SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법

준회원 장 유 정*, 종신회원 정 수 환*, 준회원 문 형 권*, 최 재 덕*,
정회원 원 유 재**, 조 영 덕**

An Authentication Schemes for Anti-spam in SIP-based VoIP Services

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

요 약

본 논문에서는 SIP 기반의 VoIP상에서 스팸 위협에 대해 분석하고 이를 차단하기 위해 UAS에서 inbound proxy 서버를 인증할 수 있는 발신자 인증 기법을 제안하였다. 제안된 기법은 UAS로 들어오는 메시지가 inbound proxy를 통해 전송됐는지 여부를 검증하기 위해 inbound proxy 서버와 UAS 간 사전에 공유하고 있는 패스워드를 기반으로 HTTP Digest 인증을 적용하였다. 이는 SIP 표준의 큰 수정 없이 쉽게 적용이 가능하고 peer-to-peer로 발생되는 스팸을 효과적으로 차단할 수 있다. 본 논문에서는 상용 망에서 peer-to-peer로 스팸을 발송해보고 제안된 기법을 이용해 스팸이 차단되는 것을 검증하기 위해 오픈 소스를 이용해 구현해 보았다.

Key Words : SPIT, VoIP, Spam, SIP, Authentication

ABSTRACT

This paper proposes a message authentication scheme to resist potential spam threats in SIP-based VoIP services. Our scheme applies the extended HTTP digest authentication mechanism between the inbound proxy and the UAS to verify that a service request is coming through the valid inbound proxy. The proposed scheme is simple and requires minimal modification the current SIP standards, and effective to filter invalid peer-to-peer spam calls. In this paper, an experimental spam attack using modified open source was tested on a commercial VoIP networks to exploit the possibility of spam attacks in real environment.

Ⅰ. 서 론

최근 SIP(Session Initiation Protocol) 기반의 VoIP(Voice Over Internet Protocol) 서비스에 대한 사람들의 관심이 증가하면서 VoIP 보안의 중요성이 제기되고 있다. 특히 SIP는 텍스트 기반의 이메일 주소를 사용하므로 이메일 환경에서와 마찬가지로 수신자의 ID를 수집하기 쉽고, 기존의 PSTN (Public Switched Telephone Network)망에서 보다 더 저렴한 비용으로 상업적인 광고나 악의적인 스팸을 발송할 수 있다. 또한 IP 기반 서비스이기 때문에 스팸의 대량 전송도 가능해지므로 스팸의 위

※ 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.k, {sysmoon, cjduck}@cns.ssu.ac.kr)
** 한국정보보호진흥원 응용 기술팀 ({yjwon, ydcho}@kisa.or.kr), 교신저자 : 정수환(souhwanj@ssu.ac.kr)
논문번호 : KICS2007-05-228, 접수일자 : 2007년 5월 22일, 최종논문접수일자 : 2007년 7월 10일

협에 노출되어 있다. 이에 SIP 기반의 VoIP 환경에서 안전한 VoIP 서비스 제공을 위한 대응책이 시급히 요구된다[1][2][3].

현재 SIP 기반의 VoIP 환경에서 스팸을 차단하기 위한 표준화 작업이 IETF SIPPING WG, ITU-T SG17, IRTF ASRG에서 활발히 진행 중이다. 각 표준화 기구에서 제안하는 SIP 기반의 VoIP 스팸 차단 기술은 기존의 이메일 스팸 차단 기법을 VoIP 환경에 적용한 것이며, 이 중 발신자를 인증하기 위한 기법으로 SPF (Sender Policy Framework)[4]와 DKIM (DomainKeys Identified Mail)[5] 기법 등이 있다. 하지만 이는 inbound proxy 서버에 적용하는 기법으로 SIP 환경에서의 UAC-Proxy-UAS 전 구간을 인증하기에는 역부족하다. 따라서 UAC-Proxy-UAS 전 구간에서 안전한 시그널링 과정을 통해 발신자를 인증함으로서 스팸을 근본적으로 차단할 수 있는 인증 기법이 필요하다.

본 논문에서는 inbound proxy 서버에서 UAS로 INVITE 메시지를 전송할 때, HTTP digest 인증 기법[6]을 이용해 UAS에서 inbound proxy 서버를 인증할 수 있는 발신자 인증기법을 제안한다. 제안 기법은 기존의 SIP 모듈의 큰 수정 없이 쉽게 적용 가능하며, TLS(Transport Layer Security)[7]에서의 암·복호화 과정으로 인한 시그널링 지연 시간을 단축하고, proxy 서버에서 TLS 세션유지를 위한 메모리 오버헤드 문제를 줄일 수 있다. 또한 본 논문에서는 제안 기법을 구현해 임의의 스팸 발송 시 스팸이 차단되는 것을 보인다.

본 논문은 다음과 같이 구성되어 있다. II장에서는 VoIP 스팸 위협에 대해 분석하고 스팸 대응 관련 기술에 대해 살펴본다. III장에서는 스팸을 차단하기 위한 inbound proxy 서버와 UAS 간 발신자 인증 기법을 제안하고 IV장에서 제안된 inbound proxy 서버와 UAS간 발신자 인증 기법을 구현한다. V장에서는 TLS와 제안된 기법의 성능을 비교 분석하고 마지막으로 VI장에서 결론을 맺는다.

II. VoIP 스팸 위협 분석 및 대응 관련 기술

최근 이메일 기반의 발신자 인증 기법으로써 SPF와 DKIM 기법 등이 있다. SPF는 이메일 주소와 발송서버가 일치하지 않는 이메일에 대해 차단하는 방법이다. 먼저 발신자는 사전에 DNS 서버에 발송 메일 서버에 대한 IP 주소를 등록한 후 메일을 전송한다. 이에 수신 메일 서버는 DNS 서버에

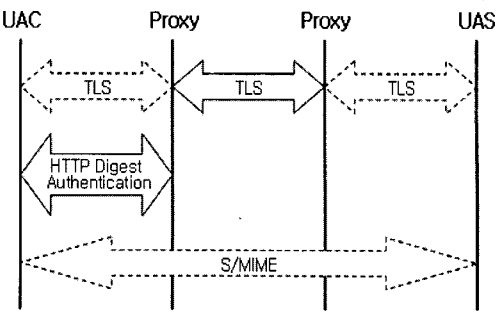


그림 1. SIP 보안 메커니즘

질의/확인을 요청해 등록된 발신 메일 서버의 IP 주소와 실제 발송된 메일 서버의 IP 주소가 일치하는지를 확인함으로서 정상 서버가 보낸 것처럼 위장된 스팸에 대해 차단할 수 있다. DKIM 기법은 메일 서버가 개인키와 공개키를 쌍으로 가지고 있고, 송/수신 하는 메일에 대해 서명과 검증을 통해 발신자를 검증할 수 있도록 한다. 스패머는 정상적인 서명 값을 생성할 수 없기 때문에 스팸 메일을 전송하더라도 수신 메일 서버에서 서명 값을 검증해 스팸을 차단할 수 있다. 한편 SIP 환경에서는 발신자를 인증하기 위한 기법으로 DKIM 기법과 유사한 Authenticated Identity 기법[8]이 있다. 이 기법은 proxy 서버 간 서명을 통해 정상적인 사용자의 SIP 메시지에 대해 outbound proxy 서버가 서명하고, inbound proxy 서버에서 서명 값을 검증하여 발신자를 인증할 수 있도록 한다. 하지만 위 기법들은 수신 서버에서 발신 서버를 인증하는 기법으로 SIP 환경에서의 UAC-outbound proxy-inbound proxy-UAS 전 구간을 인증하기에는 역부족하다.

그림 1과 같이 SIP 기반의 VoIP 환경에서는 발신자 및 발신경로를 인증하기 위해 HTTP digest 사용자 인증 기법[6]과 TLS[7] 및 S/MIME (Secure Multi-Purpose Internet Mail Extensions)[9]을 이용한다. 먼저 UAC와 UAS 양 단간의 보안을 위한 S/MIME과 각 홉 간 보안을 위한 TLS가 선택적으로 적용 가능하다. 또한 UAC와 outbound proxy 서버 간에는 HTTP digest 인증이 필수로 적용되고 outbound proxy 서버와 inbound proxy 서버 간에는 필수적으로 TLS를 적용해 발신자 및 상호 인증을 수행한다. 그러나 inbound proxy 서버와 UAS 구간에서의 TLS 보안은 선택적으로 적용되기 때문에 TLS 보안을 적용 하지 않은 경우 스패머가 UAS의 SIP URI와 IP 주소를 알고 있다면 proxy 서버를 경유하지 않는 스팸 공격이 가능하다.

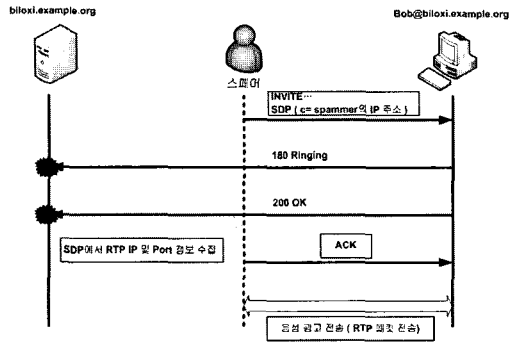


그림 2. 스팸 공격 시나리오

그림 2는 스패머가 스팸 공격자의 ID와 IP를 수집한 후 정상적인 proxy (biloxi.example.org) 서버로 위장해 UAS (Bob)에게 스팸을 발송하는 시나리오를 나타낸다. 스패머는 스팸 메시지 전송을 위해 INVITE 메시지 안에 있는 SDP 헤더 정보의 RTP (Real Time Protocol) 주소를 스패머 IP 주소로 변조하고 RTP 포트번호를 스패머가 RTP를 받을 수 있는 특정 번호로 변조한 후 proxy 서버로 위장해 UAS로 바로 스팸을 전송할 수 있다. 공격대상자는 INVITE 메시지를 받은 후, 스패머가 보낸 INVITE 메시지에 대해 원래 proxy 서버에게 180 Ringing 메시지로 응답한다. 마지막으로 공격대상자가 전화를 받으면, 원래 proxy 서버에게 200 OK 메시지를 전송한 후 RTP 세션을 열고, RTP 패킷은 스패머에게 전송된다. 스패머는 공격대상자에게 광고성 RTP 패킷을 보내기 위해 원래 proxy 서버로 가는 200 OK메시지를 스니핑 한 후 SDP 헤더 정보의 RTP 포트 번호를 파싱해 광고용 RTP 음성 패킷을 공격대상자에게 전송한다.

위와 같이 inbound proxy와 UAS 간에 TLS 보안 정책이 설정되지 않을 경우 스패머는 정상적인 proxy 서버로 위장해 UAS로 스팸을 발송할 수 있다. 이는 proxy 서버를 경유하지 않고 UAS로 바로 스팸을 전송하므로 발신자를 추적할 수 없고 이에 법적인 제재를 통한 스팸 차단이 불가능하다. 만약 proxy 서버와 UAS 간에 TLS를 적용한다면 proxy 서버에서 모든 UA에 대해 TLS 세션을 유지해야 하므로 오버헤드가 발생하고 각 메시지에 대한 암·복호화 과정으로 세션 연결에 대해 지연이 발생한다. 이에 inbound proxy 서버와 UAS 간에 발신자 및 발신 경로를 인증함은 물론 기존 TLS를 적용했을 때보다 오버헤드 및 메시지 전송의 지연을 줄일 수 있는 새로운 발신자 인증기술이 필요하다.

Ⅲ. Inbound proxy 서버와 UAS 구간 발신자 인증 기법 제안

본 논문에서는 inbound proxy 서버와 UAS 간에 TLS 보안이 적용되지 않은 경우 proxy 서버를 경유하지 않는 스팸을 차단하기 위해 UAS에서 proxy 서버를 인증하는 기법을 제안한다. 이를 SIP 프로세스에 적용하기 위해 407 Proxy Authentication Required 메시지와 유사한 497 UAS Authentication Required 메시지 및 UAS-Authenticate와 UAS-Authorization 헤더 필드를 정의한다. Proxy 서버가 INVITE 메시지를 보내면 UAS는 인증 요청을 위해 realm, nonce, uri, nc (nonce count) 등의 challenge 정보들을 UAS-Authenticate 헤더에 넣고 이를 포함한 497 메시지를 proxy 서버에게 전송한다. UAS에서 생성한 497 메시지는 그림 3과 같다.

```
SIP/2.0 497 UAS Authentication Required
Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bK74b43
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=3flal12sf
Call-ID:3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
UAS-Authenticate:
Digest realm="atlanta.example.com",
qop="auth",
nonce="f84f1ec41e6cbe5aea9c8e88d359",
opaque=""
Content-Length: 0
```

그림 3. 497 UAS Authentication Required 메시지

497 메시지를 받은 proxy 서버는 UAS와 공유하고 있는 패스워드와 challenge 정보들을 이용하여 인증 값을 생성한 후, INVITE 메시지의 UAS-Authorization 헤더에 포함하여 UAS에게 전송한다. UAS는 INVITE 메시지에 포함된 UAS-Authorization 헤더를 확인한 후 response 필드에 있는 인증 값을 검증하기 위해 사전에 알고 있는 패스워드와 challenge 정보들을 이용하여 동일한 HTTP digest 과정을 통해 인증 값을 만든다. 마지막으로 UAS는 INVITE 메시지에 포함된 인증 값과 자신이 만든 인증 값의 일치 여부를 확인함으로써 상호 인증할 수 있다. 그림 4는 제안 기법의 동작 과정을 나타낸다. 만약 스패머가 정상적인 proxy 서버로 위장해 스팸을 발송하는 경우 497 메시지에 대해 인증 값을 생성할 수 없으므로 스팸 차단을 할 수 있다. 또한 스패머가 proxy 서버와 UAS 간에 전송되는 INVITE 메시지를 캡처하여 replay attack을 시도한

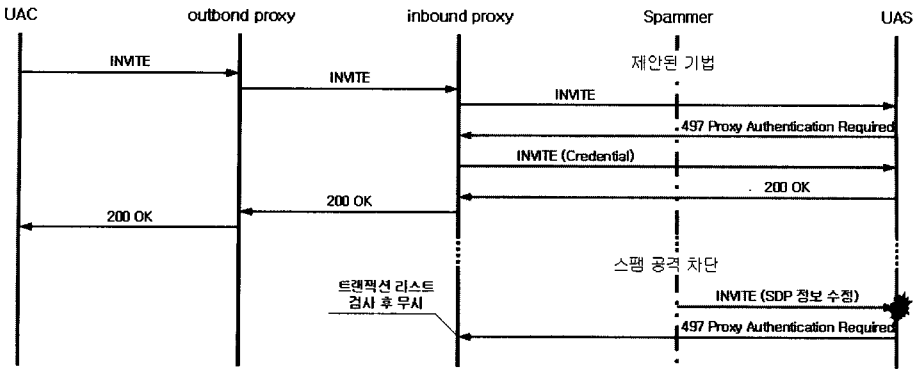


그림 4. 제안 기법을 통한 상호인증

다고 해도 UAS에서는 nc 값을 저장하여 해당 nc보다 작거나 같은 INVITE 메시지가 전송되면 replay attack으로 간주하므로 차단이 가능하다. 따라서 제안 기법은 UAS에서 inbound proxy 서버를 인증함으로써 proxy 서버를 경유하지 않는 스패머의 공격을 차단할 수 있다.

Ⅳ. Inbound proxy 서버와 UAS 구간 발신자 인증 기법 구현

본 논문에서는 제안 기법의 구현을 통해 실제 스팸 발송 시 스팸을 차단하는 것을 보인다. 그림 2와 같이 inbound proxy와 UAS 간에 TLS 보안이 적용되지 않은 경우 스패머는 UAS의 IP 주소와 ID를 사전에 알고 있다면 proxy 서버를 경유하지 않고 UAS로 직접 스팸을 발송할 수 있다. 이에 오픈 소스를 이용해 UA 및 proxy 서버에 각각 제안된 기법을 구현함으로써 스팸이 차단되는 것을 검증한다.

4.1 구현 환경

본 논문에서 스패머는 공격 대상자의 IP 주소와 ID를 사전에 알고 있고 스패머와 proxy 서버, UAS는 LAN 망에 있다고 가정한다. inbound proxy와 UAS 간 인증 기법을 구현하기 위해 리눅스 기반의 IPTEL 오픈 소스를 이용해 497 메시지를 처리할 수 있는 proxy 서버를 구현한다. 또한 VOVIDA 오픈 소스를 이용해 인증 되지 않은 INVITE 메시지에 대해 인증을 요청하는 UA를 구현한다.

4.2 구현 내용

본 논문에서는 UAS에서 inbound proxy 서버를

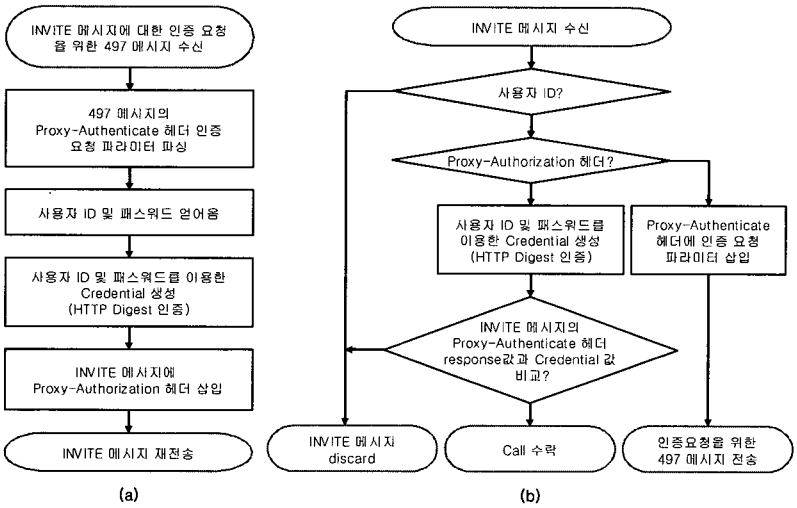


그림 5. Inbound proxy 서버(a)와 UAS(b)의 동작 과정 설계

인증함으로써 스팸이 차단되는 것을 검증하기 위해 제안 기법을 구현한다. UAS는 UAS-Authorization 헤더가 포함되지 않은 INVITE 메시지를 받으면 인증 요청을 하기 위해 realm, nonce, uri, nc 등의 challenge 값을 생성해 UAS-Authenticate 헤더를 포함한 497 UAS Authentication Required 메시지를 보낸다. 반면 UAS-Authorization 헤더가 포함된 INVITE 메시지를 받으면 HTTP digest 인증을 통한 인증 값을 생성해 INVITE 메시지의 UAS-Authorization 헤더 안에 있는 response 값을 비교한다. 이에 검증이 성공한 INVITE 메시지에 대해서만 호 연결을 한다. 한편 497 메시지를 받은 proxy 서버는 challenge 값과 패스워드를 가지고 HTTP digest 인증을 통한 인증 값을 생성한 후 INVITE 메시지의 UAS-Authorization 헤더 안에 response 값에 넣어 전송한다. Inbound proxy 서버와 UAS의 구현 설계는 각각 그림 5의 (a), (b)와 같다.

4.3 실험 결과

4.3.1 Inbound proxy 서버와 UAS 구간 발신자 인증 기법이 구현되지 않은 일반 UAS로의 스팸 발송

Inbound proxy와 UAS 간 TLS가 적용되지 않은 경우 스패머는 proxy 서버로 위장해 UAS로 직접 스팸 발송이 가능하다. 그림 6은 실제 스팸 공격을 시도한 후 스팸 공격이 성공하는 동작 과정을 캡처 프로그램 (ethereal)을 통해 캡처한 것이다.

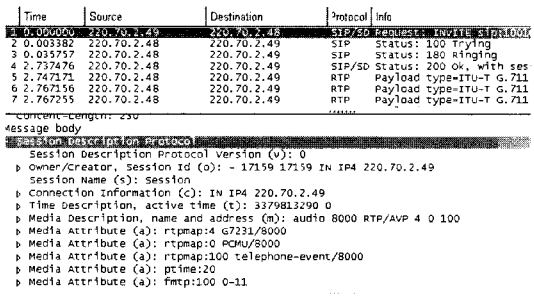


그림 6. 일반 UAS로의 스팸 발송 동작 과정

4.3.2 Inbound proxy 서버와 UAS 구간 발신자 인증 기법이 구현된 UAS로의 스팸 발송

본 논문에서 제안한 기법인 Inbound proxy 서버와 UAS 구간 발신자 인증 기법이 구현된 UA는 그림 4에서와 같이 UAS에서 proxy 서버로 인증을 요청하기 때문에 스패머가 proxy 서버로 위장해 UAS로 직접 스팸을 발송하는 것이 불가능하다. 그림 7은 실제 스팸 공격을 시도했지만 UAS에서 proxy 서버에게 인증을 요청함으로써 스팸이 차단되는 것을 보여주는 동작 과정을 캡처 프로그램 (ethereal)을 통해 캡처한 것이다.

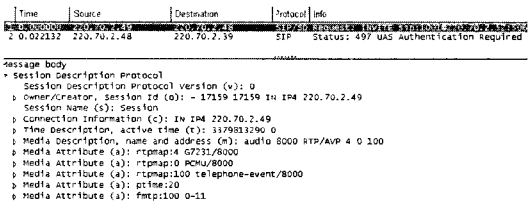


그림 7. 제안된 기법이 구현된 UAS로의 스팸 발송 동작 과정

V. 제안 기법 성능 비교

SIP상에서 UAS와 inbound proxy 서버 간 기본적으로 제공하고 있는 보안 메커니즘은 없으며, TLS가 옵션으로 제공된다. 따라서 스팸을 차단하기 위해서는 TLS를 사용하거나 본 논문에서 제안한 기법을 사용할 수 있다. 이에 본 논문에서는 TLS와 제안 기법의 성능을 스팸 차단 측면에서 비교 분석해 본다.

그림 8은 제안 기법과 TLS를 비교 분석하기 위한 메시지 절차이다. SIP 세션 설정 과정은 UAC-outbound proxy-inbound proxy-UAS의 전 구간에서 각각 TLS가 적용된 경우 각 메시지에 대해 HMAC 적용 및 세션 키를 통한 암·복호화 과정이 이루어진다. 또한 UAC와 outbound proxy 서버 구간에서의 HTTP digest 인증이 필수로 적용되므로 해시 함수가 사용된다.

반면 제안된 기법을 적용하면 UAC와 outbound proxy 서버 구간에서는 HTTP digest 인증을 통해 해시 함수가 사용되고 outbound proxy서버와 inbound proxy 서버 구간에서는 TLS 보안이 필수로 적용되므로 각 메시지에 대해 HMAC과 세션 키를 통한 암·복호화 과정이 이루어진다. 그리고 inbound proxy서버와 UAS 구간에서는 다시 한 번 HTTP digest 인증이 이루어지므로 해시 함수가 사용된다.

표 1은 스팸 공격을 차단하기 위해 TLS를 적용한 경우와 제안 기법을 적용한 경우 암·복호화 및 해시함수 사용 횟수를 나타낸다. 표1에서와 같이 제안된 기법이 SIP 메시지에 대해 총 검증 횟수가 더 적기 때문에 세션 설정을 빠르게 수행함으로써 TLS

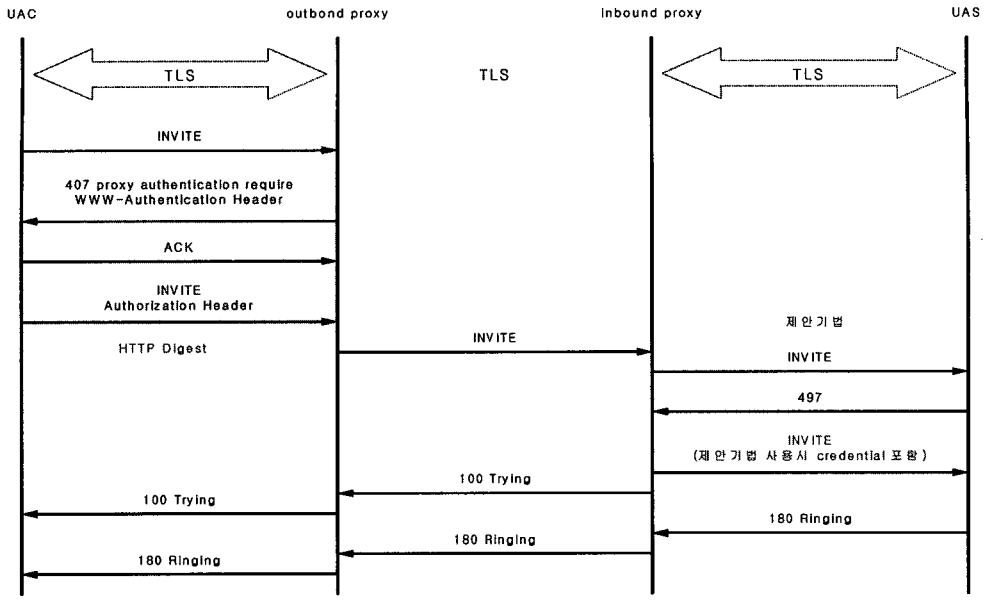


그림 8. 성능 측정을 위한 SIP 메시지 절차

를 적용했을 때 보다 계산 양에 따른 오버헤드를 줄일 수 있다. 또한 TLS를 사용하기 위해서는 인증서 발급을 위한 기반 시스템이 갖춰져야 하므로 스팸을 차단하는 측면에서는 제안 기법을 사용하는 것이 더 가볍다. 그러나 HTTP digest 인증은 dictionary attack에 취약한 문제점이 있고, TLS와 달리 메시지에 대해 기밀성은 제공하지 않는다. 또한 제안된 기법은 TLS와 마찬가지로 UAS에서 스팸을 차단하기 위한 처리를 요구하므로 UAS에서 스팸 처리를 위한 오버헤드가 발생할 수 있다. 따라서 SPF나 DKIM 기법처럼 proxy 서버에서 스팸을 차단하는 메커니즘을 접목시켜 적용하면 UAS에서의 스팸 처리 양을 줄일 수 있다.

표 1. TLS 인증과 제안 기법 성능 비교 분석

	TLS를 이용한 스팸 차단	제안 기법을 이용한 스팸 차단
암·복호화 횟수	22	6
해시함수 사용 횟수	24	10

Ⅵ. 결 론

본 논문에서는 SIP 기반의 VoIP 환경에서 UAC와 outbound proxy 서버 구간, outbound proxy 서버와 inbound proxy 서버 구간, inbound proxy 서버와 UAS 구간에서의 SIP 보안 취약성을 분석하고 특히 outbound proxy 서버와 UAS 구간에서 TLS가 적용되지 않은 경우 스패머의 공격 시나리오를 설계하였다. 스패머는 proxy 서버로 위장해 proxy 서버를 경유하지 않고 UAS로 직접 Call 스팸이나 IM 스팸을 대량으로 전송 가능하다. 기존에 존재하는 여러 스팸 차단 기술로는 발신자 및 발신경로 역 추적이 불가능하기 때문에 이러한 스팸을 근본적으로 차단할 수 없다. 이에 본 논문에서는 proxy 서버에서 UAS로 INVITE 메시지를 전송할 때, UAS에서 proxy 서버를 인증할 수 있는 발신자 인증 기법을 제안하였다. 제안 기법은 proxy 서버와 UAS 사이에 사전에 공유하고 있는 패스워드를 기반으로 UAS가 proxy 서버를 인증할 수 있기 때문에 proxy 서버를 경유하지 않는 스패머의 공격을 차단할 수 있다. 제안 기법은 인증을 위해 407 Proxy Authentication Required 메시지와 비슷한 497 UAS Authentication Required 메시지를 정의하고 UAS-Authenticate 헤더 및 UAS-Authorization 헤더를 추가하면 되므로 기존의 SIP 형식의 큰 수정 없이 쉽게 적용이 가능하며, TLS 보다 적은 암·복호화 과정 수행으로 빠른 SIP 메시지 처리가 가능하다. 또한 proxy 서버에서 UA에 대한 TLS 세션 유지하기 위한 오버헤드를 줄이므로 proxy 서버의 자원을 좀 더 효율적으로 사용할 수 있다.

참 고 문 헌

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

[2] Ram Dantu, Prakash Kolan "Detecting Spam in VoIP Networks," SRUTI'05, 2005.

[3] J. Rosenberg, C. Jennings and J. Peterson, "The Session Initiation Protocol (SIP) and Spam," IETF draft, October 2004.

[4] M. Wong, 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.

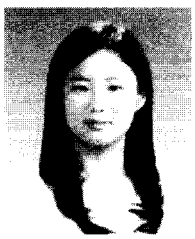
[6] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, "HTTP Authentication Basic and Digest Access Authentication," IETF RFC 2617, June 1999.

[7] T. Dierks, C. Allen "The TLS Protocol Version 1.0," IETF RFC 2246, January 1999.

[8] J. Peterson, C. Jennings, "Enhancements for Authenticated Identity Management in the SIP," IETF RFC 4474, August 2006.

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP(Session Initiation Protocol)," IETF RFC 3261, June 2002.

장 유 정 (Yujung Jang) 준회원

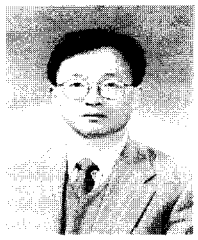


2006년 2월 : 숭실대학교 정보통신전자공학부 졸업

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

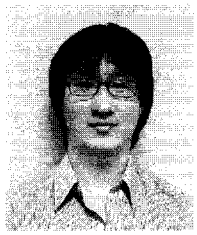
1996년 6월 : University of Washington 박사

1996년~1997년 : Stellar One SW Engineer

1997년~현재 : 숭실대학교 정보통신전자공학부 부교수

<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안

문 형 권 (Hyungkwon Moon) 준회원



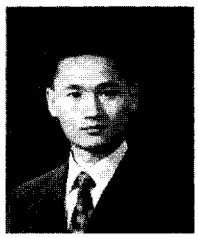
2005년 2월 : 숭실대학교 정보통신전자공학부 졸업

2007년 2월 : 숭실대학교 정보통신전자공학부 석사 졸업

2007년~현재 : 엠큐브웍스 서버 개발팀 팀

<관심분야> VoIP 보안, Java TV, IMS

최 재 덕 (Jaeduck Choi) 준회원



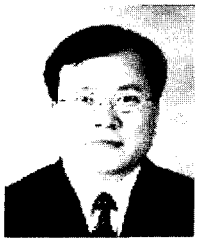
2002년 2월 : 숭실대학교 정보통신전자공학부 졸업

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