情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

일회성 암호를 이용한 효율적이고 안전한 SIP 사용자 인증 및 SDP 암호화 기법

김 정 제,[1†] 정 만 현,[1] 조 재 익,[1] 손 태 식,[2] 문 종 섭[1‡]
[1]고려대학교 정보보호대학원, [2]아주대학교

Efficient and Secure User Authentication and SDP Encryption Method in SIP

Jungje Kim,[1†] Manhyun Chung,[1] Jaeik Cho,[1] Taeshik Shon,[2] Jongsub Moon[1‡]
[1]Graduate School of Information Security, Korea University, [2]Division of Information and Computer Engineering, Ajou University

요 약

본 논문에서는 일회성 암호를 이용한 SIP UA와 서버 사이의 상호 인증 및 SDP 암호화 기법을 제안한다. 기존의 HTTP Digest 인증 기법의 취약성을 해결하기 위해 다양한 SIP 인증 기법이 연구되었지만, 여전히 취약성이 존재하거나 암호학적 연산량에 대한 부담이 존재한다. 제안 기술은 매 인증마다 해쉬함수를 사용하여 갱신되는 일회성 암호를 사용하여 복잡한 암호학적 연산을 필요로 하지 않으면서 효율적으로 사용자 인증을 수행한다. 또한 사용자 인증에 사용되는 일회성 암호를 통해 SIP 메시지의 무결성 검증 및 SDP 암/복호화를 수행하기 때문에 메시지 교환 과정에서 S/MIME, TLS 적용 시 발생하는 오버헤드를 줄일 수 있다.

ABSTRACT

This paper propose a security method that performs mutual authentication between the SIP UA and the server, check for integrity of the signaling channel and protection of SDP information for VoIP using a One-Time Password. To solve the vulnerability of existing HTTP Digest authentication scheme in SIP, Various SIP Authentication schemes have been proposed. But, these schemes can't meet security requirements of SIP or require expensive cryptographic operations. Proposed method uses OTP that only uses hash function and is updated each authentication. So Proposed method do not require expensive cryptographic operations but performs user authentication efficiently and safely than existing methods. In addition, Proposed method verifies the integrity of the SIP messages and performs SDP encryption/decryption through OTP that used for user authentication. So Proposed method can reduce communication overhead when applying S/MIME or TLS.

Keywords: VoIP Security, OTP, SIP, User Authentication

I. 서 론

VoIP(Voice over Internet Protocol) 기술은 인터넷 프로토콜(Internet Protocol: IP)과 데이터 망을 이용하여 전화를 할 수 있는 기술이다. VoIP 서비스의 사용은 PSTN(Public Switched Telephone Network)에 비해 상대적으로 저렴한 가격, 인터넷의 발전으로 인한 서비스 품질 향상, 스마트폰 사용의 급증으로 인한 모바일 인터넷의 활용 증가 등에 의해 점차 증가하여 보편화되어가는 추세에 있다. 초고속 인터넷 망의 보급 확대와 VoIP 기술의 발전에 따라 초창기의 음성 위주 IP 응용 서비스뿐 아니라 비디오, 데이터 등 각종 멀티미디어 정보를 통합 전송할

접수일(2011년 10월 4일), 게재확정일(2011년 12월 10일)
† 주저자, adusbay@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr

수 있도록 하는 기술로 변화하고 있으며, 이러한 관점에서 MoIP(Multimedia over IP) 혹은 V2oIP(Voice and Video over IP)라 부르기도 한다[1]. VoIP 서비스는 기존의 IP 기술을 이용하여 서비스를 제공하기 때문에 IP 기반의 위협들을 그대로 상속하고 있으며, 그에 따라 기존의 IP 기반의 보안 위협에 그대로 노출되어 있다. 이러한 보안 문제를 해결하기 위해 IETF SIP(Session Initiation Protocol) 표준[2]에서는 사용자 인증과 SIP 메시지 보호에 HTTP Digest 인증[3], TLS(Transport Layer Security)[4], S/MIME (Secure/Multipurpose Internet Mail Extensions) [5]과 같은 기존에 사용되고 있는 보안 프로토콜들을 사용할 것을 권고하고 있다. 사용자 인증에 사용되는 HTTP Digest 인증 기법은 사전 공격에 취약하고, SDP(Session Description Protocol)[6] 정보에 대한 기밀성을 제공하지 않는다는 문제점이 있다. 이러한 문제점을 해결하기 위해 홉 간 보안에 TLS, 종단간 보안에 S/MIME를 함께 사용한다면 안전한 상호 인증 및 SIP 메시지를 보호할 수 있다. 그러나 S/MIME은 PKI(Public Key Infrastructure) 기반의 보안 프로토콜이기 때문에 PKI 환경이 구축되지 않은 환경에서는 적용하기 어렵고, 모든 홉 간 보안을 위해 TLS를 적용한다면 프락시 서버는 모든 UA에 대한 TLS 세션을 유지하여야 하므로 많은 오버헤드가 발생 한다. 이와 같은 SIP 보안 프로토콜의 실질적인 적용 문제나 취약성을 해결하기 위해 Diffie-Hellan[7], IBC(ID-based Cryptosystem)[8], HOTP(HMAC One-Time-Password)[9] 등 다양한 암호 암호알고리즘을 사용한 인증 기법들이 연구되었다. 하지만, 제안된 기술들은 암호학적으로 많은 연산량을 요구하거나, VoIP의 모든 보안요소를 만족시키지 못한다.

본 논문에서는 OTP(One-Time Password)[10]를 이용하여 사용자 인증, 시그널링 채널의 무결성 검증, SDP 정보를 보호하는 안전하고 효율적인 보안 모델을 제안한다. 제안 기법은 해쉬함수만을 사용하여 갱신되는 OTP를 사용자 인증에 적용함으로써 기존 방법들에 비해 효율적으로 사용자 인증작업을 수행한다. 또한 OTP를 사용자 인증에 직접 사용하는 것이 아니라 SIP 메시지에 대한 메시지다이제스트 생성을 위한 키로 사용함으로써 SIP 메시지의 무결성 검증을 수행한다. 제안기법은 인증에 사용된 OTP와 매 통화마다 랜덤하게 생성되는 SIP Call-ID를 사용하여 SDP를 암호화하여 전송함으로써 TLS 보안 채널 형성에 따른 오버헤드를 줄일 수 있다. 본 논문의 구성은 다음과 같다. 2장에서 기존의 SIP 보안 기술들에 대해서 살펴보고, 3장에서 일회성 암호를 이용한 SIP 보안 모델을 제안한다. 4장에서는 제안하는 기법에 대하여 효율성 및 안전성을 검증하고 마지막으로 5장에서 결론 및 향후 연구에 대해서 설명한다.

II. 관련연구

2.1 SIP 보안 기법

SIP 표준에서 정의한 사용자 인증 기술인 HTTP Digest는 패스워드를 평문이 아닌 메시지 다이제스트 형식으로 보내기 때문에 패스워드가 외부로 노출되지 않고, 매 인증마다 임의의 난수인 비표를 통해 재전송 공격에 대비한다는 장점이 있다[3]. 하지만 SIP 서버의 UA(User Agent)에 대한 인증은 제공하지만 UA의 SIP 서버에 대한 인증은 제공하지 않고, SIP 헤더를 암호화하여 전송하지 않으므로 시도, 응답 생성과정에서 패스워드를 제외한 나머지 값들이 공격자에게 쉽게 노출되어 사전 공격에 취약하다는 문제점이 있다. 또한 HTTP Digest는 인증 기법이기 때문에 SDP 정보들에 대한 기밀성은 제공하지 않는다. SDP는 스트리밍 미디어의 초기화 인수를 기술하기 위한 포맷으로 RTP(Real-time Transport Protocol)통신을 하는 두 UA의 IP 주소, 포트 번호, 미디어 스트림 정보 및 SRTP (Secure RTP)키 정보 등을 포함하고 있다[6] [11]. 따라서 SDP 정보에 대한 기밀성이 보장되지 않는다면 미디어 스트림 정보가 노출되어 스팸 공격 등에 악용될 수 있고, SRTP 마스터 키 정보가 공격자에게 노출될 위험이 있다. 이에 SIP 표준에서는 사용자 인증에 사용하는 HTTP Digest와 더불어 홉 간 보안에 TLS, 종 단간 보안에 S/MIME의 사용을 권고하고 있다[2]. 그러나 S/MIME은 PKI 기반의 보안 프로토콜이기 때문에 PKI 환경이 구축되지 않은 환경에서는 적용하기 어렵고 양 단간 보안이기 때문에 홉 간 보안을 위해 TLS를 함께 적용하여야 한다. 하지만 모든 홉 간에 TLS를 적용한다면, TLS 역시 PKI 기반의 프로토콜이기 때문에 인증서 발급을 위한 기반 구조가 갖추어져야 하고, 프락시 서버에서 모든 UA에 대한 TLS 세션을 유지해야 하므로 오버헤드가 발생한다.

이와 같은 SIP 보안 프로토콜의 실질적인 적용 문

제나 취약성을 해결하기 위해 많은 SIP 인증 및 키 교환 기술들이 연구되고 있다. 먼저, 기존의 HTTP Digest 인증 기술에 Diffie-Hellman 키 교환 알고리즘을 사용한 사용자 인증 및 키 교환 기술이 제안되었다[12]. Diffie-Hellman 키 교환 알고리즘 기반의 기술이 HTTP Digest의 UA와 SIP 서버의 상호 인증 문제와 사전 공격 문제를 해결하였지만, Diffie-Hellman 키 교환 알고리즘은 복잡한 지수 연산을 필요로 하기 때문에 많은 암호학적 연산량을 요구한다. UA에서 수행하여야 하는 Diffie-Hellman 키 교환 알고리즘의 지수 연산을 SIP 서버에게 위임하여 UA의 부담을 경감하는 기술도 제안되었다[13]. 하지만 UA의 공개키의 계산을 서버가 대신 수행하기 때문에 Register Flooding 공격이나 Invite Flooding 공격에 취약할 수 있고, UA의 공개키에 대한 계산을 SIP 서버가 대신 수행하기 때문에 UA와 SIP 서버간의 패스워드가 노출되어 패스워드를 해쉬한 값이 알려지면 위장 공격에 취약할 수 있다.

사용자의 이메일 주소나 IP 주소와 같은 사용자의 식별자 기반의 IBC를 이용한 기법도 제안되었다[14][15]. IBC 시스템은 PKI 환경의 구축 없이 사용자의 식별자를 기반으로 공개키를 생성하고 TA(Trusted Authority)를 통해 공개키에 대응하는 비밀키를 발급받는 방식이다[8]. IBC 기반의 SIP 보안 기술은 자신의 식별자를 기반으로 한 공개키와 그에 대응하는 비밀키를 통해 SIP REGISTER 와 INVITE 과정에서 사용자와 SIP 서버 간의 상호 인증을 제공하고, UAC(User Agent Client)와 UAS(User Agent Server)간의 미디어 스트림 보안을 위한 세션키를 생성한다[14][15]. 하지만 자신의 비밀키를 TA를 통해 발급받기 때문에 Key Escrow 문제점이 있고, 사용자의 식별자를 공개키로 사용하기 때문에 비밀키가 공격자에 의하여 노출될 경우 그에 대응하는 식별자는 더 이상 사용할 수 없는 문제점이 있다.

마지막으로 일회성 암호를 사용한 기법으로는 HOTP를 사용한 인증 기법이 연구되었다. HOTP 기반의 인증 기법에서는 UA와 SIP 서버 사이에 OTP 생성을 위한 비밀값과 카운터를 공유하여 매 인증 마다 새로운 OTP를 생성하고, OTP를 SIP 메시지의 Call-ID에 포함하여 전송함으로써 UA와 SIP 서버 간의 인증을 제공한다[16]. HOTP 기반의 인증 기법은 SIP 서버의 사용자에 대한 인증을 제공하지만 사용자의 SIP 서버에 대한 인증은 제공하지 않고, SIP 메시지의 보호를 위한 메커니즘이 없기 때문에 SIP 메시지가 공격자에게 그대로 노출되는 문제점이 있다. 또한 기존에 제안된 기법들은 SDP 보호를 위한 방법은 제공하지 않기 때문에 S/MIME, TLS 등을 함께 적용해서 사용하여야 하므로 많은 오버헤드가 발생한다.

2.2 OTP를 이용한 보안 기술

OTP는 사용자가 인증을 받고자 할 때 매번 새로운 패스워드를 생성하여 인증하는 기술로 해쉬함수(Hash function)를 사용하기 때문에 효율적이고 안전한 인증 기법을 제공한다[10]. OTP 기술은 OTP 토큰과 인증 서버 간 시간이나 시드와 같은 비밀 정보를 공유하고, 이러한 정보를 해쉬함수와 같은 알고리즘을 통해 일회용 패스워드를 생성한다. 최초에 생성되는 OTP는 해쉬함수의 입력값으로 사용자의 고유값 s와 시드값 $token$을 이용하여 생성된다.

$$P_0 = H(s, token) \tag{1}$$

이후 생성되는 OTP는 이전에 생성된 OTP에 같은 함수를 적용하여 생성한다.

$$P_1 = H(P_0, token+1) \tag{2}$$

이와 같은 과정을 일반적으로 나타내면 다음과 같다.

$$P_i = H(P_{i-1}, token+i), \forall \geq 1 \tag{3}$$

위의 수식에서 볼 수 있듯이 OTP는 이전 OTP 값인 P_{i-1}을 알지 못하면 생성할 수 없고, $token$이 매번 갱신되어 시드로 이용되므로 임의의 OTP를 생성할 수 없다. 이와 같은 OTP의 특성으로 인해 키의 노출이나 재사용 문제에 대하여 높은 보안성을 유지할 수 있다.

III. 제안 기법

본 논문은 OTP를 사용하여 UA와 SIP 서버 사이의 상호 인증 및 시그널링 채널의 무결성 검증을 제공하고, UA와 SIP 서버 사이의 TLS 적용 없이 효율적으로 SDP를 암호화하는 기법을 제안한다. 제안 기

〔표 1〕 표기법

표기	정의
$H()$	안전한 일방향 해쉬함수
$H_k()$	k를 키로 사용한 안전한 일방향 해쉬함수
pwd	패스워드
M	메시지의 무결성을 검증하기 위한 메시지다이제스트
OTP	One-Time Password
s	OTP를 생성하는데 사용하는 고유값
$seed$	OTP를 생성하는데 사용하는 시드
$\|\|$	두 개의 비트열의 연접
OTP_i	i번째 생성된 OTP
OTP_{old}	이전 인증에서 사용되었던 OTP
OTP_{new}	고유값과 시드를 이용해 새롭게 생성된 OTP
E_k	k를 키로 하는 대칭키 기반의 암호화
D_k	k를 키로 하는 대칭키 기반의 복호화
C	암호화 알고리즘에 의해 생성된 암호문

법은 UA와 SIP 서버 간에 OTP 생성을 위한 고유값과 시드의 교환 절차와 호 설정과정에서의 UA와 SIP의 상호인증 및 SIP 메시지의 무결성 검증, SDP의 암/복호화 과정으로 나뉜다. 본 논문에서 사용되는 기호들은 〔표 1〕과 같다.

3.1 고유값과 시드 교환 절차

OTP 생성을 위한 고유값과 시드는 UA와 SIP 서버 사이에서 안전하게 교환되어 공유되어 있어야 한다. 본 논문에서 제안하는 기법은 초기 등록 과정에서 패스워드를 해쉬한 값을 이용하여 UA와 SIP 서버 간에 안전하게 고유값과 시드를 교환한다. 또한 인증 시 OTP에 대한 전수조사 공격(brute force attack)을 막기 위해, 일정 횟수 이상의 인증이 실패하면 해당 사용자는 차단되어야 한다. 차단된 사용자가 OTP의 재동기화를 요구할 경우 SIP 서버와 UA는 새로운 OTP의 고유값과 시드를 초기 등록단계에서 수행한 방법과 동일한 방식으로 교환할 수 있다. 이 때, SIP 서버와 UA는 마지막으로 성공했던 인증과정에서 사용했던 OTP를 이용하여 새로운 고유값과 시드를 교환한다. 고유값과 시드를 교환하는 절차는 다음과 같다.

Step 1. UA는 SIP 서버에게 SIP REGISTER 메시지를 전송하면서 고유값과 시드가 필요하다는 요청을 한다.

Step 2. SIP 서버는 고유값 s와 시드 $seed$를 생성한다. 생성된 고유값과 시드를 식 (4)와 같이 암호화하여 SIP 응답 메시지에 포함하여 전송한다. 이 때 UA의 초기 등록단계에서는 패스워드를 해쉬한 값을 암호화키로 사용하고, 인증 실패로 인한 새로운 시드와 고유값 교환 시에는 마지막으로 인증이 성공한 OTP를 암호화키로 사용한다.

$$C = E_k(s\|seed),\quad k = H(pwd) \text{ or } k = H(OTP_{old}) \tag{4}$$

Step 3. UA는 수신 받은 암호문을 식 (5)와 같이 복호화하여 고유값과 시드를 알아낸다. 그리고 고유값과 시드를 사용하여 OTP를 생성하고, 새로운 OTP에 대한 해쉬값을 식 (6)과 같이 계산하여 SIP 서버에게 전송한다.

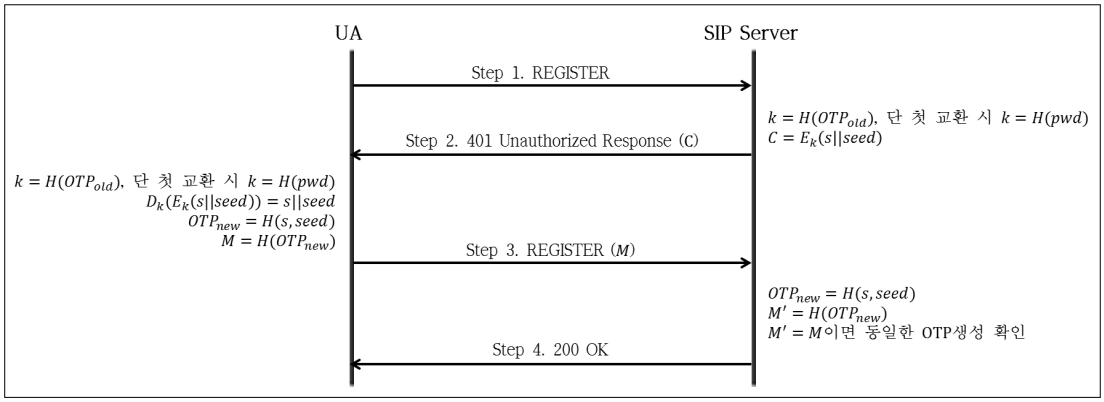
$$D_k(E_k(s\|seed)) = s\|seed,\quad k = H(pwd) \text{ or } k = H(OTP_{old}) \tag{5}$$

$$M = H(OTP_{new}),\ OTP_{new} = H(s, seed) \tag{6}$$

Step 4. SIP 서버는 자신이 보낸 고유값과 시드로 OTP를 생성한 후, 생성한 OTP에 대한 해쉬값을 식 (6)과 같이 계산한다. 그리고 생성한 해쉬값을 UA로부터 수신 받은 해쉬값과 비교한다. 고유값과 시드에 대한 교환이 성공적으로 이루어졌다면 SIP 서버가 생성한 해쉬값과 UA가 전송한 해쉬값은 동일하다. 고유값과 시드의 교환이 성공적으로 이루어져서 해쉬값이 동일하다면, SIP 서버는 UA에게 200 OK 메시지를 발송한다. 이 후 인증과정은 이 고유값과 시드를 이용해 매 인증시도 마다 새로운 OTP를 생성하여 이루어진다.

3.2 호 설정 과정

초기 등록단계에서 고유값과 시드의 교환이 성공적으로 이루어지면, UA와 SIP 서버는 고유값과 시드를 이용하여 OTP를 생성한다. 그리고 OTP를 키로 사용하는 키-해쉬함수(Keyed-hash function)를 사용하여 SIP 헤더에 대한 메시지다이제스트를 만들어서 전송함으로써, UA와 SIP 서버간의 상호 인증 및 SIP 메시지에 대한 무결성 검사를 수행한다. 매 인증마다 OTP는 이전 OTP와 시드를 이용하여 새롭게



〔그림 1〕 고유값과 시드의 교환 절차

생성되기 때문에 UA와 SIP 간의 안전한 상호 인증 및 무결성 검사를 수행할 수 있다. 또한 OTP와 매 통화마다 랜덤하게 생성되는 Call-ID를 사용하여 SDP를 암호화하여 전송함으로써 UA와 SIP 서버사이의 TLS 보안채널 형성을 위한 오버헤드를 줄일 수 있다. 호 설정과정에서 UA와 SIP 서버 간의 상호 인증, SIP 메시지의 무결성 검증, SDP의 암/복호화 과정은 다음과 같다.

Step 1. UAC는 아웃바운드 프락시 서버와 공유하고 있는 고유값 s_c와 시드 $seed_c$를 이용하여 OTP를 생성한다. OTP를 키로 사용하는 키-해쉬함수를 사용하여 SIP INVITE 메시지의 헤더 필드에 대한 메시지다이제스트 M_{c1}을 식 (7)과 같이 생성한다. 또한 SRTP 마스터 키 생성을 위한 키 정보 및 SDP의 주요 정보들을 보호하기 위해 SDP를 식 (8)과 같이 암호화한다. 이 때 키는 OTP와 랜덤하게 생성되는 Call-ID를 해쉬한 값을 사용하여 보안을 강화한다. 그리고 UAC는 생성된 메시지다이제스트와 암호화된 SDP를 SIP INVITE 메시지에 포함하여 아웃바운드 프락시 서버에게 전송한다.

$$M_{c1} = H_{OTP_c}(SIP\,INVITE\,Header) \tag{7}$$

$$C_{c1} = E_{K_c}(UAC's\,SDP),\quad k_c = H(OTP_c \| Call-ID) \tag{8}$$

Step 2. 아웃바운드 프락시 서버는 고유값 s_c와 시드 $seed_c$를 이용하여 OTP를 생성하고, UAC로부터 받은 SIP INVITE 메시지의 헤더 필드에 대한 메시지다이제스트 M_{c1}'를 식 (7)과 같이 생성한다. 자신이 생성한 메시지다이제스트 M_{c1}'와 UAC로부터 전송받은 M_{c1}이 같다면 UAC에 대한 인증과 함께 SIP INVITE 메시지의 무결성이 검증된다. 그리고 암호화 키를 이용해 SDP를 복호화 한 후 INVITE 메시지를 인바운드 프락시 서버로 전송한다. 이 때 프락시 서버 간에는 TLS가 필수로 적용되기 때문에 프락시 서버 간에는 인증 및 SDP에 대한 기밀성이 보장된다.

Step 3. INVITE 메시지를 받은 인바운드 프락시 서버는 UAS와 공유하고 있는 고유값 s_s와 시드 를 $seed_s$이용하여 OTP를 생성하고, INVITE 메시지의 헤더 필드에 대한 메시지다이제스트를 UAC와 같은 방법으로 생성한다. 또한 UAS와의 OTP와 Call-ID를 해쉬하여 암호화키를 생성하고 SDP를 암호화한다. 그리고 생성한 메시지 다이제스트와 암호화된 SDP를 INVITE 메시지와 함께 전송한다.

Step 4. UAS는 고유값 s_s와 시드 $seed_s$를 이용하여 OTP를 생성하고, INVITE 메시지에 대한 메시지 다이제스트를 생성하여 INVITE 메시지에 대한 무결성 검사 및 인바운드 프락시 서버에 대한 인증을 수행한다. 또한 OTP와 Call-ID를 해쉬하여 암호화키를 생성하고 SDP를 복호화하여 RTP 통신을 위해 필요한 정보를 얻는다. 인바운드 프락시 서버에 대한 인증이 성공하면, OTP를 사용하여 200 OK 메시지에 대한 해쉬값을 생성하고 SDP를 암호화하여 200 OK 메시지에 포함하여 전송한다.

Step 5. 인바운드 프락시 서버는 OTP를 이용하여 UAS로부터 받은 200 OK 메시지에 대한 무결성 검사 및 UAS에 대한 인증을 수행한다. UAS에 대한

인증 및 메시지의 무결성 검사가 성공하면 암호화키를 이용해 SDP를 복호화 한 후 INVITE 메시지를 아웃바운드 프락시 서버로 전송한다. 이 때 프락시 서버 간에는 TLS가 필수로 적용되기 때문에 프락시 서버 간에는 인증 및 SDP에 대한 기밀성이 보장된다.

Step 6. 아웃바운드 프락시 서버는 UAC와 공유하고 있는 OTP를 사용하여 200 OK 메시지에 대한 메시지다이제스트를 생성한다. 또한 암호화키를 사용하여 SDP를 암호화한다. 그리고 생성한 메시지 다이제스트와 암호화된 SDP를 200 OK 메시지와 함께 UAC에게 전송한다.

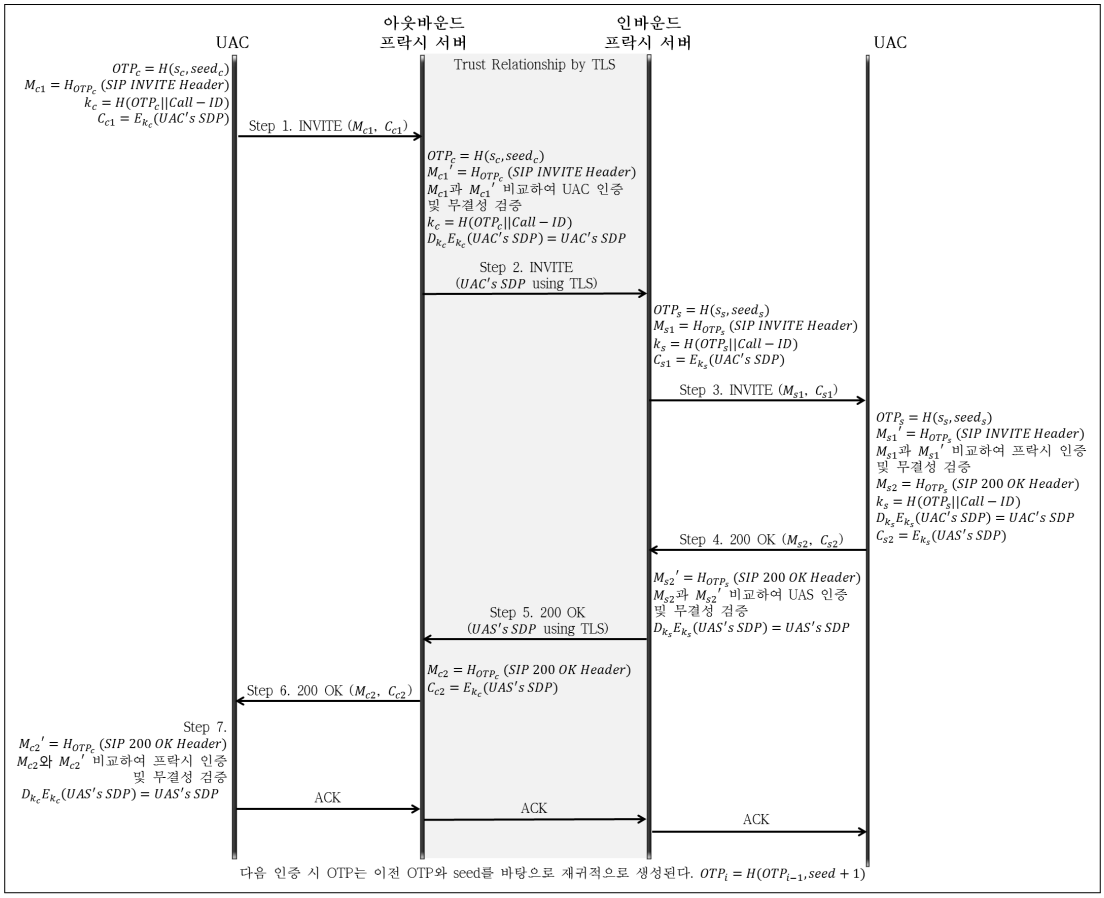
Step 7. UAC는 OTP를 사용하여 200 OK 메시지에 대한 무결성 검사 및 아웃바운드 프락시 서버에 대한 인증을 수행한다. 또한 암호화키를 사용하여 SDP를 복호화한다. 인증 및 무결성 검사가 성공하면 UAC는 ACK 메시지를 전송한다. 이후 UAC와 UAS는 SDP 안의 마스터키를 사용하여 SRTP 세션키를 생성하고 세션키를 통해 암/복호화여 미디어 스트림 전송을 수행한다. 다음 인증 시 사용될 OTP는 이전 OTP와 시드를 바탕으로 재귀적으로 생성된다.

IV. 제안 기법의 안전성 및 효율성

이 장에서는 제안 기법의 안전성과 효율성을 분석한다. 안전성 분석을 위하여, 다양한 공격 모델별로 제안기법이 어떻게 대응하는지 살펴본다. 또한 효율성 분석을 위하여 제안 기법과 기존 방법들의 암호학적 알고리즘의 수행 시간을 측정하여 비교하였다.

4.1 제안 기법의 안전성

4.1.1 재전송 공격(Replay attack)



〔그림 2〕 호 설정 과정

공격자는 이전에 정당한 SIP 사용자와 서버 사이에서 교환된 $M_{old} = H_{OTP_{old}}(SIP\,Header)$를 재사용하여 인증을 시도할 수 있다. 하지만 매 인증마다 OTP는 $OTP_{new} = H(OTP_{old}, seed+1)$와 같은 방법으로 새로 생성되기 때문에 이전에 사용된 M_{old}로는 인증에 실패하게 된다.

4.1.2 전수조사 공격(Brute force attack)

공격자는 임의의 고유값 s'와 시드 $seed'$를 통해 임의의 OTP'를 생성하여 무차별적으로 인증을 시도하여 OTP를 생성하는데 사용된 고유값과 시드를 알아내려는 공격을 시도할 수 있다. 본 논문에서 제안하는 기법은 일정 횟수 이상의 인증이 실패하면 해당 사용자는 차단되고 SIP 등록과정을 통해 OTP를 생성하기 위한 고유값과 시드를 새롭게 교환한다. 즉 공격자가 전수조사 공격을 시도하더라도 일정 횟수의 인증이 실패하면 자동적으로 차단되기 때문에 공격에 성공할 수 없다.

4.1.3 패스워드 추측 공격(Dictionary attack)

공격자는 SIP 메시지를 스니핑 한 후 $H_{OTP}(SIP\,Header)$와 $E_{H(OTP||Call-ID)}(SDP)$에 대한 사전 공격을 통해 OTP를 알아내려는 시도를 할 수 있다. 즉 본 논문에서 제안하는 기법의 안전성은 사용하는 키-해쉬함수와 대칭키 암호화 알고리즘의 안전성에 기반 한다고 볼 수 있다. 키-해쉬함수로 HMAC-MD5를 사용한다면, 공격자는 같은 메시지 다이제스트를 생성하기 위해 같은 비밀키를 사용하는 약 2^{64}개의 알려진 평문을 필요로 한다[17]. 하지만 본 논문에서 제안하는 기법은 매 인증마다 새로운 OTP를 암호화키로 사용하여 메시지다이제스트를 생성하기 때문에 공격자는 공격에 성공할 수 없다. 또한 SDP를 암/복호화하기 위해 AES-128을 사용한다면, 공격자는 $E_{H(OTP||Call-ID)}(SDP)$에 대한 암호화키를 알아내기 위해 2^{128}번의 테스트를 필요로 한다. 즉 암호화키를 알아내기 위해서는 많은 시간이 걸리므로, 매 호 설정마다 새롭게 생성되는 암호화키를 알아내는 것은 불가능하다.

4.1.4 중간자 공격(Man-in-the middle attack)

UA와 서버 사이에서 세션을 제어할 수 있는 공격자가 $H_{OTP}(SIP\,Header)$와 $E_{H(OTP||Call-ID)}(SDP)$를 가로채서 임의의 $H_{OTP'}(SIP\,Header)$와 $E_{H(OTP'||Call-ID)}(SDP)$를 전송하는 중간자 공격을 시도할 수 있다. 하지만 UA와 서버는 각기 자신이 가지고 있는 고유값과 시드를 통해 OTP를 생성하기 때문에, 공격자가 OTP를 변경할 경우 UA와 서버는 잘못된 인증값을 감지하게 되고 SDP에 대한 복호화에 실패하게 된다. 이는 OTP를 모르는 공격자가 사용자와 서버 사이에서 중간자 공격을 할 수 없음을 의미한다.

4.2 제안 기법의 효율성

기존에 제안된 방법들은 SDP를 암/복호화하기 위한 방법은 제공하지 않기 때문에, 기존에 제안된 방법들과 본 논문에서 제안한 기법의 효율성을 검증하기 위해 사용자 인증에 사용된 암호 알고리즘의 수행시간을 비교하였다. 본 논문에서 제안하는 방법에서 사용자 인증에 사용하는 키-해쉬함수와 DH 키 교환 알고리즘을 사용한 방법[12][13]의 DH 키 교환 알고리즘, IBC 기반[14][15]의 페어링 연산을 반복적으로 30번씩 수행한 후, 평균을 내어 각각의 단일 암호 알고리즘의 수행 시간을 측정하였다. 이렇게 구해진 단일 암호 알고리즘의 수행시간에 각각의 인증기법에서 암호 알고리즘을 사용한 횟수를 곱해 실질적으로 인증에 수행되는 시간을 계산하였다. 제안 기법의 수행시간 측정을 위해 키-해쉬함수로 HMAC-MD5를 사용하였다. 키-해쉬함수와 DH 키 교환 알고리즘의 구현을 위해 yaSSL[18] 라이브러리를 사용하였고, 페어링 연산은 PBC Library [19]를 사용하여 구현하였다.

실험 환경은 Intel Core2 Duo P8800 CPU 기반의 노트북으로 다른 프로세스의 영향을 최소화하기 위해 윈도우즈 7의 안전모드 상에서 수행시간을 측정하였다. 단일 암호화 알고리즘의 수행시간에 대한 측정 결과는 [표 2]와 같고, 실질적으로 각각의 인증 기법에서 암호 알고리즘을 수행한 횟수를 곱한 암호학적 총 연산량은 [표 3]과 같다.

본 논문에서 제안하는 기법은 상호 인증을 위해 UA와 SIP 서버가 각각 OTP를 생성하기 때문에 총 4번의 키-해쉬함수 연산을 필요로 한다. DH 키 교환 알고리즘을 사용한 방법[12][13]은 상호 인증을 위해 한 번의 DH 키 교환 연산을 필요로 한다. IBC 기반의 사용자 인증 및 키 교환 방법[14][15]은 상호 인증을 위해 UA와 SIP 서버가 각각 페어링 연산을 수

〔표 2〕 단위 암호 알고리즘 수행 시간

	Security size	Execution Time		
		평균	분산	표준편차
T_H	1024 bit	28.1 μs	1.82	1.35
T_D		23131.5 μs	258365.08	508.30
T_P		90324 μs	1569252.41	1252.70

T_H: HMAC-MD5 Operation
T_D: Diffie-Hellman Key Agreement Operation
T_P: tate pairing

〔표 3〕 상호 인증에 필요한 암호학적 총 연산량 비교

제안 방법	Time Cost
Proposed scheme	$4T_H$
DH 키 교환 알고리즘 기반의 방법〔12〕〔13〕	T_D
IBC 기반의 방법〔14〕〔15〕	$2T_P$

행하기 때문에 총 2번의 페어링 연산을 필요로 한다. 본 논문에서 제안하는 기법은 사용자 인증에 4번의 키-해쉬함수 연산을 필요로 하지만 키-해쉬함수 연산의 연산 속도가 다른 암호화 알고리즘에 비해 훨씬 빠르기 때문에, 기존에 제안된 방법들에 비해 더 효율적인 상호 인증이 가능하다. 또한 기존에 제안된 방법들은 SDP 암/복호화를 위해 종 단간 보안에 S/MIME, 홉 간 보안에 TLS를 적용하여야 한다. 따라서 UA와 SIP 서버간의 TLS 설정을 위한 핸드쉐이크 과정이 추가적으로 필요하고, SIP 서버에서 모든 UA에 대한 TLS 세션을 유지해야 하므로 많은 오버헤드가 발생한다. 하지만 제안 기법은 UA와 SIP 서버 사이에 TLS의 적용 없이 사용자 인증에 사용된 OTP와 랜덤하게 생성되는 Call-ID를 이용하여 SDP 암호화키를 생성하기 때문에 효율적인 SDP 암/복호화를 지원한다.

V. 결론

기존의 SIP 인증 및 키 교환 기술은 SIP의 보안요구사항을 제대로 충족시키지 못하거나 많은 암호학적 연산량을 요구하였다. 또한 SDP 보호를 위한 방법은 제공하지 않기 때문에 S/MIME, TLS 등을 함께 적용해서 사용하여야 하므로 많은 오버헤드가 발생한다. 이에 본 논문에서는 OTP를 사용한 효율적이고 안전한 VoIP 보안 모델을 제시하였다. 제안 기법은 OTP를 사용하여 사용자 인증, 시그널링 채널의 무결성 검증, SDP 정보에 대한 암/복호화를 수행한다. 제안 기법은 OTP를 사용하여 높은 보안성을 제공하면서, 많은 계산량을 요구하지 않으므로 효율적으로 VoIP 시스템에 대한 보호가 가능하다. 또한 제안 기법은 기존 SIP 파라미터에 약간의 수정만으로 구현이 가능하기 때문에 이미 널리 사용되고 있는 SIP 환경에 쉽게 적용할 수 있다. 향후 연구로는 OTP를 사용한 다자간 컨퍼런스 시스템의 보안을 위한 기술과 SIP 서버 간에 TLS가 적용되지 않은 경우, OTP를 사용하여 안전하게 SDP 암/복호화를 제공할 수 있는 기술이라 사료된다.

참고문헌

〔1〕 강신각, "인터넷 텔레포니(VolP) 포럼 (www.voip-forum.or.kr)", TTA 저널, 84, pp. 176-181, 2002년 11월.
〔2〕 J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002.
〔3〕 J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", IETF RFC 2617, June 1999.
〔4〕 T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", IETF RFC 5246, Aug. 2008.
〔5〕 S Turner, "Secure/Multipurpose Internet Mail Extensions", IEEE Internet Computing, vol. 14, no. 5, pp. 82-86, Sep. 2010.
〔6〕 M. Handley, V. Jacobson, and C. Perkins, "SDP: Session Description Protocol", IETF RFC 4566, July 2006.
〔7〕 E. Rescorla, "Diffie-Hellman Key Agreement Method", IETF RFC 2631, June 1999.
〔8〕 A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", Advance in Cryptology, CRYPTO'84, LNCS 196,

pp. 47-53, 1985.
〔9〕 D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-based One-Time Password Algorithm", IETF RFC 4226, Dec. 2005.
〔10〕 N. Haller, C. Metz, P. Nesser, and M. Straw, "A One-Time Password System", IETF RFC 2289, Feb. 1998.
〔11〕 F. Andreasen, M. Baugher, and D. Wing, "Session Description Protocol Security Description for Media Streams", IETF RFC 4568, July 2006.
〔12〕 C. Yang, R. Wang, and W. Liu, "Secure authentication scheme for session initiation protocol", Computers & Security, vol. 24, no. 5, pp. 381-386, Aug. 2005.
〔13〕 최재덕, 정수환, "효율적이고 안전한 SIP 사용자 인증 및 키 교환", 정보보호학회논문지, 19(3), pp. 73-82, 2009년 6월.
〔14〕 J. Ring, K. Choo, E. Foo, and M. Looi, "A New Authentication Mechanism and Key Agreement Protocol for SIP Using Identity-based Cryptography", Proceeding of AusCERT Asia Pacific Information Technology Security Conference, pp. 57-72, May 2006.
〔15〕 C. Yeun, K. Han, and K. Kim, "New Novel Approaches for Securing VoIP Applications", Sixth International Workshop for Applied PKC, Dec. 2007.
〔16〕 T. Guillet, R. Moalla, A. Serhrouchni, and A. Obaid, "SIP Autehntication based on HOTP", Proceedings of the 7th international conference on Information, communications and signal processing, pp. 685-688, Dec. 2009.
〔17〕 H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", IETF RFC 2104, Feb. 1997.
〔18〕 YaSSL, http://www.yassl.com/yaSSL/Products-cyassl.html
〔19〕 PBC Library, http://crypto.stanford.edu/pbc/download.html

〈著者紹介〉

김 정 제 (Jungje Kim) 학생회원
2009년 2월: 중앙대학교 컴퓨터공학과 학사 졸업
2009년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 VoIP 보안, IPTV 보안, 컨텐츠 보안, 네트워크 보안

정 만 현 (Man-Hyun Chung) 학생회원
2006년 2월: 동국대학교 컴퓨터학과 학사
2009년 2월: 고려대학교 정보보호대학원 석사
2010년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 패턴인식, 시스템 보안, 네트워크 보안

조 재 익 (Jaeik Cho) 학생회원
2005년 2월: 동국대학교 컴퓨터학과 학사 졸업
2008년 2월: 고려대학교 정보보호대학원 석사
2008년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

손 태 식 (Taeshik Shon) 정회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 컴퓨터 공학 석사
2005년 8월: 고려대학교 정보보호대학원 박사
2007년~2011년: 삼성전자 DMC 연구소 책임연구원
2011년~현재: 아주대학교 정보컴퓨터공학부 부교수
〈관심분야〉 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

문 종 섭 (Jongsub Moon) 종신회원
1981년 2월~1985년: 금성 통신 연구소 연구원
1991년: Illinois Institute of technology 졸업(전산학 박사)
1993년~현재: 고려대학교 전자 및 정보공학부 교수
〈관심분야〉 생체인식, 침입탐지, 운영체제