MIKEY 확장 기반의 멀티미디어 통신을 위한 키협상 메커니즘

김중만, 현호재, 원유재

한국정보보호진흥원

seopo@kisa.or.kr hjhyun@kisa.or.kr yjwon@kisa.or.kr

Key Negotiation Mechanism for multimedia communication based on Multimedia Internet KEYing (MIKEY) Extension

Kim Joong Man Hyun Ho Jae Won Yoo Jae

Korea Information Security Agency

요 약

MIKEY(Multimedia Internet KEYing)는 멀티미디어 전송을 위한 키관리 프로토콜로 IETF에서 VoIP 보안을 위한 핵심프로토콜로 제안되었으며, 미디어 암호 프로토콜인 SRTP(Secure RTP)에서의 키교환 프로토콜로 고려하고 있다. 그러나 MIKEY는 효율성 및 단순성을 보장하기 위해 새로운 키교환 방식을 제안하는 대신 기존에 사용하던 키교환 방식을 차용하였다. 따라서 MIKEY의 보안 특성 및 MIKEY가 차용하고 있는 키교환 방식들을 분석한다. 또한 MIKEY와 SIP를 통합한 후 MIKEY의 키교환 방식들에 대해 협상할 수 있는 키협상 메커니즘을 제안한다.

1. 서 론

VoIP에서 하나의 표준 프로토콜로써 IETF(Internet Engineering Task Force)에서 제안한 SIP(Session Initiation Protocol)[1]는 텍스트 기반 응용 계층의 프로토콜로 클라이언트/서버 구조를 가지며, 인터넷을 이용한 원격회의, 인터넷 전화, 인스턴트 메시지 등의 서비스와 같이 음성 통신이 가능한 단말간의 호 설정 기능을 제공한다. 또한 SIP에서는 호 신호에 대한 보안 기능을 정의하고 있으며, SIP메시지에 대한 기밀성, 무결성과 사용자 인증 기능을 제공한다. 반면, SIP는 호 신호에 대한 프로토콜 정의는 되어 있지만, 미디어 전송에 대한 내용은 별도로 정의하고 있지 않으며, IETF의 또 다른 표준 프로토콜인 SRTP(Secure RTP)[2]에서 정의하고 있다. SRTP는 미디어 전송에 대한 암호 프로토콜이지만, 암호 키에 대한 키 교환 프로토콜을 따로 정의하지 않고, MIKEY(Multimedia Internet KEYing)[3] 표준 프로토콜에서 이를 정의하고 있다. MIKEY는 현재 멀티미디어 전송을 위한 키관리의 표준으로 고려되고 있으며, SIP 메시지내에서 MIKEY를 사용하고자 하는 연구도 진행 중이다[4].

따라서 본 논문의 2장에서는 멀티미디어 통신을 위한 키교환 프로토콜로 고려되고 있는 MIKEY의 보안특성 및 키교환 방식들을 분석하며, 3장 장에서는 MIKEY와 SIP를 통합하는 기존의 연구 내용을 분석하고, 4장에서는 MIKEY의 여러 키교환 방식들에 대한 키협상 메커니즘을 제안하고, 그 키협상 메커니즘과 SIP 메시지를 통합하는 과정의 예를 든다.

2. MIKEY(Multimedia Internet KEYing)

(1) 개요

MIKEY는 유무선 통합환경, 멀티미디어 세션, peer-to-peer 통신 뿐 아니라 멀티캐스트 및 그룹통신, 그리고 VoIP 미디어 채널 보호를 위한 SRTP에서의 키교환을 위해서 IETF에서 제안되었다. MIKEY는 일반적인 암호학적 표준 프로토콜(암호를 위해 counter-mode를 적용한 AES, MAC 인증을 위해 HMAC-SHA1 등이 사용됨)을 사용한다. MIKEY는 하나의 Transport Encryption Key (TEK) Generation Key (TGK)와 Cryto-Session Bundle(CSB)를 위한 보안정책(예를 들면, SRTP 세션 등)들을 교환하는 방법을 제공해 주며, 또한 하나의 암호 세션을 위한 하나의 마스터키(TEK)를 생성하는 방법을 제안한다.

(2) MIKEY의 보안특성

가. 상호 인증

일반적인 상호인증 기법은 시도/응답 방식을 사용한다. 즉, 각 통신 당사자들에게 하나의 값이 주어지고, 그 값에 대한 일방향 함수 연산 과정을 수행한다. 예를들면, 그러한 값에 공유된 비밀값이나 전자 서명값이 더해진다면, 더욱더 강한 인증 기능을 제공하게 된다. Replay 공격 예방을 위해서는 시도값을 매번 달리해야 한다. 하지만, 상호인증은 최소한 3번 이상의 메시지 교환을 필요로 한다. 메시지 교환 수를 줄이기 위해서 MIKEY는 시도값으로 timestamp를 사용하며, 응답값을 초기 메시지내