VoIP 스팸 차단을 위한 Proxy 서버와 UAS 간의 발신자 인증 기법

*문형권, *최재덕, *장유정, *정수환, **원유재
*숭실대학교 정보통신전자공학부, **한국정보보호진흥원
*{sysmoon, cjduck, lilyuwjd}@cns.ssu.ac.kr, *souhwanj@ssu.ac.kr, **yjwon@kisa.or.kr

Sender Authentication Scheme between the Proxy Server and UAS for VoIP Spam

*Hyoungkwon Moon, *Jaeduck Choi, *Yujung Jang, *Souhwan Jung, **Youjae Won
*School of electronic engineering, Soongsil University
**KISA IT Infrastructure Protection Division Applied Security Technology Team

요 약

SIP가 IP 기반 네트워크에서 VoIP 통신을 위한 시그널링 프로토콜로 자리 잡으면서 VoIP 환경에서도 스팸이 발생할 수 있는 취약점이 많이 존재하게 되었다. 특히, proxy 서버와 UAS간 발신자 인증 기법의 부재로 VoIP 스팸 공격이 가능하다. 본 논문에서는 proxy 서버에서 UAS로 INVITE 메시지를 전송할 때 발생할 수 있는 스팸 공격을 차단하기 위해 UAS에서 proxy 서버를 인증할 수 있는 발신자 인증 기법을 제안하였다. 제안 기법은 proxy 서버와 UAS 사이에 이미 공유하고 있는 패스워드를 기반으로 UAS가 proxy 서버를 인증할 수 있기 때문에 proxy 서버에서 TLS 사용으로 인한 오버헤드를 줄일 수 있고, INVITE 메시지에 Authorization 헤더만 추가하여 간단하게 구현할 수 있다.

I. 서론

SIP (Session Initiation Protocol)를 기반으로 하는 VoIP (Voice Over IP) 서비스의 장점과 이에 대한 기업들의 관심이 증가하면서 VoIP에 대한 보안의 중요성이 제기되고 있다. VoIP 스팸의 종류는 크게 Call 스팸, IM (Instance Message) 스팸 [1], Presence 스팸 [3]으로 나뉜다. 이와 같은 VoIP 스팸은 이메일 스팸과 비슷한 형태로써 원하지 않는 음성 통화, 메시지를 전달하여 VoIP 서비스 이용을 불편하게 한다. PSTN 망에서 텔레마케팅 회사들은 하나의 콜(Call)을 생성하기 위해서 오직 한 개의 전화선만을 사용할 수 있으며, 하나의 콜에 대한 사용요금을 지불해야 하기 때문에 비용적인 측면에서 부담이 컸다. 하지만 IP 망에서 VoIP 스팸을 이용하면 한 번에 수천 개의 주소에 같은 메시지를 보낼 수 있으며, 기존 네트워크 망을 이용하기 때문에 비용적인 부담을 줄일 수도 있다. 따라서 스패머는 스팸 발송에 대한 요금 부담을 줄이고, VoIP 서비스 환경에서 대량의 스팸을 자동화 된 툴을 사용하여 상업적인 광고나, 악의적인 메시지를 보낼 수 있다.

SIP 기반의 VoIP 시스템에서는 HTTP Digest 사용자 인증방법과 TLS를 이용하여 발신자 및 발신경로를 인증하고 있다. UA (User Agent)와 proxy 서버 구간에서는 콜 연결시 HTTP Digest 방법을 사용하여 기본적으로 사용자 인증을 수행하고, proxy 서버 간에는 IPsec 또는 TLS를 사용하여 발신자 및 상호 인증을 수행한다. 그러나 proxy 서버와 UAS (User Agent Server) 구간에서는 proxy 서버가 INVITE 메시지를 UAS로 전달할 때 UAS가 proxy 서버에 대한 인증을 수행하지 않기 때문에 proxy 서버를 위장한 스패머에 의해 스팸 공격이 가능하다. SIP 표준에서 정의한 것과 같이 proxy 서버와 UAS 간에 TLS를 사용할 수도 있지만, proxy 서버에서 모든 UA에 대해 TLS 세션을 유지해야 하는 오버헤드 문제와 각 메시지에 대한 암·복호화 과정으로 세션 연결에 대해 지연이 발생한다.

본 논문에서는 proxy 서버에서 UAS로 INVITE 메시지를 전송할 때, UAS에서 proxy 서버를 인증할 수 있는 발신자 인증기법을 제안하였다. 제안 기법은 기존의 SIP 모듈의 큰 수정 없이 빠르게 적용 가능하며, TLS에서의 암·복호화 과정으로 인한 시그널링 지연 시간을 단축하고, proxy 서버에서 세션유지를 위한 메모리 오버헤드 문제를 줄일 수 있다.

본 논문의 2장에서는 SIP 기반의 VoIP 스팸을 차단하는 기술에 대해서 살펴보고, 3장에서는 스패머의 공격 방법과 본 논문에서 제안하는 proxy 서버와 UAS 간의 발신자 인증기법에 대해서 설명한다. 또한 4장에서는 TLS와 제안된 기법의 성능을 비교 분석하고, 마지막으로 5장에서 결론을 맺는다.