BcN 환경에서 안전한 VoIP 서비스를 위한 스팸대응 기술 연구

성 경* · 김석훈**

A Study on Spam Protection Technolgy for Secure VoIP Service in Broadband convergence Network Environment

Kyung Sung* · Seok-Hun Kim**

요 약

VoIP 서비스는 인터넷 기반기술을 사용하므로 인터넷망에서 발생하는 보안위협이 내재해 있고 실시간 서비스 특성으로 기존 보안 솔루션의 수정이나 변경 없이 보호하기는 어려운 면이 있고, 단일 망으로 음성 · 데이터 통합서비스를 제공하기 때문에 상대적으로 데이터 망만을 보호하기 위한 노력과 비용이 복잡해지고, IP망에서 발생 가능한 보안 위협이 내재되어 있고, 단일 망으로 음성 · 데이터 통합서비스를 제공하기 때문에 상대적으로 데이터 망만을 보호하기 위한 노력과 비용이 복잡해지고, IP망에서 발생 가능한 보안 위협이 내재되어 있다. 본 논문에서는 VoIP 스팸에 대한 정의와 VoIP 스팸 기술에 대한 분석 그리고 VoIP 스팸을 막을 수 있는 여러 가지 대응방법들에 대해서 설명을 하도록 한다.

ABSTRACT

There is a difficult plane letting a security threat to occur in Internet networks as VoIP service uses technology-based the Internet is inherent, and you protect without adjustment of the existing security solution or changes with real-time service characteristics. It is a voice to single networks The occurrence security threat that it is possible is inherent in IP networks that effort and cost to protect a data network only are complicated relatively as provide service integrated data.

This paper about various response way fields to be able to prevent analysis regarding definition regarding VoIP spam and VoIP spam technology and VoIP spam.

키워드

VoIP, SIP, SPAM, BcN, Secure

Ⅰ. 서 론

인터넷 전화 서비스는 값싼 인터넷 망을 이용하기 때문에 기존 전화요금을 획기적으로 절감한다는 점과 IP 기술을 기반으로 인터넷 콜센터, 다자간 회의시스템, 화상전화서비스, 사용자 위치정보 제공 등 다양한 애플리케이션 개발에 응용력이 크므로 향후 인터넷 전화는 우리 생활에서 밀접한 통신수단으로 자리를 잡을 것

* 목원대학교 컴퓨터교육과
** (주)파라곤베이스

접수일자 : 2007. 12. 12

이다[1].

그러나 VoIP 서비스는 인터넷 기반기술을 사용하므로 인터넷망에서 발생하는 보안위협이 내재해 있고 실시간 서비스 특성으로 기존 보안 솔루션의 수정이나 변경 없이 보호하기는 어려운 면이 있고, 단일 망으로 음성・데이터 통합서비스를 제공하기 때문에 상대적으로 데이터 망만을 보호하기 위한 노력과 비용이 복잡해지고, IP망에서 발생 가능한 보안 위협이 내재되어 있다. 특히 공중전화망과 유・무선 인터넷의 연동이 가능한 인터넷전화 서비스의 피해 파급력은 단일망을 넘어서 통합망에 이르기까지 피해가 확산될 수 있으며 음성 패킷의 전달은 양단간 전화 서비스의 흐름이란 점에서 통화내용이 불법적으로 노출 되는 것을 방지하기 위한 기술 개발의 필요성이 대두되고 있다[2].

VoIP 기술은 기존 IP 기술을 이용하여 음성통신 서비스를 제공하기 때문에 IP 기반의 위협들을 그대로 상속하며, VoIP 서비스 제공을 위한 신규 기술들로 인해 발생하는 새로운 위협들을 가지고 있다. 그 중에서도 공격 가능성 및 피해 규모 등을 고려할 때, 도청, 서비스 거부공격, 서비스 오용공격, 스팸 공격 등은 가장 문제가 될 수 있어 서비스 확산에 장애가 될 수 있다는 문제점이 있다. 기존 전화망의 회선기반 방식과 다르게 VoIP 서비스는 IP 기반의 인터넷 기술을 기반으로 음성통화가 이루어짐에 따라, 인터넷 망에서의 보안위협을 내포하고 있다.

Ⅱ. 관련 연구

2.1 VoIP 서비스 형태

VoIP는 공중전화망 같은 이기종 망과 연동하여 서비스 제공이 가능하므로 그림 1과 같이 4가지 서비스 시나리오를 도출할 수 있다. 이기종 망간 연동 시 반드시 게이트웨이(Inter-working) 기능이 동반되어야 한다[3].

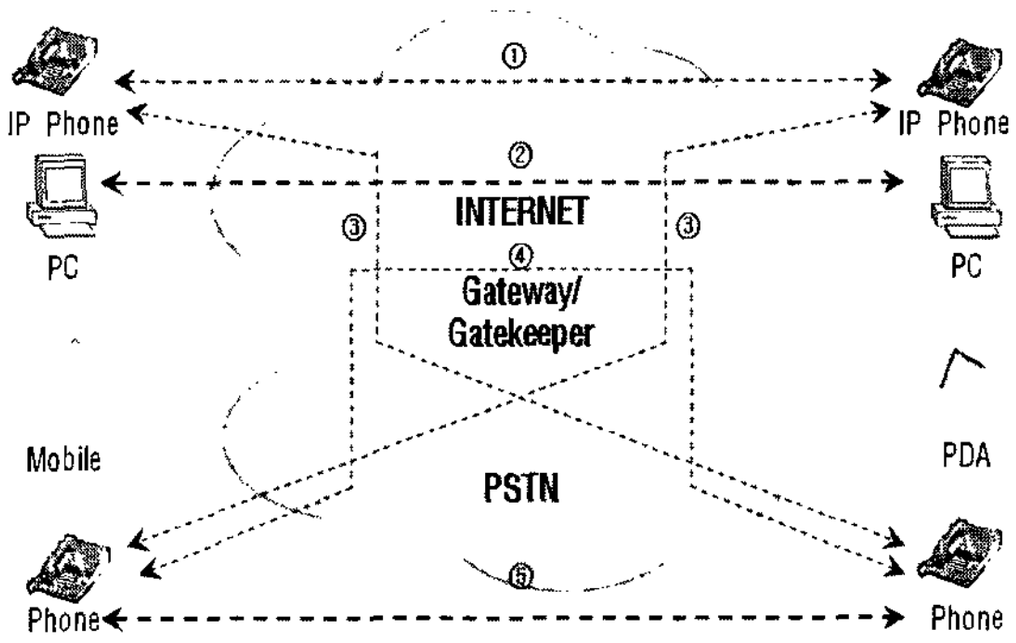

그림 1. 인터넷전화 서비스
Fig. 1 Service of VoIP

- IP Phone to IP Phone : 공중전화망을 경유하지 않고 인터넷을 통하여 IP 주소와 착·발신번호를 할당받은 IP 전화기들 간의 음성서비스를 제공
- PC to PC : 공중전화망을 경유하지 않고 인터넷을 통하여 통신 ID 또는 IP 주소 등을 보유한 통신 커뮤니티 간 음성서비스를 제공
- IP Phone(PC) to Phone : 인터넷과 공중전화망(또는 무선망)을 상호 연동하여 IP 주소와 착·발신번호를 할당받은 IP전화기와 일반 유선(무선)전화 간 음성서비스를 제공
- Phone to Phone은 공중전화망의 일반전화가 인터넷을 경유하여 다른 공중전화망의 일반전화와 연결하여 음성서비스를 제공(대부분의 국제전화)
- 공중전화망 기반의 일반 유선전화 서비스 제공

2.2 VoIP 주요 프로토콜

H.323과 SIP는 비슷한 기본 구성을 가지고 있다. H.323과 SIP는 기능상 비교 하였을때 패킷 망을 사용하고 있으며 많은 유사점을 가지고 있다. H.323과 SIP의 기본 호(Basic call)와 특별 제어(Feature control)는 대체로 단말기에서 수행되며, 추가적인 형태의 서비스들을 지원하기 위하여 서버(게이트키퍼, 프록시 등)가 제공된다[4].

부가서비스적인 측면에서 보았을 때 부가서비스를 위한 표준안의 완성도는 H.323과 SIP가 현저히 다르게 나타난다. 즉, H.323이 부가서비스의 표준화를 이끌어 가고 있다. 이것은 H.323과 SIP를 비교하는 것을 어렵게 만들지만 SIP가 H.323과 비슷한 방향으로 나아갈 것을 또한 예상할 수 있다. 둘 다 새로운 형태의 구현을 위한 규칙과 표준화된 절차를 호 특별 제어(call control features)를 위하여 일반적인 프레임워크를 정의하고 있다[5].

2.3 VoIP 보안위협 사항

VoIP 보안 위협은 IP 기반 망에서 발생할 수 있는 모든 보안 위협이 예상 가능하지만, 공격 가능성 및 피해 규모 등을 고려할 때, 도청, 서비스 거부 공격, 서비스 오용 공격, 세션 가로채기, VoIP 스팸으로 크게 분류 할 수 있다[6].

- 도청 : LAN 구간에 대한 도청, WAN 구간에 대한 도청, 단말기 도청
- 서비스 거부 공격 : 시스템 자원고갈, 회선자원고갈, 해킹을 통한 시스템 장애
- 서비스 오용 공격 : 등록정보 변조, 관리상의 오류공격, 시스템 해킹을 통한 설정 변경
- 세션 가로채기 : Invite 세션 가로채기, SIP 하이 잭킹
- VoIP 스팸 : Call 스팸, IM 스팸, Presence 스팸, 피싱
- 패스워드 취약점 : 스위치의 기본설정되는 로그인 및 패스워드(admin/admin, root/root 등) 사용에 따른 취약점으로 포트 감시를 통한 대화 도청 가능
- IP 주소 매핑 정보노출 : VoIP를 사용하는 다른 가입자의 식별번호(전화번호 등)를 알면 대상 장비에 호를 시도하고, 프로토콜 분석을 통해서 상대방 전화기의 IP 주소를 알수 있음.
- 웹 서버 인터페이스 : VoIP 교환기와 단말기는 원격관리를 위해 웹 서버 인터페이스를 갖는 경우가 많으나, 공격자에게 기밀 정보를 얻기 위해 평문 HTTP 패킷들을 가로챌 수 있는 빌미 제공.
- IP 전화기 넷마스크 취약성 : IP 전화기의 서브넷 마스크와 라우터 주소를 수정하여 장비가 보내는 패킷을 공격자의 MAC 주소로 송신할 수 있도록 할 수 있음.

Ⅲ. VoIP 스팸대응 및 보안대책 기술

3.1 VoIP 스팸 및 종류 비교분석

스팸(spam)이란 원치 않는 비상업적 혹은 상업적으로 사업적 관계를 갖지 않는 사람이 보낸 모든 통신'을 말한다. 스팸은 일방적이고 대량으로 보내지는 메시지로 인터넷 이메일이 대표적이다. SIP는 IP 기반 네트워크에서 통신을 위한 시그널링 프로토콜로 자리잡고 있으므로, 이메일 스팸과 같이 SIP 기반의 시스템에서도 스팸이 발생할 수 있다. SIP 기반의 VoIP 스팸에 대한 정의를 Call 스팸, IM 스팸, Presence 스팸과 같이 세 가지로 분류하여 설명하고 각각의 스팸에 대한 특징을 분석한다.

- Call 스팸

Call 스팸은 SIP INVITE 메시지를 임의의 사용자들에게 음성, 비디오, 인스턴트 메시지 등의 통신을 위해서 대량으로 전송한 후, 세션을 시도하는 방법이다. VoIP 환경에서의 Call Spam에 대한 가능성을 의심해 볼 수 있겠지만, Call 스팸은 현재 PSTN 망에서 텔레마케팅과 같은 형태로 나타날 수 있다. 예를 들면, 텔레마케터(spammer)가 랜덤하게 선택된 사용자들에게 SIP INVITE를 통해 전화를 걸고, INVITE를 수신한 사용자가 응답을 하여 세션이 이루어지면 텔레마케터는 불필요한 광고를 할 수 있게 된다.

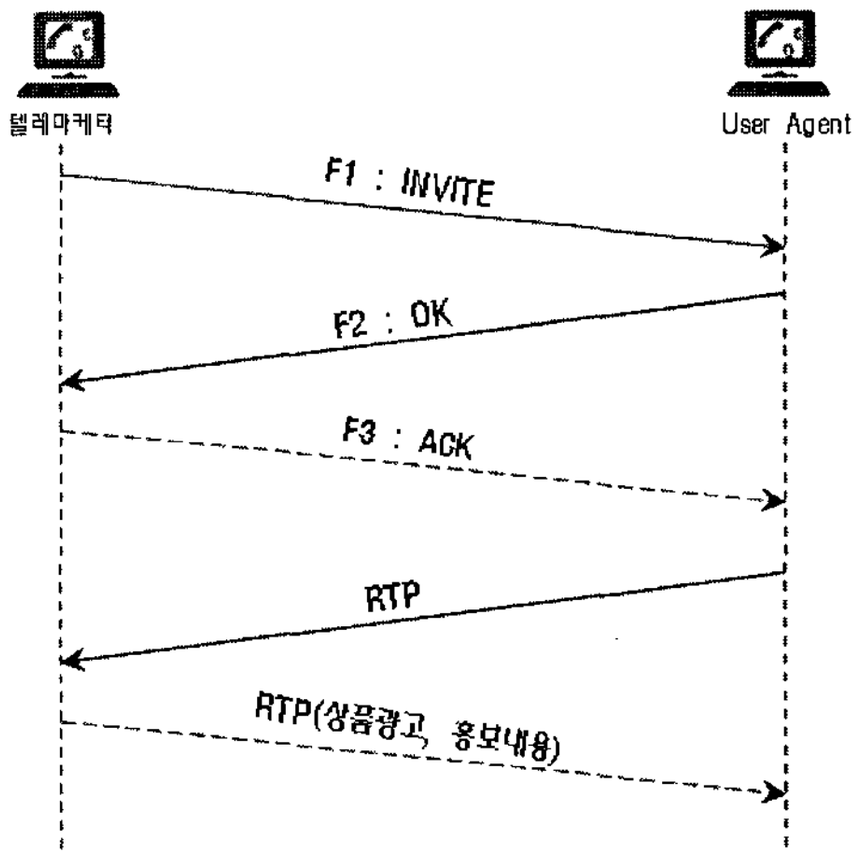

그림 2. 콜 스팸 사례
Fig. 2 Example of Call Spam

• IM 스팸

IM(Instant Messaging) 스팸은 이메일 스팸과 유사한 형태의 스팸 기술로 그림 2와 같은 방법을 사용하여 일방적이고 대량으로 전송하는 인스턴트 메시지이다. 이 스팸 기술은 IM을 위한 확장된 SIP 메시지를 사용하여 이루어지지만 INVITE, OPTION, SUBSCRIBE와 같은 일반적인 SIP Request 메시지들의 Subject 헤더를 이용하여 그림 3과 와 같이 송신자에게 자동으로 불필요한 문구를 보여줄 수 있다. IM 스팸은 이메일 스팸과 매우 유사한 형태이고 소요되는 비용도 비슷하지만 이메일 스팸보다 더 큰 영향력이 있다. 이메일 스팸은 사용자가 메일을 보는 동작에 의해서 나타나거나 바로 삭제가 가능하지만 IM 스팸은 자동적으로 팝업 되기 때문에 모든 스팸 정보가 사용자에게 나타날 수있다. 그러나 IM 시스템의 대부분이 화이트 리스트(white lists)를 사용하여 메시지를 주고받기 때문에 IM 스팸이 실제 환경에서 큰 영향력은 없다.

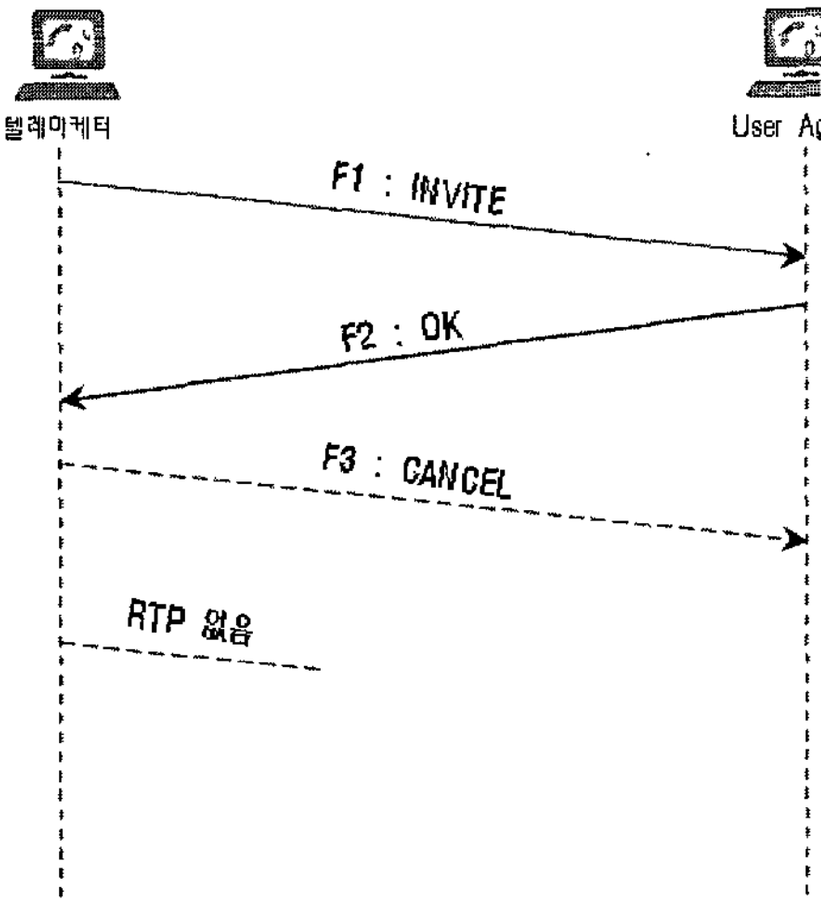

그림 3. IM 스팸 사례
Fig. 3 Example of IM Spam

• Presence 스팸

프리젠스 스팸은 IM 스팸 기술과 유사한 기술로 일방적이고 대량으로 보내지는 프리젠스 요청 메시지이다. 이 스팸 기술은 IM 메시지를 보내거나 다른 형태의 통신을 하기 위해 사용자의 "버디 리스트" 또는 "화이트 리스트"의 획득을 목적으로 SIP 메시지인 "SUBSCRIBE"요청 메시지를 사용하는 기술이다. 대부분의 프리젠스 시스템들이 동의 기반의 프레임워크를 제공하기 때문에 프리젠스 스팸의 영향력은 미비하다.

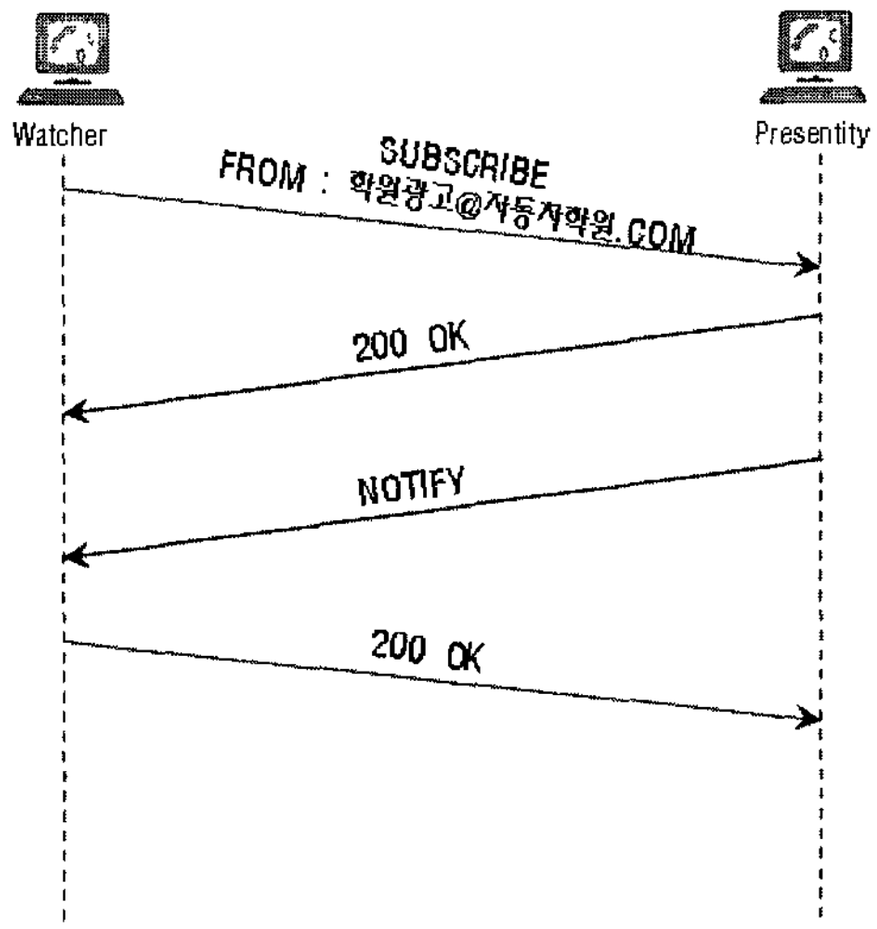

그림 4. Presence 스팸 사례
Fig. 4 Example of PresenceSpam

3.2 VoIP 정보보안 대책

• 안전한 네트워크 및 시스템 구축 : 사설 IP 망으로 구축하여 내부 VoIP 단말 및 시스템들에 대한 구성정보를 외부에 노출시키지 않는 기법을 적용하고, VLAN 적용을 통해 일반데이터망과 VoIP 망을 논리적으로 분리하여 VoIP 관련 트래픽 이외의 트래픽을 차단하는 기법을 적용한다. 또한, 미디어 채널에 대한 전송매체 공유되는 환경에서의 도청을 방지하기 위하여 더미 허브가 아닌 스위칭 장비를 적용한다. 미디어를 공유하는 경우 인터넷에 공개되어 있는 간단한 VoIP 음성통화 도청 프로그램이 설치된 컴퓨터를 통해 매우 쉽게 도청이 가능하기 때문이다.

• VoIP 장비 접근제어 : VoIP 단말에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술을 적용한다. VoIP 단말기에서 수신하는 호설정을 위한 제어 메시지가 정당한 교환시스템으로부터 전송된 것인지 검증하기 위하여 교환시스템을 인증하고 그렇지 않은 트래픽은 차단한다. 그리고 통화를 하는 합당한 상대방으로부터의 트래픽은 허용하고, VoIP 단말기를 관리하기 위한 관리시스템이 정당한지 여부를 검증하기 위한 관리시스템을 인증하고 그렇지 않은 관리신호는 차단한다.

VoIP 교환시스템에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술로 인증을 우회하는 악의적 공격을 방지하기 위하여 발신자 및 발신경로를 인증하고 인가되지 않은 트래픽을 차단하고, 교환시스템 관리를 위한 관리시스템 및 원격 관리자의 트래픽은 허용한다. 네트워크 장비에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술을 적용하는 방법으로 네트워크 장비 관리를 위한 관리시스템 및 원격 관리자의 트래픽은 허용하도록 한다.

• 네트워크 접근제어 : 사업자 네트워크에 대한 악의적 공격자의 접근을 차단할 수 있는 침입차단 기술을 적용하는 방법으로 일반적으로 알려진 공격을 수행하는 공격자 트래픽을 차단하고, VoIP 서비스에 대한 악의적 공격자 트래픽을 차단한다. VoIP 서비스가 활성화 됨에 따라, 교환시스템 및 VoIP 사용자를 대상으로 하는 공격이 증가할 것으로 예상되기 때문에 LAN, WAN 네트워크에 악의적 공격자의 접근을 차단할 수 있는 침입차단 기술을 적용한다.

3.3 VoIP 스팸대응 및 정보보안을 위한 시스템 구조

안전한 VoIP 스팸대응 및 보안체계를 구축한다면 그림 5와 같이 보안정책서버, 네트워크 서버군 및 엑세스망에 보안시스템을 구축하고, 보안이벤트 발생, 트래픽 소통상황, 시스템 자원 사용을 탐지 및 모니터링하여 종합적으로 분석 및 대응할 수 있는 S-VoIP 시스템을 구축하고 보안정책 서버에 다음과 같은 VoIP 스팸 대응기술을 마련한다.

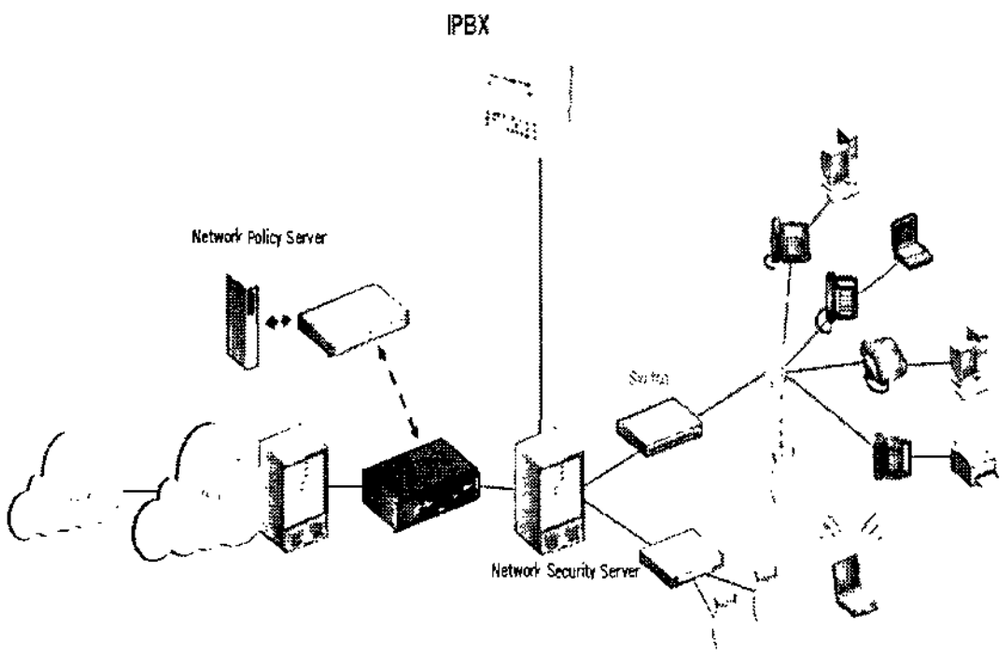

그림 5. VoIP 보안시스템 구조
Fig. 5 Architecture of VoIP Security System

• Content 필터링 대응기술

이메일 스팸에서 사용되는 가장 일반적인 형태의 스팸대응 기술이다. 스팸 필터는 이메일의 콘텐츠를 분석하고 내용을 파악하여 스팸 정보를 걸러내는 방식이다. 대표적인 Contents 필터링으로 베이지언(Bayesian) 스팸 필터가 있다. 그러나 콘텐츠 필터링 방식은 Call 스팸의 경우 다음과 같은 두 가지 이유로 완벽한 해결책이 못된다. 첫째, 전화가 왔을 경우 사용자는 전화를 받기 전까지는 콘텐츠의 내용을 파악할 수가 없다. 콘텐츠는 통화를 시작하면서부터 전달되기 때문에 콘텐츠를 파악하여 필터링을 하기에는 부적절하다. 둘째, 음성 메일(voicemail) 형태와 같이 콘텐츠가 음성, 비디오로 되어 있을 경우 음성 및 비디오 인식기술이 현재까지 정교하지 않기 때문에 콘텐츠를 분석하여 스팸인지 아닌지 판단하는데 어려움이 있다. 또한 음성 패턴을 파악하여 스팸에 대한 필터링을 수행할 수 있지만, spammer는 사용자에게 정보를 전달하는데 지장이 없을 정도의 잡음을 발생시킴으로써 콘텐츠 분석을 난해하게 할 수 있다. 콘텐츠 필터링 기술은 Call 스팸보다는 이메일 스팸과 유사한 IM 스팸 대응 기술로 적합하다.

• Balcklist 대응기술

블랙리스트는 spammer의 주소를 리스팅 하여 주소 매핑에 의해 스팸을 차단하는 방식이다. 리스트에 포함되는 주소는 이메일 주소(spammer@domain.com) 또는 도메인 전체 이름(spammers.com)으로 설정할 수 있다. 단순한 블랙리스트는 이메일 스팸에 대해서 다음과 같은 두 가지 이유로 효율성이 떨어진다. 첫째, 이메일 주소는 쉽게 스푸핑(spoofing)될 수 있으며 spammer는 스푸핑된 주소를 사용하여 다른 사람으로 위장할 수 있다. 만약 spammer가 블랙리스트에 없는 임의의 주소를 사용하여 메일을 보낸다면 블랙리스트는 무용지물이 된다. 둘째, 이메일 주소를 위조해서 사용하지 않더라고 이메일 주소는 얼마든지 새로 생성할 수 있다. 하나의 도메인 내에서 생성할 수 있는 이메일 아이디의 수는 무제한이며, 하나의 도메인을 생성하여 사용하는 비용도 저렴하다. spammer의 이메일 주소가 사용자의 블랙리스트에 등록되면 spammer는 새로운 이메일 주소를 생성하여 스팸 정보를 보낼 수 있고 다음(Daum), 야후(Yahoo)와 같은 이메일 서비스 제공업체의 도메인을 이용하여 스팸 정보를 보낸다면 블랙리스트의 도메인 전체 이름을 통

한 필터링도 불가능하다. 결과적으로 이메일 아이디가 쉽게 생성될 수 있기 때문에, 블랙리스트를 통한 스팸 대응은 큰 효과를 기대하기 힘들다.

• White 리스트 대응기술

화이트 리스트는 블랙 리스트의 반대 방식으로 유효한 사용자의 이메일만 받아들인다. 화이트 리스트 방식은 스푸핑된 주소를 사용하여 사용자의 화이트 리스트에 등록될 수 있지만, 강력한 아이디 인증방법을 사용하여 이러한 문제를 예방할 수 있다. 결과적으로 화이트 리스트와 사용자에 대한 인증방법이 함께 사용되어야만 스팸 대응에 효과가 있다. 그러나 화이트 리스트 방식은 "introduction problem"이 있다. 정당한 송신자가 사용자에게 처음으로 통신하고자 할 경우에 화이트 리스트에 없기 때문에 통신을 할 수 없는 문제이다. 정당한 사용자의 통신요청과 spammer의 스팸정보를 구별하는 것은 쉽지 않다. 인터넷 메신저와 같은 IM 시스템에서는 화이트 리스트가 유용하게 적용될 수 있다.

메신저는 화이트 리스트와 같은 버디 리스트를 기본적으로 제공하기 때문에 리스트에 등록된 사용자와의 메시지 교환이 가능하며, "introduction problem"도 메신저에서는 상대방의 버디 리스트에 등록하기 위해서는 "동의"를 통해서 이루어지기 때문에 기본적으로 화이트 리스트를 사용한 효과를 볼 수 있다. 또한 IM 시스템은 인증 메커니즘이 제공되어 화이트 리스트 방식의 문제점을 해결할 수 있다. IM 시스템에 효과적인 화이트 리스트는 SIP에 적용할 수 있다. SIP 표준에 버디 리스트 개념과 프리젠스 시스템이 명시되어 있기 때문에 SIP 시스템에 적용하여 효과적으로 스팸에 대응할 수 있다. 이와 같이 화이트 리스트는 SIP 스팸에 적용할 수 있지만 여전히"introduction problem"이 남아 있다. 화이트 리스트 방식이 SIP 스팸에 효과적인 스팸 대응 기술이 되기 위해서는"introduction problem"을 해결할 수 있는 방법과 같이 사용되어야 한다.

• Consent-based 통신 대응기술

동의 기반(consent-based) 시스템은 블랙 또는 화이트 리스트와 함께 사용된다. 예를 들면, 사용자 Alice가 Bob과 통신할 때, Bob의 블랙 또는 화이트 리스트에 Alice에 대한 정보가 없기 때문에 초기 통신과정은 거절되고, 동의를 요청한다. 이후에 다시 Alice가 Bob에게 통신을 시도하면 Bob은 Alice가 이전에 통신을 시도 했다는 것을 알고 Alice의 요청을 승낙하거나 거절한다. 이러한 동의 기반 시스템은 프리젠스와 IM 시스템에서 폭넓게 사용되고 이메일 시스템에서는 사용되지 않는다.

SIP는 동의기반 시스템의 프리젠스, watcher information event package와 같이 누가 가입을 했는지 사용자가 알 수 있도록 표준에 명시되어 있다. 그러나 동의 기반 시스템은 IM 또는 전화 시스템에서는 효과적이지 않다. 동의 기반 시스템이 IM 또는 전화 시스템에 효과적인 것처럼 보이지만 스팸의 근본적인 특성만 바뀔 뿐이다. 스팸의 콘텐츠를 통해 불필요한 정보를 받는 것을 막을 수는 있지만, 동의요청에 의해 사람을 성가시게 하는 것은 막을 수 없다.

Ⅳ. 결 론

본 논문에서는 VoIP 스팸의 종류와 그에 대한 대응 기술들을 살펴보았다. VoIP 스팸에 대한 대응 기술들은 독립적으로 동작하기 보다는 다른 스팸 대응 기술들과 상호보완적으로 동작함으로써 노출되는 보안의 취약성을 막을 수 있었다.

앞으로 VoIP의 발전은 SIP를 기반으로 하는 서비스의 형태로 발전하게 될 것이다. 현재 SIP 프로토콜은 폭넓게 사용되고 있지만, 그 배포 수준은 폐쇄된 네트워크 공간에서 제한적으로 사용되고 있다. 또한 VoIP 서비스를 제공하는 전화 사업자들도 순수 VoIP 망으로 긴밀하게 연결되어 있지 않다. 따라서 공개된 인터넷 망을 사용하여 SIP 메시지를 송수신 하는 것은 극히 제한적인 수준이다. 이러한 환경에서 VoIP 망은 스팸에 심각한 영향을 받고 있지 않다. 하지만, 머지않아 인터넷 망에서 SIP 메시지의 송수신이 자유로워지는 시기가 올 것이고, SIP 기반의 VoIP 스팸에 대한 보안이 동작하지 않는다면 많은 사용자들의 혼란을 초래할 것이다.

추후 연구과제로는 SIP 기반의 VoIP 스팸 문제에 대한 많은 해결책이 제시되었지만, 가장 핵심이 되는 해결책은 SIP URL에 대한 인증을 제공하는 기술적인 방법과 다양하고 강화된 인증방법에 대한 연구가 필요하다.

참고문헌

[1] 국가사이버안전센터, "VoIP를 이용한 인터넷 전화의 이해와 보안대책", NCSC-TR050018

[2] 정보통신부, "VoIP 정보보호 가이드라인", 2006.12.

[3] 원유재, "VoIP 스팸 대응기술", 한국정보보호진흥원, 2007.6.

[4] Time Green and Phil Hochmuth, VoIP security a moving target, Network World, 2004. 10.

[5] Li C, Li S, Zhang D, and Chen G, "Cryptanalysis of a data security protection scheme for VoIP," IEE Proceedings Vision,Image and Signal Processing, Feb. 2006.

[6] Steven M. Bellovin, Susan Landau, Matt Bla, "The real national-security needs for VoIP," Communications of the ACM, Nov. 2005.

[7] S. Chatterjee, B. Tulu, T. Abhichandani, and Haiqing Li, "SIP-based enterprise converged networks for voice/video-over-IP: implementation and evaluation of components," IEEE Journal on Selected Areas in Communications, Oct. 2005.

[8] Yi Bing Lin, Whai En Chen, Chai Hien Gan, "Effective VoIP call routing in WLAN and cellular integration," IEEE Communications Letters, Oct. 2005.

[9] M.Narbutt, A.Kelly, P. Perry, L.Murphy, "Adaptive VoIP playout scheduling: assessing user satisfaction," IEEE Internet Computing, July. 2005.

[10] M.Manousos, S.Apostolacos, I.Grammatikakis, D.Mexis, D.Kagklis, E.Sykas, "Voice-quality monitoring and control for VoIP," IEEE Internet Computing, July. 2005.

[11] E.Wedlund, H.schulzrinne, "Mobility support using SIP," in Second ACM/IEEE International Conference on Wireless and mobile Multimeida, Aug. 1999.

[12] 김석훈 외, "VPN 기반의 음성 보안을 위한 인터넷 텔레포니(VoIP) 시스템 설계", 한국해양정보통신학회 논문지, 제 10권 5호, pp.942~949, 2006.

저자소개

성 경(Kyung Sung)

2003년 한남대학교 컴퓨터공학과 (공학박사)
1994년~2004년 동해대학교 컴퓨터공학과 교수
2004년~현재 목원대학교 컴퓨터교육과 교수
※관심분야: 정보보호 및 정보관리, 컴퓨터네트워크, 신경회로망, 컴퓨터교육

김 석 훈(Seok-Hun Kim)

2006년 한남대학교 컴퓨터공학과 (공학박사)
2006년~현재 대전보건대학 바이오정보과 겸임교수
2007년~현재 (주)파라곤베이스 기술마케팅 이사
※관심분야 : VoIP, XML, BCN, 모바일 컴퓨팅