발송자와 수신측 MTA 간의 스팸메일 거부 에이전트 설계

정용진*
*호서대학교 벤처대학원 컴퓨터응용기술학과
e-mail:zephyranthes@empal.com

A Spammail denial Agent Design between sender and receiving MTA

Yong-Jin Chong*
**Application of Computer Technology, Graduate School of Venture, Hoseo University

요 약

누구나 제한없이 전자메일을 발송할 수 있는 특성 때문에 전자메일 사용자들은 스팸메일이라는 원하지 않는 메시지의 홍수에 노출되어 있고 이미 여러 가지 방법으로 스팸메일을 제한하려하고 있다. 본 논문에서는 기존에 방식에 추가로 적용이 가능한 수신측 MTA와 발송자 사이에서 발신 확인 과정을 통한 스팸메일 검증 에이전트를 구현 한다.

1. 서론

권위있는 닐슨미디어 리서치의 통계를 예로 든다면, 전 세계적으로 인터넷 사용자의 90% 이상이 전자우편을 사용하며, 미국 성인의 1/3이 전자우편을 사용한다는 예로 볼 때 메일시스템은 인터넷 서비스 중 가장 으뜸가는 서비스 중에 하나일 것이다.[1]

전자메일은 현대인의 필수 커뮤니케이션 수단으로 자리매김하고 있으며, 전자메일을 이용한 다양한 서비스가 가능하기 때문에 그 활용가치가 무궁무진하여 전자메일은 학술 연구용의 범위를 벗어나 기업과 일반 사용자들이 인터넷에서 사용하는 서비스 중 가장 중요한 서비스가 되었다.

하지만 누구나 제한 없이 전자메일을 발송할 수 있는 특징 때문에 원하지 않는 스팸메일이라는 메시지의 홍수에 노출되어 있다. 스팸메일이 사회문제로 등장한 것은 불과 2-3년 사이의 일이지만, 사회 전체에 미치는 영향력은 그 어떤 정보화역기능보다 크고 넓다. 이미 여러 가지 방법으로 스팸메일의 수신을 제한하려하고 있으나 지난 12월 한국정보보호진흥원이 네티즌 2천명을 대상으로 조사한 바에 따르면, 가장 피해를 입은 정보화 역기능으로 개인정보침해(32.7%)나 바이러스 피해(7.7%)보다 '스팸메일'(50.6%)을 꼽았다. 물론 단일 피해규모로는 개인정보침해나 바이러스 피해가 스팸메일로 인한 것보다 크겠지만, 스팸메일은 일상적이고 보다 대중적으로 발생하는 피해이기 때문에 더욱더 심각하다.[2]

전자메일에서는 수신자와 발송자가 명확히 구분되지 않고, 필요에 따라서 얼마든지 자유롭게 메일을 주고받을 수 있는 구조를 띄고 있다. 그리고 다른 보안체계에서는 공격의 특성이 명확하여 악의적 접근의 검출이 용이하지만, 스팸메일은 상대방이 요구하지 않은 메일을 대량 발송한다는 점을 제외하면 보통의 메일발송과 같은 특성을 갖기 때문에 검출이 용이하지 않다.

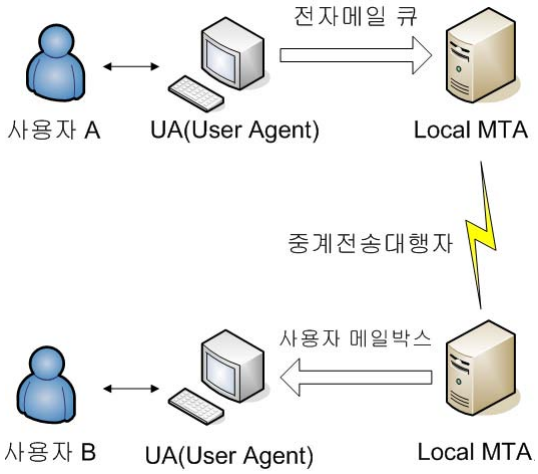
본 논문에서는 이러한 특성을 사용하여 기존에 스팸메일의 방어대책인 자동화를 통한 스팸메일을 검출해내는 시스템이 아닌 수신측 MTA와 발송자 사이에서 발신확인을 요구하는 에이전트를 설계하여 스팸메일에 대한 적극적인 방어대책을 수립한다.

2. 전자메일 시스템의 구조

전자메일 메시지는 봉투(envelope), 헤더(header),

본문(body)으로 구성된다. 봉투는 모든 수신자에게 공통으로 적용되는 정보로 구성된 메시지 필드와 각 수신자마다 달리 적용되는 정보로 구성된 수신자별 필드로 나누어진다. 헤더는 본문 형태를 정의한 정보로 구성되고, 본문은 음성, 영상, 텍스트 등의 다양한 데이터를 포함한다.

전자메일 시스템은 (그림1)과 같이 여러 개의 UA(User Agent)와 MTA(Mail Transfer Agent) 등으로 구성되며, 사용자 A가 사용자 B에게 메일을 전송하려 한다면 다음과 같은 과정을 거치게 된다.



(그림1) 인터넷 전자메일 시스템

1. 사용자 A는 UA(User Agent)에서 메일 메시지를 작성하여 Local MTA에 메시지를 전달한다.
2. Local MTA에 전달된 메일 메시지는 먼저 메일 큐에 저장된 후, 중계전송 대행자들을 거쳐 최종 목적지 MTA에 도달한다.
3. 사용자 B는 Local MTA의 수신된 메시지를 확인하고, 이 메시지를 사용자의 UA로 가져온다.

위와 같은 인터넷 전자메일 시스템은 메시지 전송에 있어서는 효율적이며 신뢰성은 있지만, 메시지의 불법, 누출, 불법 변조, 메시지 송·수신자의 신원조작 송수신 사실의 부인 등이 가능하며, 인터넷의 광범위한 특성상 송·수신자의 신원을 정확히 확인하기가 어렵다.[3]

3. 스팸메일의 현실

스팸메일이 심각한 사회적 문제로 대두되기 시작한 것은 불과 3-4년 정도밖에 되지 않았다. 초고속 인터넷망의 확산에 따른 인터넷 이용과 전자상거래의 급격한 성장과 함께 저 비용, 고 효율적 특성의 이메일광고가 마케팅 수단으로 각광을 받게 되자 IT·벤처붐으로 인해 많은 사람들이 전자상거래를 통한 e-Business 시장에 뛰어 들었으며, 초기자본이 많지 않은 소규모 사업자들에게 이메일 광고는 저렴하면서도 가장 효과적인 마케팅 수단으로 이용되어 스팸메일의 유통량은 매우 빠른 속도로 증가해 왔다.

그러나 이메일 광고가 무분별하고 무차별적으로 전송되고 특히 그 광고내용 자체가 불법적인 것들이 점차 증가함에 따라, 이제는 거의 모든 사람들이 스팸메일로 인한 피해를 호소하고 있으며, 이메일 마케팅 자체는 사람들로부터 외면을 당하고 있다.

IT 시장조사 전문기업인 IDC의 조사 자료에 의하면 전 세계적으로 하루 평균 약 54억 통, 연간으로는 총 1조9천6백억 통의 스팸메일이 유통되고 있으며, 또한, 페리스 리서치(Ferris Research)가 올해 초 발표한 조사 자료에 따르면, 지난해 스팸메일로 인한 미국의 피해는 89억 달러(약 10조8400억원), 유럽은 25억 달러(약 3조400억원)로 추산된다. 우리나라의 경우에도 한국정보보호진흥원에서 매년 실시하는 정보화 역기능 실태조사의 2002년 결과에 따르면 전자우편 계정 1개당 스팸메일 수신 개수는 평균 8.35개로 나타났다. 하루 평균 스팸메일 수신량을 계산해 보면 34.89개로 나타나고 있다. 이는 2001년 1일 평균 스팸메일 수신량인 4.66개에 비해 7.5배 정도가 늘어난 수치이다. 전자우편 전체 수신량이 5배 정도 늘어난 것을 감안할 때 전자우편 중 스팸메일 수신량이 증가하고 있음을 알 수 있다.

이를 1년 간 국내에 유통되는 총 스팸메일량으로 환산하면 대략 3천억 통 정도이며, IDC의 자료와 비교하게 되면 전 세계 스팸메일 유통량 중 한국이 15% 이상을 차지하고 있음을 알 수 있다.[2]

스팸메일은 전자우편 이용자에게는 많은 시간과 비용을 낭비하게 하며, 웹메일 서비스 업자에게는 인터넷 체증 가중 및 통신속도저하 등 유무형의 큰 피해를 야기하고 있다.[4]

4. 스팸메일 방어 대책 및 방안

스팸메일 방어 대책은 UA에서 특정 발송자나 키워드를 검색하여 메일 수신 여부를 결정하는 스팸메일 필터링과 수신측 MTA에서 스팸메일 릴레이(relay)에 이용되는 서버 목록을 수집하여 스팸메일

을 발송하는 서버로부터의 메일수신을 거부하는 메일서버 필터링이 있다.

스팸메일 필터링은 아웃룩 사용자는 「도구」의 메시지 규칙 등에 키워드를 입력하거나 스패머를 등록하여 스팸메일을 차단할 수 있으며, 웹메일 이용자는 웹메일 기능에 키워드를 등록하거나 스패머를 특정 편지함으로 이동시켜주는 메일 필터링 기능을 이용하여 차단할 수 있다.

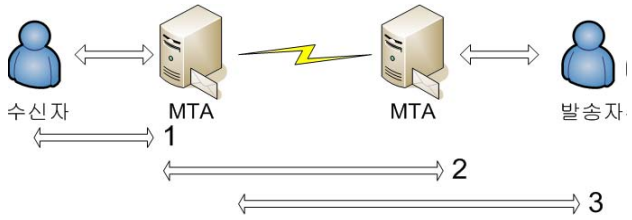
스팸메일서버 필터링은 메일서버관리자에 의해 상습적으로 이용되는 스팸메일 발송서버 리스트를 확보하여 추가하고, 수신량 통계와 사용자의 신고에 따른 추가로 꾸준히 수신거부목록을 관리한다.

또한 스팸메일 차단 소프트웨어를 이용하여 스팸메일을 차단할 수도 있다. 현재 국내에 다양한 기능을 가진 스팸메일 차단 소프트웨어가 출시 중에 있으며 정보 통신윤리위원회는 국내에 출시된 스팸메일 차단 소프트웨어 기능을 보완한 스팸메일 차단 소프트웨어를 개발하여 2003년 하반기에 전 국민을 대상으로 무료 보급하기도 되어있다.[5]

하지만 위에서 알아본 스팸메일 필터링의 경우 특정 키워드로 메일 수신을 거부할 경우 때때로 스팸메일이 아닌 수신메일도 걸러질 수 있는 문제가 있고, 스팸메일서버 필터링은 스팸메일 릴레이에 이용되는 서버목록은 일단 공격이 시작된 후에 발견할 수 있다는 점과 상대서버 관리자가 고의로 스팸메일 발송에 이용하지 않고 악의적으로 이용당했을 경우 상대방 서버가 스팸메일발송에 이용되지 않을 때 상대방 서버로부터의 메일을 수신하지 못하는 단점이 있다.

5. 스팸메일 방어대책에 대한 개선방안

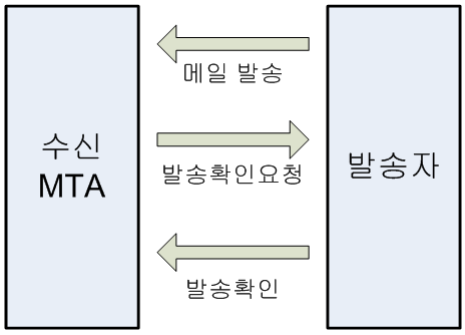
현재 스팸메일 방어 대책은 본래의 메시지에 책임을 져야하는 발송자는 제외하고 수신측 UA와 수신측 MTA, 수신측 MTA와 발송측 MTA사이에 한해서 이루어지고 있다. 이를 개선하여 본 논문에서는 (그림2)의 3번 항목에 해당하는 메일 수신시 수신측 MTA에서 발송자에게 확인 메시지를 보내 발송 메일의 성격을 질의할 수 있는 에이전트를 개발한다.



(그림2) 스팸메일 방어 대략도

이를 위하여 주어진 목표들을 달성할 수 있는 일련의 구체적인 행동(action)들과 그들의 실행 순서(order)를 자동으로 구해주는 계획기반 에이전트 시스템(plan-based agent system)을 설계한다.[6]

(그림3)과 같이 발송자로부터 서버 내 사용자에게 메일이 수신되었을 경우 수신측 MTA는 그 메일에 대한 발송확인을 요청하는 메일을 원 발송자에게 발송한다. 수신측 MTA에서 발송자에게 메일을 발송하면 발송자의 계정이 존재하는지, 메일 계정에서 거부되었는지 혹은 메일이 수신되었는지 여부를 알 수 있다. 이 점을 이용하면 가짜 메일 경로를 이용한 무차별적 대량 발송을 검출해낼 수 있다. 그리고 추가적으로 발송자가 메일 발송 확인에 응한 메일을 분류한다면 사용자에게 사용 편의를 제공할 수 있다. 더욱이 메일 수신자에게 수신허용목록을 작성하도록 유도하면, 발송측 메일 발송의 불편함도 감소하게 될 것이다.



(그림3) 수신측 MTA와 발송자간의 스팸메일검출

이 방법은 일반 전자메일 발송자가 항상 메일에 관한 확인메일에 대한 발송확인을 응해준다는 보장은 할 수 없기 때문에 수신 메일함과 별도로 한시적으로 메일을 보관하는 메일 저장 공간이 필수로 요구된다. 또한 이 방식은 기존의 메일서버간의 데이터 통신에 비해 최대 3·n의 네트워크 부하를 가져올 수 있다. 하지만 기존에 이용되고 있던 방식과 함께 적용하여 수신허용목록과 수신거부목록에 들어있는 발송자에게 확인과정을 거치지 않게 할 경우 어느 정도의 네트워크 부하의 감소가 가능하다.

6. 결론

현재 스팸메일이 네트워크 자원 소모와 전자메일 사용자에게 많은 시간적 수고를 끼치는 현실이지만

광고효과를 원하는 발송자에 의해 발송량이 줄어들지 않고 있다. 현재상황과 같이 수신측 MTA와 수신자들만 대책을 강구하는 경우 다른 보안항목과 마찬가지로 상호간에 기술이 발전하여 더욱 지능적이고, 공격적인 발송으로 진화할 확률이 높다.

또한 현재 스팸메일에 대한 보안 대책들은 정보침해나 바이러스 등 타 보안 대책들에 비교하여 기능과 효과 면에서 많이 부족하고 자동화를 강화할수록 잘못된 긍정(false positive)의 발생 확률이 높은 것이 사실이다. 이에 본 논문에서는 개인정보침해나 바이러스 피해 등과는 달리 발송자에게 발송확인을 요구해도 해킹의 범주에 포함되지 않는다는 전자메일시스템의 특성을 이용하여 수신측 MTA와 발송자 사이에서 스팸메일을 검증하는 에이전트를 설계하였다.

본 논문에서 설계한 발송자와 수신측 MTA간의 스팸메일 거부 에이전트는 서버에 새로운 에이전트 기능을 추가하여야하기 때문에 네트워크와 서버 측 시스템 사용량은 증가하게 되고, 발송과정에 확인이 필요하므로 기존의 방법보다 발송과정도 복잡해지는 단점이 존재 하지만, 특정한 암호화 기법이나 등록과정을 요구하지 않고 기존의 메일서비스와 연동이 가능하면서 신뢰성을 향상시킨 효율적인 전자메일서비스를 제공하는데 유용하게 사용될 수 있다.

참고문헌

[1] 김홍남 “리눅스에서의 메일 시스템” 정보처리학회지 제 6권 제 6호 1999.11.

[2] 주덕규 “스팸메일의 문제점 및 대책방안” 정보통신윤리 2003년 6월호

[3] 한국전산원 “2003년 한국인터넷 백서”, 한국전산원

[4] 우준, 하영국, 임신영, 이재광 “자바 기반의 배달 증명이 가능한 전자메일 시스템 구현“ 한국정보처리학회 논문지 제 6권 제 11호, 1999. 11.

[5] David Wood “Programming internet email“ O′Reilly

[6] 김인철 “계획 기반 에이전트 시스템“ 정보처리학회지 제4권 제 5호 1997. 9.