스팸메일 차단 시스템 설계 및 구현

김진만* · 장종욱*

*동의대학교 컴퓨터공학과

Design and Implementaion of The Spam E-Mail Filtering System

Jin-man Kim* · Jong-wook Jang*

*Dongeui University

E-mail : iricejm@dongeui.ac.kr

요 약

전자메일은 과거 매우 특이한 커뮤니케이션 방식이었으나 이제 그것은 일상의 통신방법 중 하나로 정착 되었다. 개인적인 목적에서부터 중요한 비즈니스적인 목적으로까지 이용되고 있는 전자메일은 그 특성상 보안에 취약하고, 그를 이용한 상업적 또는 악의적인 목적으로까지 이용되기도 한다. 그래서 최근 스팸메일의 차단과 상업성 광고 메일에 관련한 문제가 대두되고 있으며, 그에 관련된 대처 방안들이 많이 나오고 있는 실정이다. 이 논문에서는 스팸메일 및 상업적 목적의 광고성 메일등의 분류 및 차단에 관련하여 세 가지 측면 즉, 서버 레벨 차단, 네트워크구조 레벨 차단, 클라이언트 레벨 차단방법 중 클라이언트 레벨에서의 스팸메일차단 시스템을 설계하고, 구현하였다.

ABSTRACT

E-mail was very particular way of communication in the past, but it becomes one of daily communication methods now. Due to E-mail has a property which is not complete for security, sometimes it is used for purpose of commercial or badthings, therefore it becomes the latest problem to keep off a Spam-mail and commercial advertising E-mail, many ways to keep off were perposed for it.

In this paper, I explained how to sort and keep off these Spam-mail and commercial advertising E-mail with three way, prevention by server level, prevention by construction of network level, prevention by client level. we designed a prevention system for Spam-mail and implemented it by Visual Basic.

키워드

스팸메일, 메일 필터링, 패킷 필터링

Ⅰ. 서 론

정보 사회의 편리한 도구로서 전자우편은 인터넷에서 가장역사가 오래된 서비스로 상대방의 ID만 알고 있으면 대부분 무료로 이용하거나 저비용으로 세계 어느 곳이나 상관없이 전달할 수 있으므로 개인적 목적에서부터 중요한 비즈니스 목적으로까지 널리 이용되고 있다. 이렇게 전자우편은 정보사회의 유용한 필수 통신 수단으로 자리 잡고 있다. 하지만, 이러한 전자우편의 유용성을 역이용하여 광고나 홍보메일 같은 이용자가 원하지 않는 메일을 무분별하게 전송하는 스팸메일(Spam E-mail)이 만연하고 있다. 이로 인해 개인의 프라이버시 침해가 심각한 문제가 되고, 인터넷 등 통신망의 이용질서를 무너뜨리는 사회적인 문제로까지 확산되고 있다. 이러한 스팸메일의 폐해가 심각하여 상업적으로, 제도적으로, 기술적으로 이에 대한 대책이 수립되고 있다[1].

본 논문에서는 스팸메일 차단 기법들을 고찰하고, 정보통신망 이용촉진 및 정보보호 등에 관한 법률시행규칙 중 개정령안인(제11조 제1항과 제2항 관련) 영리

목적의 광고성 전자우편 문구표시기준[2]을 토대로 이용자 수준에서 스팸메일을 차단할 수 있는 스팸메일 차단 시스템을 설계 및 구현한다.

본 논문의 구성은 다음과 같다. 2장에서는 세가지 측면에서 스팸메일 차단하는 기법을 설명한다. 3장에서는 이용자측면에서 스팸메일 차단 시스템의 설계현에 관하여 언급하고, 4장에서는 스팸메일 차단 시스템 구현 결과를 언급한다. 그리고 마지막으로 5장에서는 본 논문의 결론을 맺는다.

II. 관련연구

2.1 서버 레벨에서 차단 기법

표 1. 메일서비스 업체별 스팸방지 기술

구분	수신거부기능
다음	o 수신차단주소 지정 : 100개 o 특정 조건 필터링 : 발신자, 수신자, 참조, 제목 단어 등 o '스팸메일 걸러내기' 운영(필터링의 일종) - 내부기준 및 회원의 스팸신고를 바탕으로 스팸메일이라 판단된 메일이 수신될 경우 휴지통으로 이동 - 4단계의 스팸메일 걸러내기 수준 선택 가능 o '스팸신고'란 운영
야후	o 수신차단주소 지정 : 100개 o 특정 조건 필터링 : 발신자, 수신자, 참조, 제목 및 본문 단어 등 o '대량편지함' 운영(필터링의 일종) - 스팸 성격의 상업성 메일을 대량편지함으로 자동 분류 o 스팸담당자에게 스팸신고 가능
드림위즈	o 수신차단주소 지정 : 무제한 o 특정 조건 필터링 : 발신자, 수신자, 참조, 제목 및 본문 단어 등 o '스팸신고'란 운영
라이코스	o 특정 조건 필터링 : 발신자, 수신자, 제목 단어 등 o 고객센터에서 스팸신고 접수
코리아닷컴	o 수신차단주소 지정 : o 특정 조건 필터링 : 발신자, 수신자, 제목 및 본문 단어 등 o '스팸신고'란 운영
한미르	o 수신차단주소 지정 : 50개 o 고객센터에서 스팸신고 접수하나 특별한 조치를 취하지는 않음
MSN	o 수신차단주소 지정 : 250개 o 수신차단도메인 지정 : 250개 o 특정 조건 필터링 : 발신자, 수신자, 참조, 제목 단어 등 o '광고성 편지 차단' 실시(필터링의 일종) - '광고성 편지' 혹은 '스팸 메일'로 간주되는 편지를 받은 편지함이 아닌 광고성 편지함으로 보냄 - 3단계의 차단 수준 선택 가능 o 스팸담당자에게 스팸신고 가능

서버 레벨에서의 차단 기법은 현재 가장 많이 이용하고 있는 웹 메일 서비스업체 업체별로 스팸방지 기술을 알아보면 표 1과 같다.

표 1은 메일서비스 업체별 스팸방지 기술[4]을 표로 보여주고 있다.

표 1에서와 같이 웹 메일 서비스 업체에서 제공해주는 메일필터링은 서비스 업체별로 기본적으로 필터링 수준을 정하여 발신자, 수신자, 참조, 제목 및 본문 단어 등의 특정조건 필터링을 제공해주고, 이용자가 수신차단 주소나 도메인을 지정하여 이용자가 원하지 않는 메일을 차단할 수 있도록 하고 있음을 알 수 있다.

이처럼 서버에서 제공해주는 메일 필터링은 이용자가 서버가 제공해주는 필터링 수준을 설정하고, 받고 싶지 않은 메일을 차단할 수 있다고는 하지만 아직은 미흡한 면이 많고, 이용자가 매번 서버에 접속하여 차단되지 않은 메일에 대하여 차단을 해야 하는 불편함과 또 원하는 메일이 받아지지 않을 수 있는 문제가 발생할 수 있다.

2.2 네트워크구조 레벨에서 차단 기법

네트워크 보안을 위해 다양한 보안정책을 수행해 나가며 보안상 취약한 부분들을 수정함으로서 시스템의 보안 수준을 높이는 것은 중요하다. 이와 더불어 꼭 필요한 것이 바로 네트워크의 흐름을 제어할 수 있는 패킷필터링 이다.[5] 외부로부터 여러거지 침입방법에 대해 미연에 방지 하기 위해서는 외부 네트워크에서 내부 네트워크로 들어오는 패킷들에 대해 패킷 필터링을 적용할 수 있다. 패킷 필터링은 보안 정책에 따라 라우터와 방화벽[6]을 통해 구현할 수 있다.

우리는 여기서 악성스팸메일을 네트워크 구조레벨에서 차단할 수 있는 방법에 대해 알아본다.

그 방법은 메일 게이트웨이 서버를 사용하는 방법으로 메일서버가 여러대인 경우 하나의 메일서버로 메일을 집중시킨 후 다시 최종 메일 서버로 포워딩 하는 방식이 있다. 이 방식은 중앙 집중식 메일서버 S/W로 관리하고, 이메일 보안 버그 구멍을 단일화 시켜 그 효율성을 증대 시키는 장점을 가지고 있다. 이는 라우터의 패킷 필터링 기능을 이용하여 구현할 수 있다. 그림 1은 Sisco Router Extended Access-List를 적용한 메일게이트웨이 구성도를 보여주고 있다.

이 메일게이트웨이는 프락시를 이용하여 IP 주소 및 TCP포트를 이용하여 네트워크 접근제어를 할 수 있으며 추가적으로 사용자 인증 및 파일 전송시 바이러스 검색기능과 기타 부가적인 기능을 한다. 프락시 서버는 클라이언트와 서버 사이에 존재하며 그 접속을 관리하고, 이미 연결된 연결에 대해서 데이터 전달을 위한 전달자의 기능을 한다. 메일게이트웨이는 사용자

의 발신 IP를 확인하고 접근 규칙에 따라 내부서버로 접속허용 여부를 결정한다.

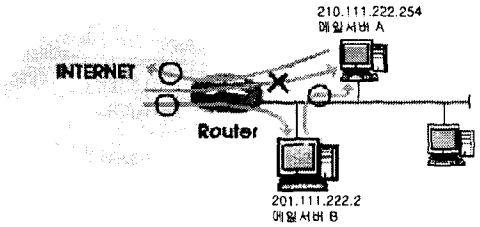

그림 1. 메일게이트웨이 구성도

2.3 클라이언트 레벨에서 차단 기법

그림 2는 대표적으로 많이 사용되고 있는 아웃룩 익스프레스(Outlook Express)에서 메일 필터링 기능을 보여준다.

그림 2에서처럼 아웃룩 익스프레스에서는 규칙의 조건을 선택하고, 규칙에 대한 동작들을 선택해서 POP3서버로부터 가져온 메일을 분류하고, 차단할 수가 있다. 규칙의 조건들은 여러 가지를 선택할 수가 있으며, 각 규칙조건에 대한 동작들을 선택해서 하나의 메일 규칙을 만든다. 이러한 메일규칙들은 여러 경우에 대하여 설정할 수가 있다.

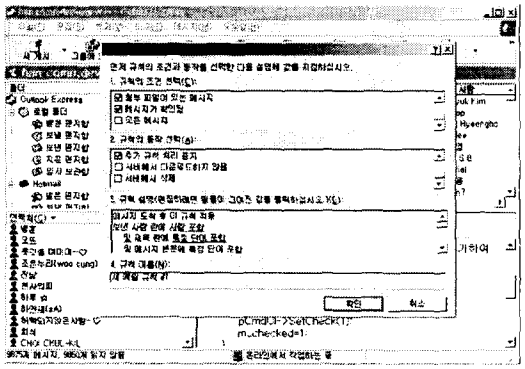

그림 2. Outlook Express에서의 메일규칙 설정

아웃룩 익스프레스 이외에 유도라, 네스케이프 메신저, 아웃룩2000등의 이메일 클라이언트 프로그램이 있으며, 이러한 프로그램들도 아웃룩 익스프레스와 인터페이스만 조금씩 다를 뿐 비슷한 기능들을 가지고 있었다. 이는 모두 웹 메일 서비스에서 제공해주는 필터링 기능들보다 좀더 구체적인 방법으로 메일을 필터링하고 있다. 발신자, 수신자, 제목, 본문 등에 특정단어나 패턴이 있는지 검사하여 수신, 회송, 삭제, 복사 등의 동작처리를 설정할 수 있도록 되어 있었다.

지금까지 우리가 원하지 않는 전자메일을 차단하는 방법들을 세 가지 측면에서 살펴보았다. 웹 메일 서비스에서의 메일 필터링은 아직 까지 미흡한 면이 많이 있었으며, 네트워크 구조레벨에서의 스팸메일 차단은 주 메일 서버로의 스팸메일 전달을 네트워크 레벨에서 차단해 버릴 수 있다는 강점을 가지고 있었지만, 메일에 대한 구체적인 분류 및 차단이 어렵다는 것을 알았다. 그리고 이메일 클라이언트를 이용한 메일 필터링에도 강력한 기능이 제공될 않는 등의 그 한계가 있음을 알았다.

III. 스팸메일 차단 시스템 설계

본 논문은 앞서 설명한 세 가지 방법의 스팸메일 차단 기법들을 통해서 한 가지 중요한 사실을 얻을 수 있었다. 서버차원에서 스팸메일을 필터링하는 방법 외에 이용자 수준에서 필터링 기법을 개발하여 스팸메일에 대한 피해를 줄일 필요가 있다는 것이다. 그래서 우리는 이메일 클라이언트인 Microsoft Outlook 2000을 기반으로 이용자가 POP3[7]서버로부터 가져온 메일을 분석하여 광고성 및 스팸메일을 분류하고 차단하는 프로그램을 설계하고, VB(Visual Basic 6.0) 응용프로그램 개발툴을 사용하여 구현하였다. [8, 9]

본 논문에서 구현한 스팸메일 차단 시스템을 설계하는데 가장 큰 주안점은 이용자 측면에서 복잡한 설정 없이 간단 조작으로 원하지 않는 전자메일을 차단할 수 있는데 두고 있다.

아웃룩 2000을 사용하는 이용자가 자체 필터링 규칙을 정의 하지 않고도 [그림3]과 같이 POP3서버를 통해 가져온 메일을 이메일 주소, 제목, 본문 내용을 검사하여 미리 정의해 놓은 필터링 규칙을 적용하여 메일을 분류 및 차단을 하고, 본문 내용 중 URL 정보를 검색하여 정보통신 윤리위원회 DB를 이용. 음란 및 유해 사이트 정보를 분석해서 우선적으로 필터링하고, 차단하게 된다.

적용한 필터링 규칙은 정보통신망 이용촉진 및 정보보호 등에 관한 법률시행 규칙 중 개정령안인(제11조 제1항과 제2항 관련) 영리목적의 광고성 전자우편 문구표시기준을 토대로 크게 두 가지로 분류하고 각각의 세부 규칙들을 정의하였다. 그리고 메일의 정의를 네 가지로 분류하였다.

기본적인 필터링 규칙은 "광고메일"과 "스팸메일" 두개로 분류를 하고, 네 가지 메일의 정의는 "일반메일", "일반광고", "홍보성 광고", "스팸메일"의 세부 분류를 둔다. 그렇게 해서 검사되는 메일은 스팸메일 차단 수준에 따라 메일을 필터링해서 "광고메일"과 "스팸메일"로 분류되어 차단하게 된다.

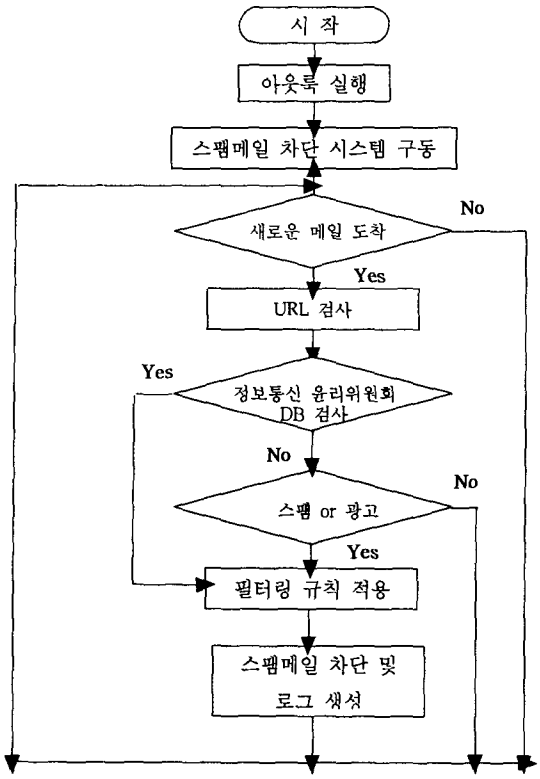

그림 3. 전체 프로그램 구성도

IV. 스팸메일 차단 시스템 구현

그림 4는 아웃룩 2000과 연동하여 동작하고 있는 스팸메일 차단 프로그램의 환경설정 화면을 보여주고 있다.

이 프로그램은 시스템 트레이에서 동작하며 아웃룩 2000의 받은 편지함에 새로운 메일이 도착시 시스템의 환경설정에 따라 스팸메일을 필터링하고 차단하게 된다.

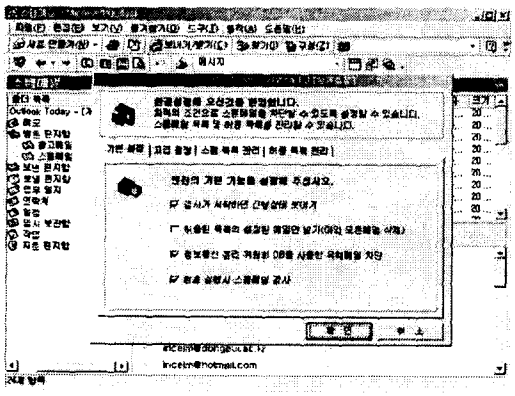

그림 4. 스팸메일 차단 시스템 구현

환경설정은 "기본설정", "고급설정", 스팸목록관리", "허용목록관리"로 나눠진다. "기본설정"에서는 엔진의 기본 기능을 설정해주고, 정보통신 윤리 위원회 DB를 사용여부를 결정해 줄 수 있다. "고급설정"에서는 스팸메일 차단 수준을 설정하고, "스팸목록관리"에서는 검사된 스팸목록을 관리하고, "허용목록관리"에서는 이용자가 허용하는 이메일 어드레스를 관리할 수 있다. 허용목록에 등록된 이메일에 대해서는 필터링과정을 거치지 않고 "받은 메일함"에 남아 있게 된다.

V. 결론 및 향후 연구방향

본 논문에서는 다양한 스팸메일 차단 기법들 중 이용자 중심의 이메일 클라이언트 차원에서 스팸메일을 차단하는 프로그램을 개발하였다. 클라이언트 차원에서 스팸메일을 차단하는 프로그램은 이미 몇몇 있지만 본 논문에서는 기존에 사용하고 있는 이메일 클라이언트 프로그램인 아웃룩 2000을 그대로 사용하면서 간단한 환경설정 만으로 이용자가 원하지 않는 메일을 차단할 수 있는 스팸메일 차단 프로그램을 개발한데 그 의의를 두고 있으며, 기존 프로그램과 차이점은 정보통신 윤리 위원회 DB를 사용하여 음란 및 유해메일을 URL 검사를 통해 차단하는 기능을 구현한 것이다.

본 논문에서는 아웃룩 2000과 연동되도록 구현하였지만, 향후 다양한 이메일 클라이언트 프로그램과 연동해서 동작하도록 기능을 추가할 예정이다. 그리고, 앞으로 좀더 편리하고, 쉽게 메일을 관리할 수 있는 또, 사용자가 원하지 않는 스팸메일에 강한 이메일 클라이언트를 개발할 예정이다.

참고문헌

[1] 정준우, "전자상업광고물인 스팸메일의 법적 문제점과 그 해결방안", 상업법연구 제19권 제2호, pp.311-356, 2000.

[2] [영리목적의 광고성 전자우편 문구표시기준] http://www.mic.go.kr

[3] 강영순, 이용백, 김태현, 조숙현, 맹성현, "전자우편 문서의 효율적인 분류를 위한 전 처리", 「한국정보과학회 봄 학술 발표논문집」 Vol. 29. No. 1 pp.493-495, 2002.

[4] [메일서비스업체별 스팸방지 기술] http://www.spamcop.or.kr/

[5] [네트워크 보안과 패킷필터링] http://www.plus.or.kr/Book/SecurityPLUS-2nd

[6] [방화벽]
http://kmh.yeungnam-c.ac.kr/Network/firewall/f1.html
[7] [이메일 파워 가이드]
http://kmh.yeungnam-c.ac.kr/subdoc3/mail_guide/index.html
[8] Gordon Padwick, Ken Slovak, 「Programming Microsoft® Outlook® 2000」, SAMS, 1999.
[9] Dwayne Gifford, 「Outlook 2000 VBA Programmer's Reference」, Wrox, 1999.