다단계 구조를 가진 침입 탐지 및 방어 시스템의 구현

민욱기°, 장혜영, 최종천, 조성제
단국대학교 컴퓨터과학전공
wearemin@naver.com, chenil99@hanmail.net, godofslp@dankook.ac.kr, sjcho@dankook.ac.kr

Implementation of an Intrusion Detection and Prevention System with Multi-level Structures

Ukki Min°, Hyeyoung Chang, Jongcheon Choi, Seongje Cho
Dept. of Computer Science and Statistics, Dankook University

요 약

본 논문에서는 네트워크 포트 기반의 오용침입 탐지 기능 및 센서 객체 기반의 이상침입 탐지 기능을 갖춘 리눅스 서버 시스템을 제안한다. 제안한 시스템은 먼저 정상적인 포트 번호들 및 알려진 공격에 사용되고 있는 포트 번호들을 커널에서 동적으로 관리하면서, 포트 할당 시마다 감사로그를 기록하며 공격에 사용되는 포트인 경우에는 접속을 불허하여 침입을 방어한다. 알려지지 않은 이상침입 탐지를 위해서는 주요 디렉토리마다 센서 파일을, 주요 파일마다 센서 데이터를 설정하여 센서 객체가 접근될 때마다 감사로그를 기록하면서, 이들 센서 객체에 대해 불법적인 접근이 발생하면 해당 접근을 불허한다. 본 시스템은 네트워크 기반의 침입 탐지 및 호스트 기반의 침입 탐지 등 다단계로 구축되며 특정 침입들을 미리 예방할 수도 있다.

1. 서 론

침입 탐지 시스템(IDS: Intrusion Detection System)은 네트워크 또는 호스트에서 일어나는 사건 및 사용자 행위들을 감시하면서 침입 여부를 파악하기 위해 그 사건들을 분석하고 침입에 대응하는 시스템이다[1]. 즉, IDS는 시스템의 비밀성, 무결성, 가용성, 인증 등을 위협하는 모든 상황을 탐지하는 것을 목표로 하며, 침입자의 불법적인 사용뿐만 아니라 합법적인 사용자의 오용이나 남용도 발견할 수 있다[2]. 보통 IDS는 원시 데이터의 소스(탐지 영역)에 따라 호스트 기반 방식과 네트워크 기반 방식으로 분류되며, 침입탐지 방법(유형)에 따라 오용탐지(misuse detection)와 이상탐지(anomaly detection)로 분류된다[3].

본 논문에서는 리눅스 서버 상에서 센서 객체 기반의 이상침입 탐지 기능에 네트워크 포트 기반의 오용침입 탐지 기능을 갖춘 침입탐지 및 방어 시스템의 구현에 대해 기술한다. 우리는 이전에 센서객체(센서 파일 및 센서 데이터 포함)라는 일종의 덫을 이용한 이상침입탐지시스템을 제안하였다[2]. 그 시스템에서, 임의의 지역/원격 프로세스가 센서객체를 건드리면 감사로그를 생성하게 되고 인가되지 않은 접근일 경우에는 침입으로 판단하여 이에 대응하게 하는 기법으로, 알려지지 않은 침입탐지를 위해 호스트 수준 및 네트워크 수준에서 이중으로 구현하였다. 이 기법에 추가적으로 본 논문에서는, 네트워크 포트 기반의 오용침입 탐지 기능을 확장 구현한다. 즉, 정상 포트들 및 공격에 사용되는 포트들을 커널에서 동적으로 관리하면서 새로운 포트가 열릴 때마다 감사로그를 생성하며 불법 연결일 경우 접속을 불허한다. 제안한 기법을 LKM(Loadable Kernel Module) 기능을 사용하여 구현한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 알아보고, 3장에서는 시스템의 구성에 대해 기술한다. 4장에서는 시스템의 구현 및 실험에 대해 살펴보고, 5장에서는 결론을 짓고 향후 연구에 대해 언급한다.

2. 관련 연구

2.1 센서객체를 적용한 침입탐지시스템

센서객체를 이용한 침입 탐지 시스템(SIDS: Sensor based IDS)은 호스트 기반 및 네트워크 기반의 침입탐지시스템이다[2]. SIDS에서 센서는 주요 디렉토리를 보호하기 위한 "센서 파일" 객체와 주요 파일을 보호하기 위한 "센서데이터" 객체를 의미한다. "센서객체"는 침입자를 잡기 위한 일종의 덫으로 인가되지 않은 누군가에 의해 센서객체가 건드려지게 되면 침입 또는 이상행위라고 판단되어, 적절한 대응을 하게 된다. 호스트 기반에서는 각 센서객체 접근시마다 감사 자료를 생성하고 인가되지 않은 프로세스를 종료시킨다. 네트워크 기반에서는 트래픽을 분석하여 센서객체를 전송 여부를 조사하여 침입이라고 판단될 경우 추적정보를 기록 후 접속을 차단한다[1][2]. SIDS는 새로운 유형의 이상침입을 탐지하는 기법으로 볼 수 있으며, 미리 잘못된 행동패턴을 알고 있는 경우를 위한 오용탐지기법 대한 고려가 충분하지 않다.

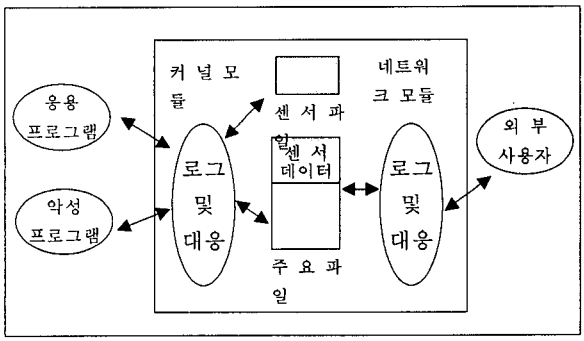
2.2 LKM (Loadable Kernel Module)

단일체(monolithic) 커널 구조인 리눅스에서는 커널 기능을 손쉽게 추가/삭제하기 위해 적재가능한 커널 모듈(LKM)을 제공한다. 모듈은 필요할 때 마다 업로드와 다운로드가 가능하기 때문에 시스템을 재부팅 할 필요 없이 커널의 기능을 확장할 수 있으며, 이로 인해 메모리를 효율적으로 사용할 수 있다. 잘못된 모듈로 커널이 정지할 수 있다는 단점이 있지만, 신중히 작성하면 많은 장점을 가진다. 또한 모듈은 로드 된 후에는 커널 코드와 동등하게 실행되기 때문에 성능의 저하 없이 효율적으로 작동가능 하다[2][4].

3. 시스템 설계

3.1 시스템 개요

본 논문에서는 리눅스 시스템에서 다양한 공격 유형에 좀 더 효과적으로 대응할 수 있는 다단계 구조를 가지는 침입탐지 시스템을 제안한다. 즉, 센서기반의 이상침입탐지 기법에 네트워크 포트 기반의 오용탐지 기법을 추가하여 개선한 침입 탐지 시스템을 구현한다. 기존에 제안된 SIDS(Sensor based IDS)의 구성은 (그림 1)과 같으며, 이 시스템의 주 목적은 알려지지 않은 이상침입 탐지에 있었다. 이 연구를 바탕으로 본 논문에서는 공격의 행동패턴을 알고 있는 경우를 위한 오용탐지 기법을 추가하여 통합하였다. 확장된 기능의 주요 목적은 포트 관리를 감시하면서 이미 알려진 웜과 바이러스, 트로이 목마와 같은 악성 프로그램이 사용하는 특정 포트를 차단하는 것이다.

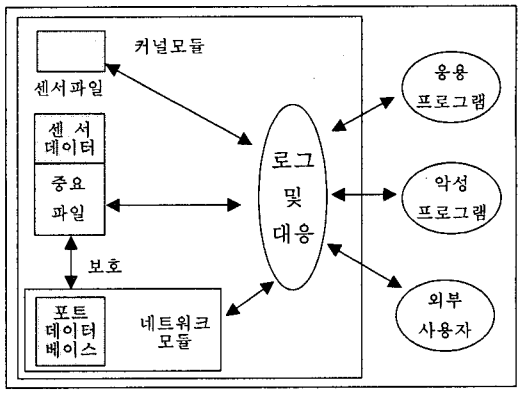


(그림 1) SIDS 시스템 구성도

3.2 개선된 시스템 구성

본 시스템에서 제안하는 구성은 (그림 2)와 같다. 먼저, 알려지지 않은 유형의 이상침입을 탐지하기 위해 주요 디렉토리마다 센서파일을, 주요 파일마다 센서데이터를 설정하여 이들 센서를 통해 접근을 제어한다. 주요 파일의 경우, 호스트 내부의 접근은 허용하되 감시하며 네트워크를 통한 외부 유출은 네트워크 트래픽 분석을 통해 차단하고 추적한다. 센서들은 특권 프로세스에 의해 동적 관리되며, 센서의 주 목적은 정보의 접근제어 및 외부로의 불법유출 예방이다.

이에, 추가로 네트워크 포트 관리모듈이 통합되어 있어, 포트가 할당될 때마다 관련 정보를 로그로 남기며 악의적인 프로그램에서 사용되는 포트가 접근될 때는 그 포트를 차단한다. 체계적인 방법을 통해, 웜, 바이러스, 백도어, 트로이목마 등의 악성 프로그램이 주요 파일을 불법으로 접근할 때, 또한 포트를 불법으로 사용하려할 때 효과적으로 대응할 수 있으며, 따라서 침입을 예방하는 효과도 있다.



(그림 2) 시스템 구성도

(그림 2)의 포트 데이터베이스에는 정상포트 번호들과 기존에 알려진 악성 프로그램들이 사용하는 불법포트 번호들을 분류하여 관리한다. 이 포트 데이터베이스는 중요한 파일로 불법 사용자에 의해 수정/삭제되지 말아야 하며 외부로 유출되지 않아야하므로 "센서데이터"로 보호 받게 구성한다.

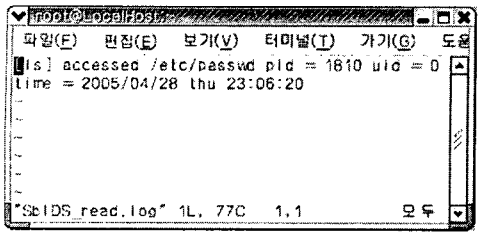
4. 구현

4.1 실험 환경

본 시스템을 구현하기 위해 펜티엄4 1.7GHz기반의, Linux Redhat 9, 커널 버전은 2.4.22를 사용하였다. 컴파일러는 gcc v3.2.2를, 커널 모듈에서 사용되는 라이브러리 함수로는 klib를 이용하였다[5]. 손쉬운 설치와 효율적 모듈관리를 위해 LKM으로 구현하였으며, 시스템 콜 가로채기(hooking)방법을 이용하였다.

4.2 호스트 기반 침입탐지 모듈 및 대응

각 프로세스의 센서 접근을 감시하고 정보의 접근제어를 위해 sys_open(), sys_read(), sys_close(), sys_fork(), sys_unlink() 등의 커널 내부 함수를 수정하였으며, "센서"를 접근했을 때 실행된 명령의 절대경로, PID, 사용자ID, 접근시간 등을 기록한다. "센서파일"은 루트권한의 프로세스라도 접근을 했다면 로그를 기록한 다음, 인가된 프로세스가 아니면 해당 프로세스를 종료시킨다[2]. 센서데이터가 접근되면, 해당 프로세스 정보를 로그로 남기고 네트워크 기반 침입탐지 모듈과 협력하여 대응한다. (그림 3)은 루트사용자가 passwd 파일을 접근하였을 때, 기록된 SbIDS_read 로그 파일의 예이다.



(그림 3) "센서 데이터"의 로그 (SbIDS_read.log)

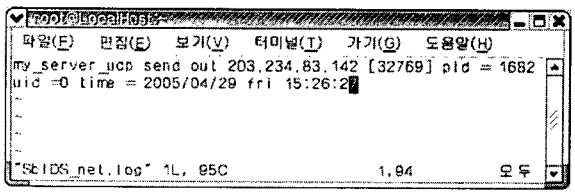
4.3 네트워크 기반 침입탐지 모듈 및 대응.

서버에서 포트 할당을 위해 bind()가 호출되면 sys_socketcall()에 의해 sys_bind()가 호출된다. 따라서 포트 감시 및 차단을 위해 sys_bind() 함수를 수정하였다. sys_bind()는 TCP와 UDP 모두 sys_bind()를 사용하므로 sys_socketcall()을 후킹하여 원래의 sys_bind() 대신에 새로 구현된 NIDS_sys_bind()가 실행되게 하였다(그림 4).

```
NIDS_sys_bind() {
   if(새로운 포트번호가 포트리스트에 있으면 ) {
        로그를 남기고 원래의 sys_bind는 실행금지.
   }else {
        원래의 sys_bind가 실행.
   }
}
```

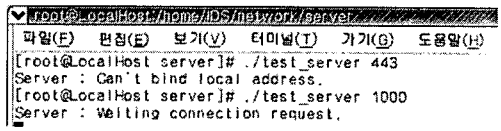
(그림 4) NIDS_sys_bind() 의사코드

알려지지 않은 공격에 의해 주요 정보가 네트워크를 통해 유출되는 것을 막기 위해 sendto() 함수가 수정되어, 센서데이터가 포함된 패킷이 감지될 경우 로그를 남기고 차단하게 하였다. 센서데이터가 포함된 파일 유출 여부를 확인하기 위해 my_server_udp라는 네트워크 프로그램을 작성하여 실행하였다. 관련 로그가 (그림 5)에 나타나 있으며, sys_read()에서 생성된 로그 파일과 함께 분석하여 PID 값을 확인하여 정확한 유출 경위를 확인할 수 있다.

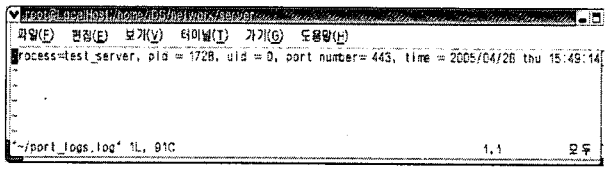


(그림 5) SbIDS_net.log 파일에 기록된 내용

포트기반 침입탐지를 위해 (그림 6)과 같이 test_server라는 네트워크 서버 프로그램을 작성하여 클라이언트의 접속을 기다리게 하였다. 만약, 1000번 포트는 정상 포트이고, linux /slapper-A 웜이 443번 포트를 사용한다면[6], 웜이 443번 포트를 열려고 할 때, 포트정보 데이터베이스에 443번이 불법 포트로 등록되어 있으므로 443번 포트는 거절됨을 확인할 수 있다. (그림 7)은 포트 데이터베이스에 불법 포트로 등록된 포트가 접근될 때, port_log.log에 기록된 내용을 보여주고 있다. 기록되는 정보는 실행된 명령, PID, UID, 접근 시간 등이다.



(그림 6) 간단한 TCP/IP 서버프로그램 테스트



(그림 7) port_logs.log 파일에 기록된 내용

포트 데이터베이스 파일은 커널 수준에서 관리되며, 정상적인 포트번호와 알려진 공격에 사용되고 있는 포트번호들을 동적으로 유지한다. 데이터베이스에 등록되어 있지 않은 포트 번호가 요청될 경우, 잠정적인 위협으로 간주하고 로그를 남겨 관리자에 통보하도록 구현 중에 있다. 또한, 제안한 침입탐지 및 방어 모듈로 인해 유발되는 성능 상의 오버헤드를 측정 중에 있다.

5. 결론 및 향후 연구

본 논문에서는 오용 및 이상 침입탐지 기법과 호스트 및 네트워크 기반의 침입탐지 기법을 제안하고 프로토타입을 구현하였다. 즉, 새로운 유형의 침입을 탐지하기 위해서는 센서(덫) 기반의 모듈을, 알려진 악성 프로그램들에 의한 침입을 탐지하기 위해서는 포트 기반의 모듈을 구현하여 통합함으로써 다단계 구조를 가지는 침입 탐지시스템을 구축하였다. 침입탐지 모듈은 LKM 기법을 이용하여 간단히 설치가 가능하도록 하였다.

참고문헌

[1] 장철연, 조성제, 최종무, "LKM을 이용한 센서기반 침입탐지 및 보호 시스템, 한국정보과학회 2003 가을 학술발표논문집(I), 제 30권 2호, pp.694-696, 2003. 10.

[2] 장철연, 조성제, "LKM을 이용한 센서기반 침입 탐지 시스템", 단국대 석사학위논문, 2003.

[3] 김윤정 "ISO/IEC IDS 기술 표준 동향" (http://www.kisa.or.kr) 2001.

[4] Peter Jay Salzman "The Linux Kernel Module Programming Guide" 2001.

[5] 이호, Linux Kernel Library Project, http://linuxkernel.net

[6] http://www.sophos.com