, piyawad.k@isan.msu.ac.th).

media streams (SDES) is known as a way to negotiate the key for SRTP. The keys transported in the SDP attachment of a SIP message. SDES defines a new attribute, called "*crypto*". The attribute is used to negotiate cryptographic parameters for SRTP streams. Also, SDES transports the encryption and authentication algorithms, master key and salts of a sender as well as a lifetime of the master key, as shown in Fig 2.

Furthermore, the MitM attack is also identified as another problem for SDES since it can access the cryptographic parameters. In this regard, SDES can be claimed to provide the least secured keying protocols compared with that provided by either ZRTP or DTLS-SRTP, as proposed in[4].

ZRTPis a keying exchange protocol using a Diffie-Hellman technique. Despite the use of the technique, ZRTP can still be attacked by MitM using an ARP spoofing, as seen in[4], [11].

DTLS-SRTP is designed to exchange the keys and negotiate the RTP format to suite the DTLS[12]. By doing so, the information transported is protected by the SRTP while the DTLS performs tasks such as negotiating the keys and other materials used within SRTP. Public Key Infrastructure (PKI) is required for DTLS to fulfill such tasks. Despite employing the PKI, DTLS can still be intercepted by a third party using a fakecertificate. Also, it has not yet fully implemented.

III. Motivation

Information interceptions on the VoIP can simply be done by using available tools such as Cain & Abel and Backtrack. To prevent such interception, various keying protection techniques are proposed in literature. However, such techniques have not yet efficiently solved the problem. In this paper, we therefore investigate how to enhance SDES key protection protocol (the most widely used key management protocol) in order to protect the information from MitM.

IV. Our MSDES Design

SDES is a keying exchange technique in SIP while a new SDP attribute, knownas "crypto", is identified and used to negotiate cryptographic parameters for the SRTP. However, it does not provide sufficient security. Further security requirements may be TLS or IPSec. However, both of them cost a serious overhead at SIP agents. In particular, TLS has a high cost related to the need of Certificate Authority (CA).

Even worse, SIP is usually communicated in a clear-text format where, obviously, the keying exchange protocol such as SDES provides insufficient security, as seen in the following attribute:

a=crypto: <tag> <crypto-suite> inline: <key||salt> [session-parms]

The *tag*field is a unique numeric used as an identifier by answerer to indicate, which crypto attribute is acceptable. The *crypto-suite* field is described encryption and authentication transforms, witch to be used for SRTP media streams. The *key||salt*are key information deriving from concatenating master key and salt,and then converting to a base64 format. The *session-parms*areoptional session parameters (i.e. master key lifetime, etc).

The crypto-suites are defined by SDES, using AES and SHA1 to provide encryption and authentication, respectively. These crypto-suites can be demonstrated as follows:

AES_CM_128_HMAC_SHA1_80,
AES_CM_128_HMAC_SHA1_32, and
F8_128_HMAC_SHA1_32.
(more detailscan be found in[6]).

While the same crypto-suite is used by both the offerer and answerer, the same keys and salts are not used by each side. Therefore, each side will generate and pass these parameters using SDP. At this point,the other data security protocol (i.e.SIP on TLS) should be used in order to provide confidentiality for the SDP messages.

In general, the attribute "crypto" in SDES is transported in a clear-text format. For this reason, the research underpinning this paper has been carried out using MSDES security technique. It encrypts the information transported using User Agent Password (UAP), which is used in the SIP proxy registration. The key-info (key||salt) encryption for the keys is performed using UAP as follows:

a=crypto: <tag> <crypto-suite> inline: E(uap, <key||salt>) [session-parms]

In the experiment, SIP proxy functioned as the key management using the UAP of the User Agent Client (UAC) and the User Agent Server (UAS), as seen in Fig. 2.

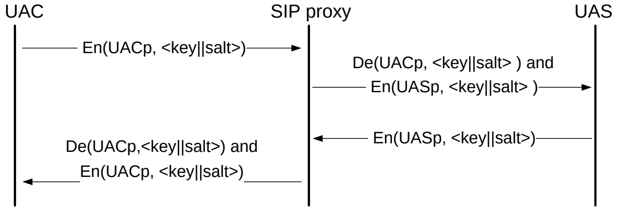

Fig. 3. Encrypted key in SDP.

As presented in Fig. 3, the UAC starts the information transport by an inline encryption using UAC password, and *<crypto-suite>* encryption algorithm (i.e. AES 256 bits). After that, the SIP proxy encrypts the password using an UAS password for the information transportation. The encryption is also performed once when the information has reached the UAS. This process facilitates the exchange of cryptographic parametersto make the SRTP morese cured. So, it isprotectedfrom MitM although the SIP is transported in a clear-text format.

V. Experimental Evaluation

This research has developed a technique for the keying exchange protocol to be used for the SRTP by enhancing SDES. We name this new keying protocol as MSDES (More SDES). The implementation is done by using JAVA (JDK 1.6) and JAIN. There are two modules: one is for the SIP proxy while the other module is for the SIP client. The efficiency of this system design has been evaluated in comparison to SDES, ZRTP, and DTLS-SRTP, using the following indicators.

A. *Signal Confidentiality Requirement (Sig. Conf.)*

This indicator is used to evaluate whether the key exchange protocols need the other confidentiality implementation, such as IPSec or TLS.

B. SIP Forking

In general, SIP *forking* is used to send an invitation (INVITE) to multiple locations of user registrations. This can happen where the user accessesto the communication from various locations, such as from home and from the office at the same time.

Where *fork* happens in *n* locations and registers to the use of SRTP, the master key would be sent repeatedly to each of the locations. However, there would only be one location activating the communication; all other locations, *n-1* spots, would be disconnected from this transport.

In spite of the design, those *n-1* locations would be granted the master key, whichleakage of the key canobviously happen.

C. Media before SDP Answer (Media Clipping)

When the UAC generates anINVITE message as the start to the session, this is called an *offer*. The UAS then provides anothermessage called an *answer*, which the user would have to prepare for the reception of the media in the format requested.

However, the choice of the format is for the receiver. In case that the RTP is sent before the reception of 200OK, the user requesting the media would not be able to know either the RTP attributes or the location where the media is sent. This would lead to a problem known as “media clipping”.

D. Shared-Key Conferencing

Any conference has the central of system control, calledSIP-relatedconferencing. This feature controls the participations and the functions of all participants such as when they join (JOIN) or leave (LEAVE) the conference. The separation of keys for each pair of the participants would cause the*Conference Bridge* to overload. Also, some complication of the keys management can occur. Therefore, concerning these problems, shared keys are proposed to help.

E. Session Recording

In terms of business practice, some business wants to record their conversationsmade with the clients to serve various purposes, including those of training and service improvement.

F. Man in the Middle (MitM) Attack

The interceptions of information transportation are able not only to seize the information being sent but also to record the information. So, a good keying protocol has to protect against this problem. Also, to provide such as protection, some protocols may need to depend on PKI, which would be complicated and costly. Even worse, PKI can be attacked using a spoof certificate as mentioned before.

VI. Experimental Result

A. Summary of Feature Set

From TABLE Iif SDES is used as a key management protocol, forking and media clipping remain problematic. If ZRTP and DTLS-SRTP are used as a key management protocol, shared-key conferencing and session recording remain problematic. However, three key management protocols (SDES, ZRTP and DTLS-SRTP) are subjective to key interception issue.

However, in feature forking,the design of MSDES can protect key leakage because key parametersare encrypted by our technique. Furthermore, the MSDES does not require confidentiality of signaling.

TABLE I: Summary Table.

Indicators	SDES	ZRTP	DTLS-SRTP	MSDES
Sig. Conf.	Yes	No	No	No
Forking	Key leakage	Yes	Yes	No Key leakage
Media Clipping	Yes	No	No	Yes
Shared-key conferencing	Yes	No	No	Yes
Session Recording	Yes	No	No	Yes
Using PKI	No	No	Yes	No

B. MitM Protection Effectiveness

MitM attacks remain the key concern for every key management protocol mentioned previously [2], [4], [11]. The concern indicates that SDES, ZRTP, DTLS-SRTP have not yet been able to prevent the MitM intercepting the information transportation. Among these key-management, protocols, SDES is most likely to be attacked. A technique proposed to prevent the attack is SIPS. However, as shown in [9], still, SIPS could possibly be attacked by MitM. The design of experimental scenarios on a test-bed to test the attack of MitM has shown in Fig. 4.

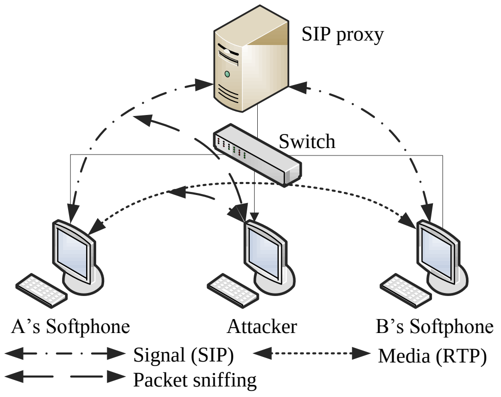

Fig. 4. MitM scenario.

Cain and Abel is used as an attacking tool. From our experiments, when a communication is made using RTP, there is an obvious voice interception. However, once there is a protection provided by SRTP (key management with MSDES), the test shows that there is no interception compared with the use of SDES with signalconfidential, as the SIP presented in TABLE II

TABLE II: SDES and MSDES MitM.

Criteria	SDES		MSDES	
	SIP	SIPS	SIP	SIPS
MitM attack	✓	✓*	×**	×

✓: Attacks are possible ×: Attacks are impossible (Not a problem)
* Attacks are possible, mitigated through certificates
** Attacks must rely on SIP hash brute-force.

C. Experiments on SIP-Hashed UA Password Brute-Force

Since MSDES canprotectthe master key and salt by using anUA password, a possible attack on MSDES is brute-forcing the SIP hashed UA password. So, we have done a further experimental set to analyze this weakness. Aspresented in TABLE III,a test conductedbyCain&Abel is performed on aMicrosoft Windows 7 PC equipped withan Intel Core i5 750 @2.67 GHz and 4.00 GB of RAM.

The test utilizeda password of 6characters comprisingnumbers, small caps, small caps&all caps, number&small caps number&smallcaps&all caps. Each of these password components is predefined as thebest caseaccording to the time it is cracked.

TABLE III: BRUTE-FORCE SIP HASHES.

Password	Predefined	Cracked time
534567	0123456789	2.50 (sec)
gftkhy	abcdefghijklmnopqrstuvwxyz	3.43 (minute)
HiVdfP	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ	3.21(hours)
45gh8f	abcdefghijklmnopqrstuvwxyz0123456789	7 (minute)
3sK9gA	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789	8.52 (hours)
5Zq*y9xI	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=	>) 24hours(

As shown in theTABLE III, a password comprising complex components (with 8 characters long or more) shows aless possibilityto be attacked using the brute-force technique. Furthermore, this possibility could be none when a PC is used. Hence, we suggest the users of MSDES to set good UA passwords for their clients.

VII. CONCLUSIONS

This paper delivers an enhancement of the key protection management using SDES,the most widely used key agreement protocols. With respect to the key leakage problem, the MSDES, proposed by this research, has confirmed a more secured media keying protocol. Also, it can be performed using less overhead and costs compared with ZRTP and DTLS-SRTP, the two widely known keying protections, yet remain challenged by the problem of keys interception.

ACKNOWLEDGEMENT

This work is supported by Mahasarakham University, Thailand Research Fund and Nation Research Council of Thailand.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Spark, M. Handley, and E. Schooler, "SIP: Session initiation protocol," *IETF RFC*, vol. 3261, June 2002.

[2] P. Gupta and V. Shmatikov, "Security analysis of voice-over-IP protocols," In *Proceeding of the IEEE Computer Security Foundations Symposium*, pp. 49-63, July 2007.

[3] D. Butcher, L. X. Yang, and G. H. Jin, "Security challenge and defense in VoIP infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics (Part C: Applications and Reviews)* vol. 37, no. 6, pp. 1152-1162, November 2007.

[4] K. Gurbani and V. Kolesnikov, "A survey and analysis of media keying techniques in the session initiation protocol (SIP)," *IEEE Communications Surveys and Tutorials*, 2010, vol. 99, pp. 1-16.

[5] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The secure real-time transport protocol (SRTP)," *IETF RFC*, vol. 3711, March 2004.

[6] F. Andreasen, M. Baugher, and D. Wind, "Session description protocol (SDP) security descriptions for media streams," *IETF RFC*, vol. 4568, July 2006.

[7] P. Zimmermann, A. Johnson, and J. Callas, "ZRTP: Media path key agreement for unicast secure RTP," *IETF RFC*, vol. 6189, April 2011.

[8] D. Mcgrew and E. Rescorla, "Datagram transport layer security (DTLS) extension to establish keys for the secure real-time transport protocol (SRTP)," *IETF RFC*, vol. 5764, May 2010.

[9] Oxid.it. "Cain and Abel," [vol. 8 January 2010]. [Online]. Available: http://www.oxid.it/cain.html.

[10] M. Moser, M. Aharoni, and J. Muench, "Remote-exploit," [vol. 8 January 2010]. [Online]. Available: http://www.remote-exploit.org/.

[11] M. Petraschek, T. Hoeher, and O. Jung, "Security and usability aspects of man-in-the-middle attack on ZRTP," *Journal of Universal Computer Science (JUCS)* 2008, vol. 14, pp. 673-692.

[12] E. Rescorla, Inc. RTFM, and N. Modadugu, "Datagram Transport Layer Security," *IETF RFC*, vol. 4347, April 2006.

Somnuk Puangpronpitag received the Ph.D. in Computer Network from the University of Leeds, UK. He is currently a director of Information Technology and Advanced Network (ISAN) research laboratory. He is also an Associate Dean for Research & International Affairs, Faculty of Informatics, Mahasarakham University, and an IT crime specialist for the department of justice, Thailand. Hisresearch interests include network performance engineering, network security and applied cryptology.

Piyawad Kasabai is a research assistant of ISAN Lab, Mahasarakham University, Thailand. He received the master degree inInformation Technology from Mahasarakham University. Hisresearch interests include computer network, network security and Voice over IP (VoIP) security.