SIP P2P 스팸 방지를 위한 인증 및 SDP 암호화 키 교환 기법

준회원 장 유 정*, 종신회원 정 수 환*°, 준회원 최 재 식*, 최 재 덕*,
정회원 원 유 재**, 조 영 덕**

A Session Key Exchange Scheme for Authentication and SDP Encryption to Protect P2P SPIT in SIP

Yujung Jang* *Associate Member*, Souhwan Jung*° *Lifelong Member*,
Jaesic Choi*, Jaeduck Choi* *Associate Members*, Yoojae Won**, Youngduk Cho** *Regular Members*

요 약

본 논문에서는 SIP 기반의 VoIP 망에서 발생할 수 있는 스팸 위협에 대해 분석하고 이를 차단하기 위해 UA와 프락시 서버 간에 인증 및 SDP를 암호화할 수 있는 키 교환 기법을 제안한다. 기존 HTTP 다이제스트 인증은 호 설정 시 마다 사용자 인증을 위해 매 번 challenge 값을 전송해야 하므로 많은 메시지 교환 과정이 요구되고 SDP에 대한 기밀성도 제공하지 않는다. 제안 기법은 본 논문에서 분석한 스팸 위협을 차단하기 위해 등록 과정에서 세션 마스터 키 및 초기 nonce를 교환하고 이 키를 인증 키 및 암호화 키로 유도해 사용하므로 호 설정 시 challenge 값 전송에 따른 메시지 교환 과정과 S/MIME 또는 TLS 적용 시 발생하는 오버헤드를 줄일 수 있다.

Key Words : SPIT, VoIP 스팸, 키 교환, 인증, SDP 암호화

ABSTRACT

This paper analyzes spam threats and proposes key exchange scheme for user authentication and SDP encryption to protect potential spam threats in SIP-based VoIP services. The existing HTTP digest authentication scheme exchanges many message because challenge is sent for every establishment of the session and doesn't provide a confidentiality of SDP. To protect SPIT, our scheme exchanges initial nonce and a session master key for authentication and SDP encryption during registration. In our scheme, the challenge and response procedure is not necessary and the communication overhead is much less than applying S/MIME or TLS.

Ⅰ. 서 론

현재 VoIP (Voice over Internet Protocol)는 전통적인 PSTN (Public switched telephone network) 망을 대체하는 IP 네트워크 기반의 음성 통신 서비스이다. 특히 VoIP는 기존의 PSTN 망 보다 더 저렴하게 이용 가능하고 음성 통신 뿐 아니라 데이터 통신을 이용한 여러 부가 서비스를 제공할 수 있어 각광을 받고 있다. 산업 전문 미디어인 TMCnet에 따르면 VoIP 서비스는 2006년보다 125% 성장해

※ 본 연구는 숭실대학교 교내연구지원과 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음 (2006-S-043-02, VoIP정보보호기술)
* 숭실대학교 정보통신전자공학부 통신망보안 연구실 (lilyuwjd@cns.ssu.ac.kr), (souhwanj@ssu.ac.kr)(° : 교신저자),
(choijs, cjduck@cns.ssu.ac.kr), ** 한국정보보호진흥원 응용 기술팀 ({yjwon, ydcho}@kisa.or.kr)
논문번호 : KICS2007-09-393, 접수일자 : 2007년 9월 04일, 최종논문접수일자 : 2007년 11월 22일

사용자 수가 9백만 명이 넘었다고 한다. 그러나 이러한 오픈 네트워크상에서는 정상 호의 발송 뿐 아니라 비정상 호의 발송도 쉬워지므로 이메일과 같이 스팸에 대한 문제를 고려하지 않을 수 없다. 이에 SIP (Session Initiation Protocol) 기반의 VoIP 환경에서 스팸을 차단하기 위한 표준화 작업이 IETF SIPPING WG과 ITU-T SG17에서 활발히 진행 중이다. 각 표준화 기구에서 제안하는 SIP 기반의 VoIP 스팸 차단 기술은 기존의 이메일 스팸 차단 기법인 화이트/블랙리스트, 콘텐츠 필터링, 평판 시스템 등을 VoIP 환경에 적용한 것으로 정상적인 경로를 통해 발송된 스팸을 차단할 수 있다[1][2][3]. 반면 본 논문에서 살펴 볼 P2P (Peer-to-Peer) 스팸과 같은 비정상적인 경로를 통해 발송된 스팸은 각 홉 간에 인증을 하지 않으면 차단하기 어렵다. 이메일 기반의 스팸 차단 기법에도 인증 관련 기법인 SPF (Sender Policy Framework)[4]나 DKIM (DomainKeys Identified Mail)[5] 기법 등이 있지만 이 역시 프락시 서버에 적용하는 기법으로 P2P로 발송된 스팸은 차단하기 어렵다. 기본적으로 SIP 프로토콜은 메시지를 주고받을 때 사용자 인증을 위해 HTTP 다이제스트 인증 기법을 제공한다. 하지만 HTTP 다이제스트 인증은 패스워드 기반의 인증 메커니즘으로 패스워드 추측 공격에 취약하고 호 설정 시 마다 인증을 위해 challenge 값을 전송해야 하므로 많은 메시지 교환 과정이 요구된다. 또한 SDP (Session Description Protocol) 정보에 대한 기밀성을 제공하지 않기 때문에 RTP (Real-time Transport Protocol) 통신을 하는 두 UA (User Agent)의 IP 주소 및 포트 번호와 미디어 스트림 정보가 노출되어 스팸 공격에 대해 다양한 취약성이 존재한다. 따라서 UAC (UA Client)와 UAS (UA Server) 사이의 전체 구간에서 인증이 가능하고 SDP에 대한 기밀성을 제공하는 것은 물론 호 설정 과정의 오버헤드를 줄일 수 있는 스팸 차단 기법이 필요하다.

본 논문에서는 UA가 프락시 서버에 등록할 때 마스터 키를 공유해 호 설정 시 인증 및 암호화 키로 사용할 수 있는 키 교환 기법을 제안한다. 제안 기법을 사용해 공유된 키로 인증 및 SDP에 대해 암호화를 할 경우 호 설정 시 challenge 값 전송에 따른 메시지 교환 과정과 TLS 보안 채널 형성에 따른 오버헤드를 줄일 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 VoIP 스팸 위협에 대해 분석하고 스팸 대응 관련 기법을 살펴본다. Ⅲ장에서는 스팸을 차단하기 위한 프락시 서버와 UA 간 인증 및 SDP 암호화 키 교환 기법을 제안하고, Ⅳ장에서 제안된 기법에 대한 안전성을 분석한다. Ⅴ장에서는 S/MIME 및 TLS와 제안된 기법을 비교 분석하고, 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. VoIP 스팸 위협 분석 및 대응 관련 기법

SIP 상에서 발생하는 스팸은 크게 두 종류로 생각해 볼 수 있다. 정상적인 UAC가 프락시 서버를 거쳐 UAS로 스팸을 발송하는 경우와 비정상적인 경로를 통해 P2P로 스팸을 발송하는 경우가 있다. 전자의 경우에는 이메일 기반의 스팸 차단 기법을 사용하면 어느 정도 차단이 가능하다. 하지만 후자의 경우에는 프락시 서버를 거치지 않고 P2P로 발송되기 때문에 새로운 기법을 고려해야 한다. 이에 본 논문에서는 비정상적인 경로로 발송되는 P2P 스팸의 위협에 대해 분석해 보고 이를 차단하기 위해 기존에 연구된 인증 및 SDP 암호화 기법을 살펴본다.

기본적으로 SIP 기반의 VoIP 환경에서는 사용자 인증을 위해 HTTP 다이제스트 인증 기법[6]과 S/MIME (Secure Multi-Purpose Internet Mail Extensions)[7] 및 TLS (Transport Layer Security)[8]를 제공한다[9]. S/MIME은 UAC와 UAS 양 단간의 보안을 위해서 선택적으로 적용 가능하고 TLS는 각 홉 간의 보안을 위해서 선택적으로 적용 가능하다. 또한 UAC와 아웃바운드 프락시 서버 간에는 HTTP 다이제스트 인증이 필수로 적용된다. 하지만 HTTP 다이제스트 인증은 패스워드 추측 공격에 취약할 뿐 아니라 프락시 서버에 대한 인증은 선택적으로 제공된다. 또한 프락시 서버 간에는 TLS가 필수로 적용되지만 프락시 서버와 UA 간에는 사용자에 의해 선택적으로 제공되기 때문에 TLS와 같은 보안을 적용하지 않은 경우 스패머는 아웃바운드 프락시 서버 또는 인바운드 프락시 서버로 위장해 UAC나 UAS에게 P2P로 스팸을 발송할 수 있다. 또한 SIP 호 설정 시 INVITE 메시지나 200 OK 메시지의 SDP에 대해 기밀성을 제공하지 않는다면 스패머는 SDP 분석을 통해 음성 통화를 하는 두 사용자의 IP 주소 및 포트 번호, 미디어 스트림 정보 등을 알 수 있다. 이를 이용해 스패머는 UAC나 UAS에게 P2P로 스팸 발송이 가능하고 심지어 통화 내용에 대한 도청도 가능하다. 다음은 발생 가능한 스팸 시나리오를 상세히 나타낸다.

2.1 임의의 200 OK 전송을 통한 P2P 스팸 발송

그림 1과 같이 스패머는 UAC가 UAS와 통화를 하기 위해 보낸 INVITE 메시지를 스니핑하고 UAS가 INVITE에 대한 응답을 하기 전에 임의의 200 OK 메시지를 생성해 프락시 서버가 보낸 것처럼 UAC에게 전송한다. 이 때 200 OK 메시지의 SDP 정보 중 주소 정보 (IP 주소와 포트 번호)를 스패머의 주소 정보로 대체한다. 스패머는 INVITE 메시지 안의 SDP 정보를 참고로 UAC에게 광고성 RTP를 전송한다. 이 시나리오는 1:1 통화는 가능하나 사용자가 통화를 요청할 때만 스팸을 발송할 수 있는 제약이 따른다.

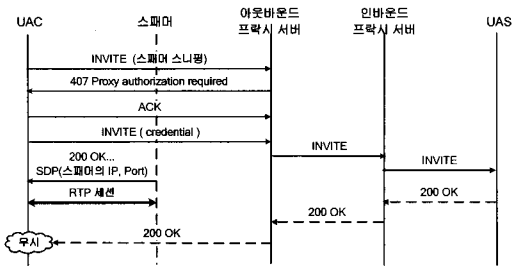


그림 1. 임의의 200 OK 전송을 통한 스팸 발송

2.2 인바운드 프락시 서버로 위장한 스패머의 P2P 스팸 발송

그림 2와 같이 스패머는 인바운드 프락시 서버로 위장해 UAS에게 INVITE 메시지를 전송한다. 이 때 INVITE 메시지의 SDP 정보 중 주소 정보를 스패머의 주소 정보로 대체한다. 이 INVITE 메시지를 받은 UAS는 응답으로 200 OK 메시지를 원래의 프락시 서버에게 보낸다. 스패머는 이 200 OK 메시지를 스니핑 해 RTP 통신을 위한 정보를 수집하고, UAS에게 임의의 ACK 메시지를 생성해 보낸다. 그 후 스패머는 UAS에게 광고성 RTP 패킷을 전송한다. 이 시나리오는 무료로 1:1 통화를 할 수 있을 뿐 아니라 스패머는 언제든지 스팸을 발송할 수 있다.

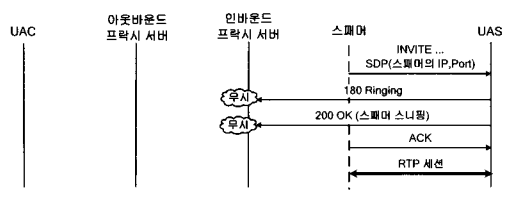


그림 2. 인바운드 프락시 서버로 위장한 스패머의 스팸 발송

2.3 RTP 패킷 스푸핑을 통한 P2P 스팸 발송

스패머는 UAC와 UAS 간 전송되는 INVITE 메시지와 200 OK 메시지를 스니핑한다. UAC와 UAS 간에 정상적으로 호 연결이 되면 그림 3과 같이 기존에 스니핑 한 메시지의 SDP 정보를 바탕으로 RTP 정보를 얻는다. 스패머는 UAC가 UAS에게 보내는 RTP 패킷을 스니핑 해 광고성 RTP 패킷을 생성한다. 이 때 생성하는 RTP 패킷 헤더의 SSRC (Synchronization Source) 값은 스니핑 한 RTP 패킷과 동일해야 하며 순차번호 값은 기존 것 보다 커야한다. 스패머는 UAC에게 임의로 BYE 메시지를 전송하고 UAS에게는 생성한 RTP 패킷을 전송한다. 이 시나리오는 1:1 통화는 불가능하지만 스패머가 UAS로 RTP 패킷을 전송하는 것은 가능하므로 광고성 RTP 패킷을 UAS에게 전송할 수 있다.

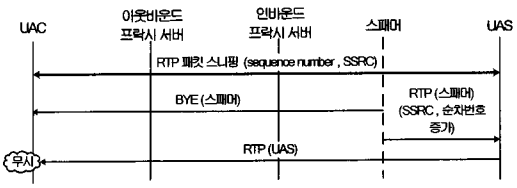


그림 3. RTP 패킷 스푸핑을 통한 스팸 발송

2.4 스팸 대응 관련 기법

앞에서 언급한 시나리오와 같이 UA에서 프락시 서버를 인증하지 않고 SDP에 대한 기밀성을 제공하지 않을 경우 다양한 스팸 발송이 가능하다. 이를 차단하기위해 HTTP 다이제스트 인증을 사용해 아웃바운드 프락시 서버에서 UAC를 인증하는 것처럼 UAS가 인바운드 프락시 서버를 인증하도록 하는 기법[10]이 제안되었다. 하지만 이 기법 또한 HTTP 다이제스트 인증 기법을 사용하므로 패스워드 추측 공격에 취약하다. 이에 Yang 등이 HTTP 다이제스트 기법에 DH (Diffie-Hellman) 알고리즘을 적용한 인증 기법[11]을 제안했다. 이는 패스워드 추측 공격을 차단할 뿐만 아니라 프락시 서버와 UA가 상호 인증을 수행한다. 먼저 UA는 DH 개인키 r_1을 선택하고 공개정보 $(p,\ g)$를 바탕으로 DH 공개키 t_1을 생성한다. 이 t_1과 프락시 서버에 사전에 등록한 패스워드를 해쉬한 값 $H(pw)$를 XOR (exclusive-OR : $\oplus$)하고 이 값과 *username* 값을 프락시 서버에 전송한다.

$$t_1 = g^{r_1} \bmod p$$

이 정보를 받은 프락시 서버는 패스워드를 해쉬한 값 $H(pw)$를 계산해 t_1 값을 얻을 수 있다.

$$t_1 = (t_1 \oplus H(pw)) \oplus H(pw)$$

프락시 서버 또한 DH 개인키 r_2를 선택하고 t_1과 같이 공개정보를 바탕으로 DH 공개키 t_2를 생성한다. UA와 프락시 서버는 t_1, t_2 값을 이용하면 세션 키 K를 계산한다.

$$K = g^{r_1 r_2} \bmod p$$

프락시 서버는 t_2와 $H(pw)$를 XOR 연산한 값, t_1과 K를 해쉬한 값, *realm* 값을 UA에게 전송한다. 이 정보를 받은 UA는 t_2와 K 및 $H(t_2 \| K)$ 값 계산하여 프락시 서버를 인증한다. 그 후 UA가 계산된 K를 *username* 및 *realm* 값과 다시 해쉬해서 보내주면 이를 받은 프락시 서버 역시 K와 *username* 및 *realm* 값을 해쉬해서 받은 값과 동일한지 검증함으로써 UA를 인증한다.

이는 모든 메시지를 전송할 때 적용 가능하고 이에 모든 메시지에 대해 인증을 할 수 있다. 또한 패스워드를 인증에 바로 사용하는 것이 아니라 DH 공개키 값과 XOR 연산을 한 후 사용하므로 패스워드 추측 공격에 안전하다. 하지만 이 기법은 인증을 위해 각 메시지마다 DH을 적용하므로 오버헤드가 크고 인증할 때마다 challenge 값을 전송해줘야 한다. 또한 SDP에 대한 기밀성을 제공하지 않으므로 여전히 스팸 공격에 취약하다.

스팸 대응의 또 다른 방법으로는 SIP 메시지 인증 및 SDP 암호화를 위해 S/MIME을 적용할 수 있다. 그러나 S/MIME은 공개키 기반이므로 인증서 발급을 위한 기반 구조가 갖추어져야 하고, 인증을 위해 SIP 헤더를 해쉬한 S/MIME 바디 부분이 전체 메시지에 추가되어야하므로 메시지 길이가 커지는 오버헤드가 발생한다. S/MIME은 홉 간 보안이 아닌 UAC와 UAS 구간과 같이 양단간 보안이기 때문에 인바운드 프락시 서버로 위장해 UAS에게 P2P로 발송하는 스팸에는 취약하다. 만약 UA와 프락시 서버 간에 인증 및 SDP 암호화를 위해 TLS를 적용한다면 S/MIME과 마찬가지로 인증서 발급을 위한 기반 구조가 갖추어져야 하고 프락시 서버에서 모든 UA에 대해 TLS 세션을 유지해야 하므로 오버헤드가 발생한다. 또한 각 메시지에 대한 암·복호화 과정으로 세션 연결 시 지연이 발생한다.

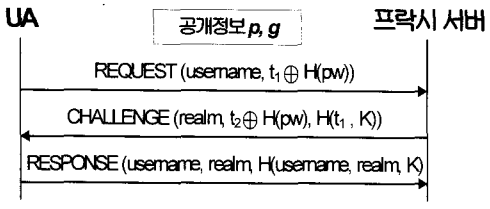


그림 4. DH을 이용한 HTTP 다이제스트 기법

따라서 UA와 프락시 서버 간 상호 인증이 가능하고 SDP에 대한 기밀성을 제공하는 것은 물론 S/MIME이나 TLS를 적용했을 때 보다 오버헤드 및 메시지 전송의 지연을 줄일 수 있는 새로운 인증 기술이 필요하다.

Ⅲ. 인증 및 SDP 암호화를 위한 키 교환 기법

본 논문에서는 UA와 프락시 서버 간 TLS 보안이 적용되지 않은 경우 다양한 스팸 공격에 대응하기 위해 UA와 프락시 서버를 인증하고 SDP를 암호화하기 위한 키 교환 기법을 제안한다. 제안 기법은 등록 시 공유한 마스터 키 값과 초기 *nonce*를 이용해 호 설정 시에 인증 및 SDP의 기밀성을 제공함으로써 다양한 스팸 공격을 차단한다.

3.1 시스템 계수

본 논문에서 제안된 기법을 설명하기에 앞서 제안된 기법에 사용되는 용어를 정의한다.

표 1. 시스템 계수 정의

표기	정의
n_{ci}	UAC와 프락시 서버 간 i번째 nonce 값
n_{si}	UAS와 프락시 서버 간 i번째 nonce 값
K_{CA}	UAC와 프락시 서버 간 인증 키 값
K_{CE}	UAC와 프락시 서버 간 암호화 키 값
K_{SA}	UAS와 프락시 서버 간 인증 키 값
K_{SE}	UAS와 프락시 서버 간 암호화 키 값

3.2 등록 과정

제안 기법에서 등록 과정은 Yang 등이 제안한 인증 기법을[11] 개선하여 그림 6과 같이 세션 마스터 키 K를 생성하는 과정이다. 이 과정을 통해 등록 시 상호 인증을 할 수 있고 생성된 마스터 키를 호 설정 시 인증 및 SDP 암호화에 사용한다. 또한 등록 성공을 알리는 200 OK 메시지를 통해 초기

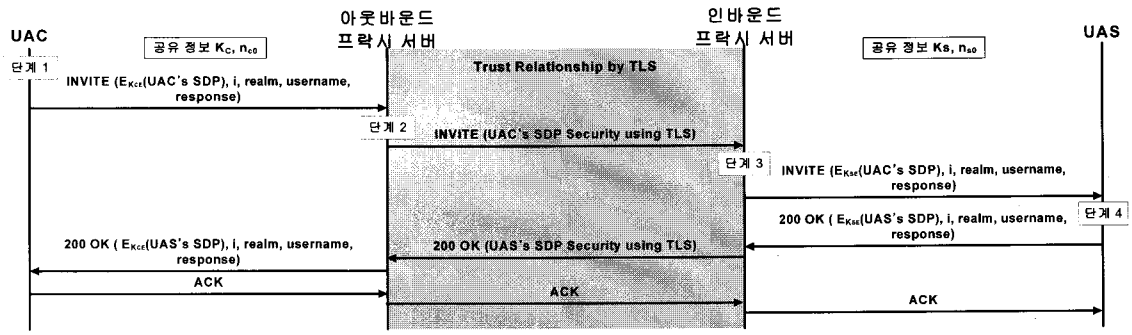


그림 5. 호 설정 시 세션 키를 이용한 인증 및 SDP 암호화 과정

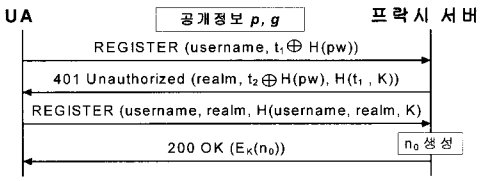


그림 6. 등록 과정

*nonce*를 공유함으로써 호 설정 시 인증을 위해 전송되는 메시지 수를 줄이고 재전송 공격도 차단할 수 있다. 이 때 초기 *nonce*는 둘 사이의 마스터 키를 이용해 암호화해 전송한다.

3.3 호 설정 과정

등록 과정을 마친 UA와 프락시 서버는 둘 사이에 공유된 마스터 키 K와 초기 *nonce* (n_0)를 가지고 있다. UA와 프락시 서버는 공유된 K를 이용해 상호 인증을 위한 키 K_A와 SDP 암호화를 위한 키 K_E를 각각 유도한다. 이 때 랜덤하게 생성되는 call-ID 값을 이용하여 보안을 강화할 수 있다. 인증 및 암호화 키를 유도하는 방법은 다음과 같다.

$$K_A = H(K \parallel call\text{-}ID \parallel \text{"Authentication Key"})$$
$$K_E = H(K \parallel call\text{-}ID \parallel \text{"Encryption Key"})$$

또한 n_0를 이용해 *nonce* 값을 해쉬 체인으로 생성한다. 매 메시지 전송 시 마다 다른 n_i를 사용해 인증 시 사용함으로써 따로 challenge 값을 전송할 필요가 없고 재전송 공격도 차단한다.

$$n_i = H(n_{i-1})$$

그림 6은 UAC가 UAS에게 호 설정을 요청해 호가 설정되는 과정을 보여주고 그에 대한 상세한 내용은 다음과 같다.

단계 **1**. UAC가 INVITE 메시지를 전송할 때는 생성된 *nonce* n_{c1}와 인증 키 K_{CA} 값을 넣어 해쉬하고 (*response*), 암호 키 K_{CE}를 이용해 SDP를 암호화해 아웃바운드 프락시 서버에게 전송한다. 이 때 *nonce* 값은 UA와 프락시 서버에서 각각 초기 n_0 값을 이용해 생성하므로 동기화 문제가 발생할 수 있다. 따라서 몇 번째 *nonce*인지를 나타내는 변수 i 값을 같이 전송함으로써 동기화 문제를 해결한다.

$$response = H(n_{c1} \| username \| K_{CA} \| realm)$$

단계 **2**. INVITE 메시지를 받은 아웃바운드 프락시 서버는 *response* 값을 계산해 받은 *response* 값을 비교한다. 이를 통해 아웃바운드 프락시 서버는 UAC를 인증하고, 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.

단계 **3**. INVITE 메시지를 받은 인바운드 프락시 서버는 UAS와 등록 시 공유한 마스터 키 값 K_S와 n_{s0}를 이용해 UAC와 마찬가지로 *response* 값을 계산한 후 SDP를 암호화 해 UAS에게 전송한다.

단계 **4**. UAS는 *response* 값을 계산해 받은 INVITE 메시지의 *response* 값과 비교해 인바운드 프락시 서버를 인증한다. 또한 암호화 된 SDP를 복호화 해 RTP 통신을 위해 필요한 정보를 사용한다. 인바운드 프락시 서버에 대해 인증이 성공한 경우 200 OK 메시지를 전송해 호 설정에 응한다. 이 때 역시 새로 생성한 *nonce*를 이용해 *response* 값을 계산하고 SDP를 암호화 해 전송함으로써 추후에 상호 인증 및 SDP에 대한 기밀성을 제공할 수 있

도록 한다. 200 OK 메시지 전송 시에도 INVITE 메시지 전송과 마찬가지로 *response* 값 생성/검증, SDP 암·복호화를 이용해 상호 인증 및 SDP에 대한 기밀성을 제공한다.

Ⅳ. 안전성 분석

이번 장에서는 본 논문에서 제안한 기법의 안전성에 대해서 논한다.

4.1 재전송 공격 (Replay attack)

만약 공격자가 credential 값을 포함한 INVITE 메시지를 스니핑 해 재전송 공격을 시도하더라도 UA와 프락시 서버 간에 각 메시지를 전송할 때마다 *nonce* 값을 각각 생성하므로 기존 *nonce* 값으로 인증된 메시지는 검증에 실패한다. 또한 *nonce* 값이 노출되더라도 인증 키 값을 모르기 때문에 인증 값을 생성할 수 없다.

4.2 패스워드 추측 공격 (Dictionary attack)

기존 HTTP 다이제스트 인증 기법을 이용해 인증할 경우 공격자는 인증에 성공한 REGISTER 메시지나 INVITE 메시지의 challenge 값과 *response* 값을 이용해 패스워드 추측 공격을 시도할 수 있다. 하지만 제안 기법은 기존 HTTP 다이제스트 인증 기법과 달리 패스워드를 직접적으로 인증에 사용하는 것이 아니라 DH 세션 키와 패스워드의 해쉬 값을 XOR한 후 유도해 사용하므로 패스워드 추측 공격에 안전하다. 또한 매 등록 시마다 마스터 키를 새로 생성하고, 매 호 설정마다 call-ID를 이용해 인증 및 암호 키를 새로 유도하기 때문에 패스워드를 알아내기는 매우 어렵다.

4.3 서버 스푸핑 (Server spoofing)

만약 공격자가 프락시 서버로 위장해 P2P 스팸을 발송하더라도 제안 기법을 적용하면 프락시 서버에서 UA를 인증하는 것 뿐 아니라 UA에서도 프락시 서버를 인증하기 때문에 서버 스푸핑은 불가능하다.

4.4 중간자 공격 (Man-in-the middle attack)

등록 과정 시 공격자가 서버에게 전송되는 메시지 $t_1 \oplus H(pw)$를 가로채 임의의 값 $t_1' \oplus H(pw')$으로 바꾸어 서버에 전송하더라도 이를 받은 서버는 $t_1'' = t_1' \oplus H(pw') \oplus H(pw)$로 계산해 t_1''라는 새로운 값을 얻는다. 따라서 서버는 $(t_1'')^{r_2}$값을 키로, 공격자는 $(t_1')^{r_2}$값을 키로 가지게 된다. 이는 사용자의 패스워드를 모르는 공격자가 사용자와 서버 사이에서 중간자 공격을 할 수 없음을 의미한다.

4.5 데닝-사코 공격 (Denning-Sacco attack)

이 공격은 마스터 키가 노출되었을 경우 이를 통해 패스워드를 알아낼 수 있는 공격이다. 하지만 마스터 키 K는 $g^{r_1 r_2} \bmod p$이므로 패스워드에 관한 정보를 가지고 있지 않다. 따라서 이 공격으로부터 안전하다.

위에서 언급한 것과 같이 제안된 기법은 재전송 공격, 패스워드 추측 공격, 서버 스푸핑, 중간자 공격, 데닝-사코 공격에 대해 안전하다.

Ⅴ. 제안 기법 비교 분석

SIP 환경에서 제안 기법은 기존의 S/MIME 또는 TLS보다 효율적으로 스팸을 차단할 수 있다. 그림 7은 S/MIME 및 TLS를 적용했을 때의 호 설정 과정을 보여준다.

S/MIME이 스팸 차단을 위해 SIP에 적용된 경우, UAC와 UAS 간에 상대방의 공개키로 SDP를 암호화하고 메시지 헤더를 자신의 개인키로 서명한다. 즉, 공개키 기반의 암·복호화 과정이 이루어진다[7]. TLS가 SIP 전 구간에 적용된 경우에는 UA와 프락시 서버 간에 인증서를 이용해 SIP 세션 설정 전에 TLS 핸드셰이크 과정이 이루어져야 한다. TLS 세션이 설정된 이후에 SIP 노드들은 TLS 세션키를 이용해 SIP 각 메시지에 대해 HMAC 적용 및 대칭키 암·복호화 과정을 수행한다[8]. 또한 S/MIME 또는 TLS를 적용한 경우에는 UAC와 아웃바운드 프락시 서버 구간에서 HTTP 다이제스트 인증을 기본적으로 적용하기 때문에 해쉬 함수가 추가로 사용된다[6]. 반면 제안된 기법은 그림 5와 같이 SIP 각 메시지를 전송할 때 인증을 위해 해쉬 및 대칭키 암·복호화 과정만 수행한다.

표 2는 스팸 공격을 차단하기 위해 S/MIME 및 TLS가 적용된 경우와 제안 기법을 적용한 경우에 암호 연산 횟수, SIP 메시지 교환 횟수, 보안 요구사항 등을 비교한 표이다. S/MIME의 경우 암호화 및 서명 모드를 기반으로 비교하였다. 표 2에서와 같이 해쉬 함수 사용 및 대칭키 암·복호화 횟수는 TLS가 가장 많고 그 다음으로 제안 기법, S/MIME 순으로 적다. 하지만 해쉬 함수 사용 및 대칭키 암·복호화의 경우는 간단한 연산이므로 오버헤드

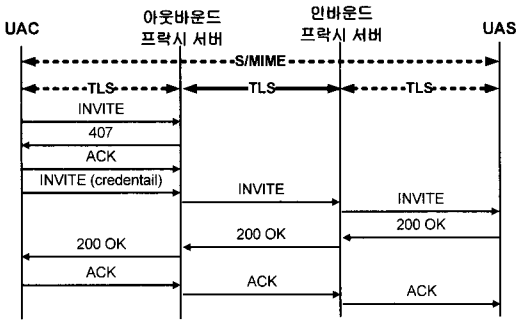


그림 7. S/MIME 또는 TLS를 적용한 호 설정 과정

표 2. S/MIME, TLS와 제안 기법 비교 분석

	S/MIME를 이용한 스팸 차단 (암호화 및 서명 모드)	TLS를 이용한 스팸 차단	제안 기법을 이용한 스팸 차단
해쉬 함수	9회	26회	22회
대칭키 암·복호화	0회	18회	14회
공개키 암·복호화	7회	0회	0회
공개키 서명·검증	7회	0회	0회
SIP 메시지 교환	12회	12회	9회
추가적인 보안 협상과정	×	TLS 설정을 위한 핸드셰이크 과정	×
PKI 기반	○	○	×

측면에서 호 설정 시 많은 영향을 주지 않는다. 하지만 공개키를 이용한 암·복호화 및 서명·검증은 많은 계산 량이 요구되므로 스팸 차단을 위해 S/MIME을 적용했을 경우 제안 기법을 적용했을 때 보다 호 설정 시 오버헤드가 더 발생한다. 또한 S/MIME의 경우 호 설정 시 교환하는 SIP 메시지 수도 제안 기법보다 많고, PKI 기반이므로 인증서 발급을 위한 기반 시설이 구축되어야 한다. 따라서 UA간 보안을 위해 S/MIME을 적용하기에는 많은 제약이 따른다. 한편 TLS를 사용했을 경우에는 S/MIME과 달리 공개키를 이용한 암·복호화 및 서명·검증 과정이 없지만 S/MIME과 마찬가지로 메시지 수도 제안 기법보다 많고, PKI 기반이므로 TLS 역시 인증서 발급을 위한 기반 시설을 필요로 한다. 또한 TLS의 경우에는 TLS 설정을 위한 핸드셰이크 과정이 필요하므로 제안 기법보다 스팸 차단을 위해 많은 오버헤드가 발생한다. 따라서 TLS도 마찬가지로 UA와 프락시 서버 간 TLS를 적용하기에 많은 제약이 따른다.

Ⅵ. 결 론

본 논문에서는 SIP 기반의 VoIP 환경에서 스팸에 대한 취약성을 분석하고 UA와 프락시 서버 간 TLS가 적용되지 않은 경우 스패머의 공격 시나리오를 설계하였다. 기존 SIP는 UA가 프락시 서버를 인증하는 과정이 선택적이고, SDP 암호화도 제공하지 않아 여러 경우의 스팸 발송이 가능하다. 또한 HTTP 다이제스트 인증 기법을 사용함으로 패스워드 추측 공격에도 취약하다. 이에 본 논문에서는 스팸을 차단하기 위해 UA와 프락시 서버 간 서로 인증을 할 수 있고 SDP에 대한 기밀성을 제공하기 위한 키 교환 기법을 제안하였다. 제안 기법은 S/MIME이나 TLS를 적용했을 때보다 인증 및 SDP 암호화를 위한 오버헤드가 적고 S/MIME이나 TLS와 달리 인증서가 필요하지 않으므로 인증서 발급을 위한 기반 시설 또한 필요로 하지 않는다. 따라서 제안 기법을 적용하면 S/MIME이나 TLS를 적용했을 때 보다 좀 더 효율적으로 P2P 스팸을 차단할 수 있다.

참 고 문 헌

[1] Yacine Rebahi, Dorgham Sisalem, and Thomas MageDanz, "SIP SPAM Detection," ICDT 2006, pp. 68~73, August 2006.

[2] Ram Dantu and Prakash Kolan "Detecting Spam in VoIP Networks," SRUTI'05, pp. 31~37, July 2005.

[3] J. Rosenberg, C. Jennings, and J. Peterson, "The Session Initiation Protocol (SIP) and Spam," IETF draft-ietf-sipping-spam-05, July 2007.

[4] M. Wong and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1," IETF RFC 4408, April 2006.

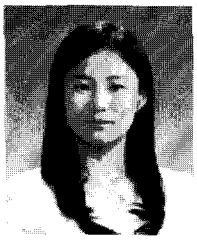
[5] J. Fenton, "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)," IETF RFC 4686, September 2006.

[6] 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.

[7] B. Ramsdell, "S/MIME Version 3 Message

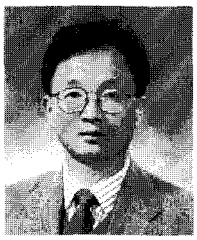
Specification," IETF RFC 2633, June 1999
[8] T. Dierks and C. Allen "The TLS Protocol Version 1.0," IETF RFC 2246, January 1999.
[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP(Session Initiation Protocol)," IETF RFC 3261, June 2002.
[10] Souhwan Jung and Jaeduck Choi, "Authentication between the Inbound Proxy and the UAS for Protecting SPIT in the Session Initiation Protocol (SIP)," IETF draft-jung-sipping- authentication-spit-00, March 2007.
[11] Chou-Chen Yang, Ren-Chiun Wang, and Wei-Tong Liu, "Secure authentication scheme for Session Initiation Protocol," Comput. Secur. Vol. 24(5), pp. 381~386. October 2004.

장 유 정 (Yujung Jang) 준회원



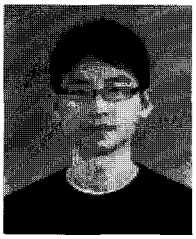
2006년 2월 숭실대학교 정보통신전자공학부 졸업
2006년~현재 숭실대학교 정보통신공학과(석사과정)
<관심분야> VoIP 보안, 네트워크 보안

정 수 환 (Souhwan Jung) 종신회원



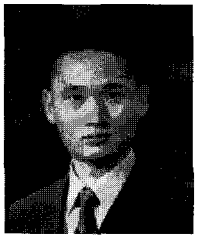
1985년 2월 서울대학교 전자공학과(학사)
1987년 2월 서울대학교 전자공학과(석사)
1998년~1991년 한국통신 전임연구원
1996년 6월 University of Washington(박사)
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안

최 재 식 (Jaesic Choi) 준회원



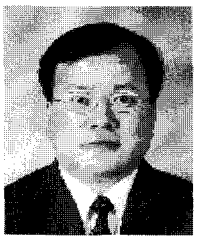
2007년 2월 숭실대학교 정보통신전자공학부 졸업
2007년-현재 숭실대학교 전자공학과(석사과정)
<관심분야>VoIP 보안, 네트워크 보안

최 재 덕 (Jaeduck Choi) 준회원



2002년 2월 숭실대학교 정보통신전자공학부 졸업
2004년 2월 숭실대학교 정보통신공학과(석사)
2005년~현재 숭실대학교 정보통신전자공학과(박사과정)
<관심분야> 이동 네트워크 보안, VoIP 보안, 네트워크 보안

원 유 재 (Yoojae Won) 정회원



1985년 2월 충남대학교 계산통계학과 졸업
1987년 2월 충남대학교 계산통계학과(석사)
1998년 8월 충남대학교 전산학과(박사)
1987년 2월~2001년 2월 한국전자통신연구원 팀장
2001년 3월~2004년 8월 안랩유비웨어 연구소장
2004년 9월~현재 한국정보보호진흥원 IT기반보호단 응용기술팀 팀장
<관심분야> 멀티캐스트 보안, 무선통신 보안, IPv6 보안, 멀티미디어 컨텐츠 보안, VoIP/IPTV 등 신규IT 서비스 보안

조 영 덕 (Youngduk Cho) 정회원

2000년 2월 아주대학교 정보및컴퓨터공학부 졸업
2002년 2월 아주대학교 정보통신공학과(석사)
2002년~현재 한국정보보호진흥원 IT기반보호단 응용기술팀
<관심분야> VoIP 보안, 신종스팸 대응, 네트워크 보안, 신규IT서비스 보안