SIP 기반 VoIP 환경에서 스팸 문제점과 대응 기술에 대한 고찰*

최상명[1], 김은숙[2], 강신각[2], 염흥열[1]

[1]순천향대학교 정보보호학과, [2]한국전자통신연구원 표준연구센터

Combating SIP Spam By Technical Means

Sang-Myung Choi[1], Eun-Sook Kim[2], Shin-Gak Kang[2], Heung-Youl Youm[1]

[1]Department of Information Security Engineering, SoonChunHyang University,

[2]Protocol Engineering Center, ETRI

요 약

기존 전화에 비해 저렴한 가격으로 서비스의 제공이 가능한 VoIP 서비스의 증가는 SIP 스팸이라는 역기능을 낳았다. SIP은 표준 VoIP 프로토콜로 현재 SIP 기반의 VoIP 서비스의 개발이 활발하게 진행 중에 있다. 이에 본 논문은 SIP 기반 VoIP 환경에서의 스팸 유형을 살펴본 후 이를 해결하기 위한 스팸 대응 기술로 기존의 이메일 스팸 대응 기술을 비교, 분석한다. 또한 이메일 스팸 대응 기술을 기반으로 제안된 현재 SIP 스팸 대응 기술을 알아보고 앞서 분석한 대응 기술의 SIP 기반 VoIP 환경에서의 적용 가능 여부를 생각하여 가장 적합한 스팸 대응 기술을 제시한다.

I. 서론

스팸은 원하지 않은 상업 메일로, 기술 중립적 용어이다. 하지만 스팸은 이메일에만 국한되지 않으며 VoIP 환경에서도 나타날 수 있다. 최근 VoIP 서비스에 대한 관심이 크게 증가하면서 앞으로 나타나게 될 역작용 기술로써 VoIP 환경에서의 스팸 문제점을 생각해 볼 수 있다.

VoIP란 Voice over Internet Protocol의 약자로, 인터넷 망을 이용하여 음성을 전송하는 기술을 말한다. 흔히 인터넷 전화라고도 불린다. 현재 IT839의 8대 서비스 중의 하나로 각광 받고 있으며 기존 전화에 비해 저렴한 가격으로 서비스의 제공이 가능하여 앞으로 크게 발전할 가능성이 있는 기술이다.

SIP[1]은 표준 VoIP 프로토콜로 현재 SIP 기반의 VoIP 서비스의 개발이 활발하게 진행 중에 있으며 이에 스팸은 SIP 기반의 VoIP 환경에서 발생할 것이다.

본 논문에서는 SIP 기반 VoIP 환경에서 스팸 유형을 살펴보고 이를 해결하기 위해 기존의 이메일 스팸 대응 기술을 비교, 분석하여 SIP 기반 VoIP 환경에 적용 가능한 스팸 대응 기술을 모색해본다. 또한 현재 제안된 SIP 스팸 대응 기술을 알아보고 앞서 분석한 대응 기술과 비교하여 SIP 기반 VoIP환경에서 가장 적합한 스팸 대응 기술을 제시한다.

II. SIP 스팸 유형

SIP은 Session Initiation Protocol의 약자로 VoIP 시그널링 프로토콜 종류의 하나로 IETF에서 발표한 표준 VoIP 프로토콜이다. SIP은 각 사용자들을 구분하기 위해 이메일 주소와 비슷한 SIP URI를 사용함으로써 사용자는 IP주소에 종속되지 않고 서비스를 제공받을 수 있

* 본 연구는 ETRI 연구 과제로 ETRI의 지원을 받아 수행중임.

다. TCP와 UDP 모두 사용할 수 있으며 request와 response 구조로 되어 있다. 응용계층 프로토콜로써 TCP와 UDP 모두 사용할 수 있으며 request와 response 구조로 되어있다. HTTP와 SMTP의 syntax와 semantics의 많은 부분을 그대로 사용하며 HTTP와 유사한 transaction을 한다.

이러한 SIP기반의 VoIP 환경에서의 SIP 스팸은 Call 스팸, IM 스팸, Presence 스팸과 같이 3가지 유형으로 분류가 가능하다[2],[3].

■ Call 스팸

스팸 전달을 위한 통신을 맺기 위해 임의의 사용자에게 대량의 SIP INVITE 메시지를 전송하는 것을 말한다. 사용자가 응답하면, 스패머는 실시간 매체를 통하여 자신의 메시지를 재생한다. 현재의 PSTN망에서의 텔레마케팅과 같은 형태의 SIP에 적용된 텔레마케팅으로 나타날 수 있다.

값비싼 비용을 지불해야 하는 기존 PSTN을 이용한 Call 스팸은 SIP 기반의 VoIP 환경에서는 매우 저렴한 비용으로 스팸 발생 시스템을 구축할 수 있다. SIP Call은 이메일과 유사하게 하나의 UA(User Agent)에서 다량의 Call을 초기화하고 병렬적으로 발생시킬 수 있고, Call이 성립되면 스팸 소프트웨어에서 녹음된 음성을 전달한 후 Call을 끊을 수 있다. 이 모든 것이 저렴한 PC상에서, 공개된 소프트웨어를 통해 간단하게 반복 재생, 구현될 수 있다.

■ IM 스팸

이메일 스팸과 유사한 형태의 스팸 기술로 IM을 위한 확장된 SIP 메시지를 사용하여 이루어진다. 또한 일반적인 SIP Request 메시지들의 Subject 헤더를 이용하여 송신자에게 자동으로 불필요한 문구를 보여줄 수 있다.

대부분의 IM 시스템이 사용자의 의지와 상관없이 자동으로 메시지를 팝업하며, 화이트 리스트를 사용하는 IM 시스템에서는 적용이 불가능하다.

■ Presence 스팸

IM 스팸과 비슷하며, SUBSCRIBE 요청 메시지를 이용하여 스팸 정보를 전달하는 방법이다. 화이트 리스트와 상관없이 스팸을 전달할 수 있지만 정보의 양이 제한적이다.

III. 기존 이메일 스팸의 대응 기술

기존 이메일 스팸의 대응 기술은 크게 필터링 기법을 이용하는 방법과 인증 기술을 이용하는 방법으로 분류할 수 있다.

1. 필터링 기법

필터링 기법을 이용하는 방법은 그레이리스팅 방법, 휴리스틱 필터링 방법, Bayesian 필터링 방법 등이 있다[7].

■ 그레이리스팅 방법

수신자가 새로운 머신으로부터 메일을 수신하면 일단 임시의 에러 메시지를 되돌리고, 송신 머신이 추가로 해당 메일을 다시 전송하면 적법한 MTA로 인정하는 방법이다. 스팸을 보내는 MTA는 일반적으로 재시도를 하지 않는다는 특성을 이용하는 방법으로 놀랍게 효과적이고 설치가 매우 간단한 특징이 있다.

■ 휴리스틱 필터링 방법

일단 스팸성 시험을 시도하여 여기서 스팸에 대한 점수를 계산하고 이를 근거로 스팸여부를 판단하는 방법이다.

■ Bayesian 필터링 방법

사람이 필터를 훈련시켜서 스팸 여부를 판단하는 방법으로 사용자 인터페이스가 존재해야 하며, 사용자 훈련 과정이 필요하다.

2. 인증기법

인증기법에는 다음과 같은 SPF, DKIM 등의 방법이 있다.

■ SPF[6]

Sender Policy Framework의 약자로 송신자가 자신의 영역 내에 존재하는 DNS에 자신을 대신하여 보낼 수 있는 머신을 나타낸다. 수신자가 이 DNS의 내용을 조회하여 해당 MTA로부터 온 메일이면, 이를 수신하고 그렇지 않으면 추가적인 보안 정책을 적용하게 된다. 하지만 이 방법은 도메인을 인증하는 것이지 사용자를 인증하는 것은 아니다.

■ DKIM[4]

Domain Key Identified Mail의 약자로 송신자가 헤더에 서명문을 넣어서 전송하고, 수신자

는 송신자의 DNS 서버에서 서명문을 검증하기 위한 공개키를 구하여, 공개키의 유효성과 서명문의 유효성을 검증하게 된다. 둘 다 통과하면 스팸이 아닌 메일로 판단한다.

현재 IETF에서 표준화되고 있는 방법으로, 가장 효과적인 대책중의 하나이다.

IV. SIP 스팸 대응 기술 분석

SIP 스팸 대응 기술에는 다음과 같은 기술들이 있다.

■ Address Obfuscation

스팸을 보낼 주소의 획득을 어렵게 하기 위해 메일 주소를 이미지로 나타내는 등의 방법으로 모든 스팸 대응의 필수적인 방법이다.

■ Content Filtering

Content의 내용을 분석하여 스팸 여부를 판단하는 방법이다.

■ Black Lists

스팸 필터가 스패머를 확인하는 주소 목록을 유지하고 있는 방법으로 주소는 사용자 이름과 도메인 이름을 포함한다. 하지만 다음과 같은 두 가지 이유로 인해 매우 유용한 방법은 아니다. 첫 번째, 이메일 주소는 위조하기가 매우 쉬워서 송신자가 다른 사람인척 하는 것이 가능하다. 두 번째, 송신자가 주소를 위조하지 않더라도, 주소를 쉽게 생성할 수 있다.

■ White Lists

White Lists는 Black Lists의 반대로, 사용자가 수신하고자 하는 유효한 송신자의 목록이다. 주소 위조에 취약하나, 강한 아이디 인증 메커니즘이 이 문제를 해결할 수 있다.

■ Consent-Based Communications

상대방에게 추가 요청 메시지를 전송한 뒤 동의 했을 경우에 상대방의 White Lists에 자신의 주소가 등록되는 방법이다.

■ Reputation System

수신자는 송신자의 평판도를 확인하여 통신을 수신할지 말지에 대하여 결정하게 된다.

■ Limited Use Addresses

사용자가 여러 개의 이메일 주소를 생성하여 사람들에게 서로 다른 이메일 주소를 알려준다. 특정 주소로 스팸이 도착하기 시작하면, 사용자는 그 주소를 폐기하고 다른 주소로 변경한다.

이 방법의 단점은 사람들이 사용자에게 연결하는 것을 어렵게 만들 수 있다는 것이다.

■ Turing Tests

송신자에게 사람만 응답할 수 있는 퍼즐이나 질문을 요청하여 응답할 수 있도록 하는 기법이다.

■ Payments at Risk

메일을 보내기 전에 미리 수신자 측의 계좌에 일정 금액을 예치하고, 수신자가 스팸이 아니라고 판단하면 돌려주는 방법이다.

V. 효과적인 스팸 대응 기술

본 논문에서는 앞서 살펴본 다양한 스팸 대응 기술 중 SIP 기반의 VoIP 환경에 적용 가능한 다음과 같은 효과적인 스팸 대응 기술을 분석한다.

1. 서명문 기반 스팸 대응 기술[4]

서명문 기반 방법은 송신 도메인의 신원을 확인하며, 서명문 검증후 검증 결과에 따라 추가적인 정책인 버림, 수용, 검역, 추가적인 조치를 취할 수 있는 장점이 있다. 서명문 검증 방법은 수신된 메일의 유효성을 검증하기 위하여 메일의 무결성을 검증하는 과정과 공개키의 유효성을 검증하는 과정으로 구성되어 있다.

이 과정은 서명문을 헤더에 부가하는 과정, 메시지를 검증하는 과정, 키 등록 서버를 이용하여 키를 관리 과정, 그리고 명성 서비스 과정으로 구성된다. 먼저 서명문을 헤더의 부가하는 과정의 경우, 송신 영역에 있는 MTA는 메시지를 서명하여 서명문과 공개키를 헤더에 삽입하며, 인가 정보는 특정의 이메일 주소와 공개키를 결합시키는 것으로 일반적으로 신뢰 데이터베이스에 저장되어 있다. 서명문을 검증하는 과정의 경우, 헤더에서 공개키를 꺼내어서, 공개키를 이용하여 서명문을 검증하고, 공개키의 유효성을 확인하기 위하여 키 등록 서버나 DNS를 이용하여 해당 공개키의 유효성을 확인한다. 따라서 이 과정은 서명문 검증 과정과 송신자 공개키 검증 과정으로 구성될 수 있다. 키 등록 서버를 이용하는 키 관리 과정의 경우, 두 가지 대안이 존재하며, 하나는 DNS를 이용하여 검증

하는 방법이고, 다른 하나는 별도의 키 등록 서버를 두어 검증하는 과정이다. 키 등록 서버는 사용자 레벨 키인가를 지원하기 위한 최대의 융통성을 제공하며, DNS와 이메일 인가를 관리적으로 구분하는 기능을 제공한다.

또한 평판 서비스는 서명된 메시지에 대한 추가적인 보안 정책의 적용을 가능케 한다. 평판 시스템은 송신 영역의 등급을 결정하여 이를 이용하여 바람직한 영역인지 바람직하지 않은 영역인지를 구별하며, 일반적으로 등급은 도메인에 대하여 수행되나, 개별 사용자 차원에서도 적용될 수 있다.

이밖에 특징은 역방향 호환성 유지, 융통성 있는 키 등록 방법, 송신자에서 수신자까지의 경로에 대한 지원, 사용자 또는 도메인 레벨에서 인가 기능 제공, 추가적인 정책 선택 등을 들 수 있다. 현재 이 방식은 IETF DKIM 워킹 그룹에 제안되어 표준화가 진행되고 있는 방식으로 대표적인 서명문 기반 방식이라고 할 수 있다.

2. 신분확인 기반 스팸 대응 기술[5]

인증된 신분 확인을 이용한 SIP 스팸 대응 기술로 "draft-ietf-sip-identity-02"에서 제안한 방법도 효과적이다. SIP 최종 사용자의 신원을 확인하는 방법으로 안전하고 인증된 아이덴터티를 분배하는 방법을 제안하는 것을 정의하였다.

송신 도메인이 헤더에 대한 해쉬값을 계산하여 이를 그 도메인을 위한 인증서로 서명하여, 새로운 헤더에 넣는다. 수신 도메인은 새로운 Identity-Info 로 주어진 URI를 통하여 송신 도메인의 공개키를 조회한다. 수신 도메인은 콜을 인증하게 되며 사전 연계나 신뢰 관계는 가정하지 않는다.

이를 위해서는 다음과 같은 2개의 SIP 헤더가 필요하다.

- Identity

To/From 주소, Call-id, SIP-Date, Contact 주소, 그리고 message-body 에 대한 해쉬된 서명값을 갖는다.

- Identity-info

인증서를 갖고 있는 곳을 포함하는 HTTPS URI 또는 SIPS URI을 나타낸다.

VI. 결론

기존의 필터링 방법은 여러 가지 방법이 존재하나, 인증 기법을 이용한 방법이 최선의 방법이 될 것으로 예측된다. 따라서, 인증 기법을 이용한 스팸 대책의 개발이 필요하나, 기존의 휴리스틱한 방법을 이용한 대책이 동시에 적용되어서 스팸의 가능성을 차단해야 할 것으로 전망된다.

특히 SIP 기반의 VoIP 환경에서의 효율적인 스팸 문제점 해결을 위해 인증된 신분 확인을 이용한 신분확인 기반 스팸 대응 기술에 대한 상세한 분석과 연구를 계속 진행하고 기존의 스팸 대응 기술들과의 적절한 결합을 모색하는 연구 활동을 진행해 나가야 할 것이다.

[참고문헌]

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A.R. Johnston, J. Peterson, R. Sparks, M. Hand-ley, and E. Schooler, "SIP: Session Initiation Protocol", IETF, RFC 3261, June 2002.

[2] 정수환, "VoIP 스팸과 보안", 한국정보통신기술협회, TTA 저널, 2006년 4월.

[3] J.Rosenberg, C. Jennings, "The Session Initiation Protocol (SIP) and Spam", draft-rosenberg-sipping-spam-01, October 2004.

[4] E. Allman, J. Callas, "DomainKeys Identified Mail Signatures (DKIM)", draft-ietf-dkim-base-02, May 2006.

[5] J. Peterson, C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-02, May 2004.

[6] Sender Policy Framework (SPF), http://spf.pobox.com/

[7] IRTF Anti-Spam Research Group, http://asrg.sp.am/