OTP를 이용한 스팸 메일 차단 모듈 설계

추연수° 이재식 김정재 조창현 전문석
숭실대학교
lets-priase@hanmail.net°, j30231@memoz.net,
argniss@empal.com, chjo@hist.co.kr, mjun@computing.ssu.ac.kr

Design of Module for Spam Mail Blocking with OTP(One Time Password)

Yeoun-Soo Choo°, Jae-Sik Lee,
Jung-Jae Kim, Chang-Hyun Cho, Moon-Seog Jun
Soong - Sil University

요 약

인터넷 사용의 증가로 많은 사람들이 기존의 편지나 업서를 사용하던 것을 전자 메일(e-mail)로 대체하고 있다. 전자 메일은 텍스트뿐만 아니라 그림, 음성, 동영상까지 전송이 가능하며 필요한 문서들도 첨부가 가능하여 많은 사람들에게 호응을 얻고 있지만 광고 메일이나 음란 사이트 홍보 메일로 사용되면서 많은 전자 메일 사용자들에게 정신적 피해를 주고 있으며 메일링 서비스를 하고 있는 업체들에게 큰 유해를 끼치고 있다. 본 논문에서는 사용자가 요구하지 않은 광고성 스팸 메일을 OTP(One Time Password)를 이용하여 효과적으로 차단하는 모듈을 제안, 설계한다. 기존의 차단 방식은 메일 서버에 저장된 메일들을 삭제하는 방식으로 메일 서버에 많은 과부하를 주며 메일 서버의 저장 용량을 낭비하여 사용자로 하여금 꼭 필요한 메일들을 송, 수신 하지 못할 수도 있었다. 본 논문에서 제안하는 시스템은 스팸 메일로 분류된 메일들을 메일 서버 자체에 저장하지 않는 방식을 사용하여서 기존의 문제점을 해결하였다.

1. 서 론

인터넷의 사용의 비중이 늘어나면서 전자 메일(e-mail)의 사용이 기하급수적으로 늘어나고 있다. e-mail은 사용자의 요구에 따라 텍스트뿐만 아니라 소리와 그림 등과 같은 멀티미디어적인 요소를 전달할 수 있는 기능이 추가되어 서비스 되고 있다. 이러한 서비스는 기존의 e-mail 유저에게 보다 다이나믹한 환경을 제공함으로서 많은 호응을 얻었고 상업적인 목적으로 많이 사용되어 기존의 예상하지 못했던 문제점을 낳고 있다.

여러 가지 문제점이 있겠지만 스팸 메일을 통해 메일 서버의 큰 부하로 인한 메일 서비스 장애 및 인터넷 대역폭 낭비와 개인 저장 용량의 오버플로워로 인한 필요한 메일 미수신과 원하지 않은 성인 광고 메일 수신으로 인한 정신적 피해를 입는 문제가 가장 심각하다고 할 수 있겠다.

본 논문에서는 이러한 스팸 메일에 대한 문제를 해결하고자 OTP를 이용한 스팸 메일 차단 시스템을 제안 설계한다. 본 논문에서 제안한 스팸 메일 차단 모듈은 송신자가 수신자에게 메일을 전달하기 위해서는 수신자의 메일 서버로부터 인증 번호를 부여 받아야 하며 인증 번호를 가지고 있지 않은 메시지는 수신자의 메일 서버에서 차단하는 메커니즘을 가짐으로서 스팸 메일을 차단하는 기능을 한다.

본 논문의 구성은 2장에서 스팸 메일 차단 기술에 대해서 기술하고 3장에서는 제안하는 스팸 메일 차단 메커니즘과 모듈, 메일 클라이언트에 대해 기술하며 4장에서는 결론과 향후 연구 방향을 제시한다.

2. 관련연구

2.1 스팸 메일 차단 기술

2.1.1 특정 조건에 대한 필터링

이 방식은 수신자의 메일 클라이언트에서 설정된 조건을 만족하는 메일만 수신하는 방식이다. 수신자의 메일 클라이언트는 다음과 같은 조건들을 필터링 조건으로 설정할 수 있다.

1. 특정한 IP
2. 특정한 메일 주소
3. 특정한 텍스트가 포함된 메일 제목
4. 특정한 텍스트가 포함된 메일 내용
5. 특정한 색이 많이 사용된 그림을 포함한 메일

위와 같은 조건들은 사용자가 메일 클라이언트에서 설정할 수 있으며 메일 클라이언트에서 위와 같은 기능을 지원하여야 한다.[1]

2.1.2 Opt-in 방식

불특정 대다수에게 무작위로 보내지는 스팸 메일을 규제하는 방식 중 Opt-in 방식은 수신자의 사전 동의를 얻어야 메일을 발송할 수 있도록 하는 방식을 말한다.

Opt-in 방식은 이용자의 권리를 중시하는 방식으로 광고 메일등의 스팸 메일을 보낼 때는 반드시 사전에 수신자의 동의를 구해야한다.[2]

2.2 OTP(One Time Password)

일회성 패스워드(OTP)는 사용자 인증이 필요한 곳에서 한번 사용한 후 폐기하는 패스워드이다. OTP는 Challenge Number를 생성하는 시기에 따라 Challenge-Response 방식과 Time Synchronous 방식이 있다.

Challenge-Response 방식은 사용자가 Log-in을 하면 서버는 사용자에게 Challenge Message를 전송하고 사용자는 PIN과 메시지를 이용하여 OPT를 생성, 서버로 인증 요청을 받는 메커니즘이다.

Time Synchronous 방식은 난수 생성 알고리즘을 통해 일정한 시간마다 난수를 발생시키고 사용자가 Log-in할 때, 서버에서 발생된 난수 값과 사용자가 가진 난수 값이 일치하는지의 여부를 통해 승인을 하는 메커니즘이다.[3]

3. 제안하는 OTP를 이용한 스팸 차단 모듈

본 논문에서는 스팸 메일을 차단하기 위해서 기존의 메일 서버에 스팸메일 차단 모듈을 추가하여 스팸 메일을 차단하는 시스템을 설계한다. 기존의 대부분의 스팸 메일 차단 시스템들은 메일 서버에서 모든 메일들을 일단 수신한 후 수신자가 자신에게 필요하지 않는 메일을 스팸 메일로 분류하여 스팸 메일을 차단하거나 메일 클라이언트에서 수신자의 메일 수신 패턴을 학습하여 수신자가 수신하는 메일 패턴에서 벗어나는 메일들을 스팸메일로 분류하여 스팸 메일을 차단하는 방식을 취하고 있다.

하지만 본 논문에서 제안하는 스팸 메일 차단 시스템은 OTP를 메일 서버에서 생성하여 송신자를 인증하고 이 인증을 거친 메일만 메일서버에 저장하기 때문에 상당히 많은 양의 저장 공간을 낭비하지 않을 수 있다. 기존의 스팸 메일 차단 서비스는 수신자의 메일 서버에 상당히 많은 양의 메일이 저장되기 때문에 낭비되는 저장 공간이 상당히 많았다. 본 시스템은 스팸 메일 차단과 더불어 메일 서버의 저장 공간을 효율적으로 사용할 수 있는 장점이 있다.

3.1 스팸 메일 차단 메커니즘

제안하는 스팸 메일 차단 모듈의 동작 메커니즘은 그림 1 과 같다. 송신자가 수신자에게 메일을 송신하기 위해 메일 클라이언트를 열어 수신자 메일 서버에 송신 요청을 하면 수신자의 메일 서버는 OTP를 생성한 후 송신 요청을 한 송신자에게 OTP를 인터넷을 통해 전송한다. 이 때 수신자의 메일 서버는 수신자에게 OTP를 전송함과 동시에 Time Count를 시작한다. 메일 서버에서 생성된 OTP는 180초 동안만 유효하다. 송신자의 메일 클라이언트는 추가된 SMTP Header 필드에 전송받은 OTP를 삽입하여 송신자의 메시지 내용과 함께 SMTP 프로토콜을 이용하여 수신자의 메일 서버로 보낸다.

수신자의 메일 서버에서는 전송된 SMTP Header 필드의 OTP를 추출한 후 스팸 메일 차단 모듈의 생성 OTP List에 저장된 OTP와 비교하여 유효성 여부를 확인한다. 송신자가 보내온 메시지의 OTP가 유효하면 메일 서버는 해당 수신자의 메일 저장 공간에 저장하고 해당 OTP가 유효하지 않으면 스팸 메일 차단 모듈은 송신된 메일을 삭제하며 송신자에게 OTP 시간초과 오류 메시지를 전송한다. 한번 사용된 OTP는 OTP 생성 List에서 Time Count와 함께 삭제된다.

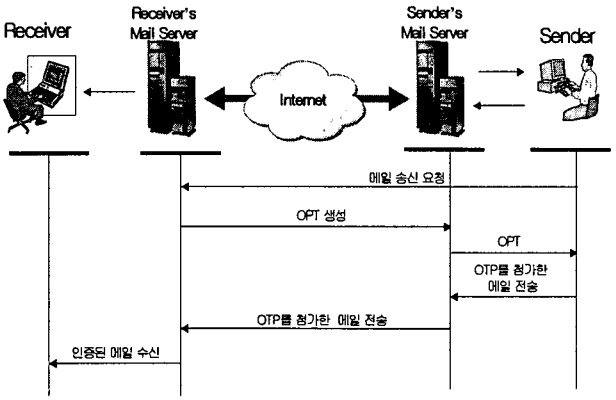

그림 1 제안하는 스팸 메일 차단 메커니즘

3.2 제안하는 SMTP Header 필드

SMTP(Simple Mail Transfer Protocol)는 전자 메일을 보낼 수 있는 TCP/IP 프로토콜이다. SMTP에 미리 정의된 필드는 Sender, From, Subject, Body, Replyto 등으로 구성되어 있어서 이것들이 메일의 주요한 내용과 구성을 이룬다. 본 논문에서는 기존의 SMTP의 Header 필드에 8바이트의 인증 필드를 추가하여 수신자 메일 서버에서 생성하여 송신자에게 전달되는 인증을 위한 OTP를 전송하기 위한 필드로 사용한다. 인증번호 역할을 하는 OTP는 송신자가 보낸 메일 송신 요청 메시지의 답으로 송신자의 메일 클라이언트의 인증번호 필드에 자동 삽입된다.

3.3 스팸 메일 차단 모듈과 메일 클라이언트

3.3.1 스팸 메일 차단 모듈

스팸 메일 차단 모듈의 구성은 그림 2와 같다. 이 모듈은 여러 개의 조그마한 모듈들로 구성되어 있으며 구성하고 있는 모듈들로는 OTP 생성모듈, Time Counter 모듈, 유효성 검사 모듈들이 있으며 그 외에 생성된 OTP를 저장하는 OTP List와 SMTP를 이용하여 송신자에게로 OTP를 보내고 받기 위한 Interface가 스팸 메일 차단 모듈을 구성하고 있다.

- OTP 생성 모듈 : 송신자의 메일 송신 요청이 있을 시 OTP를 생성하여 인터페이스를 통해 송신자에게 전달한다. OTP를 송신자에게 전달하기 시작할 때 해당 OTP에 대한 Time Counter를 시작하도록 메시지를 Time Counter 모듈에게 전달한 후 생성된 OTP를 모듈 내에 있는 OTP List에 저장한다.
- Time Counter 모듈 : OTP 생성 모듈에서 송신자에게 OTP를 전송한다는 메시지를 송신하면 해당 OTP의 Counter를 시작한다. OTP에 대한 Counter가 Time out 되면 OTP List로 해당 OTP 삭제 메시지를 전송한다.

· 유효성 검사 모듈 : 유효성 검사 모듈은 인터페이스를 통해 들어온 OTP와 OTP 생성 모듈에서 생성되어 OTP List에 저장된 OTP와 비교하여 정상적인 OTP인지 판단한다. 정상적인 OTP를 가진 메일은 서버에 저장되고 그렇지 않으면 삭제한다.

스팸 메일 차단 모듈은 수신자의 메일 서버에 삽입되어 작동하며 수신자 메일 서버가 수신된 메일을 저장하기 전에 OTP를 확인하여 메일을 수신할 지 여부를 결정한다.

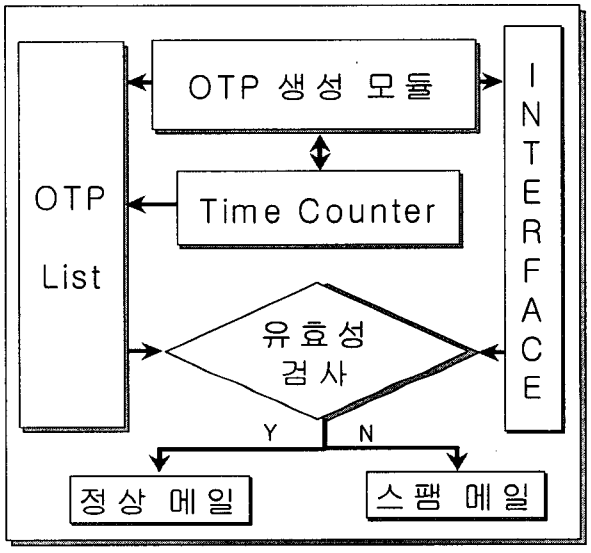

그림 2 스팸 메일 차단 모듈 구조

3.3.2 메일 클라이언트

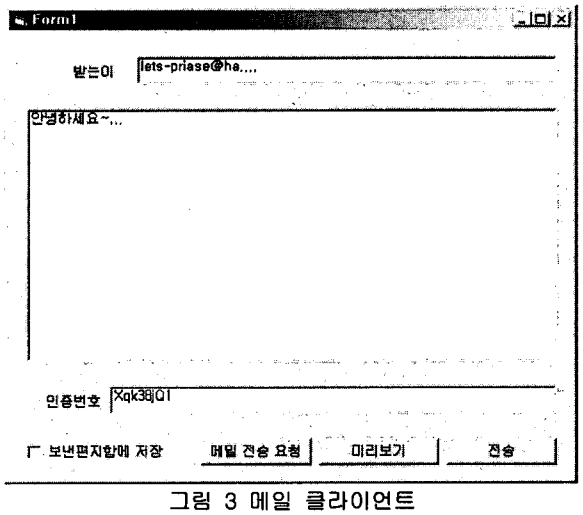

그림 3 메일 클라이언트

수신자의 메일 서버에서 보내온 OTP는 그림 3 과 같이 인증번호 기입란에 자동 삽입되며 인증번호를 첨부한 후 보내고자 하는 메시지를 입력한 후 수신자에게 메일을 전송한다. 이 때 송신자는 인증번호를 부여 수신한지 180초 안에 메일을 전송해야 한다. 그렇지 않으면 OTP Time Counter가 Time Out 되어 전송받은 OTP는 사용할 수 없게 되고 다시 발급 받아야 한다. 메일을 송신자에게 전송하기 위해서는 수신자의 메일 서버에서 OTP를 받아야 하기 때문에 불특정 다수에게 메일을 전송되는 스팸 메일의 경우 상당한 작업 양을 거쳐야만 한다.

4.결론 및 향후 연구 방향

본 논문에서는 스팸 메일은 메일 서버 자체에 저장 조차 되지 않는 OTP를 이용한 스팸 메일 차단 모듈을 설계하였다. 본 논문에서 제안한 스팸 메일 차단 모듈은 기존의 스팸 메일 차단 방식과 달리 스팸 메일은 메일 서버에 저장되지 않기 때문에 개인 메일 저장 공간의 용량이 스팸 메일로 인해 낭비되는 것을 방지할 수 있어 개인 저장 용량 부족으로 꼭 필요한 메일을 전송 받지 못하는 경우를 효과적으로 방지할 수 있다. 또한 매번 랜덤하게 바뀌는 OTP 인증 번호를 사용하여 한번 인증을 받고 그 인증 받은 것으로 스팸 메일을 전송하는 방법을 막을 수 있는 장점이 있다.

하지만 본 논문에서는 수신자가 선택적으로 가입하여 활동하고 있는 인터넷 커뮤니티나 속한 기관의 공지사항을 위한 메일도 스팸 메일로 분류되어 차단되는 경우가 생길 수 있으므로 이 부분에 대한 연구가 더욱 이루어져야 하며 OTP를 보다 효과적으로 송신자에게 전달할 수 있는 방법이 연구되어야 할 것이다.

참 고 문 헌

[1] 정옥란, 조동섭, "개인화된 분류를 위한 웹 메일 필터일 에이전트", 정보처리학회, 논문지 B, 제10-B권 제 7호, 2003.

[2] 백수현 "공인인증을 이용한 Spam Mail 대처방안에 관한 연구",숭실대학교, 2004

[3] N. Haller, "A One Time Password System", Bellcore, RFC2289, 1998.

[4] 추연수, 김정재, 전문석, "라이선스 보호를 위한 유, 무선 디바이스와 Agent 기반의 DRM 시스템 설계", 정보처리학회 춘계학술대회 논문집 12권 11호, 2005.

[5] Jonathan B. Postel, "Simple Mail Transfer Protocol", Information Sciences Institute University of Southern California, RFC821, 1982.

[6] 김성찬, 이상훈, 전문석, "정크메일 차단을 위한 FQDN 확인 시스템의 구현 및 평가", 한국정보처리학회, VOL·12-C NO 03, pp.361 ~ pp.368, 2005.

[7] G. Lindberg, "Anti-Spam Recommendations for SMTP MAT's" Chalmers University of Technology, RFC2505, 2000.