리눅스 기반 실시간 네트워크 침입탐지대응관리 및 감내시스템

李明玉*, 이은미**
*동신대학교 정보통신공학부
**동신대학교 사회과학부
e-mail: mikelee@dsu.ac.kr

Linux Based Real Time Network Intrusion Detection, Protection, Management and Fault Tolerance Security System

Mike Myung-Ok Lee*, Eun-Mi Lee**
*School of Information & Communication Eng., Dongshin University
**School of Social Science, Dongshin University

요 약

이 논문에서는 리눅스 기반VDPM(Virus Detection Protection Management)시스템을 제안하고 개발한 응용SW로 감지, 차단 및 관리 방법을 제시한다. 제안된 LVPM시스템은 첫째특정탐색 및 전체탐색 알고리듬에 의하여 개발된 VDPM시스템은 신종 바이러스까지 탐지하는 모든 종류의 바이러스 탐지(VDPM_hawkeye) 모듈, Virus체크하는 감시 및 Virus체크후 교정, 제거하는 방지(VDPM_medic)모듈, DB를 update하는 기능을 가지는 관리(VDPM_manager)모듈과 원격 DB관리 및 Virus결과 보고 기능(VDPM_reporter) 모듈로 되어 있으며 지능적인 Virus방지 시스템, 둘째 네트워크 패킷을 분석하여 네트워크를 통한 웜 바이러스 탐지 및 대응 시스템과 셋째 네트워크 패킷을 분석하여 네트워크를 통한 네트워크형 악성 소프트웨어 대응 시스템을 포함한 바이러스 보호 통합 시스템을 구현하였다. 더불어 호스트와 네트웍기반의 통합적인 IDS가 방화벽(Firewall)시스템과 연동하여 IDS 단독 차단이 불가능한 공격을 차단하는 소프트웨어 시스템을 개발하는 것이며 관리자가 사용하기 쉬운 GUI환경으로 구현하였고 대규모 분산 네트워크 환경에서 효율적인 리눅스기반 침입탐지방지관리 솔루션을 제시한다.

1. 서론

리눅스는 핀란드 헬싱키대학의 리누즈 토발즈라는 학생이 취미삼아 처음으로 만들었던 운영체제 시스템으로서 GPL(General Public License)에 따라 개발되고 있으며 소스코드는 누구나 자유롭게 사용할 수 있다. 그러나 자유로운 것만큼 외부로부터 쉽게 공격을 받을 수 있고 이러한 문제는 앞으로 네트워크를 통한 인터넷 사용자가 엄청나게 증가함에 따라 그리고 인터넷 접속 가능한 차세대 이동통신 휴대폰이나 PC나 무선단말기에도 해킹(혹은 바이러스)라는 공격으로 더욱 빠르고 전세계적인 넓은 지역으로 전파되는 위험성이 증가될 전망이다. 한국정보보호센터에서 처리한 해킹 사고를 운영체제별로 분류가 가능한 경우 약 절반 이상의 시스템이 리눅스였으며, 리눅스 계열에서는 90% 이상이 리눅스에서 발생한 해킹 사고였다. 국내외적으로 많은 피해를 입었던 DDoS(Distributed Denial of Service)도 결국엔 일부 취약한 기계들이 사전에 해킹을 당해 이용된 것이다. 또한 최근 급속도로 증가하고 있는 인터넷 쇼핑몰 및 개인 운영 서버들이 리눅스 플랫폼 기반으로 만들어지고 있음을 볼 때, 리눅스 보안 관리에 대한 노력이 더욱 절실하게 요구되고 있다. 이 논문에서는 리눅스 기반 VDPM(Virus Detection Protection Management)시스템인 LVPM(Linux-Based VDPM)을

제안하고 개발한 응용SW로 감지, 차단 및 관리 방법을 제시한다.

2. 리눅스 보안 및 LVPM

리눅스가 보안상 문제가 되는 이유는 먼저 OS내부 구조가 완전히 공개되어 있어 리눅스 커널(kernel)은 누구나 소스를 구해서 분석할 수 있다는 점이다. 또한 가격이 저렴하고, 성능이 뛰어나고 사용방법이 쉬워짐에 따라 리눅스 사용자의 급속한 증가를 가정왔다는 점이다. 그러한 장점아닌 단점으로 인하여 보안 구멍이 발견되면 그것을 이용한 공격도구는 리눅스용이 가장 먼저 만들어 진다는 점이다[1]. 리눅스 혹은 유닉스 바이러스는 기존 윈도우나 DOS형태의 바이러스와 구현 방법이 유사하며 커널(Kernel)의 함수를 이용하여 감염되는 경우가 많으며 관리자 권한이 있는 경우는 원할하게 작동되고 있다. 커널 관련 보안 기능은 IP 패킷 수준에서 걸러내기(패킷 필터링), 매스커레이딩, NAT 지원과 리눅스 커널의 버전업에 따른 패킷필터링 툴의 변화등이 있다. 체계적인 정책과 룰을 통한 강력한 방화벽 구축 및 보안 강화가 가능하다.

이러한 리눅스 바이러스 유형은 트로이 목마, 백도어 공격이 있는데, 기존의 프로그램이나 스크립트가 실행될 때 허가되지 않은 행위를 할 수 있는 숨겨진 프로그램이나 쉘 스크립트를 이용한 형태와 리눅스 시스템 자체의 버그나 설정상 취약점을 이용한 해킹 기법인 웜(Worm) 형태가 있는데 이는 다른 시스템에는 직접적인 영향을 미치지 않고 기억장소 내에서 자기 자신을 계속적으로 증식하는 프로그램으로 네트워크를 통해 대규모로 자동 전파된다는 점이다[1][2]. 통신정보보호기술의 한 부류인 서비스 차원인 안티바이러스와 침입차단시스템의 본 연구는 리눅스 응용으로 VDPM의 절차는 네트워크를 통한 바이러스를 탐지한 후에 네트워크 데몬에 의한 패킷 흐름도를 감시하여 DB에 저장하여 관리하는 시스템(그림 1)이다.

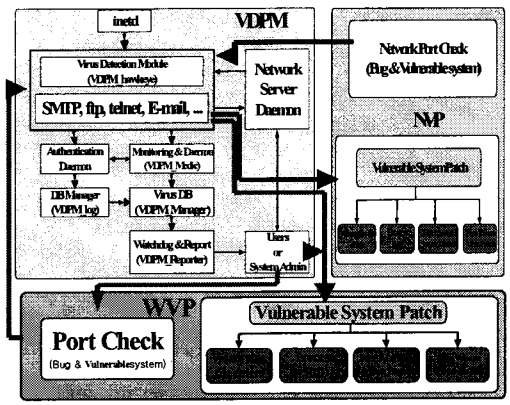


그림 1. LVPM 시스템 구성도

현재 정보보호 기술은 미국이 전세계의 50% 이상을 차지하고 있으며 미국 제품 시장은 본 연구에서 주장하는 바이러스 탐지, 침입차단시스템 및 인증 분야가 주도하고 있다[3]. 이러한 제품 중의 하나가 본 연구가 제안하는 VDPM시스템이다. 부분별로 요약하면 아래와 같다.

■Monitoring System Calls : File open, Write, delete 및 Append와 같은 File관련 System을 Call을 감시하고 문제점을 log 파일로 기록을 남기도록 설계

■Virus판단 여부 : Virus pattern을 Normalize시켜 수치화된 결과값에 근거하여 Virus여부를 판단

■Virus차단 방법 : 모든 ELF파일 체크하여 DB로 관리하고, 정기적인 점검이 필요하다. 특히 ELF파일들이 변경될 때마다 DB Manager에게 알려주는 방법: - Linux : Firewall로 모든 외부traffic을 차단하든지 혹은 Linux Router를 사용하여 ICMP기반이나 Spoofing으로 차단

3. 바이러스 방지 시스템 GUI구현

현재 국내의 정보보안관련 기술개발은 매우 낙후되어 있는 실정이며, 해외 선진국에서 개발된 사용제품들이 국내 업체를 통해 수입되어 보급되는 것이 대부분이다. 국내에 자체적으로 개발되고 있는 기술분야는 상업적 투자가치가 큰 Rule-based 기반의 침입차단시스템 관련기술에 거의 편중되어 있어 침입탐지시스템의 개발로 안전한 시스템 구축이 필요하다. 따라서 본 연구에서는 Process-based인 Host 기반 및 네트워크 기반의 침입탐지 시스템을 제시한다. 기본적으로 침입탐지 시스템은 방화벽을 통과한

외부침입자 뿐만 아니라 내부 사용자의 불법적인 사용, 남용, 오용행위를 탐지하는 목적으로 개발하였고 탐지 후 방지 및 관리하는 종합적인 보안 시스템이고 통계적인 침입정보와 지능적인 탐지, 침입 위험 수위에 따라 5단계 레벨을 구분하여 위험성 통보하도록 구현하였다[4]-[5]. 개발 환경은 Redhat Linux의 kernel 2.4. 버전 이상에서 C++언어를 사용하였고, Glade GUI환경 툴을 사용하여 관리자가 사용하기 쉬운 GUI로 구현하였다. 특히 고속 실시간 침입탐지를 위하여 동적 샌드박싱(sandboxing) 알고리즘 [10]-[15]적용 하였고 임베디드 리눅스용 바이러스[16][17] 모듈도 통합하였다. 구현 현황은 아래 그림2, 3과 4에서 보이는 것처럼 구체적인 설계 과정인 프로그래밍 결과이다.

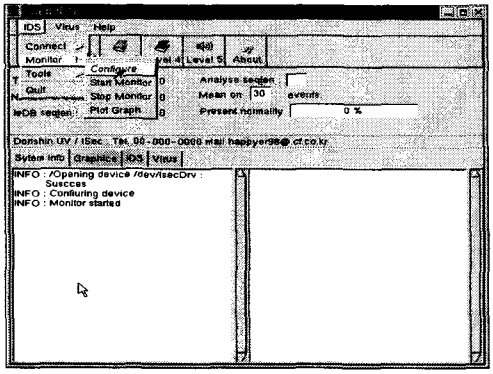
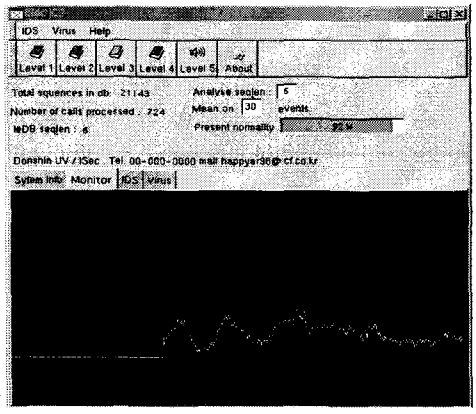
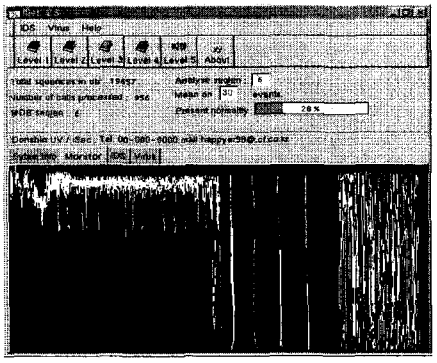


그림 2. Host/Network기반 모듈 및 GUI환경 개발(동작화면)

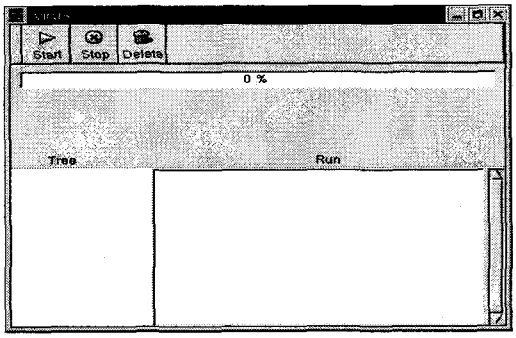


(a)

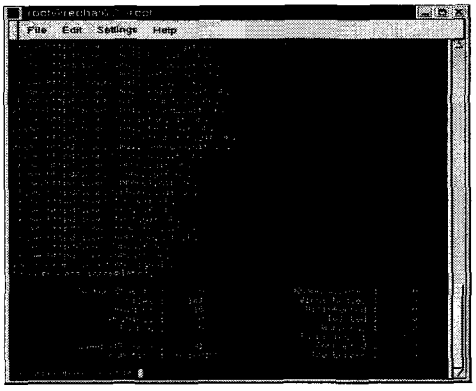


(b)

그림 3. 침입 탐지 결과 및 감내 결과.
(a)침입탐지결과 (b)비정상행위 대응 결과



(a)

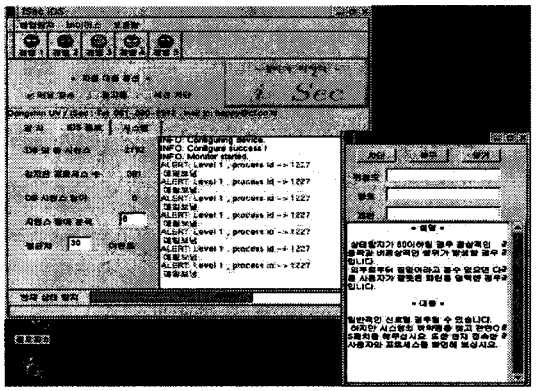


(b)

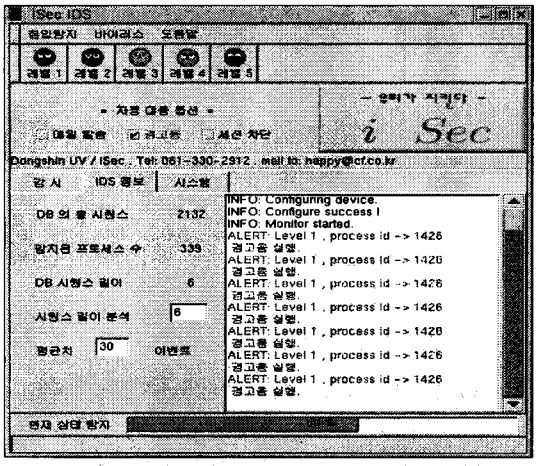
그림 4. 바이러스 탐지 및 보호 결과. (a)GUI환경
(b)바이러스탐지 및 보호 결과

또한 침입탐지시 대응(반사, 차단, 메일발송, 경고음 발생등)에 대하여 침입수준에 따라 자체적인 레벨링 등급을 5단계로 나누에 침입탐지수준 구분하여 GUI 환경하에서 그림 5처럼 구현하였고 침입탐지 시스템

에서는 호스트기반의 탐지와 네트워크 패킷을 이용한 탐지를 함께 적용할 수 있는 보안 솔루션이다.



(a)



(b)

그림 5. 침입탐지시 대응 결과. (a)메일발송
(b)경고음 발생

4. 결론

특정탐색 및 전체탐색 알고리듬에 의하여 개발된 리눅스 기반LVPM시스템을 제안하고 개발한 응용SW로 감지, 차단 및 관리 방법을 제시한다. 그 중 VDPM시스템은 신종 바이러스까지 탐지하는 모든 종류의 바이러스 탐지(VDPM_hawkeye)모듈, Virus 체크하는 감시 및 Virus체크후 교정, 제거하는 방지(VDPM_medic)모듈, DB를 update하는 기능을 가지는 관리(VDPM_ manager)모듈과 원격 DB관리 및 Virus결과 보고 기능(VDPM_reporter) 모듈로 되어 있으며 고속으로 모든 비정상 바이러스 파일을 탐지하여 정상적인 상태로 회복시켜 안전하게 관리하는 시스템이다. 네트워크 패킷을 분석하여 네트워크를 통한 웜 바이러스 탐지 및 대응 시스템과 셋째 네트워크 패킷을 분석하여 네트워크를 통한 네트워크형 악성 소프트웨어 대응 시스템을 구현하여 바이러스 보호 통합 솔루션을 제안 하였다. 마지막으로 침입수준에 따라 자체적인 레벨링 등급을 5단계로 나누에 침입탐지수준 구분하였고 최근 핫이슈가 되고 있는 리눅스 바이러스 탐지 엔진 탑재하여 관리자가 사용하기 쉬운 GUI로 구현한 시스템을 제시하였다.

참고문헌

[1] 최홍진, "[리눅스 시큐리티 강좌 1]리눅스의 시스템 보안 및 취약점", *Onthenet*, 2001년 4월호.

[2] 김판구, "컴퓨터 바이러스의 이해와 대응 방안", *IDEC 보안알고리즘 및 VLSI설계 강좌*, pp. 59-99, 2001년 8월.

[3] MACRO Technology, "MACRO Security Report", 2001년 5월, 제 1호.

[4] 김판구, "리눅스 상에서의 ELF 파일 바이러스 진단 및 차단 시스템", 리눅스 보안 연구 센터 Workshop 프로그램, 전남대학교, 2001년 5월.

[5]http://www.certcc.or.kr/paper/incident_note/2001/in2001_010.html

[6]http://www.certcc.or.kr/paper/incident_note/2001/in2001_009.html

[7] http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml #8

[8] D. Farmer and W. Venema, "Improving the security of your site by breaking into it,"

[9] T. Lane and C.E. Brodly, "An application of machine learning to anomaly detection," 20th NISSC, 1997.

[10] T.F. Lunt, "Automated audit trail analysis and intrusion detection: A survery," *Proc. of 11th National Computer Security Conf.*, 1998.

[11] 한국정보보호센터, *호스트기반 침입탐지 시스템 개발에 관한 연구*, 1998.

[12] H. Debar, M. Dacier and A. Wespi, "Towards a taxonomy of intrusion-detection system," IBM Research Division, Zurich, Switzerland, July 1998.

[13] P. Rolin, L. Toutain and S. Gombault. "Network security prob. in CCS'94," *ACM Conf. Computer and Communication Security*, pp. 229-240, Nov. 1994.

[14] D. Farmer, Cops overview, available from http://www.trouble.org/cops/overview.html, May 1993.

[15] D. Farmer and E. Spafford, "The cops security checker system," *Proc. Summer USENIX Conf.*, pp. 165-170, Anaheim, CA, June 1990.

[16] D.R. Safford, D.L. Schales, D.K. Hess, "The tamu security package: an ongoing response to internet intruders in an academic environment," *USENIX Security Symp.*, pp. 91-118, Santa Clara, CA, October 1993.

[17] D. Farmer and W. Venema, "Improving the security of your site by breaking into it,"