기존 메일스캐너 시스템의 비교분석 및 새로운 방안 제안

김영현° 윤세안, 최은정, 최주영, 유주영, 김명주
서울여자대학교 대학원
{callingme°, ysa7724, chej, jhchoi90, ruyi77, mjkim}@swu.ac.kr

Analysis and Comparing existing mail scanners and a proposal of new technique

Younghyun Kim° Sean Yoon, Eunjung Choi, Jooyoung Choi, Jooyoung Yu, Myuhngjoo Kim
Dept. of Computer Science & Engineering, Seoul Women's University

요 약

본 논문에서는 정보화 사회에 있어서 E-mail 사용의 확산과 그에 따라 발생하는 컴퓨터 바이러스, 웜, 스팸메일 등의 출현에 따른 문제의 예방책으로써 메일서버스캐너를 제시한다. 이러한 필요성에 기반하여 기존의 개발된 메일스캐너의 개념을 이해하고 기능을 분석한다. 기능 분석을 통해 각각의 메일스캐너의 단점을 개선하고 장점을 강화하는 등의 새롭게 보강된 메일서버스캐너 기술을 제안한다.

1. 서 론

인터넷을 통한 전자상거래, E-mail 등 여러 서비스의 이용은 확대 증가하는 추세를 보이고 있다. 대표적으로 E-mail의 사용은 쉽고 빠르다는 장점을 기반으로 그 이용수가 기하급수적으로 늘어나고 있다. 지난 2002년 6월 KRNIC에서 발표한 인터넷 이용자수 및 이용 행태에 관한 보고서에 따르면 전체 인터넷 이용자 가운데 E-mail 보유자의 이용자의 수가 전체의 81.4%이며 이들의 주 평균 E-mail 송수신량은 49.2통으로 조사되었다[1]. 상당량의 컴퓨터 바이러스, 웜 등의 악성코드의 확산이 E-mail을 그 통신 수단으로 하고 있기 때문에 그 피해 또한 감지하기 어려운 수준에 이르고 있다.

이와 같은 흐름을 감안할 때 보다 적극적인 예방의 필요성이 요구된다. 그 대안으로 메일서버용 바이러스 스캐너를 통해 송수신 메일을 필터링함으로써 컴퓨터 바이러스를 탐지하고 폭주하는 스팸 메일을 차단하며 알려지지 않은 바이러스에 대해서도 판단하는 등의 기능을 제시할 수 있다. 이러한 필요성에 기반하여 본 논문에서는 기존에 개발된 공개용 메일스캐너 시스템의 기능을 비교·분석함으로 장점과 단점을 파악하고 그 기능의 개선과 더 강화된 메일서버스캐너의 새로운 기술을 제안하고자 한다.

2. 기존 메일스캐너의 기능 분석

2.1 Procmail & Sanitizer[3]

procmail은 메일 프로세서로 메일 메시지의 헤더와 본문을 필터링함으로 특정 정보에 따라 적절한 조치를 수행하는 프로그램이다. MTA(Mail Transfer Agent)인 sendmail을 통해 수신되는 메일을 MDA(Mail delivery Agent) 수준에서 필터링(filtering)할 때 사용된다[2]. 수신되는 메일의 헤더 정보를 바꿀 수 있고 본문의 내용을 각각의 문자집합(character set)에 따라 코드 변환시킬 수 있는 등 강력한 필터기능을 적용한다. procmail의 수행은 sendmail.cf에 포함시켜 명시적으로 실행시키거나 사용자가 홈 디렉토리에 .forward 파일을 두어 실행시킨다. sendmail이 sendmail.cf에서 path를 설정해 줌으로 procmail을 호출한다. 호출된 procmail은 먼저 자신의 환경을 설정하고 표준 입력으로 넘어오는 메일을 끝까지 읽는다. 그리고 메일의 헤더와 본문을 구분한 후 홈 디렉토리에 .procmailrc를 읽어 그 내용대로 처리한 후 메일스풀에 저장한다. 만일 홈 디렉토리에 .procmailrc가 없으면 /etc/procmailrc가 실행된다. 또한 procmail의 ruleset인 sanitizer를 통해 감염된 파일 등의 공격에 효과적으로 대응할 수 있다. procmail은 필터링하는 도구로써 가장 많이 사용되고 있긴 하지만 incoming 메시지에 대해서만 필터링을 하고 한 메시지에 대해 여러 개의 경고 메일이 발생할 가능성이 있다는 것과 무엇보다 관리의 어려움이 크다는 단점을 지적할 수 있겠다.

2.2 Inflex[4]

Inflex는 메일서버에서 로컬이나 외부로 나가는 E-Mail을 검사한다. Inflex는 sendmail이 sendmail.cf 대신에

inflex.cf 파일을 설정파일로 사용하도록 함으로서 원하는 기능을 구현한다. 그러므로 /etc/sendmail.cf 설정을 바꾸지 않고도 incoming/outgoing 메일을 검사할 수 있게 된다. Inflex는 Inbound & Outbound 정책기능을 통하여 메일 바이러스, 인터넷 웜 등의 첨부 여부를 조사하고 사용자에게 불필요하거나 위험한 파일 타입과 임의의 파일 이름까지 확인하여 필터링 할 수 있도록 설정할 수 있다. 임의의 파일이름과 파일유형에 대해서도 필터링하는 기능을 제공한다. 그리고 아웃룩 버퍼오버플로우 공격도 막을 수 있다. 즉각적인 대응을 위해 Inflex는 48시간 안에 업데이트가 되는 Anti-virus 패키지와 연동하여 탐지되지 않는 바이러스로부터의 공격에 즉시 대응할 수 있도록 해준다. inflex는 백신과 연동하여 사용이 가능하고 관리 및 운영이 용이하다는 장점이 있지만 첨부파일이 없는 메일에 대해서는 동작하지 않는다는 단점을 가지고 있다.

2.3 AmaVis[5]

AMaVis(A Mail Virus Scanner)는 메일이 sendmail이나 qmail 같은 MTA를 통해 도착하였을 때 첨부 파일을 분리하여 바이러스 검출 프로그램으로 검사한다. 이 메일 메시지가 procmail에 보내지기 전에 사용되는 incoming 메일 스캐너의 일종이며 상용 안티바이러스 제품들과 함께 사용될 수 있다. E-mail을 구성파트, 첨부파일 디코딩, 그리고 압축풀기로 세분화하고 각각 파트들은 하나 이상의 바이러스 스캔에 의해 필터링된다. 만약 첨부파일이 압축되었으면, AMaViS는 첨부파일의 압축을 해제한 후 안티바이러스 소프트웨어를 이용하여 검사한다. 감염된 메시지들은 격리되고 그 메시지를 수정하여 로컬 관리자와 보낸 사람에게 보낸다.

2.4 MIMEDefang[6]

MIMEDefang은 MIME e-mail 스캐너라고 부른다. 그 기능으로는 스팸 필터링, 바이러스 스캐닝, 다른 이 메일 필터링에 응용 가능한 해결책을 제공한다. MIMEDefang은 MIME 메시지를 분리하여 삭제하거나 수정할 수 있다. MIMEDefang의 보안 정책들은 설정파일에서 설정하도록 한다. 대응으로 Allow, Accept with, warning, Drop, Drop with warning, Defang, External filter, Quarantine, Bounce가 있다.
MIMEDefang은 sendmail 8.12.x와 사용이 된다. 그렇기 때문에 sendmail을 새로 컴파일하고 sendmail.cf를 새로 만들어야 하는 불편함을 가지고 있다.

2.5 Anomy Mail Sanitizer[7]

Anmoy mail sanitizer는 Red Hat Linux에서 개발이 되었고 qmail, postfix, exim등의 여러 MTA들과 사용된다. Anomy는 JavaScript나 HTML 태그들을 포함하는 Java를 비활성화 시키는 기능을 제공한다. 그리고 incoming 메일을 대상으로 액티브 컨텐츠 공격과 같은 잠재적으로 위험을 가지는 HTML 코드들을 비활성화 시킨다.
Anomy mail sanitizer는 첨부된 파일의 바이러스 스캐닝을 하고, 첨부파일의 파일이름을 기준으로 차단시키거나 다른 파일명으로 바꾸어 주는 기능을 한다. 룰(rule)은 정책집합에 의해 정의되어진다.

2.6 기타

그 외에도 간단한 기능들로 필터링하는 도구들이 있다. 다른 도구들에 비해 매우 간단한 VBS[8]라는 툴이 있다. 이것은 첨부파일의 실행 가능한 파일 확장자를 다른 문자로 바꾸어 실행되지 못하게 함으로 웜 바이러스만을 막도록 설계되었다. MIME 메시지를 평문 메시지로 전환해 주는 perl 프로그램인 StriptMIME[9]이 있다.
Qmail-scanner[10]은 qmail에서 동작하는 Scan4virus로도 잘 알려져 있으며 이것은 anti-virus protection function들을 사용하여 상용 바이러스 스캐너와 함께 사용될 수 있다. 그리고 헤더의 특별한 문자열을 포함하는 E-mail이나 특정 파일 이름이나 파일형태를 포함하는 E-mail을 탐지할 수도 있다. MailFilt[11]는 정규표현(regular expression)을 사용하는 보안 규칙이다.

3. 보강된 메일스캐너 기술 제안

새롭게 제안하고자 하는 메일서버스캐너를 유형분석을 기반하는 메일서버스캐너인 FAM(Form Analysis- based Mail server scanner)이라 이름한다. FAM의 흐름과 그 구성상의 특징은 다음과 같다. SMTP 프로토콜을 이용하여 메일서버의 외부로 보내지기 전의 메일과 SMTP 프로토콜을 이용하여 메일서버 외부에서 인터넷을 통해 메일서버의 내부로 들어와 우편함에 저장되는 메일이나 메일서버 로컬에서 전송되는 메일이 우편함에 저장되는 메일이 해당 송신자의 메일박스로 이동되기 전에 스캔하여 스팸메일 및 악성코드 감염메일 등을 검사하고 그에 따른 적절한 대응을 한다[12].

3.1 FAM의 주요 기능 및 특징

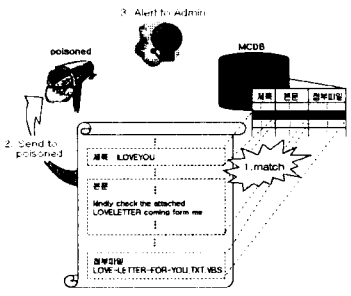
3.1.1사용자 환경의 다양한 구축

FAM은 메일서버의 전체에 적용되는 환경을 설정하기

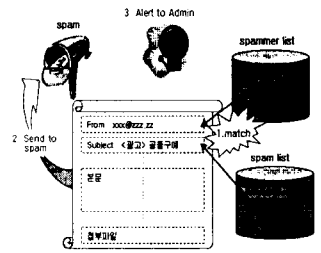
위한 관리자용 환경설정파일과 각각의 계정의 사용자의 특성에 따라 선택적으로 그리고 사용자의 E-mail 사용 패턴에 따라 적용하기 위한 개인용 환경설정파일을 두어 사용자별 환경 구축의 다양화를 취할 수 있도록 한다.

3.1.2 단계별 스캐닝 기술

메일의 효과적인 분류를 위해 세 단계로 계층화를 하였는데 첫 번째 단계에서는 [그림1]에서 보는 바와 같이 기존의 알려진 악성코드에 관한 정보를 구축해 놓은 MCDB와의 매칭알고리즘을 활용하여 감염된 메일을 탐지하고, 두 번째 단계에서는 [그림2]와 같이 스팸메일을 차단한다. 그리고 세 번째 단계에서는 메일의 구조에 따른 악성코드의 형태분석(메일 메시지의 수신자, 제목, 본문, 첨부파일 등의 특성들을 미리 분석하여 시스템화해 둔다.)을 기반으로 한 스코어 시스템을 이용하여 메일의 위험정도를 책정하여 그에 따라 처리할 수 있도록 하였다.



[그림 1] 알려진 악성코드의 차단



[그림 2] 스팸메일 차단

3.1.3 특정 유형 분석에 따른 로그로 통계 분석

FAM은 계층화된 메일 스캐닝의 세 번째 단계인 형태분석 단계에서 남겨진 로그 기록들을 기반으로 스팸메일 발신자의 정보와 악성코드 감염가능 메일의 정보 등을 통계적으로 분석하여 얻을 수 있으며 이 기능을 통해 알려지지 않은 바이러스에 대한 처방 또한 가능하게 하였다. [표1]에서와 같은 최종 점수에 대한 처방을 이용한다.

[표 1] 스코어의 합에 따른 처방

score_sum	처방
0	정상 : 정상적인 형태의 메일이다
1~50	주의 : 악성코드의 감염도는 낮으나 메일 형식이 비정상적이므로 메일을 열어볼 때 주의를 요한다
51~99	경고 : 악성코드의 감염도는 보통이나 메일을 열기 전 백신을 이용한 바이러스 체크가 필요하다
100이상	위험 : 악성코드의 감염도가 높다. 메일을 열지 않고 삭제하는 것이 좋다.

score_sum=0 으로 초기화되어 있다.

각 메일은 송신자 분석, 제목 분석, 본문 분석, 첨부파일명 분석의 단계를 거치며 해당 case와 일치하는 경우 score_sum= score_sum+score를 계산하여 score_sum에 따른 처방을 한다.

4. 결론

본 논문을 통하여 송수신되는 메일 필터링의 필요성에 대해 논하고 기존의 공용 메일스캐너 시스템에 대해 개관하였다. 그것을 기반으로 각 기능의 장점을 통합하고 단점으로 드러난 관리의 어려움, 메일 메시지의 헤더, 바디, 첨부파일 중 일부만을 필터링하는 등의 사항들에 대한 보완의 필요성을 직시하여 새로운 메일서버용 스캐너의 방안을 제안하였다. 제안하는 메일서버스캐너는 알려진 악성코드, 스팸메일을 차단하고 유형분석을 기반으로 스코링 시스템을 도입하여 알려지지 않은 악성코드에 대한 차단까지 가능하게 하였다. 이 논문을 통해 제안한 메일서버용 스캐너는 향후 신종 악성코드의 출현과 그에 따른 피해까지도 예방하는 대안이 될 것이다.

참고문헌

[1] 한국인터넷정보센터(KRNIC), 통계자료
[2] Bryan Costales with Eric Allman, "Sendmail", O'REILLY, 1997
[3] ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html
[4] http://www.pldaniels.com/inflex/
[5] http://www.amavis.org/
[6] http://www.roaringpenguin.com/mimedefang/
[7] http://mailtools.anomy.net/
[8] http://adsl-nolte1.rz.rwth-aachen.de/progs/vbs/
[9] http://www.phred.org/~alex/stripmime.pl
[10] http://qmail-scanner.sourceforge.net/
[11] http://people.oven.com/bet/mailfilt
[12] 윤세안, 악성코드의 유형분석을 통한 메일서버스캐너의 설계 및 구현, 2002