제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

전자메일 바이러스에 의한 스팸 메일 전파 차단 시스템

남강운*, 김준모**, 우진운*, 조성제*
*단국대학교 정보컴퓨터학부
**한국정보보호진흥원, 기술단, 시스템기술팀
e-mail:skywonny@hitel.net

A System for Blocking Spam Mail Propagation by E-mail Viruses

Wonny Nham*, Joonmo Kim**, Jinwoon Woo*, and Seongje Cho*
*Division of Information and Computer Science, Dankook University
**Information Security Technology Division, Korea Information Security Agency

요 약

최근에 유포되고 있는 악의적인 소프트웨어로 Melissa와 Love letter와 같은 전자우편 바이러스가 있는데, 이들은 단순히 전자우편을 열기 만해도 메일 주소록에 등록된 모든 사용자에게 자신을 유포함으로써 막대한 피해를 유발시킨다. 본 논문에서는 메일 주소 변형모듈 및 복원모듈을 전자우편 송신부에 추가 도입함으로써 전자우편 바이러스에 의한 바이러스 전파를 차단하는 시스템을 제안한다. 변형모듈은 송신자 행위에 의해서만 수행되어 수신자의 메일 주소를 변형하며, 복원모듈은 송신부의 서버 단에서 전자우편 전송 시마다 수행되어 역변형 과정을 거쳐 메일 주소를 복구한다. 변형모듈은 전자우편 바이러스에 의해서는 실행되지 않도록 구현되며, 전자우편 수신부에서는 추가로 하는 작업이 전혀 없다. 제안한 시스템에서는 새로운 전자우편 바이러스 공격에 대응하기 위해서, 다형성(polymorphism) 기법도 적용한다.

1. 서론

전자우편 바이러스는 최근에 출현한 악의적인 소프트웨어로 Melissa와 Love Letter 등의 그 예이다. 이들 바이러스는 MS 워드 매크로나 비주얼 베이직 스크립트 언어로 작성되며, 수신자가 전자우편에 첨부된 파일을 열거나 전자우편 자체를 열기 만해도 활성화되어, 전자우편 패키지의 메일링 리스트에 있는 모든 사용자에게 자신을 급속히 확산시킴으로써 단기간에 큰 피해를 유발시킨다.

상용 바이러스 백신 프로그램들은 이러한 전자우편 바이러스에 대하여 예방과 치료할 수 있는 기능을 갖고 있다. 하지만 백신 프로그램들은 미리 해당 바이러스에 대한 패턴들을 갖고 있을 때에만 효력을 발휘하며, 새로운 바이러스(패턴을 갖고 있지 않은)에 대하여는 적절한 대처를 하지 못한다.

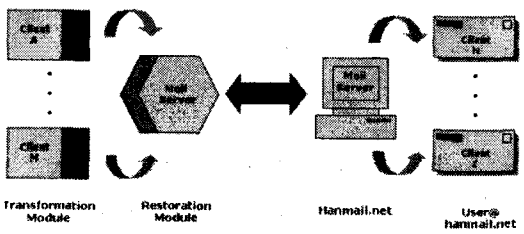
본 논문에서는 전자우편 바이러스 전파를 차단시켜 주는 시스템을 제안한다. 본 전자우편 시스템은 전자우편 바이러스에게 감추어진 두 모듈을 송신자 측에 삽입하여, 바이러스는 전자우편을 전송할 수 없게 하고 일반 사용자는 정상적으로 전자우편을 전송할 수 있게 하였다. 즉, 송신 측의 클라이언트에는 "변형 모듈"(transformation module)이 삽입되어 수신자의 메일주소를 변형하고, 송신 측의 서버에는 "복원 모듈"(restoration module)이 삽입되어 변형된 메일주소를 원래의 주소로 복원한 후, 인터넷을 통해 수신자 측에 전송한다. "변형 모듈"은 사용자의 동작에 의해서만 수행되며, "복원 모듈"은 전자우편 전송 시마다 자동적으로 수행된다. 이외에도 제안 기법이 새로운 전자우편 바이러스에 의해 공격받는 경우를 대비하여 간단한 다형성(polymorphism) 모델을 적용한다.

본 논문의 구성은 다음과 같다. 2장에서는 제안한 시스템 구성에 대해 기술하고, 3장에서는 실제 구현

한 내용 및 간단한 다형성 모델을 제시하며, 4장에서는 기대효과를 기술한다. 5장에서 결론을 맺는다.

2. 시스템 구성

전자우편 바이러스 발송을 차단하기 위한 시스템 구성이 그림 1에 나타나 있다. 전자우편은 송신자 측의 클라이언트에서 작성되어 송신자 측의 전자우편 서버로 전달되며, 그 다음 송신자 측 서버에 의해 수신자 측의 전자우편 서버로 전달되고 최종적으로 수신자에게 전송되는 형태이다.



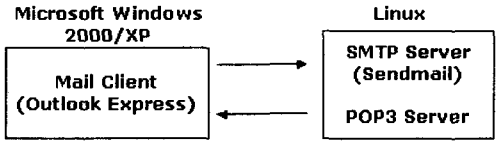
[그림 1] 시스템 구성도

그림 1에서 수신자 측의 기능 및 동작 방식은 이전과 동일하므로 설명하지 않고, 송신자 측의 수정된 사항만을 기술한다. 그림과 같이 전자우편 시스템의 송신자 측의 클라이언트에는 변형 모듈, 서버에는 복원 모듈이 새로이 추가되었다.

변형 모듈은 임의 수신자에게 전자우편을 보내기 직전에 사용자의 행위에 의해서만 수행되어 수신자의 전자우편 주소를 특정 형식으로 변환하며, 복원 모듈은 클라이언트로부터 전자우편을 받자마자 자동으로 수행되어 전달받은 전자우편 주소를 원래의 주소로 복구한다. 변형 모듈은 전자우편 바이러스에 의한 전자우편 전송 시에는 실행되지 않지만, 복원 모듈은 모든 전자우편 송신 시마다 항상 자동으로 실행된다. 즉, 송신자 측의 클라이언트 변형 모듈은 사용자에 의해서만 실행되어 변형된 전자우편 주소를 전달하며 송신자 측 서버는 변형된 주소를 복원하여 인터넷을 통해 수신자 측에 전송하게 된다.

3. 구현 및 실험

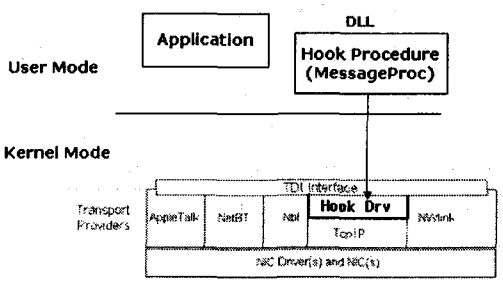
3.1 구현 환경



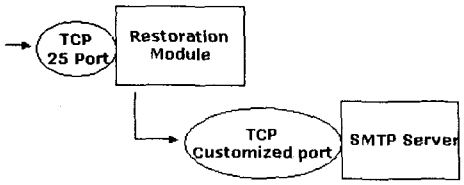
[그림 2] 송신자 측 환경

전자우편 시스템은 여러 가지 구성으로 나타날 수 있다. 본 논문에서는 송신자 측의 메일 클라이언트로 MS 아웃룩 익스프레스, 서버로 리눅스 운영체제와 SMTP를 사용하는 환경을 고려한다. 즉, 변형 모듈은 MS 윈도에서 구현되며 복원 모듈은 리눅스에서 구현된다.

송신자는 전자우편 작성 후 전자우편 전송을 위해 항상 <보내기(send)> 버튼을 누른다. 따라서, <보내기> 버튼을 누를 때만 변환 모듈을 실행하도록 하면 된다. MS 윈도 운영체제는 외부의 이벤트들에 대응해서 응용에 메시지 형태로 통지한다. 이러한 특징을 이용한 변환 모듈의 구현 예가 그림 3에 나타나 있다. 그림 3에서 MessageProc() 함수는 메시지를 중간에서 가로채는 함수이며, 통지 받은 메시지가 사용자가 메일전송을 하기 위한 행위(**send 버튼을 누른 경우**)에 대한 것이라면, 커널 안에 탑재되어 있는 TDI(Transport Driver Interface) Hook Device Driver에게 사용자 행위에 의해 송신되는 전자우편임을 알려준다[6]. TDI Hook Driver는 MessageProc()에 의해 통지 받았다면 전자우편의 수신자 주소를 변형하지만, 그렇지 않다면 변형하지 않는다.



[그림3] 변형 모듈의 구현 [6]



[그림 4] 복원 모듈의 구현

리눅스 SMTP 서버가 TCP 25번 포트와 연관되어 있으므로, 복원 모듈이 TCP 25번 포트와 바인드되도록 하고 SMTP 서버는 임의의 다른 포트로 대응시켰다. 복원 모듈은 수신한 메일 주소를 규칙에 따라 변환한 다음, 옮겨진 SMTP 서버 포트를 통하여 메일을 중계한다. Sendmail인 경우 환경 파일(sendmail.cf)의 설정을 수정하여 임의의 포트(1000)로 변경할 수 있다.[3]

DaemonPortOptions==Port=1000

3.2 실험 및 다형성 모델(polymorphous model)

전자우편 주소를 변환하고 복원하는 모듈이 바이러스로부터 숨겨져 있다하더라도 유추하기 쉬운 방식으로 구현된다면, 새로운 전자우편 바이러스에 의해 공격받을 수도 있다. 따라서 안전한 시스템을 구축하기 위해 전자우편 주소의 변환 및 복원 기법은 다양한 형태로 구현될 수 있어야 한다. 2, 3장에서 설명한 바와 같이 복원 모듈이 하는 일은 변환 모듈의 역함수이다. 변환 모듈이 x를 입력받아 f(x)를 출력한다면 복원 모듈은 f(x)를 입력받아 $f^{-1}f(x)$를 출력하게 된다.

구체적인 구현 예로, 변형 모듈은 수신자 전자우편 주소의 특정 부분에 m개 문자를 삽입하고 복원 모듈은 변형 모듈이 삽입한 문자를 제거한다. 즉, 수신자 주소가 userN@mserver.net, m=2, ?는 임의의 한 문자를 표현한다고 할 때,

① 변형 모듈은 다음의 예와 같이 수신자 주소의 제일 앞, 또는 @ 기호 앞이나 뒤, 또는 주소의 제일 뒤 등에 2개의 임의문자를 첨가한다. 이러한 조작은 단순하기 때문에 송신자의 수작업에 의해서도 가능하다.

예) ??userN@mserver.net, userN??@mserver.net, userN@??mserver.net, userN@mserver.net??

② 복원 모듈은 역으로 수신자 주소의 제일 앞, 또는 @ 기호 앞이나 뒤, 또는 주소의 제일 뒤 등에 첨가된 2개 의 임의 문자를 제거하여, 본래의 주소 userN@mserver.net를 얻는다.

현재, 본 논문에서 구현한 방식은 전자우편 주소 제일 뒤에 임의 문자를 3개 첨가 및 제거하는 방식이나, 이러한 방식은 주기적으로 동적으로 변경 가능하게 할 예정이다.

4. 기대 효과

초기 Melissa와 같은 전자우편 바이러스는 전자우편에 첨부된 파일 내에 내장되어, 첨부된 파일이 오픈될 때 전파되었다. 1999년 말에 나타난 새로운 버전은 첨부 파일을 오픈하지 않고 단순히 바이러스를 포함한 전자우편만 오픈 하더라도 활성화된다. 그 결과 표 1에 나타난 것처럼, 바이러스가 전파되는데 몇 년 또는 수개월이 걸렸던 과거에 비해 이제는 몇 시간 내에 바이러스가 급속히 전파될 수 있다[5]. 제안하는 기법을 적용한다면 큰 피해를 유발시키는 전자우편 바이러스의 전파를 방지할 수 있다.

[표 1] 바이러스 전파 시간 및 피해 규모

바이러스	발견 년도	유 형	전파 시간	추정 손해비용
Jerusalem, Cascade, Form	1990	.exe 파일	3 years	$50 million for all over five years
Concept	1995	Word macro	4 months	$50 million
Melissa	1999	E-mail enabled, Word macro	4 days	Up to $385 million
Love letter	2000	E-mail enabled, VBS based	5 hours	Up to $15 billion

5. 결론

본 논문에서는 전자우편 바이러스의 전파를 차단할 수 있는 기법을 설계하고 구현하였다. 제안한 메

일 시스템에서는, 전자우편 송신자가 <보내기> 버튼을 누를 때만 수행되는 변형 모듈이 있어 수신자 전자우편 주소를 특정 형태로 변형해서 송신자 측 서버로 전송한다. 서버에는 전자우편 전달을 중계할 때마다 자동으로 수행되는 복원 모듈이 있어 변형된 주소를 본래의 주소로 복구시켜 수신자에게 전달하게 된다. 제안한 기법은 다형성 모델을 지원하여 새로운 바이러스 공격에 안전하다.

참고문헌

[1] Jonathan B. Postel, "Simple Mail Transfer Protocol" in RFC 821, August, 1982

[2] David Wood, "Programming Internet Email", O'reilly, August, 1999.

[3] sendmail 8.11.6, http://www.sendmial.org

[4] CERTCC-KR-TR-2001-05, "메일필터링을 통한 E-mail 보안", http://www.certcc.or.kr

[5] William Stallings, "Operating Systems, 4th Edition", Prentice Hall, December, 2000, Table 15.4

[6] MS Windows DDK Document, Microsoft