# SIP 기반 VoIP 서비스에서 도청을 이용한 스팸 방지를 위한 인증 시스템 설계

윤성열* 박석천*

* 경원대학교 소프트웨어학부

# Design of User Authentication System for Anti-Spam using Wiretapping in SIP-based VoIP Service

**Sung-Yeol Yun*, Seok-Cheon Park***

Division of Software, Kyungwon University

E-mail : scpark@kyungwon.ac.kr

**요 약**

본 논문에서는 SIP 기반의 VoIP 서비스에서 발생 가능한 스팸 위협중 도청을 이용하여 Redirect 서버에서 Proxy 서버로 송신되는 패킷을 불법적으로 위·변조하여 공격하는 기법의 시나리오와 이를 차단하기 위해 발신자 인증 기법을 제안하였다. UAC가 상대편 UAS에게 INVITE 메시지를 송신할 때 Proxy 서버에서 UAS와 연결되어 있는 Proxy 서버의 주소를 알지 못한다면 Redirect 서버에서 질의를 해야 하는데 그때 Redirect 서버는 302 메시지에 Proxy 서버가 요청한 주소를 실어 보내게 된다. 이 302 메시지 패킷을 스패머가 위·변조 할 경우 Proxy 서버는 잘못된 주소가 포함된 INVITE 메시지를 생성하게 되고 스패머와 RTP 세션이 열릴수 있다. 따라서 본 논문에서는 이를 차단하기 위해 인증 메시지가 포함된 ACK 메시지를 정의하여 인증 시스템을 설계하였다.

## 1. 서론

최근 VoIP(Voice Over Internet Protocol) 서비스에 대한 관심의 증가로 보안에 대한 중요성이 강조되고 있다. 이런 VoIP 서비스를 이용하기 위해서는 단말과 단말간의 호를 성립시킬 수 있는 SIP(Session Initiation Protocol) 기술이 필요하다. SIP는 수신자의 주소를 획득하기 쉽고 일반 전화보다 더욱 저렴한 비용으로 악의적인 스팸을 보낼 수 있다. 또한 패킷 복사를 통한 대량전송도 가능하기 때문에 PSTN (Public Switched Telephone Network) 스팸보다 심각한 위협이 될 수 있다[1]. 현재 SIP 기반의 VoIP 환경에서 스팸을 차단하기 위한 표준화 작업이 IETF, ITU-T, IRTF에서 진행 중이다. 이런 표준화 기구에서 제안하는 SIP 기반의 VoIP 스팸 차단 기술은 기존의 이메일 스팸 차단 기법을 그대로 VoIP 환경에 적용한 것이며, 발신자를 인증하는 기법으로 DKIM (DomainKeys Identified Mail)[2][3] 기법과 SPF(Sender Policy Framework)[4] 기법 등이 있다. 하지만 이 기법들은 UA(User Agent)와 Proxy 서버와의 전 구간 인증을 지원하지 않는다. 따라서 전 구간에서 안전한 시그널링 과정을 통해 발신자를 인증함으로써 스팸을 근본적으로 차단할

---

* 일반대학원 전자계산학과 석사과정

** IT대학 정교수(교신저자)

수 있는 인증 기법이 필요하다.

본 논문에서는 Proxy 서버에서 Redirect 서버를 통하여 상대 Proxy 서버의 주소를 획득하는 과정에서 스패머가 패킷을 가로채서 스패머의 주소로 변조한 패킷을 Proxy 서버로 송신하여 스패머와 RTP(Real Time Protocol) 세션을 설정하게 되는 상황을 차단할 수 있는 인증 기법을 제안한다.

## 2. 관련연구

### 2.1 콜 스팸(Call Spam)

콜 스팸은 수신자가 원치 않는 다량의 콜 세션을 시도 하는 것으로 정의된다[5]. VoIP 서비스에 대한 콜 스팸 공격은 SIP 프로토콜에서 SIP INVITE 메시지의 요청으로 시작한다. SIP INVITE 메시지 요청 세션은 음성, 비디오, 인스턴트 메시징 및 기타 통신을 성립하기 위한 프로토콜 응답의 초기 과정이다.

그림1은 SIP INVITE 요청에 대해 사용자가 응답을 하면 콜 스팸은 즉시 실시간 통신으로 연결되어 광고 정보를 전달한다. 이것은 텔레마케터 스팸 행위로 이용된다.

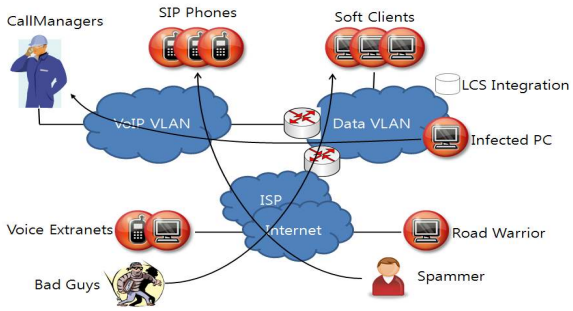


그림 1. VoIP 콜 스팸 공격

또한 SIP 프로토콜은 이메일과 유사하게 하나의 UA에서 다량의 콜을 초기화하고 병렬적으로 발생시킬 수 있다. 또한 콜이 성립되면 스팸 소프트웨어에서 녹음된 음성 메시지를 전달한 후 콜을 끊을 수 있다. 그리고 PC상에서 공개된 소프트웨어를 통해 간단하게 반복 재생을 통한 스팸 발송 시스템을 구현할 수 있고, 소프트웨어의 병렬적인 특징을 이용하여 빠르게 복제할 수 있기 때문에 스팸 콜의 VoIP 스팸의 가능성은 매우 높다.

### 2.2 SIP 기반의 발신자 인증 기법

SIP 환경에서는 발신자를 인증하기 위한 기법으로 DKIM 기법과 유사한 Authenticated Identity 기법[6]이 있다. 이 기법은 Proxy 서버 간 서명을 통해 정상적인 사용자의 SIP 메시지에 대해 UAC(User Agent Client)와 연결되어있는 Proxy 서버가 서명하고, UAS(User Agent Server)와 연결되어있는 Proxy 서버에서 서명 값을 검증하여 발신자를 인증할 수 있도록 한다. 하지만 수신 서버에서 발신 서버를 인증하는 기법으로는 SIP 환경에서의 전 구간에서 적용하기 어렵다.

그림 2와 같이 SIP 기반의 VoIP 환경에서는 발신자 및 발신경로를 인증하기 위해 HTTP digest 사용자 인증 기법과 TLS(Transport Layer Security)[7] 및 S/MIME (Secure Multi-Purpose Internet Mail Extensions)을 이용한다.

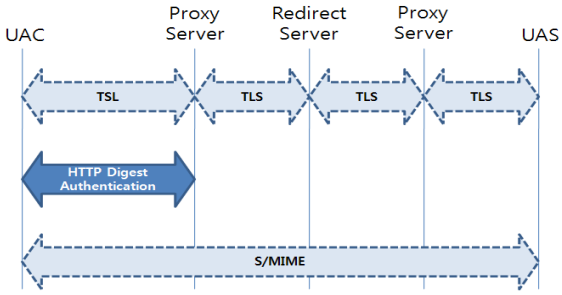


그림 2. SIP 보안 메커니즘

## 3. VoIP 서비스에서 정상 및 스팸 공격 시나리오

SIP 메시지에서 INVITE 메시지는 호를 성립하는데 있어서 처음 UA가 보내는 메시지이다. 이 INVITE 메시지에는 송신자의 정보와 수신자의 주소정보 등이 포함되어 있다. 이 INVITE 메시지를 시작으로 송신자는 수신자의 UA까지 여러 필드들을 채워가면서 호 설정 절차를 진행한다.

### 3.1 정상 시나리오

본 논문에서는 각 UA 단말이 Proxy 서버와 연결되어 있고 각 Proxy 서버는 Redirect 서버에 연결되어 있는 시스템에서 고려하였다. 그림 3은 전체 VoIP 시스템 구성도이다.

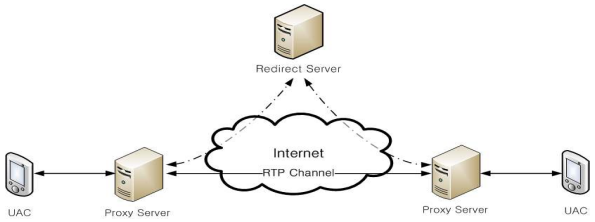


그림 3. VoIP 시스템 구성도

INVITE 메시지를 UA로부터 받은 Proxy 서버는 바로 상대편 Proxy 서버로 갈 수 있는 주소를 알고 있지 않다면 Redirect 서버에서 수신자의 주소를 얻게 된다. 얻은 주소는 302 메시지 필드에 포함되어 다시 Proxy 서버로 전송된다. Proxy 서버는 수신받은 302 메시지 내용을 파싱하여 새로운 INVITE 메시지를 생성하여 전화를 걸고자 하는 송신자의 Proxy 서버로 INVITE 메시지를 보낸다. 그림 4는 Redirect 서버가 있는 VoIP 호 성립 시나리오이다.

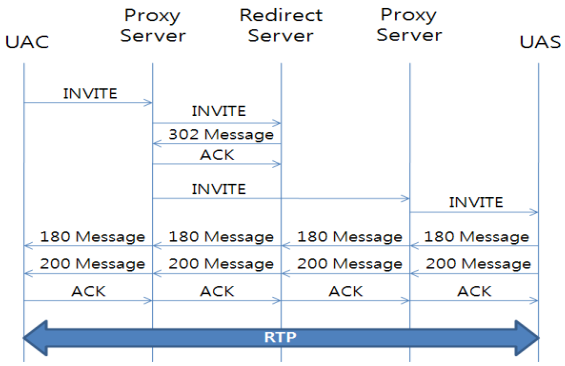


그림 4. VoIP 호 성립 시나리오

위와 같은 시나리오에서 정상적인 방법으로 302메시지를 받은 Proxy 서버는 올바른 UA가 있는 Proxy 서버로 INVITE메시지를 재 생성하여 송신한다.

### 3.2 스팸 공격 시나리오

위와 같은 정상적인 Redirect 서버와 Proxy 서버 사이에 스패머가 도청공격을 이용하여 패킷을 가로채 변조를 하면 송신자에게 잘못된 주소가 갈 수 있다. 그림 5는 스패머가 Redirect 서버와 Proxy 서버사이에 패킷을 변조하여 잘못된 RTP 세션을 설정한 시나리오이다.

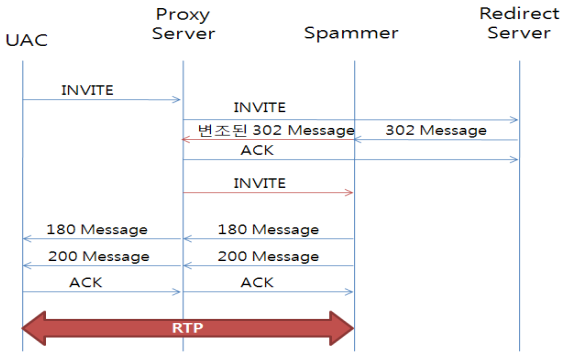


그림 5. 스패머의 공격 시나리오

이런 경우 Proxy 서버에서는 잘못된 주소가 왔는지 알수가 없으므로 스패머에게 RTP 세션이 설정되어 송신자에게 스팸 메시지가 노출 될 수 있다.

## 4. Redirect 서버와 Proxy 서버 구간 발신자 인증 시스템 제안

### 4.1 인증 필드를 추가한 ACK 메시지

인증 필드를 추가한 ACK 메시지에는 추가된 Authentication 필드가 있어서 재 인증을 위해 302 메시지에서 수신 받은 주소를 다시 필드에 포함하게 된다. 이렇게 해서 만들어진 Authentication ACK 메시지를 Redirect 서버가 수신 받은 후에 자신이 송신했던 주소와 일치하는지를 검사하게 되는데, Authentication ACK 메시지를 그림6과 같이 정의하였다.

```
ACK sip:UserB@110.111.112.113 SIP/2.0
Via: SIP/2.0/UDP ss1.wcom.com:5060;branch=z39sd3847d
Via: SIP/2.0/UDP here.com:5060;branch=3wadf22;
     received=100.101.102.103
Max-Forwords:69
Route: <sip:ss2.wcom.com;lr>
From: BigGuy <sip:UserA@here.com>;tag =9adf2
To: LittleGuy <sip:UserB@there.com>;tag=213424
Call-ID: 12315415@here.com
CSeq: 2 ACK
Content-Length: 0
Athentication: UserB, 110.111.112.113
```

그림 6. Athentication ACK 메시지 정의

### 4.2 발신자 인증 시스템 제안

Proxy 서버가 Redirect 서버에게 ACK 메시지를 송신할 때 인증 과정을 추가하여 Redirect 서버가 수신된 ACK 메시지를 파싱하여 패킷의 변경이 발견되면 올바른 주소를 재 송신하여 스패머와의 RTP 세션 설정을 막을수 있다. 다음 그림 7은 제안한 발신자 인증 시스템 절차이다.

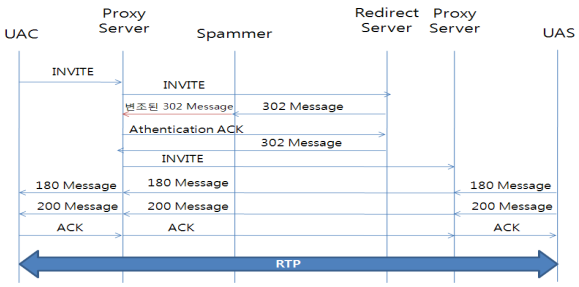


그림 7. 제안한 발신자 인증 시스템 절차

제안한 발신자 인증 시스템 절차에서는 302 메시지의 주소를 Athentication ACK 메시지에 포함하여 다시 Redirect 서버로 전송된다. Redirect 서버는 Athentication ACK 메시지에 Athentication 필드값과 302 메시지의 From 필드를 비교하여 유저의 ID와 IP정보를 파싱하여 비교한다. 만약 두 필드의 값이 다르다면 Redirect 서버는 스패머가 302 메시지를 변조된 메시지로 간주하고 Proxy 서버에게 정상적인 UAS의 주소가 포함되어 있는 302 메시지를 재전송 한다. 따라서 올바른 UAS에 RTP 세션을 열수 있다.

이 기법은 오버헤드가 심한 TCL 세션을 계속적으로 열고 있지 않아 발생하는 도청공격을 받았을 때 재 인증 방법을 이용하여 스패머의 스팸 공격을 차단 할 수 있고, 기존에 생성되는 메시지에 하나의 필드를 추가함으로써 TLS 보다 경량화된 인증 기법의 사용으로 네트워크상에서도 큰 트래픽을 유발시키지 않는다는 장점이 있다. 또한 VoIP 서비스에서 크게 패킷의 구조가 달라지지 않으므로 쉽게 서비스에 적용할 수 있다.

## 5. 결론

본 논문에서는 SIP 기반의 VoIP 서비스에서 Proxy 서버와 Redirect 서버 사이 구간에 스패머가 도청공격을 통해 변조된 INVITE 메시지를 중개하는 공격 시나리오에서 이를 차단하기 위한 인증 시스템을 제안하였다. 스패머는 자신의 주소를 INVITE 메시지에 삽입하여 송신자가 스패머의 주소로 잘못된 RTP 세션을 열수 있다. 이에 본 논문에서는 Proxy 서버가 Redirect 서버에게 받은 302 메시지에 포함된 주소부분을 이용하여 ACK 메시지를 작성하여 Redirect 서버에 재 인증을 받는 시스템을 설계하였다. 기존의 ACK 메시지를 기반으로 필드를 추가하면 되므로 SIP 형식의 큰 수정 없이 쉽게 적용이 가능하며, TLS 세션을 계속적으로 유지해서 발생하는 오버헤드보다 경량화 되었기 때문에 네트워크의 부하를 줄일 수 있다.

## [참고문헌]

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

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

[3] 장유정, 정수환, 문형권, 최재덕, 원유재, 조영덕, "SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법“, 한국통신학회논문지, ‘07-8 vol. 32 No. 8

[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] 이인희, 박대우, “VoIP 취약점에 대한 스팸 공격과 보안에 관한 연구”, 한국 컴퓨터정보학회, 2006. 12.

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

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