제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

PGP 기반의 스팸메일 검출 및 차단 시스템

최홍식[0], 김중환, 김상철
한국외국어대학교 컴퓨터 공학과 멀티미디어 정보통신 연구실
hufs_sniper@hotmail.com, jhkim@hufs.ac.kr, kimsa@maincc.hufs.ac.kr

Spam-mail detection and interception system of PGP base

Hong-Sik Choi °, Joong-Hwan Kim, Sang-Chul Kim
Dept. of Computer Science & Engineering, Hankuk University of Foreign Studies

요 약

요즘 전자우편(E-mail) 서비스를 사용하게 되면서, 스팸 메일이라고 불리 우는 광고성 메일이 무분별하게 전자우편에 침입하고 있다. 요즘과 같이 정보의 중요성과 개인의 사생활이 강조되는 시점에서 다른 사람이 중간에 메일을 가로채어 읽거나 해킹 하여 전혀 다른 내용으로 바꾸어 배포하거나 바뀐 내용을 전송하거나 ,과도한 스팸메일 때문에 자신의 메일 계정에 부하가 걸려서 중요한 메일을 못 받게 된다면 보통 심각한 일이 아닐 수 없다. 본 논문에서는 이것을 해결하기 위하여, PGP(Pretty Good Privacy) 라는 기술과 문자열 처리를 이용하여 전자우편의 보안성 향상과 문자열 처리를 통해 스팸 메일을 줄이는 방법을 제안한다.

1. 서 론

전자우편(E-Mail) 서비스는 매우 편리한 통신수단이지만 무분별한 스팸메일이 침입할 수 있고, 봉투에 넣어져 보내지는 일반적인 편지와는 달리 엽서처럼 내용까지도 그대로 보이는 구조를 지니고 있기 때문에 중간에서 다른 사람이 얼마든지 가로채고 또 변조할 수가 있는 단점이 있다. 따라서 전자우편의 신뢰성을 향상시키기 위해서는 메일이 출발지로부터 인터넷 기반의 네트웍 환경에서 무수히 많은 호스트들을 거쳐 목적지까지 도달하는 동안 보안성이 유지되고, 수신자가 신뢰성이 인증된 메일만 구분하여 수신하는 방안이 필요하다. 그리고 신뢰성이 인증되지 않은 메일은 자동으로 구분하여 별도의 인증 절차에 의해 처리되어야 한다. 지금까지 전자우편의 신뢰성 향상은 주로 보안도구인 PGP (Preety Good Privacy)와 PEM (Privacy Enhanced Mail)을 이용하여 메일의 내용을 암호화하는 방법으로 연구되고 있다. 특히 PGP는 특정한 키가 있어야 메일의 내용을 볼 수 있도록 되어 있기 때문에 기밀성, 인증, 전자서명, 압축 등의 기능을 지원하는 편리한 보안도구이다.[1,2] 또한 스팸메일의 차단은 수신거부와 필터링 기능을 활용하는 방법, 강력한 경고문을 계속 발송하는 방법, 스팸메일 전담용 메일을 만드는 방법 등이 많이 이용되고 있다. PGP는 기능적인 면과 공개된 기술로서 쉽게 이용 가능

하다는 이점이 있어서 본 논문에서는 이것을 이용한 인증서버를 구축하여 발신자와 수신자 사이에 규정된 방법으로 신뢰성이 인증된 메일만 수신하고, 인증되지 않은
메일은 불량 단어리스트에 의해 메일의 제목 및 내용의 문자열을 분석하여 자동으로 스팸메일을 구분하여 차단하게된다. 또한 개발된 시스템에서는 메일의 내용을 암호화하기 때문에 메일의 보안성도 향상시킨다. 우리의 조사에 의하면, 보안성 향상을 위한 PGP 기반으로 한 스팸메일 차단 시스템의 기존 연구에 대한 발표가 거의 존재하지 않았다.

2. 관련 연구

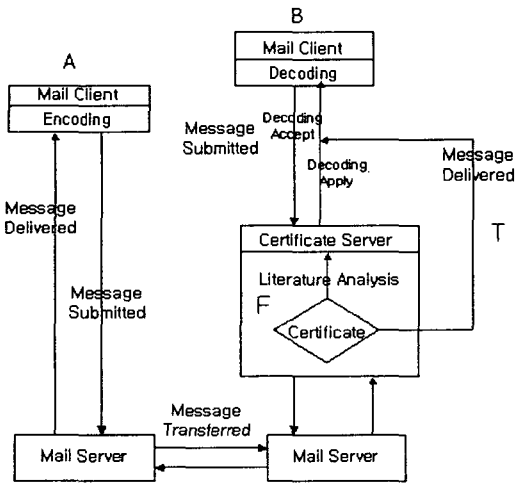
2.1 기존 연구

스팸 메일은 참으로 다양하고, 제목도 기상천외하다. 어쩔 땐 기발한 문구를 접하고 감탄하기도 하고 어떻게 메일 주소를 알고 보내는 지 신기할 따름이다.
그래서 제안된 것이 발송자가 수신자의 사전동의를 얻어야 메일을 발송할 수 있는 '옵트인(opt-in)' 방식과 수신자가 발송자 측에 수신거부의사를 접수시킨 후에야 발송자의 메일발송을 규제하는 '옵트아웃(opt-out)' 방식에 대한 논란이 대다수를 차지하고 있

다. '옵트인(opt-in)' 방식을 선호하는 쪽은 대부분 메일을 업무용이나, 개인적인 필요에 의해 사용하는 사람들일 것이고, '옵트아웃(opt-out)'을 선호하는 사람들은 마케팅이나 광고를 해야 생존할 수 있는 이유를 가진 사람들일 것이다.[3] 하지만, 우리가 조사에 의하면, '옵트인(opt-in)' 방식에 따른 스팸메일 방지에 대한 연구는 미흡하다. 따라서 우리는 이 '옵트인(opt-in)' 방식에 대한 연구를 주제로 한다. 이외의 기존의 스팸메일 제거 방식은 무조건 한번은 받은 후에 스팸메일이면 송신인 메일 주소를 통해서 수신거부를 하는 방식이나, 아웃룩처럼 차단할 단어를 직접입력해서 그 단어가 포함된 메일을 삭제하는 방식이 있고, 나라 비전의 "메일스파이더" 라는 프로그램은 IP·도메인 주소·키워드·발송시간으로 필터링을 하기도 한다. 하지만 우리의 조사에 따르면, PGP 기반의 기존의 다른 방법은 찾지 못하였다.

2.2 스팸메일 차단 처리구조

본 연구에서 개발된 시스템은 스팸메일을 차단하기 위하여 인증 처리 과정과 인증되지 않은 메일의 문자열을 분석하는 과정으로 이루어져 있다. 기존의 스팸메일 제거 시스템의 경우, 자신이 불량 단어에 대하여 정의를 해야하지만, 문자열 분석 시에는 사용자가 직접 필터링에 넣을 단어들을 입력하지 않아도 불량 단어리스트에 의해 필터링을 하고, 인증 과정은 [그림 1]과 같이 기존의 메일 서버와 사용자 각각의 계정인 클라이언트 사이에 또 하나의 인증된 메일만을 수신할 수 있게 하는 서버를 구축하여 처리한다.



[그림 1] 스팸메일 차단 처리구조

인증서버에는 인증 기능과 문자열 분석기능이 있다. [그림 1]에서 송신인 메일 클라이언트 A가 수신인 메일 클라이언트 B에게 메일을 보냈을 경우 수신인 B가 송신인 A에게 첫 번째 메일을 받은 후 그것이 스팸메일이 아니라고 했을 때 인증키를 주어서 다음부터 수신인 B가 송신인 A에게 메일을 보낼 경우는 인증서버에서 문자열 분석의 단계는 거치지 않고 바로 송신인 A에게 갈 수 있게 한다. 여기서 언급되는 인증서버 부분이 스팸메일 제거를' 위해 우리가 넣은 부분으로 PGP의 인증 기능을 이용한 부분이며, 처음 메일을 보낼 경우는 인증 서버에서는 문자열 분석을 하기 위해서 Encoding 된 메일을 수신인에게 Decoding을 요구하고, 수신자는 이것을 받아들여서 Decoding 된 메일의 내용을 가지고 문자열 분석을 하게 된다. 문자열 분석을 거친 후 송신인 A에게 전달이 되기 때문에 처음에 오는 메일이라도 스팸메일이 오는 것을 막을 수 있다. 문자열 분석은 메일의 제목 및 내용을 불량 단어리스트에 의해 자동 필터링 하는 방법을 사용한다.

2.3 문자열 분석 과정

스팸메일 차단시스템의 핵심 기능 중 하나인 문자열 분석은 불량 단어리스트에 의한 필터링으로 이루어진다. 본인의 메일 계정에 들어오는 200개의 메일을 분석한 결과 65% 정도인 126개가 스팸메일이었다. 그 중에서 "광고" 라는 문구가 메일 제목에 포함 된 스팸메일은 전체에 63% 정도를 차지하였고, 나머지 37%는 명시하지 않았다. 따라서 개발된 시스템에서는 먼저 메일 제목을 검색해서 "광고"라는 문구가 있는지 검사하고 없다면 메일 내용을 검토해서 미리 작성되어진 불량 단어리스트와 비교하여 스팸메일인가 아닌가를 구분하게 된다.

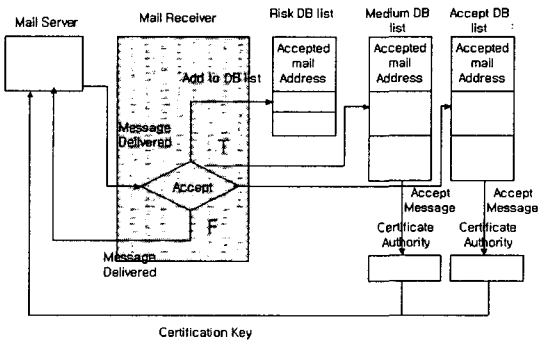
그러나 전체 메일내용을 일일이 검색하면 처리시간이 길어져 효율성이 떨어지게 된다. 이와 같은 단점을 해결하기 위해 본 연구에서는 스팸메일을 구분하는데 불필요한 조사와 불용어를 제거하고 핵심 단어만을 추출하는 전처리 과정을 두었다. 불필요한 조사는 "은","는","이","가" 등이 있고 불용어란 "이다", "했습니다", "대한", "상관" 등 제거를 해도 문장을 이해하는데 크게 어려움이 없는 것들이다. 이것들을 제거함으로써 핵심 단어들만이 남게 되며, 이 핵심문구를 불량 단어리스트에 있는 단어들과 비교하여 검색한다.

위의 처리 과정을 거쳐서 핵심 단어들을 추출하는 것을 간단한 예로 살펴보면 메일의 내용 안에 "이 상품은 밤에 사용하는 것입니다." 이란 내용이 있다면, 처리 결과는 "상품", "밤", "사용" 만 남게 된다. 그러면 이 결과에서는 불량 단어리스트에 상품, 밤이 들어가 있어 스팸 메일로 구분되고 송신자에게 리턴 메일을

보낸다. 여기서 중요한 건 불량 단어 리스트일 것이다. 불량 단어 리스트는 본인과 본인의 친구들 메일 계정에 온 스팸메일에 포함된 문자들을 분석하여서 작성하게 되었고 예를 들어 "[광고]","!!!", "성인" 이런 것들을 비롯한 약 500 여 개의 단어들이 있다. 여기서 문제점은 메일 보내는 사람에 따라서 같은 단어도 스팸 메일일 수 도 있고, 아닐 수도 있는 다는 것이다. 그 것에 대한 해결책은 추후 단어뿐만 아니라 문단 자체의 분석과 송신인 메일 주소 통하여 해결이 될 수 있다.

2.3 신뢰성 인증 과정

메일의 신뢰성 인증 과정은 [그림 2]와 같으며 송신자가 처음 메일을 보낸 메일을 받았을 경우에 스팸메일이 아니라면 다음 메일부터 스팸메일이 아님을 인증하는 방식이다. 즉, 수신인은 송신인이 처음 보낸 메일이 스팸메일이 아니고 계속 받고 싶을 때는 송신인의 메일 주소를 Accept DataBase list 에 저장하고, 스팸메일일 경우에는 Risk DataBase list 에 저장을 해서, 다시는 수신이 되지 못하도록 하며, 확실히 알 수 없을 경우 Medium DataBase list 에 저장을 하여, 문자열 분석을 통해서, 수신이 되도록 한다. 정리하여 말을 하면, 스팸메일이라고 판단되는 것은 Risk DataBase에 송신인의 메일주소를 추가하고 인증키를 보내지 않고, Medium DataBase에 추가된 것은 문자열 검색을 거쳐서 읽게 되고 Accept DataBase 에 추가 된 것은 문자열 검색과정을 거치지 않고 바로 수신인에게 전달이 되게 되는 것이다. 그 결과를 인증기에 통보하고 인증기는 송신인에게 인증키를 주게 된다. 송신인은 인증키를 수신하게 되어 다음부터는 동일한 수신인에게 메일을 보낼 때는 아무 제약 없이 바로 수신인이 신뢰하는 메일을 볼 수 있게 한다.



[그림 2] 신뢰성 인증과정

위의 [그림2]는 메일 서버에서 메일을 받았을 때의 처리에 대한 그림으로써 메일 리시버에서 받아들이면, 다음 수행의 처리를 위해서 송신인의 메일 주소를 저장하게 되는데, 불량 단어 정도에 따라서 아주 불량하면 Risk list에, 받아 들일정도(불량 단어율 20% 미만)면 Medium list 에, 신용이 가능 정도면 Accept list 에 송신인의 메일 주소를 저장하고, Medium 나 Accept list 는 메일 주소를 저장한 후 인증 권한을 메일 서버에 주게 된다.

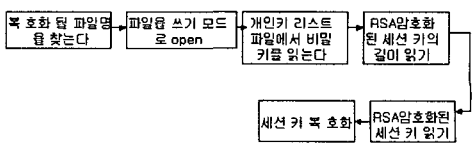
인증기가 생성하는 인증키는 개인키를 이용하여 수행한다. 파일을 개인키로 인증하여 인증 파일을 넘겨준다. 인증의 확인은 송신자의 인증이라는 것을 모두가 알 수 있는 송신자의 공개키를 적용함으로써 알 수 있다. 송신자의 메일 주소로 송신자의 공개키를 얻어서 송신자의 개인키로 인증된 것을 풀고 인증을 확인한다. 인증이 틀릴 경우는 송신자가 인증된 메일 계정에서 보내지 않은 경우이거나 처음 보내는 송신자일 경우이다. 또한 한번 인증된 메일 계정은 다음 단계인 문자열 분석을 거치지 않고 바로 수신자에게 전달이 된다.

2.4 구현

본 시스템은 Visual C++ 6.0을 사용하여 WinNT(P3 550Mhz, 256M), Win98(P4 1Ghz, 128M)환경에서 구현 되었으며, 인증과 메일의 안전을 위해서 PGP를 사용하였다. PGP의 구현에 있어서 자료를 암호화할 때는 비밀키 방식인 IDEA(International Data Encryption Algorithm), Session 키 암호화할 때는 공개키 방식인 RSA(Rivest Shamir Adleman)를 사용한다.[2]

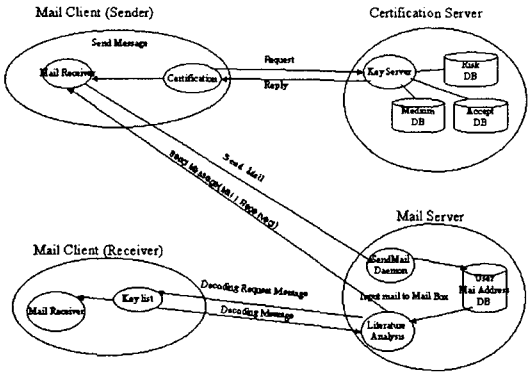
먼저 키 생성을 하게 되는데, 공개키와 개인키로 나누어 생성하고 그 키 값을 저장하게 된다. 이것이 하나의 인증키가 되는 것이다.

암호화는 수신인의 공개키를 이용하게 되는데, 이때 암호화하는 방식은 상대편 메일 주소를 이용해서 공개키 파일 리스트에서 상대편 공개키를 찾은 후 두 번째 인자의 파일을 찾은 상대편 공개키로 암호화한 후 첫 번째 인자에 암호화한 파일명을 넘겨주는 방식이다. 암호화된 파일은 수신자의 개인키를 이용하여 복호화를 하는데, 암호화된 파일을 DES(Data Encryption Standard) 알고리즘으로 복호화하고, 암호화된 세션키를 개인키로 복호화해서 넘겨준다.[4],[5]



[그림3] 복호화 순서

다음 [그림 4]는 개발한 시스템의 구조를 나타내고 있다.



[그림4] 시스템 구조

3. 실험

우리의 조사에 의하면, 지금까지의 메일 서버들은 스팸메일 차단 기능이 제공되기는 하나, 스팸 메일에 대한 기준이 뚜렷하지 않으며 단지 걸러내기 설정은 낮음, 중간, 높음으로 사용자가 설정하게 되어있다. 본 실험은 개발된 시스템의 성능을 알아보기 위한 것으로 스팸메일 차단이 어느 정도 수준인지를 나타낸다. 실험 방법은 스팸메일을 자체 제작하여, 100개의 메일을 받았을 경우, 단어의 불량정도에 따라 분류해서 실험을 해보았다. 여기서 단어의 불량 정도란 메일 안에 포함되어 있는 문자열중 소위 불량단어라 규정되어지는 (광고, 성인 광고 등..)있는 것들이 어느 정도나 포함이 되어있는가 에 따른 것이다.

불량 단어율 / 스팸 처리 능력	10%	20%	30%	40%	50%	60%
상				○	○	○
중			○			
하	○	○				

[표2] 불량 단어율에 따른 스팸 처리 능력

스팸 처리 능력에 있어서 상(70~90%), 중(60%~40%), 하(30% 미만) 으로 설정을 했다.

위의 실험결과를 보면 불량 단어율이 전체 메일 내용에서 20%가 되지 않을 경우에는 스팸처리 능력이 떨어지는 것을 볼 수 있다. 하지만 불량 단어율이 40% 이상일 경우 만족할 만한 수준의 스팸 메일 처리능력을 나타내었다. 이 실험에서 좌우되는 불량 단어리스트는 문자열 분석과정에서 언급한 대로, 본인 및 본인의 친구들의 메일에 들어온 스팸메일을 분석한 결과를 토대로 작성하였다.

4. 결론

본 연구에서는 전자우편의 보안수단으로 사용하는 PGP를 가지고, 스팸메일을 제거할 수 있는 방법에 대하여 제시하였다. PGP를 이용한 인정서비가 인증된 메일만 수신하고, 3가지 분류 (Accept, Medium, Risk)를 통해서, 인증되지 않은 메일은 문자열 분석을 하여 자동으로 스팸메일을 구분하여 차단하는 시스템을 개발했다. 이 모델을 사용함으로써, 전자우편에 대한 보안과 스팸메일에 방지에 대한 효과를 거둘 수 있다.

PGP를 사용해서 생성된 파일들은 연속적인 8-bit의 흐름이지만 대부분의 전자우편 시스템은 ASCII 문자만을 인식한다. 따라서 PGP 에서는 Radix-64 변환을 통해서 3개의 8-bit를 4개의 ASCII문자로 변화시켜서 기존의 전자우편 시스템과 호환성 문제를 해결했다. 또한 효율적인 문자열 분석을 위해 메일의 제목과 내용의 핵심 단어를 추출하여 불량 단어리스트로 검색하는 방법을 사용했다. 향후에 불용어와 조사처리에 대한 부분의 구조를 일부 수정하여 메일의 핵심 단어가 아닌 문장으로 데이터베이스에 저장을 한 후 수신자가 메일의 내용을 알고 싶을 때 열람할 수 있는 기능을 추가하면 더욱 편리한 시스템이 되리라고 본다.

5. 참고 문헌

[1]"PGP의 개념과 활용" ,PLUS (POSTECH Laboratory for UNIX Security) Security+ for UNIX II, 1997 , 남궁 재창

[2]"전자우편 보안 - PGP 활용" http://www.certcc.or.kr/concert/cs9803/present/tf02/index.htm , 정윤종

[3]NeoCast "E-mail Marketing Implementation" http://www.neocast.co.kr/crm/market_implementation.html

[4]프로그램의 세계 "RSA 알고리즘", 98년 5월

[5]Dream Security, "전자우편보안", http://maxim.dreamsecurity.co.kr/0111_55PGP.asp

[6]영진 출판사 "Visual C++ Programming Bible Ver 6.X", 이상엽