

Linux 기반의 패킷 모니터링 시스템 설계 및 구현

박재우^o, 손위석, 추영열
동명정보대학교 컴퓨터공학과

Implementation of Packet Monitoring System Based on Linux

Jae-Woo Park, Wee-Seok Son, Young -Yeol Choo

Dept. of Computer Engineering, Tongmyong University of Information Technology

요 약

본 논문에서 제시하는 패킷 모니터링 시스템은 방화벽과 모니터링 기능을 통합하여 사용자가 한 프로그램에서 사용할 수 있도록 시스템을 설계 하였다. 인터넷 응용 범위의 확대와 더불어 많은 바이러스와 보안 취약점으로 인하여 불안정한 네트워크 환경을 초래하게 되어서 모니터링 및 방화벽에 대한 관심이 늘어가는 추세이다. 따라서 본 논문에서는 네트워크에 발생할 수 있는 문제점들을 감시하고 해결하기 위해서 패킷을 캡처하여 분석한다. 그리고 상대방이 해킹을 시도하는 것을 차단할 수 있는 방법을 제시한다. 본 논문에서 제시한 기술은 네트워크 모니터링 기술을 응용한 네트워크 트래픽 관리, 분석 시스템이며 일반 사용자들이 보다 쉽고 단순하게 리눅스 환경에서 사용할 수 있게 하였다. 그리고 웹 서버에서는 네트워크 트래픽의 통계치 자료를 인터넷에서 볼 수 있도록 하였다.

1. 서론

오늘날 정보사회의 발전으로 인터넷이 빠른 속도로 보급이 되고, 보편화되는 현상을 초래하게 되었는데 이로 인하여 네트워크 트래픽은 계속해서 증가하고 있다. 많은 사용자들이 인터넷의 사용으로 회선의 부족, 네트워크 응답시간의 저하, 많은 P2P 공유프로그램, 온라인 게임 등의 요인으로 문제가 발생할 수 있다. 그래서 인터넷상의 트래픽을 확인하기 위하여 모니터링 및 분석 시스템이 부각되고 있으며, 해킹으로 인하여 방화벽 및 IDS 등의 차단 시스템이 개발되고 있다.

여러 가지의 모니터링 시스템이 개발되고 있지만 Linux System 에서 기능적으로 미흡한 면이 많으나 오픈 소스를 추구하기 때문에 지금도 개발되고 있다. 그러나 Linux 에서는 아직 모니터링 시스템 등이 많지는 않으며 GUI 를 구현하기 힘든 것이 현실이다. 기존의 Linux 상에서의 모니터링 프로그램들은 콘솔상의 프로그램이 대부분 이어서 일반 사용자들이 사용하기 힘들다.

또 기존의 모니터링 시스템들은 한 시스템에서 패킷 캡처 와 분석을 동시에 하므로 시스템 과부하 시에 패킷 손실이 발생하여 모듈 별로 나누어서 기능을 분할하여 설계하였다.

이에 따라 본 논문에서는 네트워크 모니터링 및 분석 시스템의 기능과 문제점을 살펴보고, 그러한 각종 요구 사항을 반영하여 사용자들이 Linux 상에서 모니터링을

조작하기 쉽게 한다. 그리고 웹 서버를 구축하여 Windows 상의 웹 서비스로 실시간 트래픽 량을 분석하여 그래프로 표현하여 사용자가 보기 쉽고 사용하기 쉬운 Packet Monitoring Solution(FWlab)의 설계 및 구현을 설명 한다.

Packet Monitoring Solution(FWlab)은 Linux 와 웹에서 시간-날짜 별 등을 분석하여 웹 브라우저에서 볼 수 있으며, Linux 에서 프로그램을 구현하여 Linux 상의 X-Windows 에서 GUI 로 표현하는데, 여기서 실시간 패킷 량을 표현한다. 학교나 관공서 기업 내 LAN 상에서의 패킷을 캡처 현황과 IP 주소를 리스트로 표현을 하였다. 서버나 컴퓨터의 사양을 볼 수도 있고, 필터 룰을 설정하여 자신이 원하는 범위에서 트래픽을 분석할 수도 있다. 요즘은 많은 일반 사용자들이 Linux 사용하여 웹 서버를 구축하여 자신이 직접 서버 관리자가 되는 경우가 많다. 그래서 요즘은 개인컴퓨터에서 많은 해킹 사건이 일어나고 있으며 점차 보안에 대한 인식이 바뀌게 되었다. 사용자들이 사용하기 쉬운 설정의 방화벽 기능을 첨가 하게 되었다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 모니터링 도구에 관한 분석을 간략히 정의 하였고 제 3 장에서는 각 모듈의 기능과 시스템 구조에 관하여 기술하였다 제 4 장은 구현한 화면을 스냅샷(snapshot)을 보이고 제시한 시스템이 결과를 고찰 하였다. 제 5 장에서는 결론과

앞으로의 과제에 대하여 기술한다.

2. 네트워크 모니터링 도구 분석

여러 네트워크 도구들이 많이 사용되고 있으며 Windows 및 Linux 버전 등이 있다. 분석에는 기능 및 장·단점들을 파악한다.

2.1 MRTG (Multi-Router Traffic Grapher)

MRTG 는 네트워크 링크간의 트래픽 부하량을 측정하는 도구로서 5 분 단위에서 1 년 단위까지 네트워크 트래픽의 총량을 확인하는 도구이다. 웹 기반으로 동작하여 네트워크 트래픽을 확인하기에 편리할 뿐만 아니라 C 와 Perl 로 작성되어 유닉스 플랫폼 뿐만 아니라 Windows NT 에서도 동작하는 장점이 있다. 또 MRTG 는 Snmp MIB 정보를 사용하여 패킷 캡처를 하지 않으므로 패킷 손실없이 정확한 정보를 제공해 준다. 그러나 MRTG 는 네트워크 트래픽의 총량에 대한 정보를 제공해 줄뿐 어떤 호스트에서 어느 정도의 트래픽을 발생시켰는지, 어떤 어플리케이션이 어느 정도의 트래픽을 발생시켰는지, 어떤 프로토콜이 사용되었는지 등의 정보를 제공 해주지 못하는 단점이 있다. 이러한 단점을 보완하기 위해서 패킷을 캡처하여 DB 로 전송하여 이를 분석 보완한다.

2.2 Ethereal

ethereal 은 실시간 혹은 파일에 저장해 놓은 네트워크 트래픽 정보를 분석 해주는 프로그램이다. GTK+ 기반인 유닉스플랫폼의 X-Windows 화면에서 동작하며 MS-Windows 용도 있다. 여러 다양한 프로토콜 분석을 지원하는 장점이 있다. Gerald Comb 가 50 명 이상의 프로그래머들과 함께 오픈 프로젝트로 진행 되고 있다. ethereal 은 보안 등을 위한 실시간 네트워크 모니터링에 적합한 프로그램으로 장기간의 네트워크 모니터링에는 적합하지 않지만 장점들을 보완하여 반영 하였다.

2.3 프로그램 비교사항

위에서 소개한 내용을 정리해 보면 다음 표 1 과 같다.

	분석방식	분석범위	여러노드에서의패킷 캡처	호스트 분석가능	웹 기반
MRTG	임관처리	현재상황, 매시,일,주,매달	no	No	yes
ntop	임관처리	현재상황, 매시	no	yes	yes
ethereal	심시간, 임관처리	현재상황	no	yes	no
tcpdump	심시간	현재상황	no	yes	no
snoop	심시간	현재상황	no	yes	no
NNStat	임관처리	지정된 시간 동안	yes	yes	no
UniMon	심시간	현재상황	yes	yes	no
tcplice	심시간	현재상황	no	yes	no
argus	심시간	현재상황	no	No	no
Nfswatch	심시간	현재상황	no	No	no

cwatch	실시간	현재상황	no	yes	no
P.M.S software	실시간	현재상황, 매시,일,주,매달	Yes	Yes	Yes

표 1. 기존의 시스템과 PMMS 의 비교 사항

이 시스템에서는 위에서 소개한 네트워크 모니터링의 장점들을 모아서 기능을 보강하였으며, 실시간 및 패킷의 데이터 분석과 웹 서비스를 연동하여 자세한 정보를 제공한다.

3. 각 모듈 별 기능 및 시스템 구조 설계

3.1 Linux 기능

3.1.1 패킷 캡처 모듈

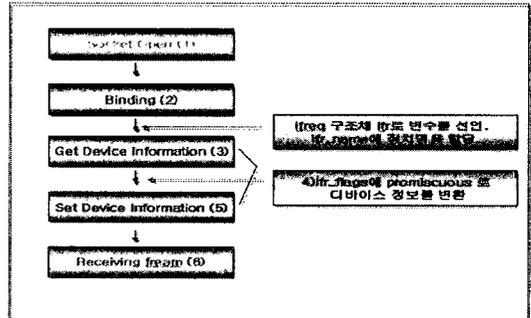


그림 1. 패킷 캡처 모듈

네트워크 상으로 지나가는 모든 패킷을 Ethernet 의 디바이스 정보를 PROMISCUOUS 로 변환하고 바뀐 디바이스 정보를 설정하여 recvfrom()함수로 통하여 이더넷 프레임 정보를 받아 들여서 패킷 캡처 한다. 데이터의 단위는 프레임이며 최대 크기는 1500 byte 이다.

3.1.2 프로토콜·서비스 별 실시간 VIEW 모듈

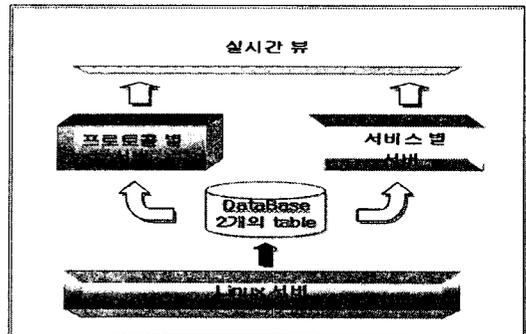


그림 2. 프로토콜·서비스 별 View 구조

리눅스 서버에서 패킷을 캡처하여 네트워크 상의 전달된 패킷의 길이를 데이터베이스에 2 개의 테이블로 나누어 개별 저장하여 프로토콜 및 서비스 별로 실시간으로 그래프로 보여진다.

3.1.3 포트 차단 모듈

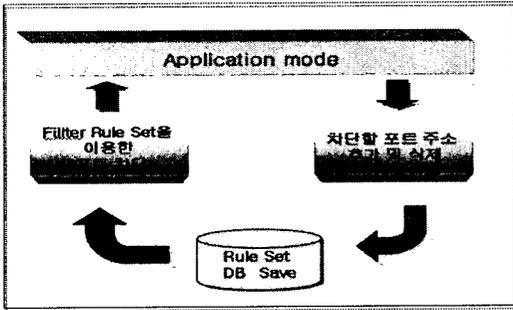


그림 3. 포트 추가 및 삭제 모듈

포트 차단 설정에서 불법적인 목적으로 침입하는 사용자로부터 막기 위해서 사용자가 프로그램에서 차단할 소스 포트 목록을 데이터 베이스에 추가하여 저장된 데이터를 필터 룰을 읽어 차단하게 된다.

3.1.4 Filter Rule 모듈

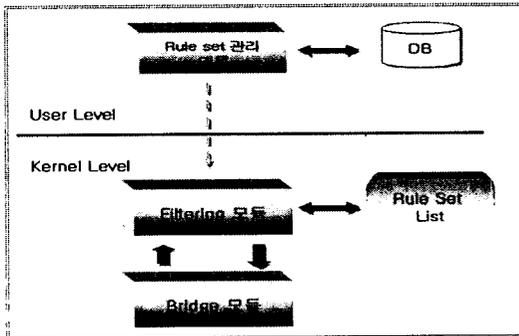


그림 4. Filter Rule 정책 모듈

Bridge 모듈을 통해 지나가는 패킷들은 Filter Rule 의 리스트에 의해 통과 여부를 결정하여 DB 에 저장하고, 정책의 추가 및 삭제는 사용자 프로그램에서 관리가 이루어진다. Filtering 모듈은 NIC(Network Interface Card)의 하드웨어 주소인 MAC 주소와 IP 주소를 통하여 외부에서 공격을 막을 수 있게 된다.

3.2 Web server 기능

3.2. 시간 및 요일·공간 별 패킷 통계치 분석 모듈

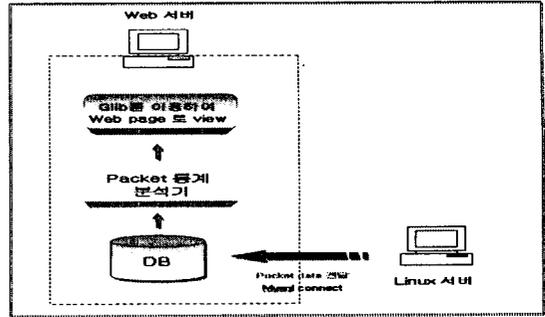


그림 5. 패킷 통계 분석 모듈

리눅스 서버에서 각 패킷의 량을 체크하여 웹 서버의 DB 에 데이터를 전송하여 패킷 분석기를 사용하여 분석한다. 여기서 Glib(그래픽 라이브러리)를 이용 웹 페이지에 GIF, PNG 파일로 뿌려서 보여준다.

3.3 전체 시스템 구조

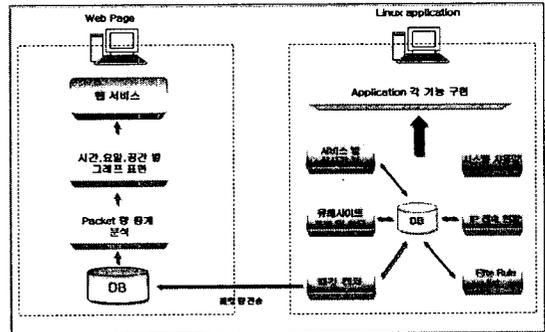


그림 6. PMSS 전체 시스템 모듈 구조

기존의 시스템들은 독립적으로 구현되어 있지만, 이 시스템에서는 web 과 linux 의 연결하여, 실시간으로 네트워크 내에 트래픽 량을 분석하여 그래프로 보여주며, 각 기능을 리눅스 상에서 구현하였다. 웹 서비스에서는 패킷의 최대, 최소 및 평균량을 보여주며, 리눅스상의 응용프로그램은 컴퓨터 시스템의 상태, 방화벽 등의 기능을 수행하게 된다.

4. 구현

1. LINUX APPLICATION

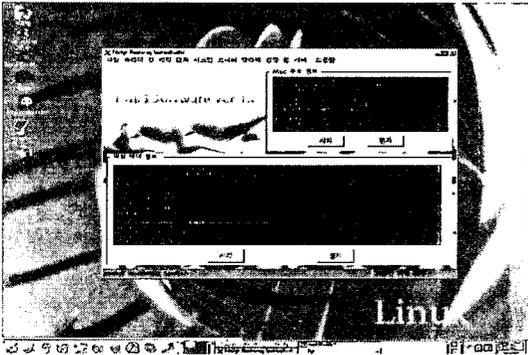


그림 7. PMMS 패킷 모니터링 메인 화면

지금 화면에서 네트워크상의 트래픽을 캡처하여 트래픽의 헤더 및 MAC 주소의 정보를 보여주고 있으며, 트래픽의 량을 서비스 및 프로토콜 별로 분류하여 그래프로 표현하여 사용자들이 알기 쉽게 나타내었다.

기존의 모니터링 시스템과는 다르게 IP 차단, 포트 차단, 필터 룰을 설정할 수 있게 하였으며, 웹 서버에 자료를 전송할 수 있게도 하였다.

2. WEB PAGE

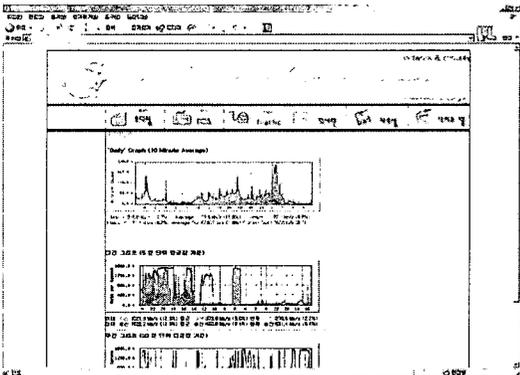


그림 8. 실시간 트래픽 웹 정보서비스 홈페이지

지금 화면은 리눅스 서버에서 데이터 정보를 받아서 DB 에 저장 된 데이터를 통해서 분석하여 Glib(그래픽 라이브러리)를 이용하여 HTML 문서에 뿌려지게 된다. 홈페이지를 이용하는 사용자들에게 보다 많은 정보와 실시간으로 트래픽의 월, 일, 시간 별 사용량 및 기술정보를 제공한다. 그리고 게시판을 이용하여 사용자들이 사용시 불편 및 문의사항을 서비스 향상에 많은 도움이 되도록 한다.

5. 결론 및 향후 과제

본 PMSS 는 웹과 리눅스를 연계로 하여 방화벽 기능 및 모니터링 정보를 서비스하도록 구현 되었다. PMMS 는 일반 다른 모니터링 프로그램과는 달리 웹과 리눅스에

서 서비스를 함께 한다는 점이 다른 점이다. 그리고 웹 서비스에서 요일, 날짜, 시간 별로 서비스하여 보다 자세한 정보를 제공할 수 있다. 리눅스 사용자들은 PMMS 를 이용하여 모니터링이 가능하고, 방화벽 기능으로 침입자들을 막을 수 있는 것이 장점이다.

앞으로의 연구는 지금 현재의 리눅스에서는 사용자가 시스템을 업데이트 하기 어렵다. 이에 업데이트가 보다 쉽게 할 수 있도록, PMMS 프로그램은 필터 룰 및 프로그램을 자동 업데이트 할 수 있게 개선사항이 요구된다.

마지막으로 기능 별로 성능의 향상이 요구되며, 보다 사용자들이 쉽게 이해하도록 프로그램의 설계가 필요하다.

[참고 문헌]

- [1] 강유 역, 리눅스 해킹 퇴치 비법, 에이콘 출판사, 2002.
- [2] 정재은, 유닉스 시스템 프로그래밍, 한빛 미디어, 2002.
- [3] DOUGLAS E. COMER and DAVID L. STEVENS, INTERNETWORKING with TCP/IP CLIENT-SERVER PROGRAMMING AND APPLICATIONS Linux/POSIX Socket Version, PRENTICE HALL, 2001.
- [4] 윤성우, TCP/IP 소켓 프로그래밍, FREELEC, 2003.
- [5] 최연숙, 김재영, 홍원기, “웹 기반의 실시간 인터넷 트래픽 흐름 측정 및 분석”, 포항공과대학교 컴퓨터공학과 분산처리 및 네트워크관리 연구실, 2000.
- [6] 이태용 역, Beginning Linux Programming 2nd EDITON, 정보문화사, 2000.
- [7] 서한수 역, MySQL 시스템 관리와 프로그래밍: 자바, PHP, 펄, C, 파이썬, 한빛 미디어, 2002.