Solaris 8 기반의 보안 강화용 LKM(Loadable Kernel Module) 설계 †

최은정[0]* 심원태** 김명주*
*서울여자대학교 컴퓨터학 전공 **(주)인젠
{chej*, mjkim}@swu.ac.kr **wtsim@inzen.com

A Design of Loadable Kernel Module enhancing the security on Solaris 8

Eun-Jung Choi* Won-Tae Sim** Myuhng-Joo Kim*
*Dept. Computer Science and Engineering, Seoul Women's University **INZEN Co., Ltd.

요 약

안전한 운영체제(Secure Operating System)는 컴퓨터 운영체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 통합시킨 보안 커널(Security Kernel)을 추가로 이식한 운영체제이다. 본 논문에서는 Solaris 8에서 동작하는 보안 커널을 설계하기 위해 안전한 운영체제와 보안 커널 개발 기술, 솔라리스 운영체제 및 커널 기술을 살펴본다. 이를 토대로 RBAC(Role-Based Access Control)을 지원하고 시스템의 취약점을 감시하는 Solaris 8 기반의 보안 강화용 LKM(Loadable Kernel Module)을 설계한다.

1. 서론

정보보호 침해사고가 증가함에 따라서 안티바이러스(Anti-virus) S/W, 호스트 기반 침입탐지시스템(H-IDS)을 비롯한 많은 제품들은 응용프로그램 수준에서 서버 보안을 위한 방어책으로 사용되어 왔다. 이러한 제품들은 단독으로는 완벽한 보안을 이룰 수 없으며 각각의 특징에 따라 상호보완적으로 동작한다. 날이 갈수록 다양화되고 발전되는 정보보호 침해사고에 효과적으로 대응하기 위해서 최근에는 다양한 보안 제품들을 통합하여 운영하는 추세를 보이고 있다. 정보보호 침해사고는 정보가 반드시 보장받아야 하는 비밀성(confidentiality), 무결성(integrity), 가용성(availability)의 세 가지 요소에 위반되는 행위라고 할 수 있다[1]. 컴퓨터 보안(Computer Security)은 컴퓨터 시스템 사용자의 허가 받지 않은 행동을 탐지하고 예방하는 것이다[2]. 이러한 컴퓨터 보안이 응용 프로그램 수준이 아닌 운영체제 수준에서 파일, 프로세서 등의 컴퓨터 자원에 대한 불법적인 접근을 앞서 방지할 수 있다면 보다 근본적인 컴퓨터 보안을 보장할 수 있게 될 것이다.

안전한 운영체제(Secure Operating System)는 컴퓨터 운영체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 통합시킨 보안 커널(Security Kernel)[3]을 추가로 이식한 운영체제이다[4]. 따라서, 운영체제 수준의 보다 근본적인 컴퓨터 시스템 보안을 가능하게 한다.

본 논문에서는 안전한 운영체제, 보안 커널, 솔라리스 8 운영체제 및 보안요소에 대해 살펴보고 솔라리스 8 기반의 보안 강화용 LKM을 설계한다.

† 본 논문은 2001년 중소기업청 산학연 컨소시엄과제 연구비의 지원으로 수행되었음

2. 안전한 운영체제

일반적인 운영체제는 사용자의 응용프로그램 사용을 통해 발생하는 시스템 호출에 대해 운영체제가 바로 처리하지만, 안전한 운영체제는 다음의 [그림 1]과 같이 보안 커널을 거치게 되면서 다양한 보안 요소들에 대한 검증과 더불어 접근제어 모듈을 통해 시스템 자원에 접근 요청을 보안 정책에 맞게 허가하게 된다.

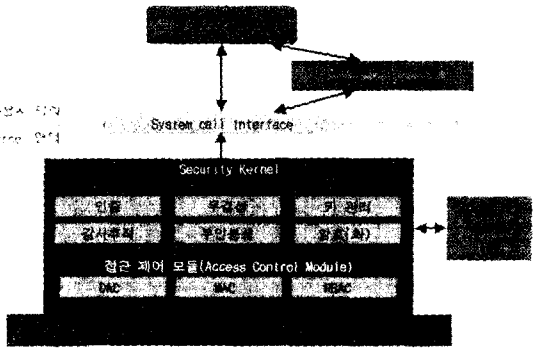

그림 1 안전한 운영체제 개념도[5]

안전한 운영체제를 통해 해당 조직내의 보안 정책 수립 및 적용이 가능하고 컴퓨터 시스템 자원에 대해 강력한 보안을 수행할 수 있다. 미국에서는 이러한 안전한 운영체제 개발을 위해 정부기관인 NSA(National Security Agency) 주도하에 1995년부터 개발을 시작하여 synergy, flask[6]를 발표하였고 민간 업체를 통해서도 상용화되어 판매되고 있는 제품도 다수이다. 국내의 경우에는 관련 연구는 이루어지고 있지만 실제 개발 실적은 최근에 들어서야 나타나고 있다[5].

2.1. 보안 커널

보안 커널은 운영체제에 포함되어 H/W, 운영체제, 이 외의 다른 컴퓨터 자원 사이의 인터페이스를 제공하여 운영체제 전반에 걸쳐서 보안 메커니즘의 적용될 수 있게 한다[7].

보안 커널 설계를 위한 요소는 다음과 같다[8][9].

- Least privilege
- Economy of mechanism
- Open design
- Complete mediation
- Permission-based
- Least common mechanism
- Easy to use

보안 커널이 제공해야 하는 기능은 다음과 같다[10].

- user identification and authentication
- mandatory access control
- object reuse protection
- complete mediation
- audit
- audit log reduction
- trusted path
- intrusion detection

보안 커널 제공 기능 중에서 가장 큰 비중을 차지하는 것이 접근제어 기술이다. 시스템 자원에 대한 허가된 접근만을 허용함으로 안전한 운영체제를 구현하게 된다.

2.2. 운영체제와 통합

운영체제는 개발 방법에 따라 두가지로 나눌 수 있다. H/W와 응용프로그램 사이에 통합된 형태로 동작하는 통합 커널(Integrated Kernal)과 기능에 따라 몇 개의 커널을 나누어 동작하는 마이크로 커널(Micro Kernel)이 있다. Solaris, HP-UX, IRIX, Linux 등이 통합 커널 형태이며 많은 운영체제가 여기에 속한다. 마이크로 커널의 경우는 Digital UNIX, MAch/mk 등 소수만이 개발되었다.

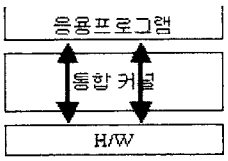

그림 2 통합 커널 기반

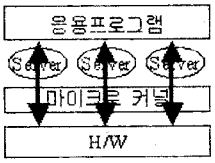

그림 3 마이크로 커널 기반

안전한 운영체제를 개발하기 위해서는 통합 커널 기반의 경우, [그림 2]에서 보이는 것처럼 커널 내부에 보안을 담당하는 부분이 포함되어야 한다. 따라서, 커널이 전체적으로 수정되어야 하는 작업이 필요하다. 그러나, 마이크로 커널의 경우 특정한 기능을 하는 커널이 서버 단위로 제공되기 때문에 보안 커널을 서버 단위로 작성하여 마이크로 커널과의 통신 채널만 형성하여 주면 된다. 마이크로 커널 기반의 운영체제가 적음에도 불구하고 안전한 운영체제 개발에서 주로 활용되는 이유가 여기에 있다[11].

3. Solaris 8 운영체제

Solaris 8은 썬(Sun Microsystems, Inc.)에 의해서 2000년 3월, 64비트에 대응하는 최신 UNIX OS로 발매되었다. Solaris 8은 다음과 같은 특징을 제공한다[12].

- 200가지 이상의 새로운 특징과 향상된 기능
- 런타임 소프트웨어의 무료 일반 사용자 라이센스
- 소스 코드 무료 이용
- 세계적인 수준의 서비스와 지원 프로그램
- 64-비트 환경
- 이전 릴리스와의 바이너리 호환성
- SPARCTM 플랫폼과 Intel Architecture 플랫폼 모두에서 중단없이 사용할 수 있는 가용성
- 혁신적이고 종합적인 소프트웨어 공동 패키지

3.1. 보안 요소

Solaris 8에서 제공하는 주요 보안 요소는 다음과 같다[13].

- B1+ 급의 보안 등급을 제공하는 시스템
- 보안 등급 설정 제공
- 최소 권한(east privilege)의 개념 제공
- 역할 기반 접근제어(role-based access control, RBAC) 제공
- Solaris 8 Operating Environment 기반 환경

솔라리스에서 제공하는 보안 요소 중에서 RBAC(role-based access control)은 다음과 같은 기능을 제공한다. RBAC을 사용해 시스템의 루트 암호를 노출시키지 않고도 제한적인 관리 능력을 할당할 수 있다. 따라서, 본 논문을 통해 설계되는 보안 커널도 RBAC을 활용하게 될 것이다[14].

3.2. 커널 구조

솔라리스는 통합커널[15] 형태이지만 Loadable Kernal Module이라는 개념을 통해서 동적으로 커널을 로드할 수 있다. 다음의 [그림4]는 Solaris 커널에서 핵심 커널과 Loadable Kernel을 보여주고 있다. Loadable System Call을 통해 모듈화된 커널을 load/unload 할 수 있다.

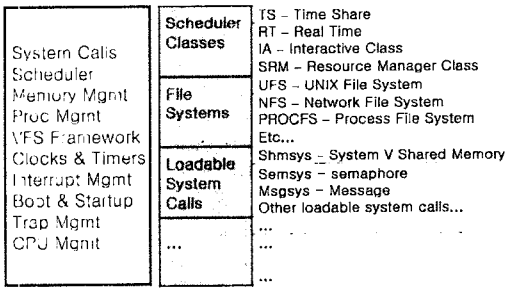

그림 4 핵심 커널과 Loadable 커널

Solaris는 이를 위해 modload, modunload 등의 명령어와 Loadable Kernel Module을 작성하기 위한 자료구조와 시스템 함수를 제공한다[16].

4. Solaris 8 기반의 보안 LKM 설계

Solaris 8의 LKM 형태를 이용한 보안 LKM을 설계한다. 안전한 운영체제의 중요 기술은 접근제어를 지원하고 더불어 시스템의 보안 취약점에 대한 점검이 가능하도록 설계한다.

4.1. 구성

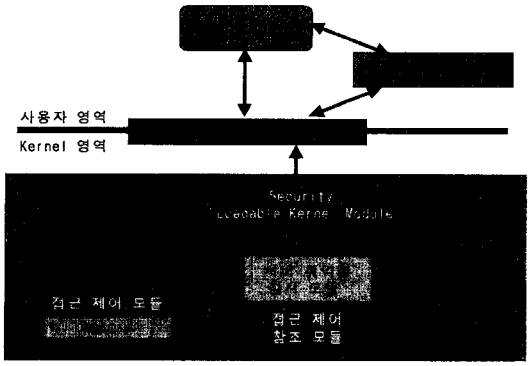

그림 5 Solaris 8 보안 LKM

보안 LKM(Security Loadable Kernel Module)은 접근제어 참조 모듈, 서버 취약점 감시 모듈, 판정 모듈로 나눌 수 있으며 취약점 등의 정보를 저장한 별도의 보안 DB(Security DB)로 구성된다.

4.2. 접근제어 참조 모듈

접근제어는 인증된 사용자에 대해 컴퓨팅 자원, 통신 자원 및 정보자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다. 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 커맨드의 발행을 포함하고 있다. 즉, 접근통제는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한부여를 위한 수단이 된다[17].

본 논문에서는 Solaris 8이 제공하는 RBAC(Role-Based Access Control) 기술을 참조하여 접근제어를 지원하여 효율성을 높인다.

Solaris 운영체제에서 제공하는 RBAC은 다음과 같은 흐름을 통해 동작한다[18].

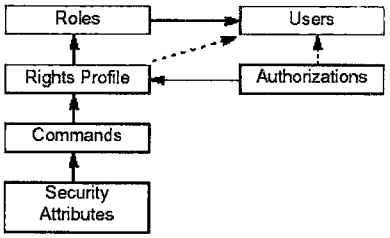

그림 6 RBAC 흐름도

4.3. 서버 취약점 감시 모듈

커널 수준에서 탐지 가능한 취약점을 감시한다. 이것은 접근제어 기술을 주요하게 다루는 기존의 안전한 운영체제를 보완하게 된다. 커널 수준에서 미리 예측할 수 있는 취약점들에 대한 감시가 이루어진다. 예를 들어 SetUID를 이용한 공격, 메모리 접근을 통한 버퍼 오버플로우 발생 등이 있다. 이러한 감시 모듈은 응용 프로그램에서 동작하는 H-IDS, 스캐너 등의 일부 기능을 커널 수준에서 수행시키는 것이다.

4.4. 판정 모듈

서버 취약점 감시 모듈과 접근제어 참조 모듈에 대한 로그를 작성하고 시스템 보안의 위협요소가 발생하면 경고를 발생하거나 해당 세션을 중지시키는 방법을 이용하여 능동적으로 대처한다.

5. 결론

Solaris 8 에서 동작하는 보안 강화용 LKM의 설계는 접근제어 기술 중심으로 전체 운영체제의 변경이 필요한 안전한 운영체제 연구와 달리, 사용하고 있는 Solaris 8 운영체제에 번거롭지 않게 추가하여 동작할 수 있다. Solaris 8이 제공하는 접근제어 기술은 RBAC을 이용하여 운영체제 기술의 활용을 가능하게 하였다. 서버 취약점 감시 모듈을 통해 원천적인 보안 강화로 강력한 시스템 보안을 제공한다.

6. 참고문헌

[1] Charles P. Pfleeger, "Security in Computing Second Edition", Prentice-Hall International Inc., pp. 4~11, February 1999
[2] Dieter Gollmann, "Computer Security", JOHN WILEY & SONS, pp. 5~9, February 1999
[3] Ames, S., et al. "Security Kernel Design and Implementation: An Introduction." IEEE Computer, v16 n7, pp. 14~23, Jul 1983
[4] 한국정보보호진흥원, "전산망 정보보호-접근통제 기술", 한국정보보호진흥원, 1996.12.
[5] http://www.kisa.or.kr/technology/sub3/SOS.htm
[6] http://www.cs.utah.edu/flux/fluke/html/flask.html
[7] Charles P. Pfleeger, "Security in Computing Second Edition", Prentice-Hall International Inc., pp292~pp297, February 1999
[8] Saltzer J., "Protection and the Control of Information Sharing in MULTICS", Comm ACM, v17, n7, pp.388~402, Jul 1974
[9] Saltzer J., Schroeder M., "The Protection of Information in Computing Systems." Proc IEEE, v63 n9, pp. 1278~1308, Sep 1975
[10] Charles P. Pfleeger, "Security in Computing Second Edition", Prentice-Hall International Inc., pp289~pp292, February 1999
[11] http://www.kisa.or.kr/technology/sub3/SOS_9901.html
[12] http://sun.co.kr/products/software/os_platforms/solaris/solaris.html
[13] http://www.sun.com/software/solaris/trustedsolaris/
[14] http://www.sun.co.kr/products/software/os_platforms/solaris/product/8/8.html
[15] Jim Mauro, Richard McDougall, "SOLARIS Internals Core Kernel Architecture", PH PTR, pp. 10~13, 15 Oct. 2000
[16] Jim Mauro, Richard McDougall, "SOLARIS Internals Core Kernel Architecture", PH PTR, pp. 116~122, 15 Oct. 2000
[17] http://www.kisa.or.kr/technology/sub3/AC_9901.html]
[18] Sun Microsystems, Inc. "RBAC in the Solaris Opening Environment White Paper", Sun Microsystems, Inc., April 2001