멀티미디어 데이터 암호화를 위한 경량화된 MIKEY기반 암호 능력 협상 메커니즘*

윤석웅○ 김중만 원유재
한국정보보호진흥원
seokung○@kisa.or.kr, seopo@kisa.or.kr yjwon@kisa.or.kr

A Lightweight Cryptographic Capability Negotiation Mechanism based on MIKEY for Multimedia Data Encryption

Seokung Yoon○ Joongman Kim Yoojae Won
Korea Information Security Agency

요 약

MIKEY(Multimedia Internet KEYing)는 IETF에서 멀티미디어 데이터 암호화를 위한 표준 키 관리 프로토콜로 제안되었으며, 미디어 암호 프로토콜인 SRTP(Secure RTP)에서 키 교환 프로토콜로 고려되고 있다. 멀티미디어 데이터 암호화를 위해 MIKEY에서는 메시지를 교환함으로써 상호간의 공통적인 암호 알고리즘을 찾아내는 협상 메커니즘을 제시하고 있다. 하지만 이러한 방법은 상호간에 지원하는 알고리즘이 많은 경우나 상이한 경우에 이를 찾아내기 위한 메시지 교환 횟수가 증가하는 등 실시간 VoIP 암호통신에는 적합하지 않다. 따라서, 본 논문에서는 메시지 교환 횟수를 줄여 실시간 VoIP 암호통신에 적합한 경량화된 MIKEY기반 암호 능력 협상 메커니즘을 제안한다.

1. 서론

인터넷 전화(VoIP : Voice over Internet Protocol)는 기존의 인터넷 망을 이용하여 멀디미티어 서비스를 제공하는 기술이다. 그러나, VoIP 서비스는 기존 IP기술을 이용하여 음성통신 서비스를 제공하기 때문에 IP기반의 위협들을 그대로 상속하므로 VoIP 서비스 보호기술이 필요하다. 이와 관련하여 IETF(Internet Engineering Task Force) 등에서는 VoIP에 보안 서비스를 제공하기 위해서 다양한 연구가 진행되고 있다. SIP(Session Initiation Protocol)[1]는 시그널링을 위한 프로토콜로 세션 설정 과정에서의 관련 데이터 보호를 위한 여러 보안 매커니즘을 제공하고 있다. 사용자 인증으로는 HTTP 인증[2], 홉간 보안을 위해 TLS(Transport Layer Security)[3], 양단간 보안을 위한 S/MIME (Secure/Multipurpose Internet Mail)[4] 등 기존 보안 메커니즘을 그대로 이용한다. 멀티미디어 데이터를 전송하는 프로토콜인 RTP (Real-time Tansport Protocol)[5]는 멀티미디어 데이터의 기밀성 및 무결성 보장을 위해 SRTP(Secure RTP)[6]를 이용한다. VoIP에서는 멀티미디어 데이터 암호화를 위한 키 관리 프로토콜로 MIKEY (Multimedia Internet KEYing)[7]를 사용하고 있다.

MIKEY에서는 멀디티미어 데이터 암호화를 위해 메시지를 이용하여 공통적인 암호 알고리즘을 찾아내는 협상 메커니즘을 제시하고 있다. 하지만 이 방법은 상호간에 지원하는 암호 알고리즘이 많을 경우 이를 선택하기 위한 메시지 교환횟수가 늘어나는 되고 이로 인해 보안통신 설정에 많은 시간이 걸리게 되어 실시간 VoIP 암호통신에 적합하지 않다.

따라서, 본 논문의 2장에서는 멀티미디어 데이터 암호화를 위한 키 관리 프로토콜인 MIKEY를 살펴보고, 3장에서는 MIKEY에서 제시하고 있는 암호능력 협상 메커니즘에 대해서 살펴보고, 4장에서 실시간 VoIP 통신을 위한 경량화된 MIKEY기반 암호 능력 협상 메커니즘을 제안한다.

2. MIKEY(Multimedia Internet KEYing)

2.1 개요

MIKEY는 TEK (Traffic-encrypting Key)와 TEK을 생성하는데 사용되는 TGK (TEK Generation Key)를 포함한 SA (Security Association)을 생성하는 것이다. TEK와 데이터 SA를 생성하는 과정은 다음과 같다.

가. 보안 파라미터와 TGK를 공유한다.

나. TGK를 이용해서 각각의 암호 세션에 대한 TEK를 생성한다.

다. TEK을 보안 파라미터와 함께 Data SA의 형태로 보안 파라미터의 입력으로 사용한다.

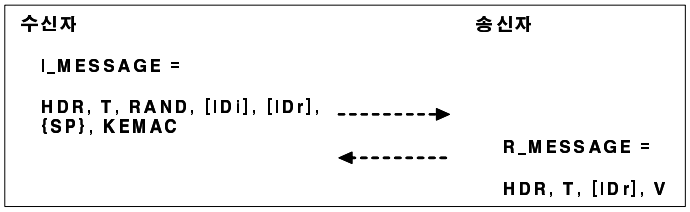
* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음 [2006-S-043-02, VoIP 정보보호기술]

2.2 키 전송 및 교환 방법

MIKEY는 TGK를 공유하기 위해서 3가지 교환 방법(사전 공유키 기반 키 공유 방법 공개키 암호 기술을 이용한 키 공유 방법 Diffie-Hellman 기반의 키 공유 방법)을 이용한다.

가. 사전 공유키 기반 키 공유 방법

공유키 기반 키 공유 방법에서는MIKEY 메시지에 대한 암호키(encr_key)와 인증키(auth_key)를 유도하는데 미리 공유된 키 s를 사용한다. 키 공유를 위한 메시지 형태는 다음과 같다.



- HDR : MIKEY 헤더
- T : 재전송 공격을 막기 위해 사용되는 타임 스탬프
- IDx: 송·수신자의 ID(IDi = 송신자, IDr = 수신자)
- RAND : 키생성을 위해 사용되는 임시 값
- SP : 실제 데이터 트래픽 보호를 위해 사용되는 보안 프로토콜을 위한 보안 정책
- V : 확인 메시지

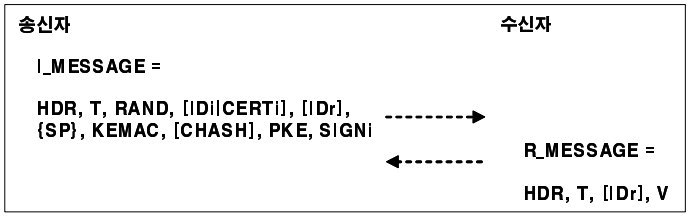
KEMAC은 여러 개의 암호화된 하위 페이로드와 MAC으로 구성된다. 각 하위 페이로드는 송신자에 의해서 임의로 선택된 TGK를 포함하고 있다. 또한 MAC은 전체 MIKEY 메시지에 대한 메시지 인증 코드이다.

KEMAC = E (encr_key, {TGK}) || MAC

- E : 암호 함수

나. 공개키 암호 기술을 이용한 키 공유 방법

공개키 암호 기술을 이용한 키 공유 방법은 다음과 같다.



공유키를 이용하는 방법과 마찬가지로Initiator가 생성한 메시지의 목적은 하나 이상의TGK 및 보안 파라미터를 안전하게 수신자에게 전달하는 것이다 이는 임의로 선택된 "envelope key"로 TGK를 암호화하여 전송함으로써 가능하다. 이 때, envelope key는 수신자의 공개키로 암호화하여 전송된다. 즉, PKE는 다음과 같이 암호화된 envelope 키를 포함한다.

PKE = E (PKr, env_key)

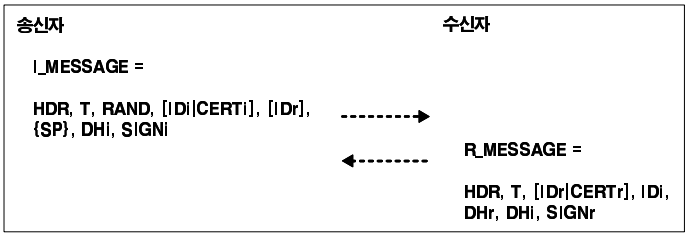
이 때, 수신자가 여러 개의 공개키를 소유하고 있는 경우에는 송신자는 CHASH 페이로드 내에 사용한 키를 표시할 수 있다. 또한 KEMAC은 다음과 같이 암호화된 하위 페이로드와 MAC으로 구성된다.

KEMAC = E (encr_key, IDi || {TGK}) || MAC

KEMAC에서 사용되는 encr_key와 auth_key는 envelope 키로부터 유도된다. SIGNi는 전체 MIKEY 메시지에 대한 전자서명이며, 송신자의 전자서명키를 이용해서 생성된다.

다. Diffie-Hellman 기반의 키 공유 방법

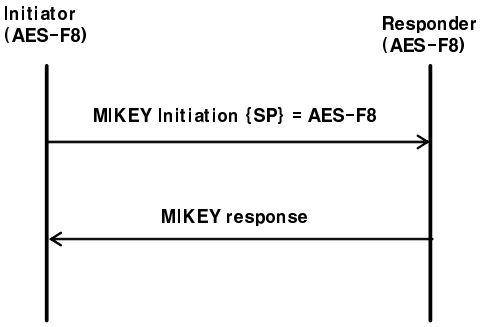
D-H 기반의 키 공유 방법은 다음과 같다



D-H를 이용할 경우에는 공유키나 공개키를 이용하는 방법과는 달리 TGK를 직접 전송하지 않는다. 즉 송신자와 수신자는 교환한 D-H 파라미터를 이용해서 'g^(xi*xr)'을 계산하여 동일한 TGK를 생성한다. SIGNi와 SIGNr은 송신자와 수신자가 전송하는 전체 메시지에 대한 전자서명이다.

3. MIKEY기반 암호 능력 협상

암호 능력 협상이란 송수신자간에 지원하는 암호 알고리즘을 교환하는 것으로 정의한다. 송수신자간에 공통적으로 지원하는 알고리즘이 있고 최초 메시지에 공통적인 암호알고리즘을 보낼 경우(그림 1)과 같이 1번의 메시지 교환으로 공통되는 알고리즘을 찾을 수 있다.

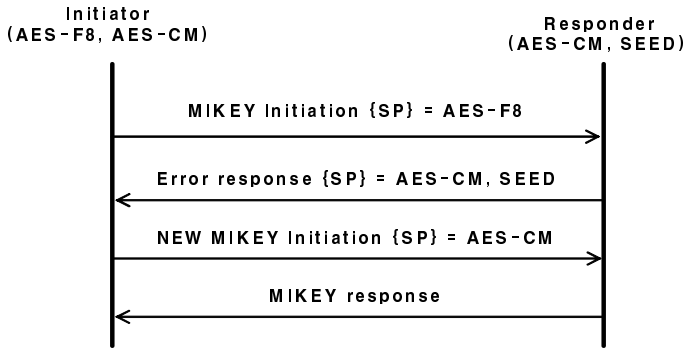


(그림 1) 암호 능력 협상 절차 I

하지만, 송수신자간 지원하는 알고리즘이 없거나 최초 메시지 안에 포함되어 있는 암호알고리즘을 지원하지 않을 경우 에러 메시지와 함께 수신자가 지원하는 암호 알고리즘 전부를 하나 이상의 보안 정책에 포함하여 송신자에게 전송하게 된다. 에러 메시지는 다음과 같이 구성된다.

에러 메시지 = HDR, T, {ERR}, {SP}, [V|SIGNr]

에러 메시지를 받은 송신자는(그림 2)와 같이 하나를 선택해서 보안통신을 맺게 된다. 만약 송·수신자간 지원하는 알고리즘이 없을 경우에는 정책에 따라서 일반통신을 여부를 결정한다.

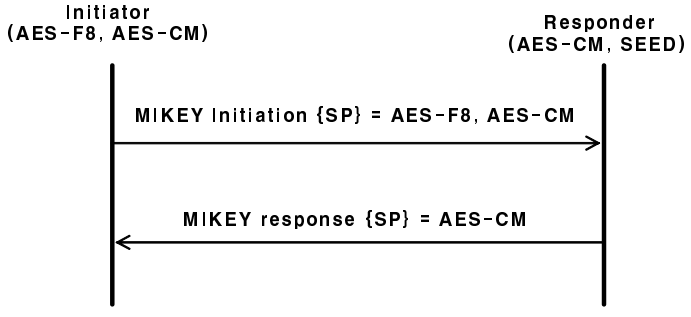


(그림 2) 암호 능력 협상 절차 Ⅱ

MIKEY에서 제공하는 암호 능력 협상 절차는 송신자가 여러 암호 알고리즘을 지원한다 할지라도 이중 하나만 선택해서 보내게 되므로 수신자가 이를 지원하지 않을 경우에는 (그림 2)에서 볼 수 있듯이, 최소 2번 이상의 메시지 교환 과정을 진행하게 된다. 이는 보안통신 설정과정에 많은 시간이 소요되므로 실시간 VoIP 통신에는 적합하지 않다. 따라서 다음과 같이 경량화된 암호 능력 협상 매커니즘을 제안한다.

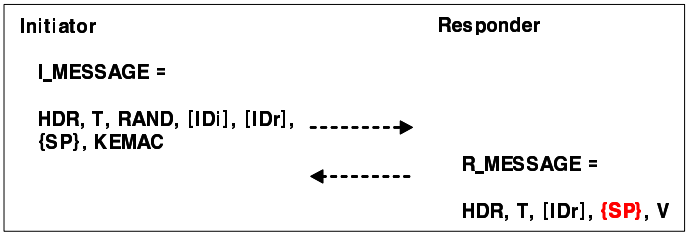
3. 제안하는 암호 능력 협상

(그림 3)에서 볼 수 있듯이, 송신자는 하나 이상의 보안 파라미터를 이용하여 지원하는 알고리즘을 전부 수신자에게 보내게 되면 수신자가 이 중 하나를 선택하여 응답 메시지에 보냄으로써 해당 알고리즘으로 보안통신을 맺게 된다.

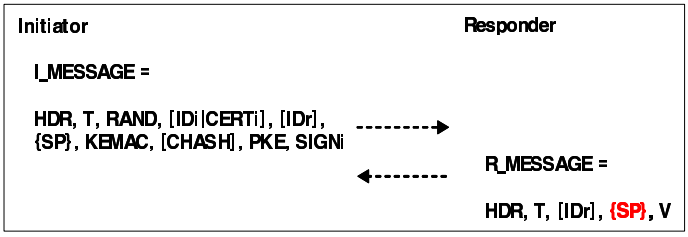


(그림 3) 개선된 암호 능력 협상 절차 Ⅰ

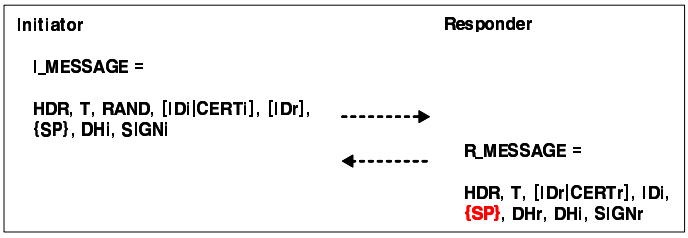
이를 위하여 응답 메시지에 보안 정책을 추가로 정의하는데 사전 공유키 방식일 경우에는 다음과 같다.



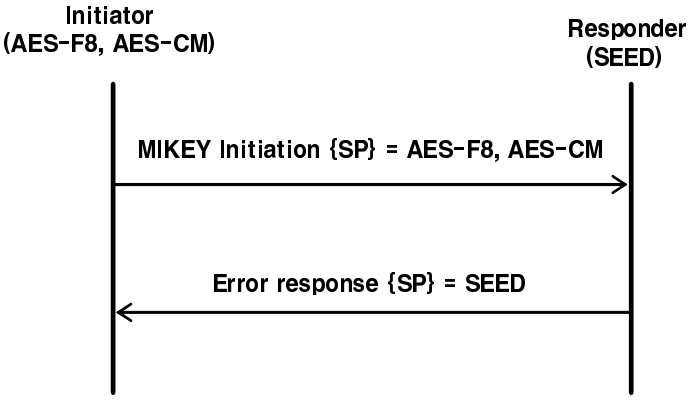
공개키 암호 기술 방식을 경우에는 다음과 같다.



D-H방식을 경우에는 다음과 같다.



만약 수신자가 송신자가 보낸 암호알고리즘을 지원하지 않을 경우 (그림 4)와 같이 에러 메시지와 함께 수신자가 지원하는 암호 알고리즘 전부를 보내게 되고 정책에 따라서 일반통신 여부를 결정한다.



(그림 4) 개선된 암호 능력 협상 절차 Ⅱ

제안하는 암호 능력 협상 메커니즘은 공통적으로 지원하는 암호 알고리즘이 있을 경우에 이를 발견하기 위하여 송신 메시지에 자신의 암호능력을 전부 실어 보냄으

로써, 송수신자간 여러 암호 알고리즘을 지원한다 할지라도 1번의 메시지 교환으로 공통적인 암호 알고리즘을 찾아낼 수 있다. 또한, 공통적으로 지원하는 알고리즘이 없더라도 1번의 메시지 교환으로 이를 찾아낼 수 있다. 이것을 정리하면 (표 1)과 같다.

(표 1) 기존 메커니즘과 제안하는 메커니즘의 성능 비교

	메시지 교환 횟수	
	공통적으로 지원하는 알고리즘이 있을 경우	공통적으로 지원하는 알고리즘이 없을 경우
기존 메커니즘	왕복 1회 이상	왕복 2회 이상
제안하는 메커니즘	왕복 1회	왕복 1회

(표 1)에서 볼 수 있듯이, 제안하는 메커니즘은 공통적으로 지원하는 암호 알고리즘이 있을 경우나 없을 경우나 이것을 찾아내기 위한 메시지 교환횟수가 왕복1회로 충분함을 알 수 있다.

4. 결론

본 논문에서는 멀티미디어 데이터 암호화를 위한 키 교환 프로토콜로 고려되고 있는 MIKEY 및 MIKEY에서 제시하고 있는 암호능력 협상 메커니즘을 분석하였다. 또한 MIKEY에서 제시하고 있는 방법을 개선시킨 경량화된 암호 능력 협상 매커니즘을 제안하였다.

본 논문에서 제시한 암호 능력 협상 매커니즘은 서로 다른 암호능력을 가진 사업자 환경이나, 송수신 단말이 지원하는 암호알고리즘이 많을 경우에도 공통된 암호 알고리즘을 찾아내는데 필요한 메시지 교환횟수가 왕복1회로 충분하여 기존 MIKEY에서 제안하고 있는 암호 능력 협상 메커니즘 보다 메시지 교환 횟수를 줄임으로써 실시간 VoIP 암호통신에 적합함을 알 수 있다.

향후 본 논문에서 제시한 암호 능력 협상 매커니즘에 대한 구체적인 설계 및 검증을 수행할 예정이다.

참 고 문 헌

[1] J.Rosenberg, H.Schulzrinne, G.Camaillo, A.Johnston, R.Sparks, M.Handly, and E.Schooler, "SIP: Session Initiation Protocol", RFC 3261, Internet Engineering Task Force, June 2002.

[2] J.Franks, P.Hallam-Baker, J.Hostetler, S.Lawrance, P.Leach, A.Luotonen, and L.Stewart, "HTTP Authentication : Basic and Digest Access Authentication", Internet Engineering Task Force, June 1999

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

[4] B.Ramsdell, "Secure/Multipurpose Internet Extensions (S/MIME) Version 3.1 Message Specification", Internet Engineering Task Force, July, 2004

[5] H.Schulzrinne, S.Casner, R.Frederick, and V.Jacobson, "RTP: A Transport protocol for Real-Time Applications", RFC 3550, Internet Engineering Task Force, July 2003.

[6] M.Baugher, E.Carrara, F.Lindholm, M.Naslund, and K.Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, Internet Engineering Task Force, March 2004.

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