관리자 인증 강화를 위한 추가적인 패스워드를 가지는 보안커널모듈 설계 및 구현

김 익 수† · 김 명 호††

요 약

공격자는 시스템에 침입하기 위해 시스템 취약점을 수집한 후, 여러 공격 방법을 통해 루트권한을 획득하여 시스템 정보를 유출 및 변조하며 더 나아가서는 시스템을 파괴한다. 이러한 공격에 대응하기 위해 침입 탐지 및 차단을 위한 보안 시스템들이 많이 개발되어 왔지만, 최근 공격자들은 보안 시스템들을 우회하여 시스템에 침입하기 때문에 많은 문제가 되고 있다. 본 논문에서는 루트권한을 획득한 공격자의 불법행위를 막기 위한 보안커널모듈을 제안한다. 보안커널모듈은 추가적인 패스워드를 통해 시스템의 관리자 인증을 강화하여, 공격자가 중요 파일을 변조하고 루트킷을 설치하는 행위를 막는다. 또한 공격자의 불법행위에 대한 경고메일을 관리자에게 실시간으로 보내서, 관리자가 메일에 포함된 정보를 통해 새로운 보안정책을 수립하도록 한다.

Design and Implementation of Security Kernel Module with Additional Password for Enhancing Administrator Authentication

Ik-Su Kim† · Myung-Ho Kim††

ABSTRACT

Attackers collect vulnerabilities of a target computer system to intrude into it. And using several attack methods, they acquire root privilege. They steal and alter information in the computer system, or destroy the computer system. So far many intrusion detection systems and firewalls have been developed, but recently attackers go round these systems and intrude into a computer system. In this paper, we propose a security kernel module to prevent attackers having acquired root privilege from doing illegal behaviors. It enhances administrator authentication with additional password, so prevents attackers from doing illegal behaviors such as modification of important files and installation of rootkits. It sends warning mail about attacker's illegal behaviors to administrators by real time. So using information in the mail, they can establish new security policies.

키워드 : 시스템 보안(System Security), 커널모듈(Kernel Module), 침입 탐지(Intrusion Detection)

1. 서 론

최근 컴퓨터와 인터넷의 발달로 정보화 발전은 그 어느 때보다도 가속화되고 있으며, 정보화 서비스 또한 다양한 형태로 우리의 생활에 유익함을 제공하고 있다. 이에 원하는 정보를 쉽고 편리하게 얻을 수 있으며 은행과 주식거래와 같은 업무도 인터넷을 통해 가능하게 되었다. 그러나 이를 악용하는 시스템 공격자들의 불법행위가 나날이 증가하고 있으며 컴퓨터에 관한 지식이 부족한 스크립트 키디들조차도 인터넷상에 공개된 침입 도구를 사용하여 시스템에 침입하고 있다. 이로 인해 개인, 대학, 기업 내의 귀중한 정보가 유출되고 있으며 상업 사이트와 공공기관의 웹 서비스가 중단되는 사례가 늘고 있다[1].

※ 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음.
† 준 회 원 : 숭실대학교 대학원 컴퓨터학과
†† 종신회원 : 숭실대학교 컴퓨터학부 교수
논문접수 : 2003년 7월 1일, 심사완료 : 2003년 9월 1일

시스템 공격자들의 공격유형으로는 직접적인 피해를 주지는 않지만 시스템 침입을 위한 준비단계인 취약점 검색이 있으며 컴퓨터와 네트워크의 서비스를 마비시키기 위해 대량의 패킷을 전송하는 서비스 거부 공격, 루트권한의 쉘을 획득하기 위한 쉘코드 공격 방법 등이 있다. 특히 쉘코드를 이용한 버퍼 오버플로우나 포맷스트링 공격방법은 쉘을 얻는데 효과적인 방법으로 2002년 7월 CERT에서 발표한 OpenSSL 버퍼 오버플로우 취약점은 공격자가 쉘코드를 이용하여 취약 시스템의 nobody 권한의 쉘을 획득할 수 있다[2]. nobody 권한의 쉘을 획득한 공격자는 /tmp 디렉터리에 접근이 가능하므로 악성 프로그램을 설치하여 또다른 컴퓨터에 서비스 거부 공격을 할 수 있다.

시스템 공격을 통해 루트권한이나 nobody 권한을 획득한 공격자는 시스템 정보를 유출 및 변조하게 되며 더 나아가서는 시스템을 파괴하게 된다. 루트권한을 획득한 공격자는 자신의 침입 흔적을 숨기고 손쉽게 시스템에 다시 접근할

수 있도록 루트킷이라 불리는 백도어 및 트로이잔 프로그램 패키지를 설치하게 되는데 이러한 루트킷들은 인터넷을 통해 쉽게 구할 수 있기 때문에 시스템 보안의 커다란 위협이 되고 있다[3]. 일반적인 루트킷들은 관리자의 세심한 로그 분석과 시스템의 현재 상태들을 조사함으로써 탐지가 가능하지만 커널 기반의 루트킷은 탐지가 매우 어렵기 때문에 최근 시스템 공격자들은 커널 기반의 루트킷을 설치하여 침입흔적을 숨기고 손쉽게 시스템에 재 침입하게 된다.

이러한 불법침입 행위를 막기 위해 보안업체와 공공기관들은 방화벽과 침입 탐지 시스템 개발에 많은 노력을 기울이고 있다. 그러나 방화벽은 사전에 IP 주소와 포트번호를 등록하여 시스템 접근을 허용하거나 거부하는 정적인 방법이며 최근에는 방화벽을 우회하는 공격 방법들이 등장하여 여전히 보안상의 문제점이 존재하며, 침입 탐지 시스템은 내장된 침입 탐지 유형을 벗어나는 새로운 침입 방법을 탐지하지 못하는 문제가 있다. 또한 이러한 보안 시스템들은 루트권한을 획득한 공격자에 대해서 어떠한 방어능력도 갖추지 못하고 있는 실정이다.

본 논문에서는 기존의 보안 시스템들이 가지는 문제점을 보완하기 위해 보안 강화를 위한 추가적인 패스워드를 가지는 보안커널모듈을 제안한다. 이 보안 커널모듈은 모듈 내에 숨겨진 패스워드를 입력함으로써 시스템 관리자와 공격자를 식별하고, 인증되지 않은 공격자의 명령에 대해서는 거부하게 된다. 따라서 공격자가 보안 시스템을 우회하여 루트권한을 획득할지라도 시스템은 공격자로부터 안전할 수 있다. 또한, 시스템 공격자가 보안커널모듈의 정보를 수집하여 무력화할 가능성을 최소화하기 위해 시스템 관리자에게만 보안커널모듈의 정보를 제공한다. 그리고 공격자의 불법 행위가 탐지되면 공격자의 프로세스를 중지하여 시스템과 공격자간의 세션을 종료하고 별도의 로그 파일을 생성하여 불법행위를 기록하며 시스템 관리자에게 경고 메일을 보내게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 일반적인 시스템 침입방법과 이에 대응하기 위해 개발된 보안 시스템에 관해 살펴본다. 3장에서는 리눅스 시스템의 보안을 강화하기 위한 추가적인 패스워드를 가지는 보안커널모듈을 설계하고, 4장에서는 설계된 보안커널모듈을 구현한다. 5장에서는 쉘코드를 이용한 공격 방법을 통해 보안커널모듈을 테스트하며 마지막으로 6장에서는 결론과 향후 과제에 대해 살펴본다.

2. 관련 연구

이 장에서는 공격자의 일반적인 시스템 침입 방법과 공격자로부터 시스템을 보호하기 위해 개발된 여러 보안 시스템에 대해 살펴보도록 한다.

2.1 일반적인 시스템 침입 방법

일반적으로 시스템 공격자는 <표 1>에 보이는 공격 단계를 거쳐 목표 시스템에 침입한다.

<표 1> 시스템 침입을 위한 공격 단계

공격 단계	공격 방법	공격 도구
취약점 정보 수집	포트 스캐너와 취약점 검색 도구를 사용하여 취약점 정보를 수집	sscan, mscan, nmap, ISS
쉘코드를 이용한 루트쉘 획득	SETUID 루트 프로그램이 수행중일 때 버퍼 오버플로우나 포맷스트링 공격을 통해 루트권한 획득	데몬 취약점을 이용한 쉘코드 사용 exploits
사용자 도 용	네트워크상에 떠도는 패킷을 캡처하거나 시스템상의 키보드를 후킹함으로써 ID와 패스워드를 도용	linsniffer, tcpdump, keylogger
루트킷 설 치	차후 시스템에 쉽게 재침입하기 위한 프로그램 설치	lrk, t0rn kit, knark

우선적으로 공격자는 포트 스캐너를 통해 목표 시스템의 열려있는 포트를 찾고 열려진 포트와 관계된 서비스 데몬 프로그램의 취약점을 수집하게 된다[4]. 이 정보를 토대로 공격자는 취약점이 노출된 데몬 프로그램에 쉘코드 공격을 하게 되며 공격에 성공하게 되면 루트권한을 획득하게 된다[5, 6]. 쉘코드는 쉘을 실행시키는 기계어 수준의 코드로서 버퍼 오버플로우나 포맷스트링 공격 방법은 이러한 쉘코드를 취약 프로그램이 사용중인 스택에 삽입한 후 쉘코드를 실행시킨다. 공격자가 쉘코드를 실행시키기 위해서는 취약 프로그램의 리턴 주소가 저장된 스택부분을 쉘코드가 위치해 있는 주소 값으로 변경하며 취약 프로그램이 리턴하게 되면 다음 실행될 코드로 쉘코드를 실행하게 된다. 취약 프로그램이 루트권한의 setuid가 설정되어 있다면 프로그램 수행중에는 루트권한을 가지게 되므로 쉘코드를 통해 얻게 되는 쉘은 루트권한의 쉘이 된다.

(그림 1) 쉘코드를 이용한 포맷스트링 공격

(그림 1)은 로컬 시스템 상에서 쉘코드를 이용하여 포맷스트링 공격방법을 수행한 결과이며 실제로 공격자는 원격에서 데몬 프로그램에 유사한 방법의 쉘코드 공격을 통해 루트권한을 획득하게 된다. 루트권한을 획득한 공격자는 다른 시스템에 침입하기 위해서 시스템을 스니핑하여 사용자의 ID와 패스워드를 얻어내며 시스템 정보를 유출, 변조, 파괴하고 차후 공격을 위해 시스템 상에 루트킷을 설치한다. 이

러한 공격은 단지 고도의 기술을 가진 공격자에 의해서만 가능한 것이 아니다. 컴퓨터에 관한 해박한 지식을 가지지 못한 스크립트 키디들도 인터넷에서 침입도구를 수집하여 쉽게 시스템 침입을 하기 때문에 현재 인터넷상에 공개된 컴퓨터 시스템들은 결코 안전하지 못하다.

2.2 루트킷 탐지 도구

공격자는 시스템에 침입한 후 침입 흔적을 제거하고 차후에 재침입하기 위해 루트킷이라 불리는 백도어와 트로이잔 프로그램 패키지를 설치하게 된다. 이러한 루트킷에는 lrk (Linux Rootkit), t0rn Kit이 있으며 이 루트킷이 시스템 상에 설치되면 공격자는 원하는 파일과 프로세스를 숨길 수 있다. 즉, 공격자가 이들 루트킷에 포함되어 있는 변조된 ls, ifconfig, find, ps 프로그램들로 원래의 시스템 프로그램을 대체하게 되면 다른 사용자들은 변조된 시스템 프로그램을 통해 서비스를 받게 되므로 특정 파일과 프로세스를 볼 수 없게 된다.

일반적으로 시스템에 설치된 루트킷을 발견하기 위해서는 로그파일의 분석과 의심되는 프로그램의 무결성 검사, 응용프로그램 내에서 사용되는 시스템 콜을 추적하기 위한 strace 프로그램을 사용할 수 있다. 또한 루트킷 탐지도구를 사용할 수도 있는데 chrootkit은 다양한 루트킷을 탐지한다. 그러나 커널 기반의 루트킷은 커널의 활동을 변경시키기 때문에 시스템 명령으로는 루트킷을 발견하기가 어려우므로 커널의 정보를 분석할 수 있는 도구인 kstat나 carbonite를 사용하여 루트킷을 탐지해야 한다[7].

루트킷 탐지 도구는 공격자의 시스템 침입이 이루어진 이후에야 루트킷의 설치 여부를 알 수 있으며 공격자가 시스템을 침입한 후에 루트킷을 설치하지 않았다면 루트킷 탐지도구는 무용지물이 된다. 그리고 이러한 루트킷 탐지 도구들은 루트킷 설치를 막을 수 없고 공격자의 루트권한 획득을 통한 불법행위 문제를 해결할 수가 없다.

2.3 방화벽과 침입 탐지 시스템

시스템 공격자들의 불법 침입에 따른 피해를 최소화하기 위해 방화벽과 침입 탐지 시스템이 개발되어 왔다. 방화벽은 외부 네트워크와 내부 네트워크 사이에 패킷필터링 기능을 가진 라우터 또는 응용 게이트웨이를 두어 IP 주소나 포트번호에 따라 외부로부터의 불법적 트래픽 유입을 막고 허가된 트래픽만을 허용함으로써 내부 네트워크에 있는 전산자원을 보호할 수 있다. 방화벽을 통해 보안성을 향상시키기 위해서는 방화벽에서 처리하는 서비스들을 분리하여 두 개 또는 그 이상의 방화벽에서 병렬로 처리하도록 설치하는 것이 효율적이다.

침입 탐지 시스템은 일정 요건을 갖추지 않은 데이터의 침입을 사전에 방지하기 위한 방화벽과는 달리 각종 침입유형에 대한 규칙을 자체적으로 내장하여 침입행동을 실시간으로 탐지하는 시스템을 말한다.

방화벽의 단점은 사전에 IP 주소와 포트번호를 등록하여 시스템 접근을 허용하거나 거부하는 정적인 방법이며, 침입탐지 시스템은 내장된 탐지룰을 벗어나는 새로운 침입방법을 탐지하지 못하는 문제가 있다. 특히 IP 단편화를 이용한 공격 방법은 방화벽을 우회하여 목적지 서버에 침입할 수 있는 방법으로, 공격자가 임의로 IP 패킷을 조작하여 전송함으로써 방화벽이 허락하지 않는 목적지 서버의 특정 서비스를 받을 수 있게 된다[8].

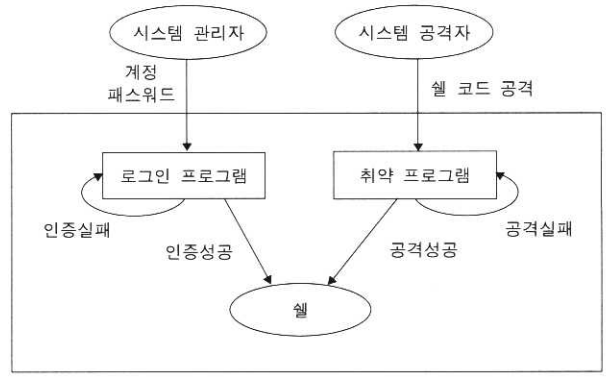
3. 보안 강화를 위한 추가적인 패스워드를 가지는 보안커널모듈 설계

2장에서 살펴본 보안 시스템에는 여러 가지 문제점이 존재한다. 즉, 공격자는 보안 시스템을 우회하여 취약 시스템의 루트권한을 획득한 후, 시스템 정보를 변조하거나 파괴하며 스니핑을 통해 다른 시스템의 사용자 계정과 패스워드를 획득하게 된다. 따라서 네트워크 보안 시스템을 우회하여 침입하는 공격자로부터 시스템을 보호하기 위해서는 시스템 자체적으로 보안을 강화해야 한다.

이 장에서는 보안을 강화하기 위한 추가적인 패스워드를 가지는 보안커널모듈을 설계한다. 이 보안커널모듈은 관리자의 인증과정을 통해 공격자의 불법 행위를 탐지하고 서비스를 거부하는 관리자 인증 기능, 보안커널모듈의 자체 정보를 공격자로부터 보호하기 위한 정보 은닉 기능, 공격자의 침입 탐지시 관리자에게 알리기 위한 로그파일 및 경고 메일 생성 기능으로 구성된다.

3.1 관리자 인증 기능

관리자 인증 기능은 보안커널모듈의 패스워드를 통해 실제 관리자를 식별하여 관리자에게는 루트권한의 모든 서비스를 제공하는 반면, 불법적으로 루트권한을 획득한 공격자에 대해서는 서비스를 거부하기 위한 기능이다.

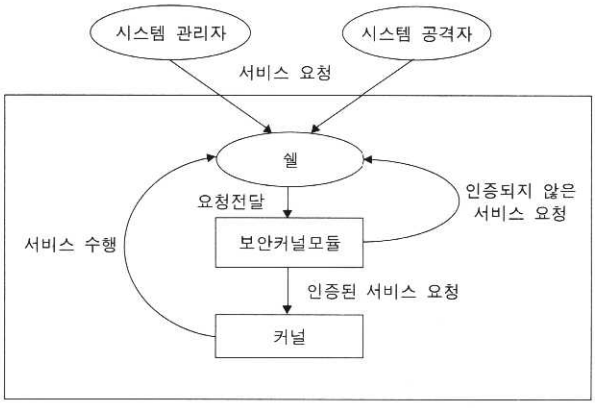


(그림 2) 정상적인 로그인을 통한 쉘 획득과 불법적인 행위를 통한 쉘 획득

리눅스 시스템은 사용자의 인증을 위해 패스워드 파일을 사용한다. 즉, 사용자가 로그인 과정에서 자신의 계정과 패스워드를 입력하면 리눅스 시스템은 입력된 정보와 패스워드 파일을 이용하여 매칭작업을 수행하게 된다. 이러한 작

업을 통해 인증이된 사용자는 쉘을 얻게 되며 이를 통해서 시스템의 서비스 이용이 가능하게 된다. 그러나 최근에는 (그림 2)와 같이 공격자가 사용자의 인증 과정 없이 시스템의 취약점을 이용한 쉘코드 공격방법을 통해 루트쉘을 획득하기 때문에 시스템 보안에 커다란 문제가 되고 있다.

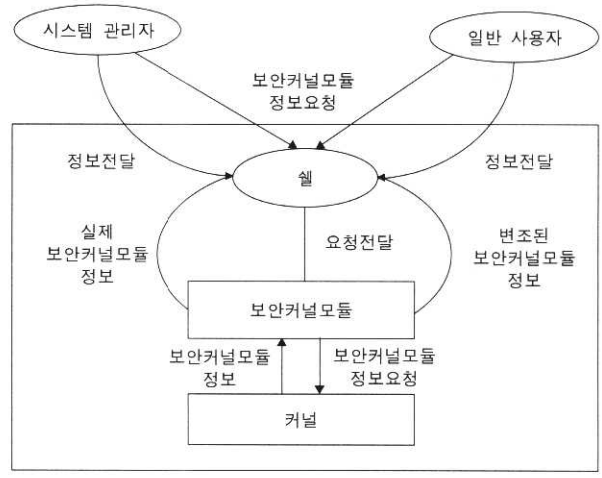
루트쉘 획득을 통한 공격자의 불법 행위로부터 시스템을 보호하기 위해서는 공격자와 실제 시스템 관리자의 명령을 식별하여 공격자의 불법 행위를 거부할 수 있어야 한다. 하지만 현재 리눅스 시스템은 루트쉘을 획득한 공격자와 실제 시스템 관리자의 명령을 식별할 수 있는 기능을 제공하지 못하는 실정이다. 그러므로 보안커널모듈은 리눅스 시스템이 공격자와 실제 시스템 관리자를 식별하여 서비스를 수행할 수 있는 기능을 제공해야 한다. (그림 3)은 보안커널모듈이 인증작업을 수행하여 공격자와 실제 시스템 관리자의 명령을 식별하는 과정을 도식화한 것이다. 쉘을 획득한 시스템 관리자는 보안커널모듈이 포함하고 있는 별도의 패스워드를 입력하여 인증 과정을 거치게 되고, 커널은 보안커널모듈에 의해 전달된 관리자의 서비스 요청을 처리한다. 그러나 공격자가 쉘코드를 이용하여 루트쉘을 획득했을 경우에는 불법적인 행위로 간주하여 서비스 요청이 커널에 전달되는 것을 막아야 한다.



(그림 3) 보안커널모듈을 통한 관리자 인증

3.2 정보 은닉 기능

정보 은닉 기능은 보안커널모듈의 자체 정보를 숨김으로써 공격자의 불법 행위로부터 보안커널모듈을 보호하는 기능이다. 보안커널모듈은 관리자와 공격자를 식별하고 그에 따라 루트 권한의 명령을 제한하기 때문에 공격자는 루트 권한을 통해 불법적인 행동을 할 수 없다. 그러나 공격자가 일반 사용자의 계정을 통해 보안커널모듈의 정보를 수집하여 보안커널모듈을 무력화할 가능성을 배제할 수 없기 때문에 보안커널모듈은 자체 정보를 일반 사용자에게 공개해서는 안된다. 따라서 (그림 4)와 같이 보안커널모듈에 관한 정보를 일반 사용자에게 제공할 때에는 보안커널모듈에 의해 필터링 작업을 거친 후 변조된 정보를 제공하고, 시스템 관리자에게는 필터링 작업 없이 실제 정보를 제공하여 보안커널모듈을 보호해야 한다.



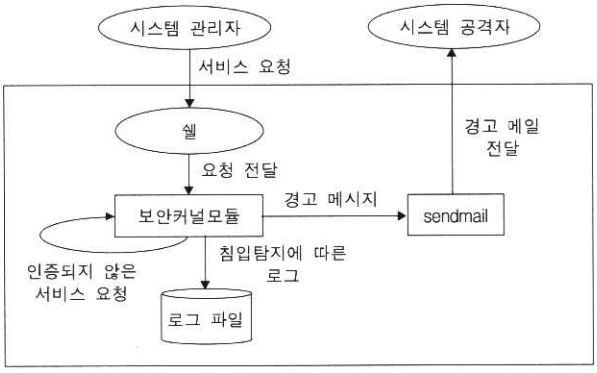
(그림 4) 필터링을 통한 보안모듈커널 정보 은닉

관리자는 외부 네트워크를 통해 시스템에 접속하여 작업을 수행해야 할 경우가 있다. 관리자가 시스템 상에서 루트 권한의 명령을 수행하기 위해서는 3.1절에서 기술했듯이 보안커널모듈에 대한 인증절차를 거쳐야 하는데, 이 때 공격자는 네트워크 스니핑을 통해 보안커널모듈의 패스워드를 획득할 수 있다. 이와 같은 공격에 대응하기 위해서 관리자는 ssh를 사용하여 데이터를 암호화해야 하지만, telnet 접속을 통해 관리자가 부주의하게 보안커널모듈의 패스워드를 입력할 수 있으므로 이에 따른 패스워드 누출 방지를 위해 보안커널모듈은 적절한 대응을 해야 한다.

3.3 경고 메일 및 로그 파일 생성 기능

경고 메일 및 로그 파일 생성 기능은 공격자의 침입을 탐지하면 침입에 관한 사실을 관리자에게 알리는 기능으로 공격자의 불법 행위로부터 발생하게 될 피해를 최소화하기 위해 반드시 필요하다. 리눅스 시스템은 개인간의 메일을 전달하기 위해 sendmail을 사용하므로, 보안커널모듈은 sendmail을 통해 관리자에게 경고 메일을 전송할 수 있다. 전송된 경고 메일에는 공격자와 피해 시스템간의 세션을 종료하여 침입행위가 더 이상 발생하지 않도록 공격자의 세션 정보가 포함되어야 한다.

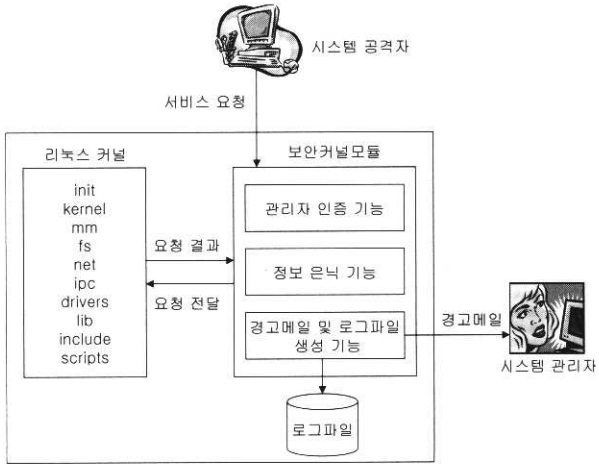
피해 호스트의 메일 시스템이 작동하지 않을 경우에는 공격자의 침입여부를 확인할 수 없으므로 침입 탐지에 따른 로그를 기록해야 한다. 그러나 시스템 공격자는 자신의 불법행위에 관한 흔적을 제거하기 위해 로그파일을 수정하거나 삭제하기 때문에 별도의 로그파일을 생성하고 보호해야 한다. 이 로그파일을 통해 시스템이 보유하고 있는 정보의 불법 유출을 방지하고 사용 원칙에 위배되는 불법 행위를 추적하기 위해서 피공격 프로그램명을 기록할 필요가 있다. 이를 통해 취약점이 존재하는 프로그램을 중지하거나 보안패치를 함으로써 시스템 보안을 강화할 수 있다. 그리고 공격자의 IP 주소를 기록하면 특정 IP 주소로부터 유입되는 패킷에 대한 보안정책을 세울 수 있다.



(그림 5) 침입 탐지에 따른 로그와 경고 메일 생성

(그림 5)는 침입 탐지에 따른 로그와 경고메일을 생성하는 보안커널모듈을 나타낸다. 시스템 공격자가 서비스를 요청하면 보안커널모듈은 인증되지 않은 서비스 요청으로 인식하고 그에 따른 로그를 생성하며, 실시간으로 침입에 관한 사실을 관리자에게 알리기 위해 경고 메시지를 생성하여 관리자에게 전달한다.

(그림 6)은 이 장에서 설계한 보안커널모듈의 전체 구성도이며 실제 관리자를 식별하기 위한 인증 기능과 보안커널모듈의 정보를 숨기기 위한 은닉 기능, 침입탐지에 따른 경고메일 및 로그파일을 생성하기 위한 기능으로 구분된다.



(그림 6) 보안커널모듈의 전체 구성도

4. 보안 강화를 위한 추가적인 패스워드를 가지는 보안커널모듈 구현

이 장에서는 3장에서 설계한 보안커널모듈의 관리자 인증 기능과 정보 은닉 기능, 침입 탐지에 따른 경고메일 및 로그파일 생성 기능을 구현한다.

4.1 관리자 인증 기능

앞서 기술했듯이 공격자는 불법적인 행위를 통해 루트의 패스워드 없이 루트 권한의 쉘을 획득할 수 있기 때문에 보안상에 커다란 문제가 있다. 관리자 인증 기능은 공격자가 루트쉘을 획득하여 루트권한의 명령을 수행하는 행위로부터 시스템을 보호하기 위해 보안커널모듈이 제공하는 기능으로써 보안커널모듈의 패스워드를 통해 실제 관리자를 식별하여 관리자에게는 루트권한의 모든 서비스를 제공하고, 불법적으로 루트권한을 획득한 공격자에 대해서는 서비스를 거부한다.

보안커널모듈이 시스템에 로드되면 보안커널모듈의 패스워드 인증에 성공하기 전에는 루트권한의 명령을 수행할 수 없고, 커널은 모든 루트권한의 명령 요청에 대해 에러 메시지를 생성한다. 따라서 관리자가 보안커널모듈의 인증을 받기 위해서는 패스워드 전달 프로그램 상에 패스워드를 입력해야 하며 이 패스워드는 보안커널모듈 내에 숨겨진 패스워드와의 매칭 작업을 통해 인증 처리가 된다. 이 때 명령 요청에 대한 서비스를 제공하는 커널은 보안커널모듈의 인증 과정에 성공한 관리자를 식별할 수 없기 때문에 보안커널모듈은 인증된 관리자의 세션과 관련된 정보들을 저장하고 이러한 정보를 가진 사용자의 요청만을 커널에게 전달해야 한다. 이 정보들은 다른 사용자와 유일하게 식별될 수 있어야 하므로 저장되는 정보들은 터미널 번호와 타입, 세션 id가 된다. 그래서 커널이 루트권한의 명령을 서비스하기 전에, 보안커널모듈은 세션과 관련된 정보를 이용하여 서비스 허용 여부를 결정하고 커널에게 명령 요청을 전달한다. 그러므로 불법행위를 통해 루트권한을 획득한 공격자의 모든 명령은 보안커널모듈에 의해 식별되어 서비스가 거부된다.

```
int init_module ( )
{
   term_num = 로드한 프로세스의 터미널 부번호 ;
   term_type = 로드한 프로세스의 터미널
               드라이버 타입 ;
   session_id = 로드한 프로세스의 세션 id ;
}
static asmlinkage int sec_sys_execve()
{
   if (서비스 요청 프로세스 정보 != 보안커널모듈 로드시
       저장된 정보)
   {
       공격 프로세스의 세션 id, 요청 명령 전송 ;
       메일 전송 시그널 발생 ;
       로그 기록 함수 호출 ;
       return 0 ;   // 서비스 수행없이 리턴
   }
   do_execve ( )   // 서비스 수행
}
```

(그림 7) 관리자 프로세스를 식별하기 위한 코드

(그림 7)은 보안커널모듈을 로드한 프로세스의 정보를 저장하고 서비스의 적합성 여부를 판단하기 위해 실제 관리자 프로세스를 식별하는 코드이다. 보안커널모듈을 로드할 때 초기화 되는 세 개의 변수인 term_num과 term_type, session_id는 커널내의 현재 프로세스 상태를 나타내는 task_struct 구조체의 포인터 변수인 current를 참조하여 할당되며, 차후에 서비스를 요청하는 프로세스를 식별하기 위해서

비교될 값이다. 커널이 시스템 명령을 처리하기 위해서는 execve 시스템 콜 함수를 호출하게 되는데 보안커널모듈에서는 sec_sys_execve함수가 execve 시스템 콜 함수를 대체하게 된다[9-11]. 이 함수 내부에서는 보안커널모듈 로드시 저장된 프로세스 정보와 서비스를 요청한 프로세스의 정보를 비교하게 되는데 만일 비교된 정보가 일치하게 되면 sec_sys_execve 함수는 해당 명령을 수행하기 위해 커널내의 함수인 do_execve 함수를 호출하여 서비스를 수행하게 된다. 그러나 정보가 일치하지 않을 경우에는 메일 전송을 위한 시그널과 공격 프로세스의 세션 id, 요청 명령이 보안커널모듈을 로드하는 시작데몬 프로세스에게 전달된다. 또한 로그기록 함수를 호출하여 불법행위에 대한 로그를 남기게 되며 서비스 거부를 위해서 do_execve 함수의 호출없이 리턴하게 된다.

새로운 세션을 통해 시스템 관리자가 루트권한의 명령을 수행하기 위해서는 로그인 직후 보안 보안커널모듈의 패스워드를 입력해야 하며 입력된 패스워드와 보안커널모듈내에 저장된 패스워드가 일치하게 되면 보안커널모듈내에 저장된 세션에 관한 정보들이 시스템 관리자의 현재 세션에 관한 정보들로 변경된다. 그러므로 새로운 세션을 통해 로그인 한 관리자의 모든 명령은 보안커널모듈을 통해 커널에게 전달되어 서비스가 수락된다.

4.2 보안커널모듈의 정보 은닉 기능

보안커널모듈의 관리자 인증 기능은 불법행위를 통해 루트권한을 획득한 공격자로부터 시스템을 보호할 수 있지만, 공격자가 보안커널모듈을 무력화 시킬 경우에는 더 이상 시스템 보안을 유지할 수 없다. 따라서 보안커널모듈은 자체 정보를 보호하기 위해 정보 은닉 기능을 제공하여 공격자의 불법행위로부터 보안커널모듈을 보호한다. 이 기능은 변조를 통해 실제 관리자가 아닌 사용자들에게 보안커널모듈의 존재 여부를 숨김으로써 보안커널모듈이 언로드 되는 것을 막고, 네트워크 스니핑에 의해 노출될 수 있는 보안커널모듈의 패스워드를 보호하여 시스템의 보안을 강화한다.

일반적인 커널 모듈은 lsmod 명령에 의한 결과와 proc 파일 시스템을 통해 모듈의 정보를 확인할 수 있으므로 관리자를 제외한 모든 사용자들에게는 보안커널모듈에 관한 정보를 공개해서는 안된다. 즉, lsmod 명령에 의한 결과와 /proc/modules 파일내의 정보들은 현재 로드되어 있는 모듈들의 리스트를 보여주기 때문에 보안커널모듈이 시스템 상에 로드되어 있을 경우 모듈명이 노출될 수 있다. 따라서 정보 은닉 기능은 실제 보안커널모듈명을 다른 이름으로 변조하여 공격자가 보안커널모듈의 오브젝트 코드를 삭제하거나 보안커널모듈을 언로드 하는 것을 막는다. 하지만 보안커널모듈을 로드한 관리자나 보안커널모듈의 패스워드를 입력하여 인증된 관리자는 보안커널모듈에 관한 실제 정보를 확인할 수 있다.

(그림 8)은 보안커널모듈에 관한 정보를 변조하기 위한 코드로서 시스템 콜 함수의 주소 리스트를 가지고 있는 sys_call_table에서 write 시스템 콜 함수의 주소를 보안커널모듈 내에 있는 sec_sys_write 함수의 주소로 변경하게 된다. 커널은 ls와 lsmod와 같은 명령을 통해 생성되는 결과를 스크린 상에 디스플레이 하기 위해 write 시스템 콜 함수를 호출하게 되는데 보안커널모듈이 로드되면 실제 커널에 존재하는 write 시스템 콜 함수를 호출하는 대신 보안커널모듈 내의 sec_sys_write 함수를 호출하게 된다. sec_sys_write 함수가 호출되면 디스플레이 되기 위한 스트링과 변조되어야 할 스트링을 비교하여 서로 일치할 경우 스트링을 변조하게 되고 변조된 스트링을 인자 값으로 전달받은 실제 write 시스템 콜 함수가 호출되어 일반 사용자들은 터미널 상에서 보안커널모듈의 변조된 정보를 보게 된다.

```
int sec_sys_write ( )
{
    char hide [ ] = "변조될 스트링" ;
    if (strstr (kernel_buf, hide) != NULL)
    {
        특정 스트링을 변조하기 위한 코드
    }
    return orig_sys_write (fd, buf, count)
}
```

(그림 8) 특정 스트링을 변조하기 위한 코드

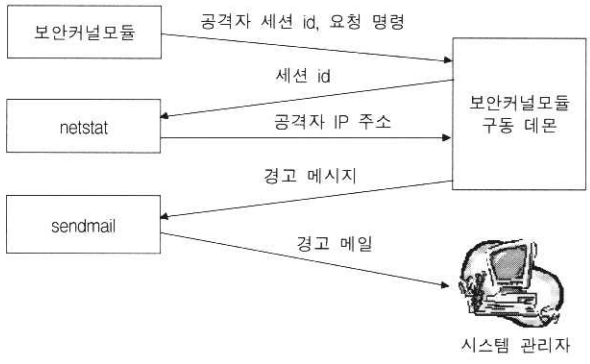
3.2절에서 기술했듯이 관리자는 외부 네트워크를 통해 시스템에 접속하여 작업을 수행해야 할 경우가 있으며, 이 때 공격자가 네트워크 스니핑을 통해 보안커널모듈의 패스워드를 획득할 수 있는 위험성이 존재한다. 따라서 전송되는 데이터가 암호화 되지 않는 telnet 연결에서 보안커널모듈의 패스워드를 보호하기 위해서는 그에 따른 적절한 보안기능이 필요하다. telnet 연결을 통해 보안커널모듈의 패스워드가 노출될 수 있는 경우는 루트권한으로 로그인을 하여 보안커널모듈의 패스워드를 입력하는 경우와 일반 사용자 계정으로 로그인하여 su 명령을 통해 루트권한의 쉘에서 보안커널모듈의 패스워드를 입력하는 경우이다. 전자의 경우 보안커널모듈은 telnet 연결에서 현재 프로세스의 uid가 0일 때 쉘의 실행을 거부함으로써 보안커널모듈의 패스워드 입력을 막을 수 있으며, 후자의 경우에는 현재 프로세스의 uid가 0이 아닐 때 su 명령을 거부함으로써 보안커널모듈의 패스워드 입력을 막을 수 있다. 이를 통해 공격자의 네트워크 스니핑으로부터 보안커널모듈의 패스워드 노출을 막을 수 있다.

4.3 침입 탐지에 따른 경고 메일 및 로그 파일 생성 기능

보안커널모듈은 관리자 인증 기능을 통해 공격자의 불법적인 요청을 탐지했을 경우 실시간으로 관리자에게 알려야 한다. 경고 메일 및 로그 파일 생성 기능은 보안커널모듈이 공격자의 침입을 탐지했을 때 별도의 로그 파일을 생성하여 불법행위에 관한 로그를 기록하고, 실시간으로 관리자에게 경고 메일을 전달하는 기능이다. 관리자는 경고 메일에 포함된 정보를 통해서 공격자의 침입여부를 알 수 있으므

로 불법행위에 대한 즉각적인 대응을 할 수 있어 시스템의 피해를 최소화 할 수 있다.

보안커널모듈은 공격자의 침입을 탐지하면 공격자의 세션 id와 요청 명령을 보안커널모듈 구동 데몬에게 전달하고, 데몬은 netstat 프로그램을 통해서 세션 id와 관련된 공격자의 IP 주소를 알아낸다. 이와 같이 수집된 공격자의 IP 주소와 요청 명령, 세션 id 정보를 포함하는 경고 메일은 sendmail을 통해서 실시간으로 시스템 관리자에게 전달된다. (그림 9)는 침입 탐지시 경고메일을 생성하고 시스템 관리자에게 전달하는 과정을 도식화한 것이다.



(그림 9) 침입 탐지시 경고 메일 생성에 대한 흐름도

〈표 2〉 메일을 통해 전달되는 메시지 형식

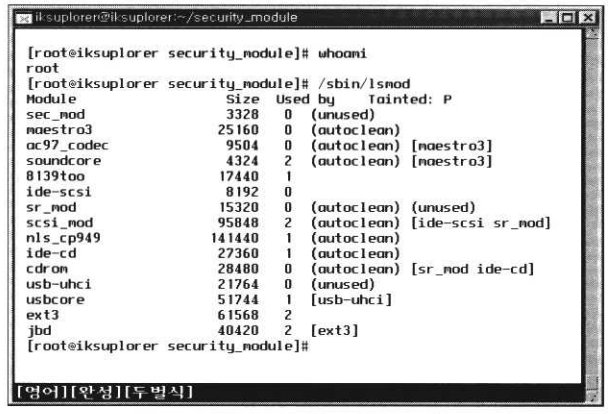
proto	local address	foreign address	pid / program name	command
프로토콜	피해 시스템 IP	공격자 IP	공격자 프로세스 id / 서버 프로그램	공격자의 요청 명령

생성된 경고 메일에는 공격자 IP 주소, 세션 id, 요청 명령외에 여러 정보들을 포함하며 <표 2>는 이 정보들을 나타낸다. local address 필드는 피해 시스템의 IP 주소를 나타내며 foreign address 필드는 공격자의 IP 주소를 나타낸다. pid는 공격자가 피해시스템과 소켓 연결이 이루어졌을 때 소켓을 소유하게 될 프로세스 id이고 program name은 피해시스템의 서버 프로그램명이며 마지막으로 command 필드는 공격자가 피해 시스템에서 요청한 명령을 나타낸다. 따라서 공격자의 침입이 탐지된 이후 관리자가 메일을 받게 되면 공격자의 프로세스를 중지시킴으로써 공격자의 세션을 끊을 수 있으며 관리자가 보안커널모듈을 로드할 때에 옵션을 통해 공격자의 세션을 보안커널모듈이 직접 끊을 수 있도록 할 수 있다. 또한 관리자는 서버 프로그램명의 기록을 통해 어떠한 프로그램의 취약점이 노출되고 있는지 분석할 수 있게 된다.

보안커널모듈은 시스템이 보유하고 있는 정보의 유출을 방지하고 불법 행위의 추적을 위한 감사 능력을 제공해야 하므로 리눅스 시스템이 제공하는 로그 파일 외에 별도의 로그 파일을 생성한다. 이 로그 파일은 sendmail이 작동하지 않을 경우 관리자가 공격자의 침입 여부를 알 수 없기 때문에 필수적인 것이다. 생성된 로그는 경고 메시지에 포함된 정보들로 이루어져 있으며 공격자로부터 로그파일을 보호하기 위해 4.2절에 기술된 정보 은닉 기능이 사용된다. 이를 통해 공격자는 보안커널모듈이 생성한 로그 파일을 찾을 수 없으며 관리자 인증 기능을 통해 로그파일에 접근할 수가 없다.

5. 실 험

보안커널모듈의 실험은 Linux kernel 2.4.13에서 쉘코드를 이용한 포맷스트링 공격방법을 통해 수행되었다.



(그림 10) 관리자의 lsmod 명령 결과 화면

보안커널모듈의 오브젝트 코드는 sec_mod.o 파일이며, 관리자가 보안커널모듈을 로드한 후 lsmod 명령을 수행하면 (그림 10)과 같이 sec_mod라는 모듈이 로드된 것을 확인할 수가 있다. 그러나 루트권한이 아닌 일반 사용자 계정을 통해서 lsmod 명령을 수행하게 되면 원래의 sec_mod라는 모듈을 볼 수 없으며 (그림 11)에서와 같이 maestro라는 이름으로 변조되었다는 것을 알 수 있다. 또한 2장에서 소개한 바와 같이 공격자가 포맷스트링 공격에 성공하게 되면 루트쉘을 획득하여 루트권한의 명령을 수행할 수 있는데, 보안커널모듈이 로드된 이후 공격에 성공할지라도 루트쉘을 통해 루트권한의 어떠한 명령도 수행할 수 없다는 것을 알 수 있다.

(그림 11) 보안커널모듈 로드후 쉘코드 공격 결과

(그림 12)는 xxx.xxx.xxx.xxx라는 시스템으로부터 관리자에게 전달되는 경고 메일로써 공격자의 IP 주소는 yyy.yyy.yyy.yyy라는 것을 알 수 있다. 관리자는 이 메일의 정보를 통해 2316번 프로세스를 중지함으로써 공격자와 시스템간의 세션을 끊을 수 있고 취약점을 갖는 서버 프로그램인 sshd의 취약점을 분석하여 시스템 침입을 예방할 수 있다.

(그림 12) 침입 탐지에 의해 관리자에게 전송되는 경고 메일

6. 결론 및 향후과제

시스템 공격자의 불법 침입에 의한 피해를 최소화하기 위해 방화벽과 침입 탐지 시스템과 같은 보안 소프트웨어와 보안 장비들이 개발되어 왔다. 하지만 이들 보안 시스템들이 갖는 문제점은 공격자가 보안 시스템을 우회하여 침입에 성공하거나, 내부 사용자가 불법행위를 통해 루트권한을 획득할 경우에 어떠한 대응도 할 수 없다는 것이다.

본 논문에서는 네트워크 보안 시스템을 우회하여 침입에 성공한 공격자로부터 피해를 최소화하기 위한 보안커널모듈을 구현하였다. 이 보안커널모듈은 관리자의 인증 과정을 통해 공격자의 불법 행위를 탐지하고 서비스를 거부하는 관리자 인증 기능, 보안커널모듈의 자체 정보를 공격자로부터 보호하기 위한 정보 은닉 기능, 공격자의 침입 탐지시 관리자에게 알리기 위한 로그 파일 및 경고 메일 생성 기능으로 구성된다. 보안커널모듈이 시스템 상에 로드되면 관리자는 관리자 인증 기능을 통해 보안커널모듈의 패스워드를 입력하여 인증을 받아야 루트 권한의 명령을 수행할 수 있다. 따라서 불법 행위를 통해 루트쉘을 획득한 공격자는 루트권한으로 시스템 명령을 수행할 수 없다. 그리고 공격자의 불법행위를 탐지하면 로그 파일 및 경고 메일 생성 기능을 통해 실시간으로 실제 관리자에게 경고 메일을 전달하고 로그파일을 생성한다. 경고 메일에는 공격자의 IP 주소와 공격자 프로세스에 대한 pid 정보를 포함하므로, 관리자는 피해 시스템과 공격자간의 세션을 종료시킬 수 있다. 또한 보안커널모듈이 여러 시스템에 설치될 경우 어떠한 시스템이 공격을 받고 있는지 식별하기 위해 피해 시스템의 IP 주소를 담고 있다. 현재 보안커널모듈은 관리자가 수작업을 통해 공격자와 피해 시스템간의 세션을 끊을 수 있도록 공격자의 pid를 제공하고 있으며 관리자가 보안커널모듈을 로드할 때에 옵션을 통해서 공격자의 세션을 보안커널모듈이 직접 종료할 수 있다. 그리고 정보 은닉 기능을 통해 보안커널모듈의 정보를 숨김으로써 공격자로부터 보안커널모듈을 보호할 수 있다.

향후 연구과제로는 침입을 탐지했을 경우 실시간으로 공격자 IP 주소의 리스트를 자동으로 등록하여 접근을 원천적으로 봉쇄하는 기능과 시스템으로 유입되는 패킷의 패턴을 분석하여 침입 여부를 판단하는 기능을 추가할 예정이다.

참 고 문 헌

[1] 한국정보보호진흥원, "12월 해킹바이러스 통계 및 분석 월보", 한국정보보호진흥원, 2002.
[2] http://www.cert.org/advisories/CA-2002-23.html.
[3] 이현우, 김영직, 전숙, "UNIX 피해시스템 분석 v1.1", 2002.
[4] Fyodor, "The Art of Port Scanning," Phrack Magazine, Vol.7, Issue 51, 1997.
[5] Aleph, "Smashing The Stack For Fun And Profit," Phrack Magazine, Vol.7, Issue 49, 1996.
[6] Andreas Thuemmel, "Analysis of Format String Bugs," 2001.
[7] 이계찬, 이현우, "Detecting Loadable Kernel Module Rootkit," SecurityMap, 2002.
[8] 정현철, "IP Fragmentation을 이용한 공격기술들", 한국정보보호진흥원, 2001.
[9] Ori Pomerants, "Linux Kernel Module Programming Guide," 1999.
[10] 이 호, "Advanced Module Programming," 2001.
[11] Pragmatic, "Complete Linux Loadable Kernel Modules," The hacker's choice, 1999.
[12] http://www.securitymap.net.
[13] http://packetstormsecurity.org.

김 익 수
e-mail : skycolor@ss.ssu.ac.kr
2000년 숭실대학교 컴퓨터학부(학사)
2002년 숭실대학교 대학원 컴퓨터학과 (공학석사)
2002년~현재 숭실대학교 대학원 컴퓨터학과 박사과정
관심분야 : 컴퓨터 보안, 병렬처리, 분산처리

김 명 호
e-mail : kmh@comp.ssu.ac.kr
1989년 숭실대학교 전자계산학과(학사)
1991년 포항공과대학교 전자계산학과 (공학석사)
1995년 포항공과대학교 전자계산학과 (공학박사)
1995년 한국전자통신연구소 선임연구원
1998년~1999년 University of Tennessee 전자계산학과 교환교수
1995년~현재 숭실대학교 컴퓨터학부 부교수
관심분야 : GRID, 병렬/분산처리, 컴퓨터 보안, 클러스터링, 리눅스