리눅스 정보보안 S/W 'Prajna'

Kernel 기반 공개 보안 솔루션 강력한 OS 보안기능 선보여

최근 Linux 시스템의 사용이 급격히 증가함에 따라 Linux시스템에서의 보안이 큰 문제로 대두되고 있으며 그에 대한 대응책으로 침입탐지 및 방지를 위한 여러 가지 방안들이 나오고 있다. 하지만 응용 소프트웨어 또는 네트워크 레벨에서 구현된 어떠한 종류의 보안 솔루션도 컴퓨터 운영체제(OS) 자체의 보안이 갖춰지지 않은 상태에서는 사상누각에 불과하다. Prajna는 이러한 문제를 근본적으로 해결하고자, 가장 기본적 보안단계인 OS차원에서 보안기능을 구현하는 프로그램(Security Kernel Module)이며, Linux 시스템의 핵심인 커널을 기반으로 운영체제 차원의 강력한 보안기능을 수행한다. 이 제품과 유사한 기존 제품들은 모두 상업용이나 Prajna는 취약한 국내보안 현실과 공개 보안소프트웨어 개발의 활성화를 위해 오픈프로젝트로 진행되고, 소스와 결과물들을 모두 인터넷상에 공개한다. 현재 Anti Hacking기능과 시스템자원의 강제적 접근제어, 모니터링, 스텔스 기능등이 있으며 앞으로 꾸준히 개발하여 뛰어난 기능을 갖추고 다양한 OS를 지원할 계획이다.

Prajna

정보통신부장관상

1. 작품명 : Prajna (Linux Kernel Security Module)

2. 제작자 : 홍정우

대표자 : 홍정우
주소 : (138-770) 서울시 송파구 잠실본동 우성4차 APT 106-1202호
전화 : 02) 422-0477
email : mithorse@hananet.net

3. S/W 요약설명

Prajna는 커널기반의 보안 프로그램(Security Kernel Module)으로 해킹사고를 미연에 방지하고 중요정보를 보호하며 시스템 자원을 통제하고 관리하는등 운영체제 차원에서 보다 안전하고 강력한 보안기능을 수행하는 보안 프로그램이다.

3.1 개발 배경

1) 기존 어플리케이션 레벨, 네트워크 레벨 보안 소프트웨어의 한계

- IDS의 문제점
  - 침입을 탐지하는 도구일 뿐 방어책은 될 수 없다.
  - 해커들이 탐지를 피해갈 수 있는 새로운 기술을 끊임없이 고안하고 있다.
  - 새로운 공격기법을 탐지해내기 위해 끊임없는 업그레이드가 필요하며,
    이에 따른 비용 증가부담이 막대하다.

- 방화벽의 웹 서비스 문제점
  - 인터넷 서비스를 위해 방화벽에 80번 포트의 접속을 허용한 경우
    정상적인 HTTP 트래픽에 숨겨진 공격을 차단하는 것이 사

실상 불가능하다.

2) 국내 보안현실의 한계

- 기존 국내 공개 보안 소프트웨어 개발의 미약
  - 기존에 국내에서 자체개발, 공개된 소프트웨어가 매우 드물다.

- 상용보안제품의 비용부담으로 인한 중소기업 보안시스템의 한계

3.2 시스템 개요

최근 Linux 시스템의 사용이 급격히 증가함에 따라 Linux시스템에서의 보안이 큰 문제로 대두되고 있으며 그에 대한 대응책으로 침입탐지 및 방지를 위한 여러 가지 방안들이 나오고 있다.

하지만 응용 소프트웨어 또는 네트워크 레벨에서 구현된 어떠한 종류의 보안제품(방화벽, 침입탐지도구 등) 도 컴퓨터 운영체제(OS) 자체의 보안이 갖추어지지 않은 상태에서는 사상누각에 불과하다.

따라서 Linux 시스템의 핵심인 **커널을 기반**으로, **운영체제 차원의 강력한 보안기능**을 설계 및 구현하였다.

3.3 구조 및 기능

Prajna는 Kernel Module로 구성되어 있으며, 부적절한 서비스 요청이나 시스템 자원과 권한 남용 등으로 침입을 시도할 경우 이를 시스템 호출 수준에서 감지, 차단하는 **Anti Hacking** 기능과 중요정보에 대한 유출 파괴 변조등을 예방하기 위한 시스템 자원의 **강제적 접근 제어** 기능, 의심의 여지가 있거나 침입에 사용될수 있는 프로그램의 시스템 호출을 추적하고 감시하는 **모니터링** 기능, 감시중인 것을 알수 없도록 정보를 은폐하는 **스텔스** 기능 등으로 이루어져 있다.

1) Anti Hacking

핵심 기능으로, 주요 시스템 호출을 커널수준에서 관리하고, 부적절한 서비스 요청이나 시스템 자원과 권한 남용으로 침입을 시도시, 수행환경을 검사하고 차단함으로 해커의 공격을 원천봉쇄한다.

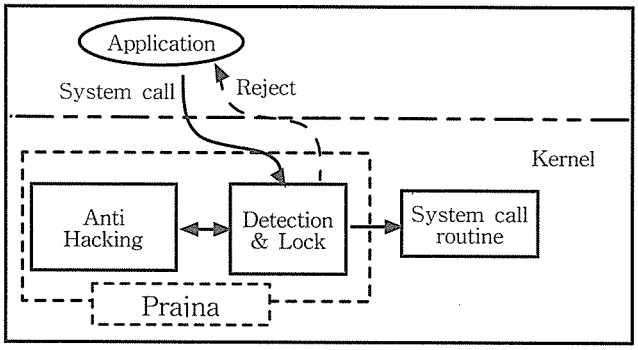

그림1. 침입시도 감지시 원천봉쇄 (출처:LIDS)

2) 모니터링 (실시간 침입탐지)

시스템의 서비스 수행상황과 프로세스, 파일, 사용자의 모든 operation history를 자세히 기록하여 실시간으로 추적, 감시한다.

예)

Nov 5 23:45:05 localhost kernel: Prajna - Linux kernel security module installing...

Nov 5 23:45:08 localhost kernel: EXECVE(uid=0)[741]: /bin/ls --color=tty

Nov 5 23:45:09 localhost kernel: EXECVE(uid=0)[742]: /usr/bin/id

Nov 5 23:45:10 localhost kernel: KILL(uid=0)[754]: called

Nov 5 23:45:13 localhost kernel: EXECVE(uid=0)[766]: /usr/bin/wc -c

Nov 5 23:45:13 localhost kernel: EXECVE(uid=0)[769]: /bin/stty erase \177

Nov 5 23:45:21 localhost kernel: OPEN(uid=0)[1186]: /lib/i686/libc.so.6, flags = 0, mode = 8

Nov 6 08:47:31 localhost kernel: EXECVE(uid=500)[1008]: /usr/bin/w

Nov 6 08:47:32 localhost kernel: EXECVE(uid=500)[1009]: /bin/ls --color=tty -l --color=tty

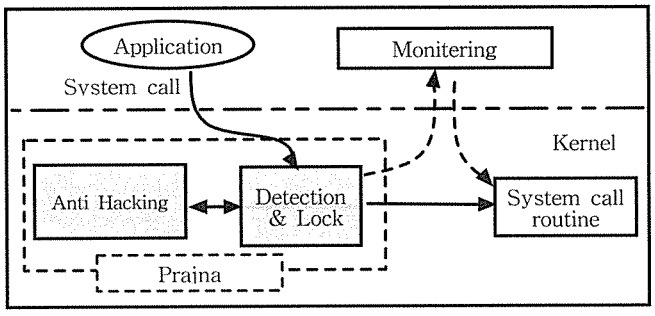

그림 2. 어플리케이션에서 서비스를 요청함 (출처:LIDS)

3) 시스템 자원의 강제적 접근제어

중요정보에 대한 유출, 파괴, 위· 변조 등 불법행위 방지와 더불어 중요 데몬 프로그램에 대한 불법 종료 방지 등을 수행한다.

4) 스텔스 기능 지원

감시중인 것을 알수 없도록 정보를 은폐한다.

3.4 메뉴 구성도

① Default
기본적인 보안셋팅 옵션

② Select Option - 각각의 기능을 On
- **Anti Hacking (Select Rule)**
- **Lock (File, Process)**
- **Monitering (Select Rule)**
- **Stealth**

예)
$ ./prajna

Prajna Linux kernel security module v0.1

Usage:
prajna [-mlchpudH] option ...

-m [command] [file] [suid] monitering specificy behavior.
-l [file filename], [pid id] locking file or process.
-c check environ variable.
-h print thie message
-p ptrace off
-d default option (ptrace off, command log, anti-hacking)
-u unloading this module
-w web anti hacking
-H [hide] [unhide] hide/unhide this module

3.5 주요 특징

1) 차별성
- 기존의 어플리케이션-레벨 보안 소프트웨어의 한계점을 벗어난 운영체제(OS) 차원의 보안시스템 (Security Kernel Module)

2) 안정성
- 기존 Kernel을 바탕으로 리눅스의 강력한 안정성을 유지하도록 구현함

3) 효율성
- 커널의 효율성을 최대한 유지하도록 구현함
- 원하는 기능만 사용가능하며 장치, 분리가 용이함

4) 독창성
- 국내 최초 공개 커널보안 프로젝트

5) 신뢰성
- 중요한 정보 - Lock 기능과 자체 stealth 등을 구현하여 신뢰를 높임

3.6 향후 목표

앞으로 꾸준히 공개 개발하여 다양하고 세련된 기능으로써 세계적인 기술력을 갖추고, 뛰어난 보안소프트웨어로 자리매김 하도록 노력할것이다.

또한 차후 다양한 OS(BSD, 솔라리스 등)를 지원할 계획이다.

4. 사용 또는 개발언어, TOOL

Kernel 2.4.x , Gcc

5. 사용시스템

사용OS	Redhat 7.1 , Kernel 2.4.x