운영체제 보안을 위한 보안 커널 설계에 요구되는 보안솔루션

김성훈° 오병균
목포국립대학교 정보공학부
{seilpart°, obk}@mokpo.ac.kr

A Study on Security Solution needed to design security-kernel for secure OS

Seong-hoon Kim° Byeong-kyun Oh
Dept. of Information Engineering, Mokpo National University

요 약

오늘날과 같은 컴퓨터와 통신 기반의 네트워크 환경에서 서버들에 대한 '개방성'은 중요한 특징이다. 그러나, 이러한 특성은 서버에 대한 불법적인 접근이나 해킹 등과 같은 침입을 시도할 수 있는 가능성을 내포하고 있다. 침입의 목표는 서버의 모든 시스템정보로서 방화벽이나 침입탐지시스템 등과 같은 네트워크기반의 보안솔루션에 의해 서버의 모든 정보를 보호하기에는 한계가 있다.

본 논문에서는 서버들이 가지고 있는 정보를 보호하기 위하여 기존의 보안커널보다 더 유연하고 안전성이 강화된 보안커널의 설계에 필요한 필수적인 보안요소들을 제안하였다.

1. 서론

오늘날과 같은 네트워크 중심의 정보화 사회에서는 다양한 정보 서비스에 의해 우리생활의 모든 분야에 편의성을 제공하지만, 다른 측면에서는 인터넷 웜, 바이러스, 해커, 사이버 테러 등과 같은 위협요소가 증가하는 추세에 있어 정보화의 역기능이 노출되고 있다. 이러한 위협요소들은 정보화 사회에서 해결해야할 중요한 과제이다.

사회의 각 분야에서는 보안을 위해 투자를 증가시키지만 보안침해사고에 의한 손실은 기대와는 반대로 계속 증가하고 있다. 이와 같은 현상은 보안 솔루션의 측면에서 두 가지의 불충분한 요인이 존재하기 때문이다. 첫째, 보안 소프트웨어들은 특정 영역의 보안을 담당하려는 경향이 있다. 둘째, 보안솔루션의 특성이 능동형이라기보다는 수동형이라는 점이다. 즉, 침입 전에 미리 방어하고 알려지지 않은 공격에 대처할 수 있는 기능이 부족하다는 것이다.

컴퓨터 내의 정보보호를 향상시키기 위한 도구는 현재의 표준 운영체제에서는 매우 부족한 실정이다. 한 통계자료에 의하면 성공한 네트워크 공격이 약 8%가 유닉스 시스템 자체의 취약점을 공격함으로 해서 이루어졌다고 한다.[1]

본 논문에서는 이러한 운영체제의 취약점을 위한 솔루션인 보안커널의 설계에 있어서 더 유연하고 안전성이 강화된 설계를 위해 필요한 필수적인 보안요소들을 제안하고자 한다.

2. 기존의 보안커널의 보안요소

여기서는 기존의 대표적인 서버보안을 위한 보안 커널인 Secuve TOS, RedOwl, Hizard, PitBull의 특징들을 요약하여 정리하고, 각 보안 커널들의 특징을 비교한다.

2.1 Secuve TOS

Secuve TOS의 보안정책은 보안이 설정된 파일에 대해 인가되지 않은 불법적 위·변조를 방지하고, 알려지지 않은 해킹을 탐지하여 차단하는 해킹방지기능을 제공한다.[5]

가. 접근제어
- 전자 서명 기반의 사용자 인증
- RBAC, MAC 접근제어
- 파일, 프로세스, 네트워크 접근제어

나. 침입탐지 및 대응
- BOF등의 최신해킹 공격 방지
- 풍부한 감사로그
- 보안위험요소관리 : setuid 프로그램 관리 및 제어

다. 통합 시스템 관리
- 관리도구 하나로 다수 서버제어 및 관리
- 시스템 관리 : 사용자 및 그룹관리, 시스템 모니터링
- 주기적인 로그관리

2.2 RedOwl

운영체제 수준에서 강력한 접근제어를 통해 주요 파일의 불법적인 변조, 탈취 등을 차단하고, 불법적인 root 권한 획득, 데몬 공격, 바이러스 및 백-도어의 불법실행 등 다양한 해킹 위협으로부터 시스템을 보호한다.[6]

가. 강제적 접근 제어
나. 다중등급 보안(MLS 보안정책)
다. 해킹방지
라. 커널 레벨 감사, 추적 구현
마. 보안정보 출력
바. 커널 모드 암·복호화 구현
사. 통합보안관리 기능

2.3 Hizard

해킹방지 기능과 시스템 및 데이터 보안을 위한 강제적 접근제어기능을 제공하는 서버보안 솔루션이다.[7]

가. 사용자 인증 및 계정관리
나. 해킹방지
다. 시스템 리소스 관리
 - 시스템정보, 상태, 실시간통보
라. 강제적 접근제어
 - 파일/디렉토리, 프로세서, Port, Registry
마. 네트워크 제어
 - 접속제어, 경유제어
바. 통합 집중 관리
 - Intall/Uninstall
 - 로깅 및 리포팅, 실시간 경보, 원격제어

2. PitBull

표준 UNIX 운영체제에 간단한 업그레이드 형태로 설치되며, 표준 운영체제에 의해 지원되는 모든 애플리케이션과 바이너리 레벨의 호환성을 지원한다. 또한 중요한 객체에 대한 접근이 시스템에 의해 강제적으로 통제되며 프로그램, 데이터, 네트워크 인터페이스는 독립된 영역으로 분리되고 서로간의 접근을 제한한다.

가. 신분확인 : 일반패스워드 방식이외의 3rdParty 인증지원
나. 임의적 접근통제 : 파일접근제어
다. 강제적 접근통제 : 등급부여에 따른 접근제어
라. 단순화된 도메인 기반 접근제어(DBAC)
마. 인증 : 파일과 프로세스간의 인증을 통한 접근제어
바. 감사, 로그 보고서 기능 제공
사. 무결성 체크로 보안성 강화
아. 네트웍 통제 : 네트워크 필터링 기능 제공

2.5 서버보안 솔루션 별 보안요소 비교

위에서 각 보안커널의 주요한 특징들을 살펴보았다. 이들 대부분은 보안커널이 갖춰야할 기본적인 기능들을 구비하고 있고 보안요소별로 특징들이 약간의 차이를 가지고 있다. 표[1]에서는 이들을 비교하여 정리하여 보았다.

3. 제안하는 보안커널 모듈의 보안요소

서버보안을 위한 보안커널의 설계에 있어서 안정성과 유연성을 강화하기 위해서는 보안커널이 갖춰야할 필수적인 보안요소를 설정하고 정립하는 것이 중요하다.

[표 1] 보안요소별 보안커널 비교

보안요소	SecuveTOS	RedOwl	Hizard	PitBull
사용자 인증 메커니즘	전자서명 기반인증	패스워드 기반	PAM/LAM	패스워드 기반
파일 접근제어	RBAC, MAC	MLS, MAC	RBAC	DMAC
프로세스 접근제어	RBAC, MAC	MLS, MAC	RBAC	DMAC
네트워크 접근제어	IP, port별	IP	IP	IP
침입탐지 및 대응	Anti-Hacking	Anti-Hacking	Anti-Hacking	
감사기능	객체별 로그분석	로그분석	로그분석	
기타	자체보호 통합관리	통합관리 커널모드암·복호화	통합관리	

본 논문에서는 해커가 시스템에 불법 침입하여 시스템관리자 권한으로 시스템 및 중요 파일을 위/변조하는 보안 위협요소를 분석하고 제안하고자 하는 필수적인 보안요소들을 네 가지 요소로 정의하고, 각 요소별로 고려되어야할 중요한 기능들을 기술한다.

3.1 보안 위협요소

가) 허가되지 않은 사용자가 운영체제, 응용서비스 및 네트워크 프로토콜 등의 취약성을 이용하여 보안솔루션 자체에 대한 관리자 권한을 불법적으로 획득하려는 위협

나) 허가되지 않은 사용자가 운영체제, 응용서비스 및 네트워크 프로토콜의 취약성을 이용하여 시스템의 주요 자원에 불법적으로 접근하여 침해하려는 위협
 - 시스템의 홈페이지 파일을 위/변조하려는 위협
 - 시스템의 서비스 관련 설정파일을 위/변조하려는 위협
 - 시스템에서 수행중인 주요 프로그램을 불법 종료하여 안정적인 서비스의 수행을 방해하려는 위협

다) 허가되지 않은 사용자가 운영체제, 응용서비스 및 네트워크 프로토콜 등의 취약성을 이용하여 시스템관리자의 권한을 획득 후, 시스템을 불법적으로 정지하여 안정적인 시스템 운영을 방해하려는 위협

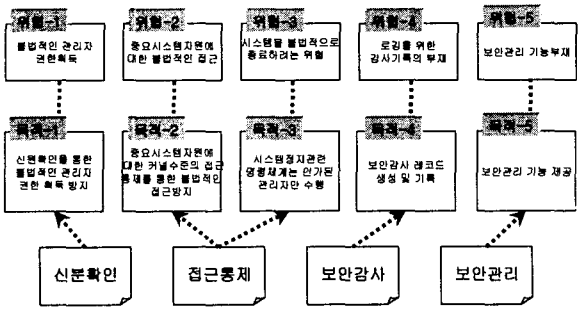
라) 보안솔루션이 다음 각 항에 해당하는 시스템 관리자 및 사용자의 보안 관련 활동에 기록되지 않아 사후 감사관리 기능이 불가능해지는 위협
 - 사용자 신분확인에 대한 시도 및 결과
 - 접근권한 설정된 파일 접근에 대한 시도 및 결과
 - 접근권한 설정된 프로세스 접근에 대한 시도 및 결과
 - 시스템을 불법 종료하려는 시도 및 결과

마) 보안솔루션이 다음 각 항의 설정, 조회, 변경기능이 정상적으로 운영되지 않아 발생할 수 있는 관리적 위협
 - 파일에 대한 특정 접근권한을 설정, 조회 및 변경
 - 프로세스에 대한 특정 접근권한을 설정, 조회 및 변경
  • 접근 권한이 부여된 파일에 대한 해당 접근 권한을 특정 프로세스에게 설정, 조회 및 변경
  • 식별 및 인증 데이터의 설정, 조회 및 변경

• 감사데이터를 위한 관리 환경의 설정, 조회 및 변경

3.2 제안된 보안요소

각 보안요소들에 대한 보안 목적과 위협요소를 도표로 표현하면 그림[1]처럼 표현할 수 있으며 해당 보안요소들에 대하여 서버보안 솔루션이 갖추어야 할 기능은 다음과 같다.



<그림 1> 보안요소에 대한 보안목적과 위협요소

가. 신분확인

- 관리자가 서버보안 솔루션을 정상적으로 운영하기 위한 행동 이전에 독자적인 인증 방식을 이용하여 관리자를 식별 및 인증하는 기능을 제공하여야한다.

• 전자서명 인증기법

• 일회용 패스워드

- 시스템에서 사용하는 ROOT권한보다 상위권한을 가진 SUPER ROOT의 권한으로 사용자 신분을 확인하여야 한다.

나. 접근통제

- 특정 사용자에게 접근권한이 설정된 파일에 대해서는 시스템관리자(root)라 할지라도 접근이 불가능하도록 하는 기능을 제공하여야 한다.

- 특정 사용자에게 접근권한이 설정된 프로세스에 대해서는 시스템관리자(root)라 할지라도 접근이 불가능하도록 하는 기능을 제공하여야 한다.

- 커널에 동적으로 커널모듈을 올리고, 내리는 행위를 시스템관리자(root)라 할지라도 수행이 불가능하도록 하는 기능을 제공하여야 한다.

- 시스템을 종료하는 명령어 및 행위에 대하여 시스템관리자(root)라 할지라도 수행이 불가능하도록 하는 기능을 제공하여야 한다.

다. 보안감사

- 시스템 구동과 동시에 다음 각 항에 대한 감사기록 레코드를 생성하여야 한다.

• 사용자 신분확인에 대한 시도 및 결과

• 접근권한 설정된 파일 접근에 대한 시도 및 결과

• 접근권한 설정된 프로세스 접근에 대한 시도 및 결과

• 시스템을 불법 종료하려는 시도 및 결과

- 상시 감사기록 레코드 생성 시, 각 감사기록 레코드별로 다음의 정보를 반드시 포함하여 기록하여야 한다.

• 주체 및 객체에 대한 식별자

• 사건 유형 및 결과

• 사건의 날짜 및 시간

- 정해진 감사기록 형태에 따라 관리자가 이해할 수 있는 형태로 감사기록을 제공하며, 정해진 감사기록 검색규칙에 근거하여 관리자의 요청에 따라 감사기록을 검색·정렬하는 기능을 제공하여야 한다.

라. 보안관리

- 식별 및 인증 기능에 따라 인가된 관리자에게 다음의 각 항에 해당하는 내용을 설정, 조회 및 변경할 수 있는 기능을 제공한다.

• 파일에 대하여 특정 접근권한을 설정, 조회 및 변경

• 프로세스에 대하여 특정 접근권한을 설정, 조회 및 변경

• 접근권한이 부여된 파일에 대하여 해당 접근권한을 특정 프로세스에게 설정, 조회 및 변경

• 식별 및 인증 데이터의 설정, 조회 및 변경

• 감사데이터를 위한 관리 환경의 설정, 조회 및 변경

- 시스템 관리자가 서버보안 솔루션이 설치된 서버에 임의의 보안관리를 위하여 원격지에서 접속시도 시 이에 관련된 모든 통신은 암호화되어야 한다.

4. 결론 및 추후 연구

본 논문에서는 보안커널 설계를 위한 보안요소들을 신분확인, 접근통제, 보안감사, 보안관리라는 네가지 측면으로 설정하고 각각의 요소별로 보안커널이 갖춰야할 필수적인 요소들을 세부적으로 제안하였다.

본 논문은 인터넷의 확산으로 인하여 각 인터넷 사이트는 서버의 수량이 점점 늘어나는 추세이므로 추후 앞에서 언급한 보안요소들을 기반으로 보안커널을 설계함으로서 기존의 솔루션보다 더 유연하고 안정성있는 보안커널을 구현할 수 있다.

참고문헌

[1] 김학범 외, "운영체제 보안기술동향", 정보보호학회지, 8권 2호 pp.63~41, 1998. 6

[2] 이정효 외, "정보통신 기반구조 보호를 위한 보안 커널 개발 동향", 정보보호학회지, 8권 4호, pp.63~49, 1998. 12

[3] Chris Wright and Cripspin Cowan, "Linux Security Modules: General Security Support for the Linux Kernel", 2002 USENIX Security Symposium, 2002. 6

[4] 박태규 외, "커널 기반의 보안 리눅스 운영체제 구현", 정보보호학회논문지, 11권 4호, pp.33~22, 2001. 8

[5] http://www.secuve.com

[6] http://www.tsonnet.co.kr

[7] http://www.secubrain.com