A New Negotiation Mechanism for Cryptographic Capabilities in SIP based Secure VoIP Service Using Priority

JOONGMAN KIM YOOJAE WON JAEIL LEE
IT Infrastructure Protection Division
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, Korea 138-803
KOREA
seopo@kisa.or.kr yjwon@kisa.or.kr jilee@kisa.or.kr

Abstract: - MIKEY(Multimedia Internet KEYing) has been proposed as a key management protocol for secure multimedia communication, which the security protocol (Secure RTP) for media encryption has considered. Since initiator and responder have different cryptographic capabilities, a negotiation mechanism, which can enable them to communicate each other securely, is required. But previous negotiation methods have several problems, which cannot satisfy backward compatibility and determine their favorite cryptographic capabilities. So we propose new negotiation mechanism, which can solve these problems using priority.

Key-Words: - VoIP, SIP, SRTP, MIKEY, Cryptographic Capability, Negotiation Mechanism, Priority

1 Introduction

SIP(Session Initiation Protocol)[1] as a standard protocol of IETF(Internet Engineering Task Force) in Voice over IP(VoIP) is a text-based application protocol and has a client-server infrastructure. SIP can be used in call signaling setup between VoIP user agents for audio/video communications such as remote internet meeting, internet phone, and instant message system.

Also SIP defines the security for a call signaling and provides security services such as confidentiality, integrity, and user authentication. But SIP does not provide the security for media transport. This security is defined by SRTP(Secure RTP), another standard protocol of IETF[2]. SRTP provides the security service such as confidentiality for audio/video communication. However SRTP does not define key exchange protocol, which is defined by MIKEY(Multimedia Internet KEYing), another standard protocol of IETF[3].

Currently MIKEY is broadly used in the key management service for multimedia communication. MIKEY may be integrated within session establishment protocol such as SIP and transported over such protocol. Recently, integration of MIKEY within SIP message is defined by another protocol of IETF[4].

So we analyze a key management protocol, MIKEY for multimedia communication in Section 2, and also discuss the integration of MIKEY within SIP message in Section 3. We propose the negotiation mechanism for discovering cryptographic capabilities such as encryption/authentication algorithm, key information, etc of correspondent's VoIP phone in Section 4. Finally, we conclude this paper.

2 MIKEY

MIKEY is a key agreement specifically designed for protected multimedia exchanges. MIKEY provides a way to exchange a Transport Encryption Key (TEK) Generation Key (TGK) and security policies for a Crypto-Session Bundle (CSB), for instance a set of SRTP sessions. It also describes the way to derive a TEK for each of the Crypto-Session (this TEK is the SRTP master key), and uses cryptographic standard algorithms, AES and HMAC-SHA1 for encryption and authentication.

2.1 MIKEY and security properties

2.1.1 Mutual authentication

A common mutual authentication scheme is to use a set of challenge/responses: each of the participants is given a number and has to perform a one-way operation involving the authentication secret on that number. For example, a hash of that number concatenated with a shared secret or a digital signature of the number, will provide strong authentication. It is important that the challenges are different each time, to prevent replay attacks. Unfortunately, this scheme requires at least three messages for the authentication

of the initiator (the initiation message, the responder sending the challenges, and the response from the initiator). To reduce the number of messages, MIKEY uses timestamp as challenges in the initiation message.

2.1.2 Replay protection

The timestamp used for the authentication challenge/response, is also used to provide replay protection. The received timestamp is stored, and a message is discarded if the same timestamp is used a second time. The number of timestamps stored, as well as the timestamp control accuracy, is considered to depend on the local security policy.

2.1.3 DoS (Denial of Service) protection

The usual protection against DoS (Denial of services) requires at least an additional roundtrip. Because MIKEY requires at most one roundtrip, it provides no specific protection against DoS.

In usual VoIP communication, the responder can wait until the phone is picked up before doing any heavy computation, thus providing some de-facto protection. In this situation, the key exchange method with low computation power, such as pre-shared key method, would be preferred.

2.1.4 Identity hiding

Identity hiding key agreements requires at least two roundtrips: for instance the first one is a key exchange and the second one is the identity exchange, encrypted with the exchanged key. Because MIKEY requires at most one roundtrip, it does not provide identity hiding, and identities are sent in clear text.

If we consider the use of MIKEY within a SIP message, identity hiding would be useless: identities are sent unencrypted in the SIP header. Therefore, identity hiding requires the encryption f the whole SIP message, for instance by using TLS (Transport Layer Security) [5] as transport protocol.

2.1.5 Perfect Forward Secrecy

Among the three key agreement types provided by MIKEY, the one based on Diffie-Hellman provides perfect forward secrecy.

2.2 Three types of key agreement

MIKEY provides three types of key agreements. The choice of using one or the other depends on the available authentication infrastructure (PKI, pre-shared key, …) and computational resources.

2.2.1 Pre-Shared Key (PSK)

This key agreement method uses a pre-shared key. It is shown in (figure 1). The response message, used to authenticate the responder, is optional. f is a pseudo-random function described in MIKEY [3].

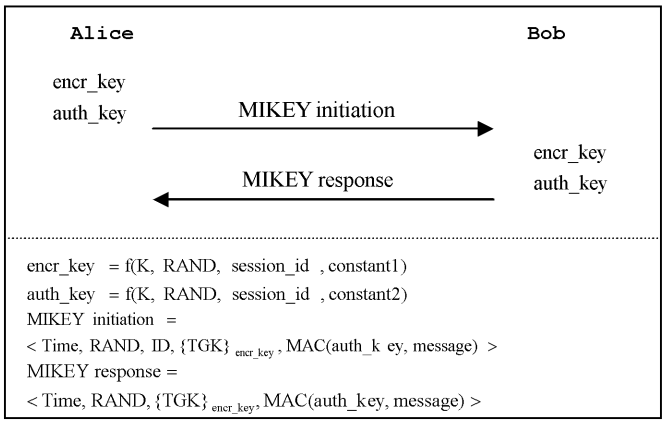

Fig. 1 Pre-Shared Key method

2.2.2 Public-Key Encryption (PKE)

This method requires Bob to have a pair of public/private key for encryption, and Alice to have a pair of public/private key for signature. It is similar to the pre-shared key method, except that an envelope key (env_key) is used instead of the shared key. This envelope key is transmitted encrypted with Bob's public key in the first message. The exchange procedure is shown in Fig. 2.

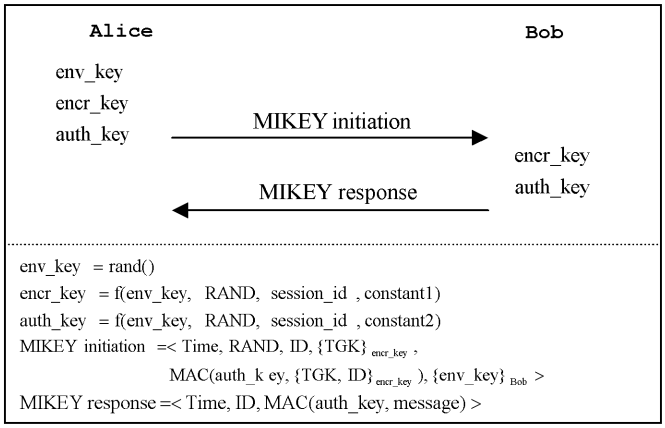

Fig. 2 Public-Key Encryption method

2.2.3 Diffie-Hellman (DH)

This method requires both Alice and Bob to have a couple of public/private key pair for signatures. The signatures are used both to protect against a man-in-the-middle attack and to authenticate each participant. This method requires more computations,

but provides perfect forward secrecy. Fig. 3 shows the process of this method.

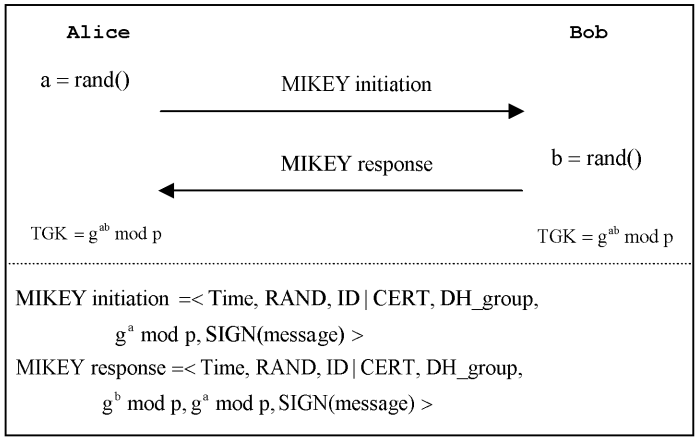

Fig. 3 Diffie-Hellman method

3 Integration of MIKEY in SIP

SIP message exchange consists of "Offer/Answer" construction as in Fig. 4. Entities except for sender and receiver are composed of SIP servers such as SIP proxy server, SIP redirect server, and Registrar. This paper supposes that SIP message exchange may be constructed without these entities as in Fig. 4.

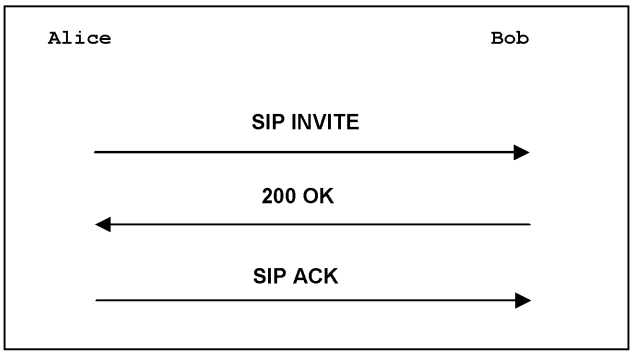

Fig. 4 SIP message exchange

SIP message consists of message header and message body as in Fig. 5. The message body uses the SDP (Session Description Protocol), which is a standard protocol of IETF [6]. SDP provides several fields and key exchange field "a=key-mgmt" [4] as in the Fig. 5.

There are several key exchange fields such as "k=" [6] and "a=crypto" [7] as well as "a=key-mgmt". The comparison of those key exchange fields is shown in Table 1. So this paper will use the key exchange field "a=key-mgmt". The encryption communication between initiator and responder needs a key exchange protocol such as MIKEY.

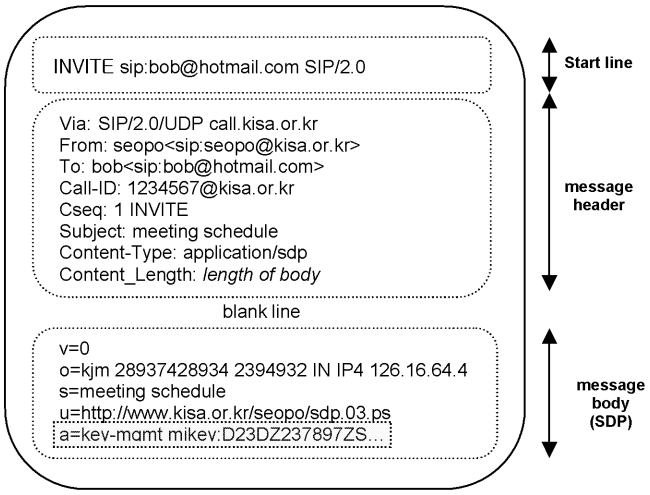

Fig. 5 SIP message (INVITE)

If MIKEY message exchange is separated from SIP message exchange, an additional message exchange for MIKEY message exchange is needed.

Table 1 key exchange fields

Field	characteristics
k=	only encryption key SDP encryption is required
a=crypto	encryption/authentication key SDP encryption is required
a=key-mgmt	authenticated key establishment SDP encryption is not required

This is much overhead. So the integration of MIKEY in SIP using a key exchange field "a=key-mgmt" is needed [7]. Fig. 6 represents the integration of MIKEY messages in SIP messages.

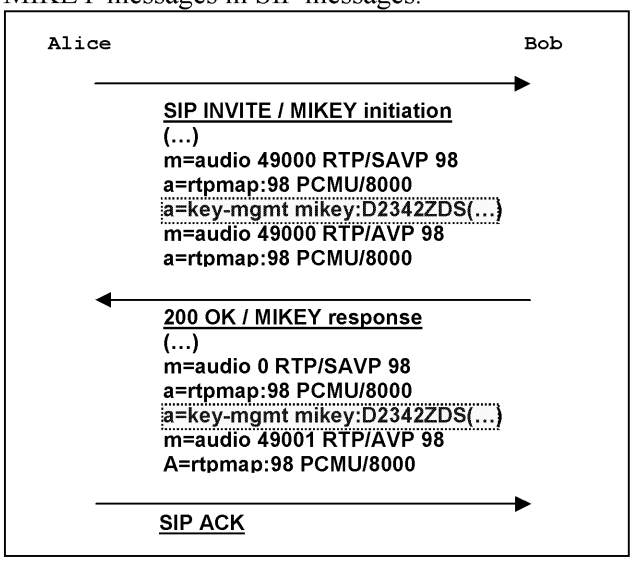

Fig. 6 Integration of MIKEY in SIP

4 The proposed negotiation mechanism

MIKEY provides three types of key agreements. Currently, additional types of key agreements for MIKEY are under standard work of IETF [8][9][10]. One of them is a key agreement, which integrates two of three types of key agreements for MIKEY, and another is a new key agreement, which can be used in MIKEY.

Besides these key agreements, there also three types of crypto-suites, which are defined by the security protocol (SRTP). These are categorized in Table 2.

Table 2 Cryptographic Capabilities

key agreement type	characteristics
PSK	Pre-Shared Key method
PKE	Public-Key Encryption method
DH	Diffie-Hellman method
crypto-suite type	characteristics
AES_CM_128_HMAC_SHA1_80	SRTP AES Counter Mode HMAC_SHA1 message authentication with 80-bit authentication tag
AES_CM_128_HMAC_SHA1_32	SRTP AES Counter Mode HMAC_SHA1 message authentication with 32-bit authentication tag
AES_F8_128_HMAC_SHA1_80	SRTP AES F8 Mode HMAC_SHA1 message authentication with 80-bit authentication tag

Since supported ability for cryptographic capabilities such as types of key agreements and crypto-suites may be different between initiator and responder, the negotiation mechanism for cryptographic capabilities is required. Until now, MIKEY has adopted two methods for negotiation mechanism as in Table 3.

In static negotiation method, if initiator's designated cryptographic capabilities are different from responder's one, initiator can not be in VoIP communication with responder securely. On the other side, automatic negotiation method might make it difficult for them to determine their favorite cryptographic capabilities. In static negotiation method, for instance, initiator's VoIP Phone has cryptographic capabilities such as a key agreement (PSK type) and a crypto-suite (AES_CM_128_HMAC_SHA1_80), while responder's one has cryptographic capabilities such as a key agreement (PKE type) and a crypto-suite (AES_F8_128_HMAC_SHA1_80).

In this situation, since initiator and responder have different cryptographic capabilities, they can not communicate each other securely with their phone.

Also, for instance, it is supposed that both initiator and responder have cryptographic capabilities including three key agreements and three crypto-suites in Table 2. In automatic negotiation method, however initiator wants to use cryptographic capabilities such as a key agreement (PSK type) and a crypto-suite (AES_CM_128_HMAC_SHA1_80) as his/her most favorites, he/she may not communicate with responder using his/her favorite cryptographic capabilities.

Table 3 Previous negotiation methods

method	characteristics
static	Only previously designated capabilities are used. **Merit :** Capabilities' designation which users wan to use, is possible **Demerit :** Backward compatibility is not guaranteed
automatic	After Identification for mutual capabilities ,users determine capabilities they will use randomly. **Merit :** Backward compatibility is guaranteed **Demerit :** Capabilities' designation which users wan to use, is not possible

So we propose a new negotiation mechanism for solving this problem. In this mechanism, both initiator and responder can assign their cryptographic capabilities in their priority order respectively, and then initiator's cryptographic capabilities are compared with responder's one using their priorities using a key exchange field "a=key-mgmt". The sample example is shown in Table 4.

For instance, it is supposed that initiator has cryptographic capabilities such as three key agreements (PSK type has first priority '0', PKE one has second priority '1', and DH one has third priority '2'), and two crypto-suites ('AES_CM_128_HMAC_SHA1_80' type has first priority '0', and 'AES_CM_128_HMAC_ SHA1_32' type has second priority '1'), and responder has cryptographic capabilities such as three key agreements (PKE type has first priority '0', DH one has second priority '1', and PSK one has third priority '2'), and two crypto-suites ('AES_CM_128_HMAC_SHA1_32'

type has first priority '0', and 'AES_F8_128_HMAC_SHA1_80' type has second priority '1') as in Table 4.

Table 4 Proposed Negotation Mechanism

	cryptographic capabilities	priority
Alice	PSK	0
	PKE	1
	DH	2
	AES_CM_128_HMAC_SHA1_80	0
	AES_CM_128_HMAC_SHA1_32	1
Bob	PKE	0
	DH	1
	PSK	2
	AES_CM_128_HMAC_SHA1_32	0
	AES_F8_128_HMAC_SHA1_80	1

In this example, it is possible for Alice and Bob to determine their favorite cryptographic capabilities such as a key agreement (PKE type) and a crypto-suite (AES_CM_128_HMAC_SHA1_32) by their priority comparison. So our proposed mechanism can be a solution for the backward compatibility, which static negotiation method can not satisfy, and can also solve the problem with which they can not determine their favorite cryptographic capabilities in automatic negotiation one. Fig. 7 shows the integration of MIKEY within SIP using our proposed negotiation mechanism

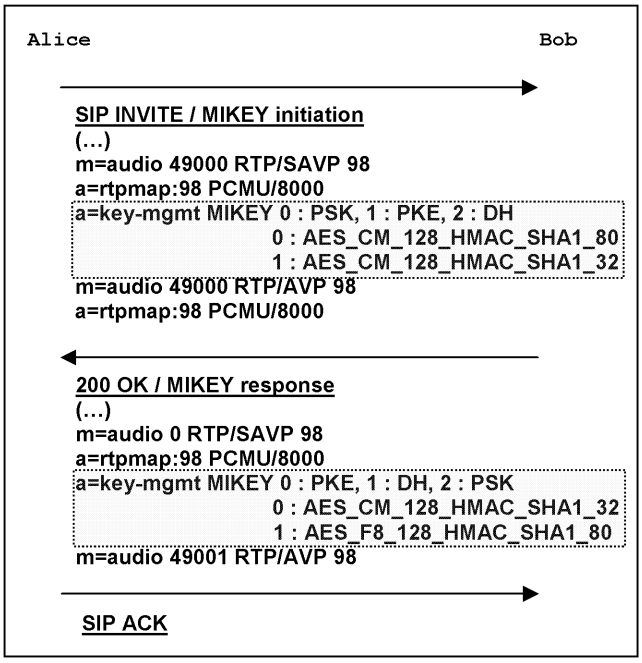

Fig. 7 Proposed Negotiation Mechanism (Integration in SIP)

5 Conclusion

This paper analyzed the MIKEY and the integration of MIKEY in SIP firstly. And we proposed a new negotiation mechanism for cryptographic capabilities using priorities. MIKEY defines the cryptographic capabilities - key agreements, crypto-suites -, which can be used in the security protocol such as SRTP.

Since initiator and responder have different cryptographic capabilities, a negotiation mechanism is needed. Previous negotiation mechanisms like static negotiation method and automatic negotiation method have several problems, which cannot satisfy backward compatibility and determine their favorite cryptographic capabilities. So we proposed new negotiation mechanism, which can solve these problems using priority.

In future, we will verify our proposed mechanism through the experimental approach and also prove the mathematical security of our proposed mechanism strictly.

References:

[1] J. Rosenberg, H. Schulzrine, G. Camarillo, A. Johonston, R. Sparks, M. Handley, and E. Schooler, SIP: Session Initiation Protocol", *RFC 3261, Internet Engineering Task Force*, 2002.

[2] M. Baugher, M. naslund, E. Carrara, and K. Norrman, The Secure Real-time Transport (SRTP), *RFC 3711, Internet Engineering Task Force*, 2004.

[3] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, MIKEY: Multimedia Internet KEYing, *RFC 3830, Internet Engineering Task Force*, 2004.

[4] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman, and E. Carrara, Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP), *RFC 4567, Internet Engineering Task Force*, 2006.

[5] T. Dierks and C. Allen, *The TLS Protocol version 1.0, RFC 2246, Internet Engineering Task Force*, 1999.

[6] M. Handley, V. Jacobson, and C. Perkins, SDP: Session Description Protocol, *RFC 4566, Internet Engineering Task Force*, 2006.

[7] F. Andreasen, M. Baugher, and D. Wing, Session Description Protocol (SDP) Security Descriptions for Media Streams, *RFC 4568, Internet Engineering Task Force*, 2006.

[8] M. Euchner, HMAC-authenticated Diffie-Hellman for MIKEY, *Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-dhhmac-11.txt,* 2005.

[9] D. Ignjatic, L. Dondeti, F. Audet, and P. Lin, An additional mode of key distribution in MIKEY: MIKEY-RSA-R, *Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-rsa-r-07.txt* , 2006.

[10] A. Milne, M. Blaser, D. brown, and L. Dondeti, ECC Algorithms for MIKEY, *Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-ecc-00.txt* , 2005.