파일 전송 프로토콜을 경유하는 실시간 바이러스 차단 시스템 설계

김두현°, 정종근, 정일용
*조선대학교 전자계산학과
mindul@cspost.chosun.ac.kr

A Design of Realtime Virus Interception System via File Transfer Protocol

Doo-Hyun Kim°, Jong-Kun Jeong, Il-Yong, Jung
Dept. of Computer Science, Chosun University

요 약

이제는 인터넷이 우리의 생활 깊숙이 들어와 온라인 쇼핑, 웹 기반 메일, 소프트웨어 업/다운로드 등 인터넷을 서핑 하는 것이 하루 세 끼 밥을 먹고, TV를 보는 것처럼 생활화되었다. 이런 인터넷을 통해 하루에도 수많은 파일들이 FTP를 통해 들어오고 나가고 있으나 현재로서는 클라이언트 단위에서 사용자가 직접 바이러스를 점검, 치료하고 있을 뿐이다. 따라서, 본 논문에서는 클라이언트에 유입되기 전 단계인 게이트웨이에서 FTP의 인터넷 트래픽을 조사하여 들어오는 파일들 중 바이러스에 감염된 파일을 체크함으로써 클라이언트에 유입되기 전에 치료 및 사용자에게 재전송 하는 바이러스 탐지 시스템을 제안한다.

1. 서론

악성소프트웨어란 컴퓨터 시스템의 데이터 파괴 및 시스템 정지 등의 악의적인 현상을 일으키는 프로그램들을 통틀어 일컫는 말이다. 악성 소프트웨어에는 컴퓨터 바이러스(Computer Virus), 트로이 목마(Trojan horse), 웜(Worm), 논리 폭탄(Logic Bomb), 그리고, 백 도어(Back door) 등이 있다. 1999년도부터 적지 않은 피해를 입혀온 러브레터 바이러스와 그 변종들은 최근 컴퓨터 바이러스의 대표적인 형태이다.

이런 바이러스는 인터넷이 급속히 확산됨에 따라 그 피해 또한 기하급수적으로 늘어만 가고 있다. 이런 바이러스를 퇴치하기 위한 백신의 대부분은 윈도우즈 클라이언트용으로 제작, 배포되고 있지만 Linux나 Unix용 백신은 고가이면서 그 숫자 또한 극히 드문 형편이다. 또한, Linux나 Unix용 백신 소프트웨어는 단순히 파일시스템에 저장된 이후에 사용자나 관리자에 의해 검사되는 선저장-후검사 방법이므로 바이러스의 침입에 적극적으로 대응하지 못하고 있는 실정이다.

본 연구에서는 리눅스 파일 시스템에 저장된 파일의 바이러스 감염여부를 검사할 뿐만 아니라 파일 전송 프로토콜(FTP)상으로 전송되어 오는 파일들을 실시간(Realtime)으로 검사하여 탐지 및 복구하는 시스템을 구축하고자 한다.

2. 관련 연구

현재 국내에는 두 개의 백신 프로그램 전문 제작 업체가 있다. 안철수바이러스연구소와 하우리가 그것인데 도스용 바이러스부터 최근에는 PDA용 바이러스까지 진단 및 치료할 수 있을 정도로 기술 발전을 거듭하고 있다.

외국 업체는 PC, Unix 기반 파일 시스템 검사부터 네트워크 기반 바이러스 방역제품까지 다양한 종류의 제품을 만들고 있으나 국내 업체는Windows 기반 PC나 Unix 기반 서버의 파일시스템에 저장된 파일들을 검사하는 제품과 E-mail의 첨부파일을 검사하는 백신 소프트웨어를 주로 생산하고 파일 전송 프로토콜(FTP)을 검사하는 제품은 아직 나오지 않은 상태이다.

3. 시스템 구성

시스템은 크게 셋으로 나누어진다. 하나는 파일 전송을 위한 FTP Daemon, 다른 하나는 Unknown 바이러스를 탐지하고 차단하는 모듈, 그리고 관리자를 위한 결과 리포트 모듈이다.

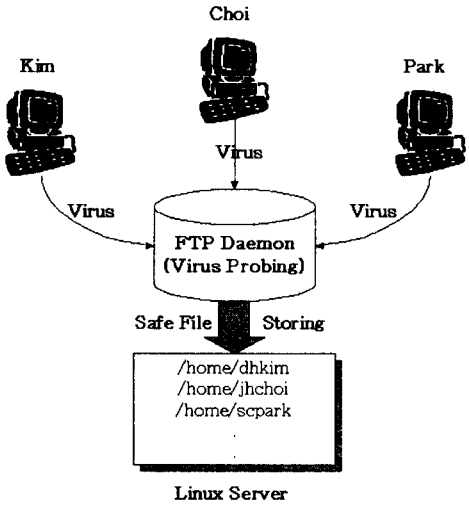

그림 3.1 시스템 구성도

우리는 다음과 같은 시나리오를 생각해볼 수 있다.
① 사용자 Kim은 바이러스에 감염된 사실을 모른 채 실행파일을 UNIX 서버로 전송하려고 한다.
② FTP 클라이언트 프로그램을 구동하여 UNIX 서버의 FTP 서버 프로그램에 접속을 시도한다.
③ 사용자 계정과 암호를 입력하고 login에 성공한다.
④ 바이너리 파일 전송을 위해 <bin> 명령을 실행하여 Binary mode로 전환한다.
⑤ 파일 전송 명령 <put>과 함께 전송할 파일명을 입력한다.
⑥ 바이러스에 감염된 파일을 전송한다.
⑦ FTP 서버 프로그램(Daemon)은 목적 디렉토리에 전송된 파일을 일단 저장한다.
⑧ 저장된 파일은 바이러스 탐지 및 차단 모듈에 의해 바이러스 감염여부를 진단되어진다.
⑨ 감염된 파일은 치료 및 복구되고 관리자 결과 리포트 모듈에 의해 보고서가 작성된다.
⑩ 사용자 Kim은 접속을 종료한다.

FTP daemon을 통해 들어온 파일은 사용자의 현재 작업 디렉토리에 저장된다. 파일의 전송이 완료되는 순간 바이러스 검사 모듈이 작동하여 파일의 감염여부를 검사하고 바이러스 발견 시 관리자와 사용자에게 통보하고 스스로 치료 또는 복구한다.

4. 시스템 구현

본 시스템은 클라이언트에 유입되기 전 단계인 게이트웨이에서 FTP의 인터넷 트래픽을 조사하여 들어오는 파일들 중 바이러스에 감염된 파일을 체크하고 치료함으로써 클라이언트에 유입되기 전에 바이러스에 감염된 파일의 유입을 막는 시스템을 구현하였다.

시스템은 크게 세 가지, 파일전송 모듈과 바이러스 검사 모듈, 그리고 결과 리포트 모듈로 이루어지고 각각의 모듈은 Shared Library로 관리된다.

4.1 파일 전송 모듈

[그림 4.1]에서는 서버와 서버간의 데이터 전송과 제어 연결(control connection)의 관계를 잘 보여주고 있다. FTP는 제어 연결에 있어 텔넷(Telnet)을 이용할 수도 있고 이미 시스템에 존재하고 있는 텔넷 모듈을 이용할 수도 있지만 대부분은 후자에 의존한다.

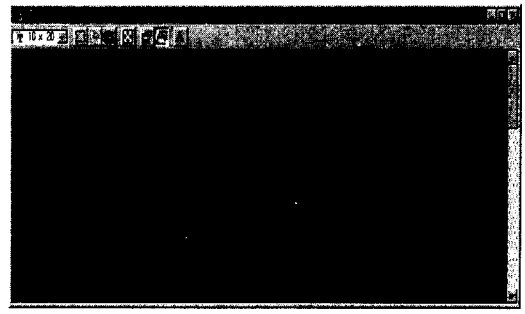

그림 4.1 시스템 접속 화면

4.2 바이러스 검사 모듈

파일 전송이 끝났으면 이제 바이러스에 대한 검사가 이루어진다. 바이러스에 대한 검사는 바이러스 엔진을 이용하여 파일 전송이 끝난 즉시 실시간으로 이루어지고 그 결과는 다시 결과 리포트 모듈로 넘겨지게 된다.

그림 4.2 바이러스 검사 화면

4.3 결과 리포트 모듈

본 시스템에서는 바이러스가 발견되었을 경우에 관리자(root@localhost)에게 메일로 구체적인 정보를 알리도록 구현하였다.

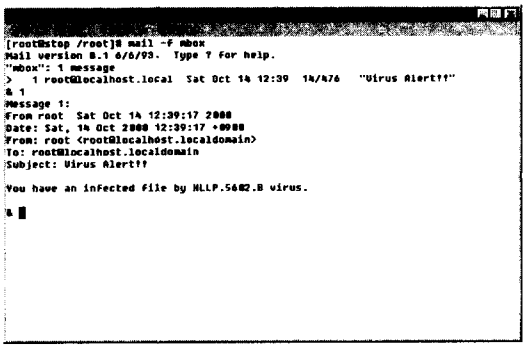

그림 4.3 바이러스 경보를 관리자에게 메일로 전송

결과 리포트 모듈은 CGI를 이용하여 서버로부터 읽어들인 정보를 웹브라우저에 표현하여 누구나 한눈에 알아볼 수 있는 리포트를 받도록 하고, 결과에 대한 리포트는 웹에서 그래프와 숫자를 이용하여 연월일별로 통계를 내고 바이러스의 종류와 감염된 파일의 이름 등에 관한 정보를 포함하게 된다.

5. 결론 및 향후 연구

본 논문에서는 리눅스 서버 시스템에서 파일 전송 프로토콜(File Transfer Protocol)을 통해 들어오는 파일들의 바이러스 감염여부를 검사하는 시스템을 제안하였다. 제안한 시스템은 별도의 프로세스를 생성하는 방법보다 데몬(daemon)을 이용함으로써 시스템의 부하를 줄일 수가 있었고, 백그라운드에서 24시간 감시함으로 바이러스 유입에 대한 위험부담을 없앨 수 있었다.

앞으로는 네트워크상의 다양한 데몬 프로그램들에서 바이러스를 효과적으로 검사 및 치료할 수 있는 네트워크 프로토콜 기반 종합 방역시스템 구축에 대한 연구가 필요할 것이다.

참고문헌

[1] Keith Haviland, Dina Gray, Ben Salama "UNIX System Programming, 2/E" 1999
[2] Kurt Wall "*Linux Programming by Example*" QUE 2000
[3] RFC 959 "File Transfer Protocol(FTP)"
[4] Richard Stones "Beginning Linux Programming, 2E" 정보문화사 2000
[5] W. Richard Stevens "Advanced Programming in the UNIX Environment" Addison Wesley 1992
[6] W. Richard Stevens "UNIX Network Programming Vol.1 2/E" 교보문고 1999

[7] "UNIX System V/386 Release 4 프로그래머 지침서" UNIX PRESS 캘라 1992
[8] 권석철, 주영흠, 김판구 "컴퓨터 바이러스 완전 소탕" 크라운 출판사 1997
[9] 김화종 "컴퓨터 네트워크 프로그래밍" 홍릉과학출판사 2000
[10] 안철수 "바이러스 분석과 백신 제작" 정보시대 1995
[11] 조선대학교 "컴퓨터 바이러스 감염 예방 시스템 개발에 관한 연구" 한국전산원 1995
[12] 조선대학교 "컴퓨터 바이러스 진단 치료 프로그램 및 감염예방시스템 구현" 한국정보보호센터 1997
[13] 리눅스 한글문서 프로젝트 http://kldp.org