한국컴퓨터정보학회 하계학술대회 논문집 제25권 제2호 (2017. 7)

송신자 자가인증 기법을 적용한 스팸차단 서버와 안드로이드 애플리케이션 구현

양인식[O], 백전성[*], 강경태[*]
[O*]한양대학교 컴퓨터공학과
e-mail: inshik@hanyang.ac.kr[O], {jsbaik, ktkang}@hanyang.ac.kr[*]

Implementation of Anti-Spam Server and Android Application Using Self-Authentication Mechanism

Inshik Yang[O], Jeanseong Baik[*], Kyungtae Kang[*]
[O*]Dept. of Computer Science & Engineering, Hanyang University

● 요 약 ●

이메일 서비스 사용자들은 스패머가 무차별적으로 발송하는 스팸메일에 의한 정신적·경제적 피해를 입고 있다. 이러한 피해를 막기 위해 필터링, RBL (Real-time Blackhole List)과 같은 스팸차단 기법이 등장하였고 많은 메일서버에서 사용되고 있다. 그러나 이는 스팸메일의 근본적인 원인은 해결하지 못하며, 높은 차단율을 유지하기 위해서는 지속적인 관리 및 업데이트가 필요하다. 이러한 한계점을 극복하기 위한 기법으로 송신자 자가인증 기법이 있다. 본 논문에서는 송신자 자가인증 기법을 적용하여, 스팸메일을 근본적으로 차단하고 지속적인 업데이트가 필요 없는 스팸차단 서버 및 애플리케이션을 구현하였다.

키워드: 스팸메일(Spam mail), 스팸차단(Spam filtering), 자가인증(Self-Authentication)

I. Introduction

스팸메일이란, 수신자가 원치 않음에도 불구하고 스패머에 의해 일방적으로 전달되는 영리목적의 불법 광고성 이메일로, 이메일 서비스 사용자의 불편함과 성가심을 유발하고 업무의 능률을 떨어뜨리는 등의 정신적·경제적 손실을 유발한다. 이러한 스팸메일을 방지 및 차단하기 위하여 필터링, RBL 등의 스팸차단 기법이 등장하였고 많은 메일서버에서 사용되고 있다[1,2]. 하지만, 이와 같은 기법은 스팸메일의 원인을 근본적으로 해결하는 방식이 아니기 때문에 스팸메일의 완벽한 차단이 불가능하다[3].

본 논문에서는 이러한 기존 스팸차단 기법의 한계점을 극복하고 스팸메일의 차단율을 높이기 위한 방법으로 송신자 자가인증 기법을 이용한 스팸차단 방법과 이 기법을 적용한 스팸차단 서버와 안드로이드 애플리케이션 구현에 관한 내용 및 특징에 대해 소개한다.

II. Preliminaries

1. 스팸메일 차단 기법

1.1. 필터링

필터링은 메일서버의 관리자가 미리 메일의 제목이나 내용, 첨부파일 등에 사용해서는 안 되는 단어들을 정하여 금칙어 필터를 만들고, 수신한 메일의 내용을 탐색하여 금칙어가 포함되어 있는 경우 차단하는 기법이다. 기법의 적용 초기에는 높은 차단율을 보일 수 있으나, 스패머들이 금칙어 필터를 피하여 메일의 내용을 변형시킨 경우에는 차단하지 못하기 때문에 지속적인 필터의 업데이트가 필요하다.

1.2. RBL

RBL은 국내외 스팸정보들을 실시간으로 취합 및 분석하여 제공하는 스팸발송 IP 리스트를 말한다. 보통 DNS (Domain Name Server) Lookup을 통해 확인하는 방식을 이용하기 때문에 DNSBL (DNS-based Blackhole List)이라고도 한다. 국내에서는 한국인터넷진흥원(KISA, Korea Internet & Security Agency)에서 관리하여 무료로 제공하는 KISA-RBL이 있으며, 1시간 단위로 리스트의 업데이트가 이루어진다. 이를 이용하여 스팸발송 IP로부터 발송된 메일을 사전에 차단하는 것이 가능하다. 그러나 리스트에 존재하지 않는 IP로부터의 스팸공격은 차단하지 못하는 한계점을 가지고 있다.

2. 송신자 자가인증 기법

송신자 자가인증 기법이란, 송신자가 발송한 메일이 수신자에게 정상메일로 도달하기 위해서는 송신자가 직접 자신이 스패머가 아님을 인증해야 하는 스팸차단 기법을 말한다. 만약 송신자가 수신자의

화이트리스트에 등록되어있지 않으면, 해당 송신자는 자가인증 서버로부터 인증 요청 메일을 받게 되며, 이를 통해 자가인증 서버로 접속하여 인증을 하는 절차를 거치게 된다. 반대로, 화이트리스트에 등록되어 있는 송신자들에 대한 메일은 스팸메일이 아닌 정상메일로 간주되어 수신자가 이를 정상적으로 수신하게 된다. 화이트리스트에는 수신자가 직접 등록하거나 인증을 마친 송신자가 등록된다.

III. Implementation

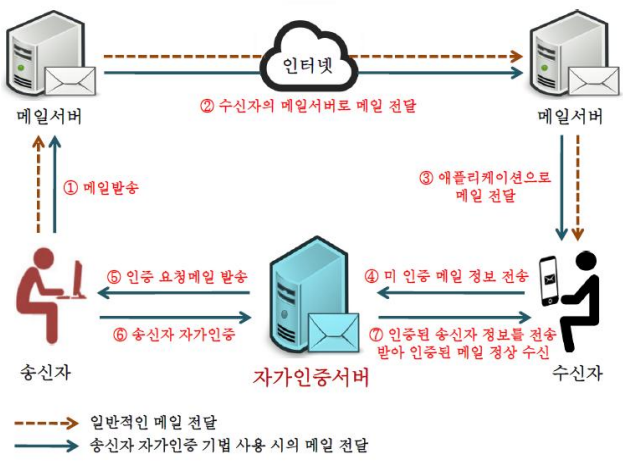

Fig. 1. Mail delivery process

1. 송신자 자가인증 기법을 위한 서버 구성

송신자 자가인증 기법에 사용되는 인증 절차를 처리하기 위하여 추가적인 스팸차단 서버인 자가인증 서버를 구현하였다. 자가인증 서버는 Fig. 1과 같이 송신자와 수신자 사이에서 동작하며 다음과 같은 작업들을 수행한다.

- 송신자에게 인증 요청메일 발송
- 송신자의 인증 처리
- 화이트리스트 관리

2. 서버 및 애플리케이션 동작 과정

구현한 애플리케이션은 먼저 받은 메일의 송신자가 화이트리스트에 등록되어있는지를 검사한다. 만약 화이트리스트에 등록되어 있지 않으면, 해당 송신자는 자가인증 절차를 거치게 된다. 자가인증 서버는 송신자에게 인증 요청메일을 발송하게 되고, 이를 확인한 송신자는 Fig. 2의 자가인증 웹페이지에 접속해 서버가 무작위로 생성한 인증번호를 입력하여 인증을 완료한다. 자가인증 서버는 인증이 완료된 송신자를 화이트리스트에 등록하고 인증정보를 애플리케이션에 전달하여, 애플리케이션이 해당 메일을 정상메일로써 수신하도록 한다.

Fig. 2. Self-authentication web page

IV. Conclusions

일반적인 메일서버가 사용하는 스팸차단 기술인 필터링이나 RBL 방식은 차단율을 높이기 위하여 꾸준한 필터 업데이트가 필요하며, 하루에 많으면 수십 회의 업데이트를 수행한다. 그럼에도 불구하고 이러한 기존 기법은 변종 스팸메일을 차단하지 못한다. 구현한 애플리케이션을 사용하면 메일서버가 미처 차단하지 못한 변종 스팸메일에 대한 강력한 차단이 가능하고, 지속적인 업데이트 없이도 높은 스팸 차단율을 유지한다. 또한, 스패머의 공격뿐만 아니라 수신자가 무심코 수신을 동의한 광고성 메일도 함께 관리할 수 있으며, 기존에 사용하던 메일 서비스의 계정을 애플리케이션에 그대로 등록하여 사용할 수 있는 편리성이 있다.

REFERENCES

[1] Anand G Sharma and Prof. VedantRastogi., “An analysis on Filter for Spam Mail”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol. 1, No. 1, pp. 174-177, Apr. 2014.

[2] DNS Blacklists and Whitelists, tools.ietf.org/html/rfc5782

[3] State of Spam and Phishing Report, symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_09-2010.en-us.pdf