韓國 컴퓨터情報學會 論文誌
第11卷 第5號, 2006. 11.

2006-11-5-2-10

VoIP 서비스의 스팸 공격에 대한 차단 연구

이 인 희*, 박 대 우*

A Study of Interception for a Spam Attack of VoIP Service

In-Hee Lee*, Dea-Woo Park*

요 약

본 논문에서는 VoIP 서비스의 취약점 중에서 파급 효과가 가장 큰 스팸공격과 차단에 대한 연구를 하였다. VoIP 서비스에 대한 스팸공격의 시나리오를 작성하고, 콜 스팸, 인스턴트 메시징 스팸, 프레즌스 스팸 공격을 실시한다. 실험실에서 스팸 공격이 성공됨을 증명하고, 사용자의 피해 사실을 확인한다. VoIP 서비스의 스팸 차단 방법의 제안에서 1) 인바이트 리퀘스트 플루드 공격의 차단 2) 블랙/화이트 리스트, 3) 역추적, 4) Black Hole-Sink Hole, 5) 콘텐츠 필터링, 6) 동의 기반 통신, 7) 콜 행위 패턴 조사, 8) 레퓨테이션 시스템을 제안하고 실험한다. 각각의 제안된 차단 방안을 VoIP 네트워크에서 실험하여 스팸차단의 보안 등급을 확인한다. 본 논문의 연구결과를 통하여 VoIP 서비스의 정보보호가 WiBro, BcN에서 확대되어 유비쿼터스 보안을 실현하는데 이바지 할 수 있도록 하겠다.

Abstract

Regarding a spam attack and the interception that a spinoff is largest among weakness of VoIP service at these papers study. Write scenario of a spam attack regarding VoIP service, and execute Call spam, Instant Messaging spam, Presence spam attack. A spam attack is succeeded in laboratories, and prove, and confirm damage fact of a user in proposals of a spam interception way of VoIP service, 1) INVITE Request Flood Attack 2) Black/White list, 3) Traceback, 4) Black Hole-Sink Hole, 5) Content Filtering, 6) Consent based Communication, 7) Call act pattern investigation, 8) Reputation System Propose, and prove. Test each interception plan proposed in VoIP networks, and confirm security level of a spam interception. Information protection of VoIP service is enlarged at WiBro, BcN, and to realize Ubiquitous Security through result of research of this paper contribute, and may make.

▸ Keyword : Hacker Attack, SPAM, Ubiquitous Security, VoIP, Vulnerability

• 제1저자 : 이인희, 교신저자 : 박대우(prof1@paran.com)
• 접수일 : 2006.10.20, 심사일 : 2006.11.05, 심사완료일 : 2006.11.12
* 숭실대학교 정보과학대학원 정보보안학과

Ⅰ. 서 론

스팸(SPAM)이란 인터넷상에서 다수의 수신인에게 무더기로 송신된 전자우편(e-mail)등의 메시지나 사업상의 관계를 갖지 않는 사람이 보낸 음성, 글씨, 화상 등의 모든 통신 내용을 말한다.

상업적 스팸 메일은 시장의 마케팅 방법 중 한가지로 사용되고 있지만, 수신자의 입장에서 스팸은 개인의 사생활을 침해하고 정보사회에 악영향을 미친다. 인터넷전화인 VoIP(Voice over Internet Protocol) 서비스 사업자의 피해 방지책 마련이 요구되며, 음성스팸의 심각성을 누차 지적하게 된것은 2006년 한국정보보호진흥원(KISA)이 발간한 'VoIP 정보보호 가이드'[1]이다.

VoIP는 인터넷전화의 핵심 기술로서 PSTN(Public Switched Telephone Network)를 통해 이루어졌던 음성 서비스를 IP(Internet Protocol) 네트워크를 사용하여 다양한 서비스로 제공하는 것이다. 음성을 디지털화 하고, 전달체계가 IP화됨으로써 전화는 물론 인터넷 팩스, 웹콜, 통합 메시지 처리, 화상회의 등의 향상된 인터넷전화 서비스가 가능하여 All IP 기반의 유비쿼터스(Ubiquitous) 시대의 업무로 전환된다. 또한 VoIP 서비스는 그림 1.과 같이 정부의 IT839전략에서 8대 신규서비스[2] 중의 하나이다.

그림 1. IT839 전략
Fig. 1 IT839 Strategy

VoIP 기술은 다양한 인터넷 서비스와 결합될 수 있는 SIP(Session Initiation Protocol)를 사용한다. SIP는 처음에 음성 통신으로 출발했으나 현재는 쌍방향 사용자간에 음성, 화상, 인스턴트 메시징(Instant Messaging)과 프레즌스 메시징(Presence Messaging) 등을 제공하는 멀티미디어 통신 프로토콜로 발전하고 있다. 프레즌스 프로토콜은 SIP를 확장해 정의된 프로토콜로 IETF SIMPLE WG에서 작업하고 있다. SIMPLE WG는 SIP가 3GPP나 NGN 등의 환경에서 시그널링 프로토콜로 채택되어 있다.

미국 IT 잡지인 redherring[3]은 2006년 8대 보안 트렌드의 하나로 스팸을 꼽았다. 즉 인터넷전화를 노린 새로운 유형의 공격 가운데 대표 사례로 스팸이 팝업 광고처럼 성가신 존재로 부각될 것이란 예상이다. 시만텍[4] 역시 2006년 10대 보안 위협의 하나로 'VoIP 위협 증가'를 꼽았다. VoIP 기술이 널리 퍼지면 VoIP가 공격의 목표가 되는 것은 시간문제라며, IP-PSTN 게이트웨이를 통해 해커가 기존 전화 시스템의 통제권을 갖게 될 수도 있음을 경고하고 있다.

VoIP 보안 위협으로는 스니핑과 서비스 거부(DoS) 공격, 스팸 등이 있는데[5], 이 중 공격하기가 쉬워서 VoIP 서비스의 반대 효과가 가장 클 것으로 생각하는 부분이 스팸부문이다.

본 논문에서는 VoIP의 취약점 중에서 파급 효과가 가장 큰 스팸공격에 대해 연구를 한다. 본 논문에서 VoIP 서비스에 대한 스팸의 공격의 시나리오를 작성하고, VoIP 스팸 공격을 실시한다. 스팸 공격 후 실험실에서 스팸 공격이 성공됨을 증명하고, 스팸을 통한 공격의 결과로 VoIP 스팸의 피해 사실을 확인한다.

본 논문에서는 VoIP 스팸 공격 후에 스팸 차단 방법을 적용한다. 적용된 1) 인바이트 리퀘스트 플루드 공격의 차단 2) 블랙/화이트 리스트, 3) 역추적, 4) Black Hole - Sink Hole, 5) 콘텐츠 필터링, 6) 동의 기반 통신, 7) 콜 행위 패턴 조사, 8) 레퓨테이션 시스템을 통한 스팸 공격의 차단 방안을 실험실 환경에 시험하고, 보안 성능 실험을 한 결과 VoIP 스팸 공격이 차단됨을 보이겠다.

본 논문에서의 이러한 연구 결과를 통하여 앞으로 전개될 VoIP 서비스에 대한 정보보호를 이룩하고, WiBro 서비스가 확대되고, BcN에서 적용되어, 이 결과 유비쿼터스 보안을 실현하는데 이바지 할 수 있도록 하겠다.

Ⅱ. 관련 연구

VoIP 서비스를 수행 할 때에 발생가능 한 스팸 공격의 내용에 대해 관련 연구를 한다.

2.1. 콜 스팸(Call Spam)

콜 스팸은 수신자가 원치 않는 다량의 콜 세션을 시도하는 것으로 정의된다.

SPIT(SPam over Internet Telephony)라고 부르는 콜 스팸은 피해가 크다. VoIP 서비스에 대한 콜 스팸 공격

은 그림 2.처럼 SIP 프로토콜에서 SIP INVITE 메시지의 요청으로 시작한다. SIP INVITE 메시지 요청 세션은 음성, 비디오, 인스턴트 메시징 및 기타 통신을 성립하기 위해 프로토콜의 응답의 초기 과정이다.

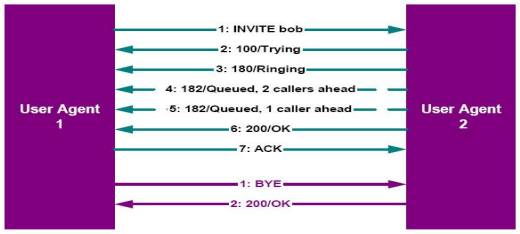

그림 2. SIP INVITE 메시지 요청과 응답
Fig. 2 SIP INVITE Message Request and Response

그림 3.은 SIP INVITE 요청에 대해 사용자가 응답을 하면 콜 스팸은 즉시 실시간 통신으로 연결돼 광고 정보를 전달한다. 이것은 텔레마케터(Telemarketer) 스팸 행위로 이용된다.

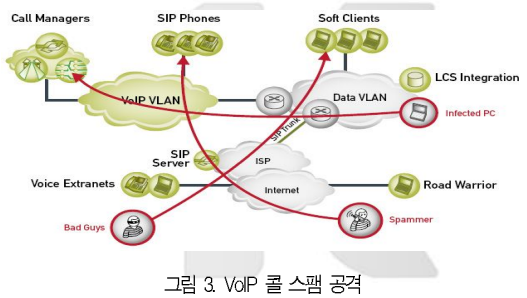

그림 3. VoIP 콜 스팸 공격
Fig. 3 VoIP Call Spam Attack

2006년 10월 우리나라에서의 콜 스팸은 이메일 스팸보다는 빈번하게 발생하지 않는다. 본 논문을 위해 주위의 일반 전화와 휴대폰 사용자 및 이메일 사용에서 스팸내용을 조사한 바에 의하면 2006년 10월 현재, 일일 약 3~5통화 정도는 콜 스팸이다. 하지만 이메일 스팸은 일일 8~30통 정도이다. 이러한 차이는 스팸을 발생시키기 위한 비용이 이메일 스팸보다 콜 스팸이 많기 때문이다.

하지만 VoIP 기반의 SIP 프로토콜을 이용한 스팸을 이용할 때에는 기존 PSTN을 이용한 콜 스팸보다 상대적으로 적은 비용인 약 1/100~1/1000 정도로 스팸 발생 시스템을 구축할 수 있다. 또한 SIP 프로토콜은 이메일과 유사하게 하나의 UA(User Agent)에서 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 재생, 구현할 수 있고, 소프트웨어의 병렬적인 특징을 이용하여 빠르게 복제할 수 있기 때문에 스팸 콜의 VoIP 스팸의 가능성은 매우 높다.

또한 VoIP 서비스에 대한 콜 스팸 공격의 진화된 방법으로써, 스패머(Spammer)들이 다량의 스팸을 발생시키기 위해서 불법적으로 자원을 도용한다. 즉 타인 소유의 서버나 PC를 해킹하거나 바이러스를 전파시킨다. 그리고 침투한 컴퓨터 자원에 스팸을 발생하는 악성 소프트웨어를 기생하게 하여, 주기적으로 스팸을 발생시키도록 할 수 있다. 이때 스팸으로 인해 콜 비용은 침해를 당한 PC나 서버의 네트워크 자원 소유자가 VoIP 서비스 대금을 지불해야 하는 피해자가 발생하게 된다.

유비쿼터스 시대에는 인터넷이 국경의 제한이나 시간, 장소의 제한을 받지 않는 국제적인 스팸의 경우에 더욱 보안의 취약점이 발생한다. PSTN에서는 국제 통화료로 계산되지만 VoIP 서비스는 지구상 어디든지 상대적으로 싼 가격에 VoIP 스팸을 전송할 수 있다.

VoIP 서비스의 콜 스팸은 수신자와 직접 통화할 수 있다는 측면 때문에 스패머에게는 더 효과적으로 광고 수단이 된다. 하지만 스팸의 수신자는 상대편이 본인의 번호를 알고 인터넷전화를 받았는데 스팸으로 판명되는 경우에는, 이메일 스팸보다 더한 불편함과 불쾌함을 야기 시키므로 공격자에게는 더욱 효과적인 공격 수단이 된다.

2.2. 인스턴스 메시징 스팸

인스턴트 메시징 스팸(IM SPAM)[6]은 이메일 스팸과 유사하다. 인스턴트 메시징 스팸은 SPIM(Spam of Instant Messaging)으로 칭한다. 인스턴트 메시징 스팸은 수신자가 원치 않는 다량의 인스턴트 메시지를 전달하며, 대개 스패머가 전달하고 싶은 광고성 내용을 담고 있다.

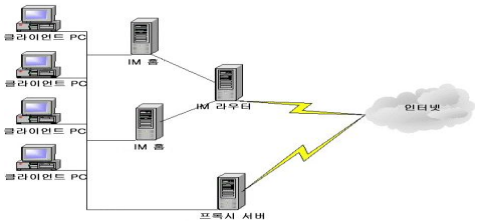

그림 4. 인스턴트 메시징 스팸 전달
Fig. 4 Instant Messaging Spam Delivery

인스턴트 메시징 스팸은 SIP MESSAGE 요청 헤더를 사용하여 전달된다. 그림 4.는 SIP MESSAGE 프로토콜을 이용한 인스턴트 메시징 스팸의 예이다.

또한 다른 요청 헤더를 사용해 사용자의 화면에 자동으로 광고 내용을 표시되게 하여, 사용자를 불편하게 만들 수도 있다. 즉 INVITE 요청 중에 장문의 제목을 삽입하면 비슷한 효과로 스팸 광고를 할 수 있다.

인스턴트 메시징 스팸은 2가지 형태가 있다. 하나는 페이지 모드(Page Mode), 다른 하나는 세션 모드(Session Mode)이다. 페이지 모드는 이메일과 유사하게 각각의 인스턴트 메시지가 별도로 구분된 메시지로 전송된다. 세션 모드는 메시지를 보내기 전에 미리 세션을 성립하고, 이후에 메시지를 교환한다. 인스턴트 메시징 스팸은 단순 메시지를 전송하는 것이기 때문에 음성을 전송하는 콜 스팸에 비해 비용이 적게 든다. VoIP 전화 사업자의 서비스를 이용하여 콜이 성립되면 콜 당 비용이 청구된다. 이 경우 비용의 지출을 피하기 위해, 인스턴스 메시지를 사용한다. 인스턴스 메시지가 메신저 리스트(Messenger List)에 있는 송신자로부터 수신되면 자동으로 화면에 팝업되어 수신자에게 나타나기 때문에 이메일 스팸보다 수신자를 더욱 귀찮게 한다.

2.3. 프레즌스 스팸

프레즌스 스팸은 원치 않는 다량의 프레즌스 요청 메시지를 전송한다. 프레즌스 요청은 프레즌스 이벤트 패키지를 위한 서브스크라이브(SUBSCRIBE) 요청 헤더를 사용한다[6]. 이러한 시도를 통하여 사용자에서 메신저 시스템의 친구 목록 혹은 화이트 목록(White List)[7]에 등록될 수 있도록 시도한다.

RFC2778에 정의된 프레즌스 모델[7]에서 쌍방향 대상은 프레즌티티(Presentity)와 와처(Watcher)로 명명된다. 프리젠티티는 자신의 현재 상태를 알려주는 유저이다. 와처는 프레즌스 정보를 요구하고 수신하는 역할을 한다. 와처는 특정 프리젠티티의 상태 정보를 얻기 위해 서브스크라이브 요청을 수행한다. 와처가 프레즌티티의 상태 정보를 요청하는 처음 과정에는 일반적으로 사용자의 동의를 구하는 메커니즘이 사용된다. 이러한 방법을 동의 프레임워크(Consent Framework)라고 하고, 와처의 프레즌스 요청이 프레즌티티에게 전달되고, 프레즌티티가 이를 승인하면 비로소 프레즌스 정보가 교환된다.

프레즌스 서비스는 상대방이 현재 상태를 나타내 주기 때문에 각 사용자의 사생활이 감시당할 수도 있다. 현재 대부분의 인스턴트 메신저들은 사용자가 IM 서버에 로그 온한 상태에서 PC를 이용한 다음 작업을 일정 시간 동안 하지 않으면 자동으로 사용자의 프레즌스 정보를 'idle'등으로 바꿔서 다른 사용자에게 알려주고 있다. 또한 사용자 사이의 대화기록이 저장되면서 프라이버시 침해 문제가 생길 수도 있다 또한 인스턴트 메시징 클라이언트는 서버에 로그온한 각 사용자의 프레즌스 정보를 지속적으로 서버에게 전달하기 때문에 프레즌스 정보의 외부 노출로 인해 생길 수 있는 사용자의 위치 추적 가능성 문제도 생각해 봐야 한다.

프레즌티티가 와처의 프레즌스 요청을 거부하는 경우에도 스팸 문제는 있다. 와처가 고의적으로 SUBSCRIBE 요청 메시지를 발생시킬 때, 영어광고@xy영어학원.com과 같은 광고를 위한 주소를 사용한다면, 이것 자체가 스팸 성격을 갖기 때문이다. 프레즌티티가 와처의 프레즌스 요청의 스팸 광고를 자주 수신하게 되면 불편을 느끼게 된다.

2.4. VoIP 스팸 공격의 방지 시스템

2006년 10월 현재 상용 서비스 중인 VoIP 서비스에 대한 콜 스팸 방지 시스템으로는 '브로드웍스' IP 센트릭스 서버[8]와 세션보더컨트롤러(SBC) 장비인 '보이스 플로우'[9]가 있다. VoIP 서비스에 대한 콜 스팸 방지 시스템의 기능은 하나의 번호에서 다양한 호가 발생하지 못하도록 하는 기능으로, 콜 스팸 방지와 음성 메일 폭탄 공격을 막는다는 조건이다. SBC에서는 하나의 IP에서 초당 몇 개의 호가 들어오는지 필터링해주며, 현재 설정된 기능은 초당 20호 이상을 음성 스팸으로 규정하여 차단하고 있다.

III. VoIP 서비스의 스팸 공격

VoIP 서비스를 이용하여, 불특정 다수에게 음성 광고 메시지를 전송하거나, 사생활 방해 및 프라이버시 침해를 가하는 공격을 실험실 환경에서 실시한다. VoIP 서비스의 스팸 공격으로는 콜 스팸, 인스턴트 메시징 스팸, 프레즌스 스팸 공격 방법을 사용한다.

3.1. VoIP 서비스의 스팸공격 실험환경 구성

VoIP 서비스의 스팸공격을 위해 다음의 실험실 환경을 구성하였다.

스팸 공격자의 시스템 사양

Notebook, Windows XP Professional SP2(OS), Intel Pentium D, 64bit, 2.66GHz(CPU), 1024 RAM(Memory), 60GB(HDD),

수신자의 시스템 사양

PC, Windows XP Professional SP2(OS), Intel Pentium D, 64bit, 2.66GHz(CPU), 512 RAM(Memory), 250GB(HDD)

VoIP PBX 및 VoIP 단말기 사양

IP PBX, Linux Redhat 9.0(OS), Asterisk 1.2.9, LinkSys IP Phone SPA941(IP Phone)

공격자의 공격 툴

Cain, Rserver, SiVuS를 이용하여 VoIP 취약점을 스캔하여 취약점을 공격한다[10].

실험에 사용된 테스트 네트워크는 그림 5.와 같다.

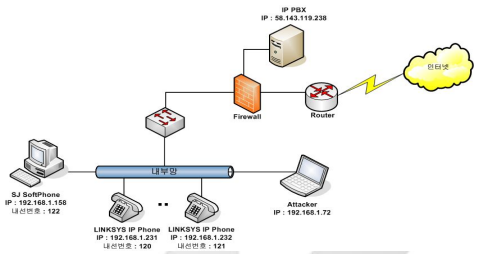

그림 5. VoIP 서비스 스팸 공격

Fig. 5 VoIP Service Spam Attack

3.2. 콜 스팸 공격

저렴하고 자동화된 세션 연결을 통한 다량의 광고음성 발송방법이다. 인바이트 리퀘스트 플루드 공격은 UDP/TCP 모든 전송 기반의 공격이다. 인커밍 콜(Incoming call)을 많이 만들면 SIP 프록시의 CPU 자원을 많이 소비시킨다. 엔드 유저에게도 짧은 시간에 많은 리퀘스트를 요구하며 서비스에 지장을 초래한다. 인바이트 플루딩 공격은 UDP을 기반으로 하기 때문에 손쉽고 파괴적으로 공격 패킷을 생성할 수 있어 주의해야 할 대상이다. 인바이트 및 다양한 메소드 리퀘스트(Method Request)의 처리 시에 프록시 서버는 많은 계산 량을 필요로 하기 때문에 보안에 취약하다고 할 수 있다. 가령 초당 3천 콜을 처리하는 프록시 서버의 경우 초당 수천 개의 UDP 패킷 공격에도 시스템의 서비스에 장애가 발생할 수 있다.

1) 공격 시나리오

(a) 그림 6.에서 수신자의 Caller-ID나 단말 IP주소 등을 수집하거나, 전화번호 생성기 등과 같은 도구를 이용하여 스팸 대상 확보한다.

(b) 자동 스팸 발송 도구를 사용하거나, 스팸 발송 도구를 포함하는 Bot, 악성코드를 PC에 감염시켜 다량의 지속적인 세션 연결을 시도한다.

(c) SIP 헤더의 Contact address 필드에 수신자의 주소를 입력하여 그림 6.처럼 INVITE 메시지를 전송, 프락시 서버 등을 경유하지 않고 수신자에게 직접 전달이 가능하여, 수신단의 인증 및 트래픽 필터링 정책을 우회한다.

(d) 사용자가 세션 연결을 수락 시 음성통화 또는 음성 사서함을 통한 스팸 광고를 발송한다.

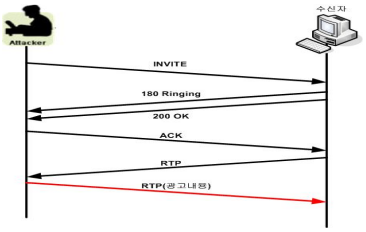

그림 6. 콜 스팸 연결

Fig. 6 Call Spam Connect

2) 공격 결과

Call 스팸은 텔레마케터가 랜덤하게 선택된 사용자들에게 SIP INVITE를 통해 전화를 걸고, INVITE를 수신한 사용자가 응답을 하여 세션이 이루어지면 텔레마케터는 광고를 할 수 있게 된다.

스패머는 SIP UAC(User Account Control)들에게 동시에 INVITE 메시지를 발송하여 통화를 시도하고, 사용자가 통화 시도에 응답하면 자동으로 ACK 메시지를 생성하여 세션을 성공적으로 성립시킨다. 통화가 이루어지면 스패머는 미리 녹음된 음성 메시지를 통해 수많은 사용자에게 손쉽게 내용을 전달할 수 있다. 또한 SIP 기반의 VoIP는 이메일 주소를 사용하기 때문에 기존의 이메일 주소 수집 프로그램을 이용하여 이메일 스팸 규모의 사용자들에게 랜덤하게 통화를 시도할 수 있다.

콜 스팸은 실시간 통신을 전제로 하기 때문에 콜을 요청하면 사용자가 응답을 하게 되고, 음성 메일을 저장함 기능에 남겨 광고를 할 수 있어 사용자를 불편을 초래한다.

3) 피해 내용

다량의 스팸에서 호를 생성하여 서비스 거부 형태 유발 가능하며 사생활 방해 및 프라이버시 침해, 개인정보를 유출한다. 또한, 사회 공학적 공격수법을 이용하여 개인 정보를 불법으로 취득하여 가져간다.

3.2. 인스턴스 메시징 스팸 공격

호가 연결되지 않아도 사용자에게 자동으로 보여 지게 되는 인스턴트 메시지를 통한 스팸 광고를 발송한다.

1) 공격 시나리오

(a) 그림 7.에서 수신자의 Caller-ID나 단말 IP 주소 등을 수집하거나, 사전에 근거한 전화번호 생성기를 이용하여 다수의 스팸 대상을 확보한다.

(b) SIP 헤더의 Contact address 필드에 수신자의 주소를 입력하여 INVITE 메시지를 전송, 프락시 서버 등을 경유하지 않고 수신자에게 직접 전달이 가능하여, 수신단의 인증 및 트래픽 필터링 정책을 우회한다.

(c) IM을 위한 확장된 SIP 메시지 또는 INVITE, OPTION, SUBSCRIBE 등의 일반적인 SIP request 메시지의 subject에 직접 텍스트 형식의 광고 문구를 기재하여 사용자가 호를 수락하지 않아도 그림 7.처럼 자동으로 스팸 광고 문구를 보여준다.

(d) 자동 스팸 발송 Bot을 사용하여 다량의 지속적인 세션 연결을 시도한다.

(e) 사용자가 호 수락 전 통화 종료하여 과금을 회피할 수 있다.

그림 7. 인스턴트 메시징 스팸 연결
Fig. 7 Instant Messaging SPAM Connection

2) 공격 결과

IM 스팸은 자동적으로 팝업 되기 때문에 모든 스팸 정보를 사용자에게 나타날 수 있다. 그러나 IM 시스템의 대부분이 화이트 리스트(White Lists)를 사용하여 메시지를 주고받기 때문에 IM 스팸이 실제 환경에서 큰 영향력은 없다.

3) 피해 내용

다량의 스팸 호 생성으로 서비스 거부 형태 유발 가능하며 사생활 방해 및 프라이버시 침해, 개인정보를 유출한다.

스패머들은 INVITE 요청 헤더에 '영어광고@어느영어학원.com'과 같은 광고성 정보를 송신자의 전화 주소로 삽입하여 INVITE 요청을 전송한다. 그리고 수신자가 이를 받아 본 후 콜이 성립되기 전에 콜을 취소해 비용이 청구되지 않도록 하며, 스팸메일을 수신한 자는 불편과 함께 본연의 업무를 방해받게 된다.

3.3. 프레즌스 스팸 공격

다량의 사용자 프레즌스 정보(친구 리스트, 자신의 상태 정보 등)를 이용하여 스팸 광고 메시지를 전달한다.

1) 공격시나리오

(a) 수신자의 Caller-ID나 단말 IP 주소 등을 수집하거나, 사전에 근거한 전화번호 생성기를 이용하여 다수의 스팸 대상을 확보한다.

(b) 사용자의 메신저의 리스트 또는 화이트 리스트를 확보하기 위해 SIP 메시지인 SUBSCRIBE 요청 메시지를 발송한다.

(b) 리스트 정보를 이용한 인스턴트 메시지 스팸 형태의 단순 광고를 보낸다.

(c) 자동 스팸 발송 Bot을 사용하여 다량의 지속적인 요청을 시도한다.

2) 공격 결과

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 프리즌스 시스템들이 동의 기반의 프레임워크를 제공하기 때문에 프리즌스 스팸의 영향력은 미비하다. 사용자들의 프리즌스를 볼 수 있는 권한이 없는 와처(Watcher)는 그들의 프리즌스 정보를 얻을 수 없다.

3) 피해 내용

다량의 스팸 호 생성으로 서비스 거부 형태 유발 가능하며 사생활 방해 및 프라이버시 침해, 개인정보를 침해한다.

IV. 스팸공격의 차단

4.1. VoIP 스팸 공격의 차단 방법의 제안

VoIP 서비스에 대한 스팸 공격을 차단할 수 있는 방법들을 제안한다. 제안된 방법들에 대한 시험실에서의 시험을 통해 스팸 차단이 되는 지의 결과를 시험한다.

1) INVITE Message 검사

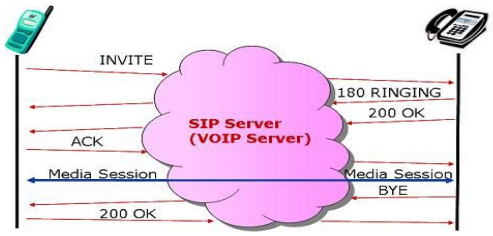

그림 8. SIP에서의 INVITE Message 체크
Fig. 8 Check INVITE Message at SIP

인바이트 리퀘스트 플루드 공격에 차단하기 위해서 그림 8.에서 SIP OK를 조사해 콜 액셉트 레벨(Call Acceptance Label)를 모니터링 한다. 또한 SYN나 ACK의 비율(rate)을 제한하며, 검증되지 않거나 불법적인 인바이트 패킷에 대한 애플리케이션 레벨의 스테이트 풀 방식의 패킷 필터링 [11]을 실시한다.

2) 블랙/화이트 리스트(Black/White List)

블랙리스트는 스패머로 식별된 주소를 데이터베이스로 구축하여, 송신자 주소에 대하여 블랙리스트의 패킷 차단을 실시한다. 하지만 송신자의 주소가 수시로 바뀔 수 있기 때문에 블랙리스트를 업데이트하고 관리해야 하는 단점이 있다. VoIP 서비스 제공자는 SIP을 제한된 포맷으로 송신자의 주소를 정하게 하고, 유효하지 않은 블랙리스트에 대해 차단한다.

화이트 리스트는 메신저에서 허용할 송신자를 사용자가 지정하여 관리하는 방식이다. 즉 인스턴트 메시지에서 등록된 송신자들만 나에게 메시지를 보낼 수 있는 방식이다.

하지만, 화이트 리스트만 사용하게 되면 나에게 처음으로 VoIP 서비스를 사용하려는 업무적인 사용자는 이용할 수 없는 상황이 발생한다. 이를 위해 화이트리스트로 콜을 요청하는 메시지는 허용하되, 스패머가 기계를 이용하여 자동화된 등록요청을 방지하기 위한 방법으로 튜링 테스트(Turing Test) 방식과 같은 자동화된 컴퓨터와 사람을 구별해 내는 방법을 응용한다.

3) 역추적(Trace Back)

VoIP 서비스의 인터넷 패킷의 특성상 IP 계층에서의 역추적 기능을 이용한다. IP 계층의 역추적 기술은 해킹대응 방식에 따라 전향적 역추적 기술(Proactive IP Traceback)의 링크 검사법, 로깅기법, PPM 기법, iTrace(ICMP Traceback)과 대응적 역추적 기술(Reactive IP Traceback)의 오버레이 네트워크 기반 역추적, 해시 기반 역추적, IPSec 기반 역추적 기술로 구분한다. 또한 리플렉토(Reflector) 공격 기반 IP 근원지 역추적 기술을 사용한다.

그림 9.처럼 VoIP 서비스를 제공하는 인터넷 네트워크상의 라우터 와 방화벽(Firewall) 및 IDS, IPS에서 패킷 정보에 대한 역추적을 실시하여 이들 네트워크 보안 시스템에서의 연계 차단 방식을 적용하여, VoIP 스팸 공격을 차단한다.

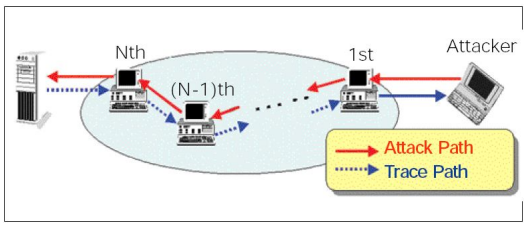

그림 9 VoIP 네트워크 보안 시스템에서의 역추적 차단
Fig. 9 Cut off Traceback at VoIP Network Security Systems

4) 블랙 홀-싱크 홀(Black Hole-Sink Hole)

이메일 주소 생성 프로그램이 확산되면서 많은 스팸메일 방지책들을 회피하고 있다. 이 결과 스팸메일이 대량으로 송수신되면서, 네트워크의 트래픽을 유발시켜, VoIP 서비스를 저해하고 있다.

스패머는 스팸메일을 이용하여 수신자에게 원하는 광고를 하기위해, 수신자의 동의를 구하지 않는 스팸메일을 송출할 때, 이메일 주소 생성 프로그램이 확산되면서 많은 스팸메일 방지책들을 회피하고 있다. 이 결과 스팸메일이 대량으로 송수신되면서, 네트워크의 트래픽을 유발시켜, VoIP 서비스를 저해하고 있다.

만약 특정 메일이 스패머로 판명되거나, 의심 받는 특정 IP에서 오는 메일을 블랙홀방법을 이용하여 유도하고, 싱크홀 방법을 이용하여 차단한다. 이 방법은 PC나 서버용으로 나오는 필터를 설치하여 스팸 메일을 원천적으로 차단하는 방법이다.

5) 콘텐츠 필터링(Contents Filtering)

콘텐츠 필터링은 수신된 이메일의 내용을 검사하고 분석해 스팸으로 의심되는 메일들을 제거하는 것으로 베이시안(Bayesian) 필터링[12] 방법을 적용한다.

하지만 콜 스팸의 제거에서는 이미 콜이 연결되고 스팸 내용을 들은 이후 콘텐츠 필터링을 처리하기 때문에 효과가 적다. 또한, 음성 및 동영상을 인식해 스팸 메일을 분류하는

것이 어렵다. 만약 스패머가 손쉽게 광고 음성 속에 노이즈를 섞거나 음성을 변조해 음성인식이 어렵도록 유도하면 필터링에 걸리지 않는다.

반면, 그림 10.처럼 IM 스팸은 평문이나 HTML/XML 기반의 내용으로 이메일처럼 콘텐츠 필터링을 적용해 차단할 수 있다.

6) 동의 기반 통신(Consent based Communication)

화이트 리스트나 블랙리스트 외에 새로운 사용자가 VoIP 서비스를 이용하고자 할 때 사용자 우선적으로 수신자에게 동의요청을 하게 되고, 동의 요청에 수락하지 않으면 VoIP 서비스는 차단된다.

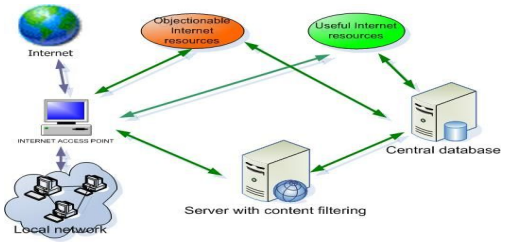

그림 10. 콘텐츠 필터링 서버의 운영
Fig. 10 Operation of Contents Filtering Server

현재 프레즌스 서비스나 인스턴트 메시징 서비스에 적용되고 있지만 이메일 스팸에는 적용하기 힘들다. 또한 VoIP 서비스의 프로토콜 특성상 스팸 문제는 항상 남아있다. 예를 들어 스패머가 고의적으로 SUBSCRIBE 요청 메시지를 발생시키면서 '30분에영어도사@XY영어학원.com'이라는 주소를 사용하면서 동의요청을 자주 받으면 수신자는 이 내용도 스팸으로 귀찮을 수 있다.

7) 콜 행위 패턴 조사

콜 행위 패턴 검사는 송신자 측면에서 검사를 하는 것이다. VoIP 서비스 제공자는 송신자가 보내는 콜의 내용, 송신자의 콜을 생성하는 주기, 횟수 및 행동 패턴 등을 분석하여 블랙리스트와 화이트 리스트를 작성한다.

스패머가 아닌 정상 사용자는 초당 발생할 수 있는 콜의 수가 제한되어 있으므로 콜의 발생 빈도에 대한 한계치(threshold), 총 발생량을 통하여 의심되는 스패머를 판별하고, 정밀한 행위 패턴조사를 통해 블랙리스트를 작성하여 블랙리스트의 스팸공격을 차단한다.

VoIP 서비스 제공자에 의한 콜 행위 패턴 검사는 콜 스팸 및 IM 스팸, 프레즌스 스팸에 적용할 수 있고, 블랙 리스트, 화이트 리스트와도 연동할 수 있다.

하지만 콜 행위 패턴 조사에서 정상적인 사용자에 대한 우연한 행위에 대한 오탐율(False Positive)[13]이 존재하므로 동의 기반 통신과 연계하여, VoIP 서비스의 질적 향상 측면에서 적용이 필요하다.

8) 레퓨테이션 시스템(Reputation System)

송신자에게 레퓨테이션 점수를 부여하는 방식으로, 그림 11.처럼 블랙리스트와 화이트리스트에 연동해 사용한다. 즉 중앙 집중적인 메시지 통신 서비스을 제공 할 때, 각 사용자에 대한 다른 사용자의 레퓨테이션을 피드백하여 점수를 관리하는 것이다. 그 결과 스팸 발신자에게 수신자는 마이너스 점수의 레퓨테이션을 부여해 스팸 발신자를 블랙리스트에 올리게 된다. 정상 발신자는 높은 레퓨테이션 점수를 받아 화이트리스트로 등록된다.

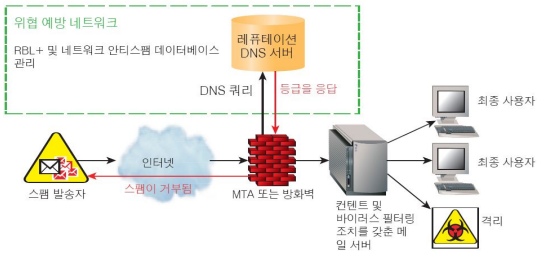

그림 11. 레퓨테이션 시스템
Fig. 11 Reputation System

레퓨테이션 시스템의 단점은 공개된 서비스망에서는 적용이 힘들다. 만약 송신자의 식별이 주소로 될 경우에, 송신자가 자주 바뀔 수 있고, 관리 대상의 송신자가 너무 많기 때문이다. 반면에 폐쇄된 VoIP 서비스 망에서는 송신자의 주소가 자주 바뀌지 않기 때문에, 서비스 제공자와 전체 고객인 송신자를 대상으로 제어가 가능하다.

한편 레퓨테이션 시스템은 고의적인 점수에 의한 오판의 가능성이 존재한다. 예를 들어, 고의적으로 레퓨테이션 점수를 높게 부여해, 스패머를 화이트 리스트에 등록하도록 유도하거나, 정상적인 고객을 고의적으로 낮은 점수를 부여해 블랙리스트에 등록하도록 유도할 수 있다. 따라서 VoIP 고객에 대한 정기적인 불편사항 접수와 현장 확인이 필요하다.

4.2. VoIP 스팸 공격의 차단 방법의 실험

VoIP 서비스의 콜 스팸, 인스턴트 메시징 스팸, 프레즌스 스팸 공격 방법을 사용하여 스팸 공격을 실시한다, 위의 제안된 방법을 실험실 환경에서 적용하여 VoIP 스팸 공격에 대한 차단을 실시한다.

1) VoIP 서비스의 스팸 공격 차단 실험 환경 구성

VoIP 서비스의 스팸공격을 위해 그림 12.와 같은 실험실 환경을 구성하였다.

스팸 공격자의 시스템 사양

Notebook, Windows XP Professional SP2(OS), Intel Pentium M 760, 2.0GHz(CPU), 512 RAM (Memory), 80GB(HDD),

수신자의 시스템 사양

PC, Windows XP Professional SP2(OS), Intel Pentium D, 64bit, 3.2GHz(CPU), 512 RAM(Memory), 250GB(HDD)

VoIP PBX 및 VoIP 단말기 사양

IP PBX, Linux Redhat 9.0(OS), Asterisk 1.2.9, LinkSys IP Phone SPA941(IP Phone)

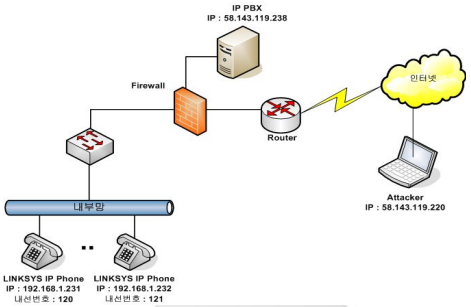

그림 12. VoIP 서비스 스팸 공격과 차단 실험 환경
Fig. 12 VoIP Service spam Attack and Interception Experiment Environment

공격자의 공격 툴

Cain은 패킷 스니핑과 패스워드 크래킹 등 다양한 기능이 포함된 통합 해킹 툴로서 스위칭 환경에서의 스니핑을 실시한다. Rserver 프로그램을 이용하여 특정 포트를 열어 공격 대상 컴퓨터를 원격 제어하고 소프트 폰이 설치된 개인 사용자의 PC 해킹을 실시한다. SiVuS를 이용하여 VoIP 취약점을 스캔하여 취약점을 공격하여 해킹을 실시한다.

그림 12.에서 VoIP 서비스의 콜 스팸, 인스턴트 메시징 스팸, 프레즌스 스팸 공격 방법을 사용하여 스팸 공격을 실시하였다. 그리고 4.1.에서 적용한 스팸 차단 방법을 실험실 환경에서 적용하여 VoIP 스팸 공격에 대한 차단을 실시한 결과 표 1.과 같은 결과를 나타냈다.

표 1. VoIP 스팸의 차단 등급
Table.1 Interception Grade of VoIP Spam

차 단 방 안	콜 스팸 공격	인스턴스 메시징 스팸 공격	프레즌스 스팸 공격
Invite Message	상	중	중
Black/White List	하	상	하
역추적기법	하	상	하
Black/Sink Hole	상	상	중
콘텐츠 필터링	상	상	중
동의기반 통신	상	중	중
콜 행위 패턴 조사	상	상	중
레퓨테이션 시스템	상	상	상

표 1.의 VoIP 스팸의 차단 등급에서는 각각의 차단 방안에 따른 콜 스팸 공격, 인스턴스 메시징 스팸 공격, 프레즌스 스팸 공격에 대한 차단 등급을 전체차단은 '상'으로, 일부 차단은 '중'으로, 차단 효과가 적은 것은 '하'로 표시 하였다.

표 1.에서 콜 스팸 공격에는 Invite Message, Black/Sink Hole, 콘텐츠 필터링, 동의기반 통신, 콜 행위 패턴 조사, 레퓨테이션 시스템의 차단 효과가 상대적으로 좋았다.

인스턴스 메시징 스팸 공격에서는 역추적기법, lack/Sink Hole, 콘텐츠 필터링, 콜 행위 패턴 조사, 레퓨테이션 시스템이 상대적으로 효과가 있었다.

프레즌스 스팸공격에서는 레퓨테이션 시스템의 차단 효과가 가장 뛰어났다.

그림 13.은 Ethereal 툴을 이용하여 패킷을 스니퍼한 결과 스팸을 나타내는 패킷이 나타나지 않아 스팸을 차단하고, 보안수준이 강화된 결과를 나타내었다.

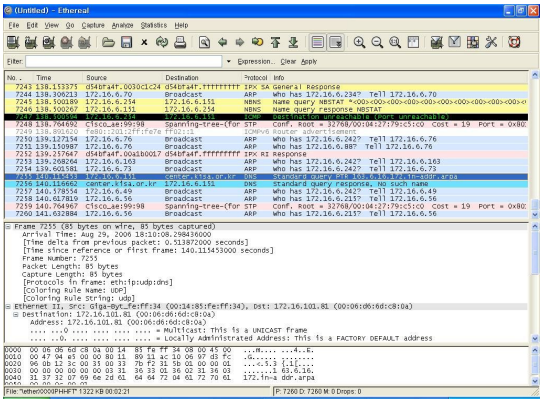

그림 13 Ethereal 이 캡처한 VoIP 패킷의 내용 확인
Fig. 13 Contents confirmation of a VoIP packets which Etherea captured.

V. 결론

본 논문에서는 IT839 전략의 8대 서비스인 VoIP 서비스의 스팸공격과 차단 방안에 대해 연구했다.

VoIP 서비스는 IP의 취약점을 모두 갖고 있으므로, 보안에 관해서도 파급 효과가 가장 큰 스팸공격에 대해 연구를 하였으며, 스팸의 공격의 시나리오를 작성했고, VoIP 스팸 공격을 실시했다. 스팸 공격 후 실험실에서 스팸 공격이 성공됨을 증명하였고, 스팸을 통한 공격의 결과로 VoIP 스팸의 피해 사실을 확인했다.

본 논문에서는 VoIP 스팸 공격 후에 스팸 차단 방법을 적용하고, 차단 방안을 실험실 환경에 테스트 하였다. VoIP 서비스의 스팸 차단 방법의 적용에서 1) 인바이트 리퀘스트 플루드 공격에 차단 2) 블랙/화이트 리스트, 3) 역추적, 4) Black Hole - Sink Hole, 5) 콘텐츠 필터링, 6) 동의 기반 통신, 7) 콜 행위 패턴 조사, 8) 레퓨테이션 시스템을 적용하고 각각의 방법을 실험하였다. 각각의 적용된 차단 방안을 VoIP 네트워크에서 실험하여 스팸차단의 강도에 따라 '상','중','하'의 보안 등급으로 확인 하였다.

본 논문의 VoIP 네트워크에서의 실험과 스팸차단의 강도에 따라 '상','중','하'의 보안 등급으로 확인연구와 실험 결과를 통하여 VoIP 서비스의 정보보호가 WiBro, BcN에서 확대되어 U-Korea에서의 유비쿼터스 보안을 실현하는데 이바지 할 수 있을 것이다.

향후 연구 되어야 할 과제로는, 암호화와 접근제어 및 인증과 무결성 검증의 방법을 구체적으로 모듈화하고 SBC나 Proxy Sever에서 SIP 공격이나, RTP Flooding 공격, DoS공격 및 패턴 매칭이 일어나지 않는 해커의 새로운 공격에 대한 방어 연구를 하여야 한다.

참고문헌

[1] 한국정보보호진흥원(KISA) 'VoIP 정보보호 가이드' 2006.1.

[2] 홍도원, 염용진, 정교일, 지성택. "IT839전략과 정보보호". 한국정보보호학회지, 제14권5호 , pp.23-31 , 2004.

[3] redherring. http://www.redherring.com. 2006.

[4] SYMANTEC. http://www.symantec.com. 2006.

[5] Thomas Poter 외 7인. "Practical VoIP Security," SYNGRESS. 2006.

[6] Miikka Poikseika, Georg Mayer, Hisham Khartabil, Aki Niemi. "The IMS IP multimedia Concets and Services," JOHN WILEY & SONS, LTD. 2006.

[7] M. Day et. al ""Instant Messaging/Presence Protocol Requirements,"" IETF RFC 2779, Feb. 2000.

[8] 브로드웍스. http://www.broadsoft.com. 2006.10.

[9] 보이스 플로우. http://www.kr.juniper.net/. 2006. 10.

[10] 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, pp155-164, 2006. 9. 30.

[11] 김영호, 손승원, 박치항. "IP Fragment 패킷을 위한 동적 패킷필터링 기법", 한국정보보호학회 동계학술대회. pp.128-131 , 2003.

[12] 김현준, 정재은, 조근식. "가중치가 부여된 베이지안 분류자를 이용한 스팸 메일 필터링 시스템" 한국정보과학회논문지, 제31권8호, pp1092-1100, 2004

[13] 박대우, 임승린. "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구." 한국컴퓨터정보학회논문지, 제11권 제2호., pp44-50, 2006. 5. 31.

저 자 소 개

이 인 희

2000년 한신대학교 컴퓨터학과 졸업 (공학사)

2005년 숭실대학교 정보과학대학원 정보보안학과 (석사과정)

2006년 숭실대학교 정보과학대학원 정보보안학과 조교

<관심분야> 사이버포렌식, 역공학, 무선 네트워크, 방화벽,

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

<관심분야> 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality