情 報 保 護 學 會 誌
第 13 券 第 4 號, 2003. 8

동적 기능 구성이 가능한 능동형 Secure OS 시스템

김 정 녀*, 손 승 원*, 이 철 훈**

요 약

능동형 Secure OS 시스템은 운영체제 커널에 접근 제어, 사용자 인증, 감사 추적, 암호화 파일 시스템, 신뢰 채널, 동적 구성 등의 보안 기능을 추가 구현하여 시스템에 발생 가능한 해킹을 방지하고 차단하는 시스템을 말한다. 이러한 능동형 Secure OS 시스템은 시스템 해킹을 탐지하거나 시스템 해킹을 감지하였을 때 동적으로 구성을 바꾸는 등의 조치를 취하는 시스템 기능이 필요하다. 본 고에서는 능동형 Secure OS의 주요 기능과 함께 핵심 기술의 구현 내용을 기술하며, 시스템내의 감사 추적 기능에 의해 능동적으로 시스템을 구성하고 실시간 조치가 가능하도록 한 능동형 Secure OS 시스템을 소개한다.

Ⅰ. 서 론

인터넷과 같은 네트워크 환경에서 유닉스가 가지는 개방성은 중요한 특징이지만, 컴퓨터 시스템내의 정보보호를 향상시키기 위한 기법은 현재 표준 유닉스에서는 매우 부족한 실정이다. 이에, 기존 유닉스 시스템의 취약점을 보완하는 패치 버전이나 업그레이드를 통한 임시 방편적인 방법보다는 원천적으로 운영체제 자체의 보안성을 강화한 안전한 운영체제의 필요성이 대두되고 있다. 또한 최근 들어 버퍼 오버플로 등과 같은 운영체제 자체의 보안상의 결함을 이용한 시스템 해킹이 증가하여, 비인가 된 사용자가 해당 시스템에 침입하여서 시스템내의 중요한 정보를 가로채거나 중요한 데이터가 들어 있는 파일들을 변경하는 등의 해킹사고가 잇따라 발생하고 있다.

기존 유닉스 시스템의 취약점을 보완하는 패치 버전이나 업그레이드를 통한 임시 방편적인 방법보다는 원천적으로 새로운 안전한 운영체제 개발과 같은 근본적인 해결 방법이 바람직하다[1]. 또한 요즈음 들어서는 공개 소프트웨어 개념에 의해 리눅스를 비롯한 FreeBSD, OpenBSD 등 많은 운영체제 들이 공개되는 추세에 있어서 더 더욱 운영체제의 보안 결함을 이용하는 시스템 해킹 수법 들이 늘고 있다. 특히, 산업 사회를 거쳐 고도의정보화 사회로 진입하면서, 고도의 각종 통신 수단이나 국가 기반 구축을 위한 시스템들이 더욱더 위험에 처해 있다. 이러한 환경에서 응용 프로그램 수준의 보안으로는 정보시스템의 완벽한 보안이 될 수 없음으로 운영체제 자체의 결함을 해결하고 시스템 차원의 정보보호 기능을 제공하는 Secure OS 기술이 필요함을 인식하여야 할 것이다.

이러한 운영체제 상에 내재된 보안상의 결함으로 인하여 발생할 소지가 있는 각종 해킹으로부터 시스템을 보호하기 위하여, 기존의 운영체제 내에 보안 기능을 추가한 능동형 Secure OS를 소개하고자 한다[1,2]. 능동형 Secure OS는 시스템 사용자에 대한 다중 수준의 식별 및 인증, 강제적 접근 통제, 임의적 접근 통제, 역할 기반 접근 통제의 최소 권한 분리 기능, 불법 정보 유출을 막을 수 있는 데이터의 안전한 저장 기능 그리고 안전한 전송기능 등의 보안 기능 요소들을 갖추어야 한다[5,11]. 더 나아가서는 사용자의 시스템 사용 현황을 파악하기 위하여 감사 추적하고 시스템내의 기능을 동적으로 구성하여 보안의 수준을 높이거나 낮추는 기능까지 확장될 수 있다.

본 고에서는 이러한 능동형 Secure OS의 기본 기능을 소개하고, 시스템 감사에 의하여 능동적으로 대처하거나, 감지된 해킹에 대한 대응을 할 수 있는

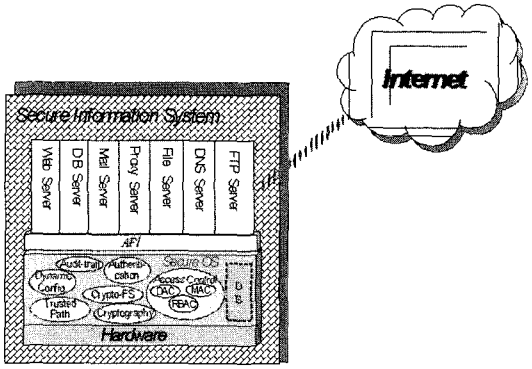
* 한국전자통신연구원(jnkim, swsohn@etri.re.kr)
** 충남대 컴퓨터공학과 부교수(chlee@ce.cnu.ac.kr)

능동형 Secure OS 시스템을 소개한다. 본 고의 구성은 2장에서 능동형 Secure OS의 개념과필요성을 살펴보고, 능동형 Secure OS의 구조, 기능 그리고 현재 구현 정도를 소개한다. 3장에서 그중 핵심 기술인 능동적인 구성 및 실시간 조치의 설계및 구현 내용을 기술한다. 4장에서 능동형 Secure OS의 핵심 기능을 바탕으로 기능들의 동적 구성과 동작 시나리오를 소개하며, 마지막으로 앞으로 더 해야 할 연구의 방향을 제시해 보고자 한다.

II. 능동형 Secure OS 시스템

1. 능동형 Secure OS 시스템 개념

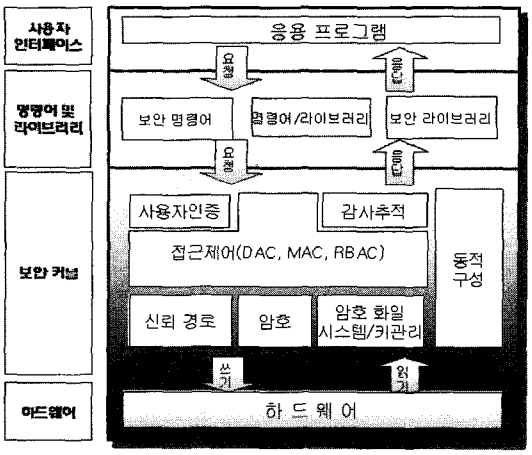
시스템에 대한 보안은 기본적으로 구조를 변경하지 않고 여러 가지 방법으로 개선될 수 있으나 아주 민감한 정보를 보호하고자 한다면, 강력한 개발 전략과 특별한 시스템 구조가 요구된다. 능동형 Secure OS는 기존의 운영체제 내에 내재되어 있는 문제점을 해결하기 위하여 운영체제를 설계하는 기술로, 운영체제 내에 보안 기능을 추가하여 운영체제의 결함을 이용한 시스템 해킹을 방지하고 시스템의 이상 상태를 감지해서 시스템의 기능을 동적으로 구성하여 보안성을 강화한 것이다. 능동형 Secure OS는 개념적으로 [그림 1]과 같이 나타낸다.



[그림 1] 능동형 Secure OS 개념도

2. 능동형 Secure OS 시스템 구조 및 기능

위와 같은 능동형 Secure OS의 기본 기능에 따라 능동형 Secure OS가 가져야 할 운영체제 구조를 기능 별로 구분한 것은 다음 [그림 2]와 같다. 능동형 Secure OS가 실행되는 정보시스템은 크게 인터넷



[그림 2] 능동형 Secure OS 구조도

서버와 데이터 운용 서버용도로 사용될 수 있다. 인터넷 서버의 경우는 웹 서버, FTP 서버, DNS 서버, Proxy 서버, Mail 서버 등을 들 수 있고, 데이터 운용 서버의 경우에는 DB 서버나 파일 서버로 쓰이는 경우이다. 그 이외에도 군이나 관공서 등에서 국가용 기반시스템으로 활용이 가능하며, 다음과 같은 기능들을 제공한다.

2.1 사용자 인증

다중 수준 보안 정책의 사용자 인증 기능을 제공한다. 기존의 신분 기반 사용자 인증은 ID와 패스워드를 가지고 인증하므로 트로이 목마 취약성을 가지고 있으므로, 사용자가 갖는 등급과 범주, 역할 그리고 스마트카드 등에 의한 사용자 신분 확인 기능을 추가한다. 이는 강제적인 접근제어의 기준이 되는 보안 라벨(Security Label)에 의한 신분 확인과 역할 기반의 접근제어에 활용될 사용자 직무에 의하여 신분을 확인할 수 있다. 이에 추가로 스마트카드에 의하여 인증을 하도록 확장하였으며, 스마트카드 인증의 경우는 각 사용자를 식별할 수 있는 키를 저장한 스마트카드를 사용하여 신분을 확인하도록 되어 있다.

2.2 감사 추적

사용자의 정보 및 상태를 로그에 기록하고 분석할 수 있도록 하는 일종의 시스템 모니터링 기능이라 할 수 있다. 예를 들자면 사용자 인증에 실패한 경우에는 사용자 인증 정보, 날짜, 시간, 성공 여부, 시도 횟수 등을 기록하도록 한다. 또한 시스템 호출 수준의 사용자 처리정보를 로그에 기록한다. 이는 setuid,

setgid, link, read, write, exec 등과 같은 중요 시스템 호출을 사용하는 경우나 보안 관리자의 접근 제어 속성을 변경하는 시스템 호출 처리 정보도 로그에 기록한다. 이는 객체에 대한 접근 여부와 시간 등을 기록하여 이상상태가 발생하였을 때 추적 할 수 있도록 한다. 그 이외에도 로그의 기록을 분석하여 이상 상태를 알릴 수도 있다. 가장 중요한 것은 로그의 크기와 시스템의 성능을 위하여 Low, Middle, High 세단계로 나누어 로그 기록이나 감사의 수준을 사용자가 정할 수 있도록 한다.

2.3 접근 제어

접근 제어 기능은 시스템 내의 자원(예를 들자면 파일, 파일 시스템, 장치, 메모리 등)에 대한 허가되지 않은 접근을 통제하여, 불법적인 자원의 사용, 노출, 수정, 파괴 등 불법적인 실행을 막는 것을 말한다. 접근 제어 정책은 다음과 같다.

o 임의적 접근 제어(DAC)
- 신분기반의 접근 제어 정책으로 주체나 또는 그들이 속해 있는 그룹들의 신분 즉 ID에 근거하여 객체에 대한 접근을 제한하는 기법으로 트로이 목마의 취약성 가진다. 메커니즘으로는 액세스 제어 리스트(Access Control List), 권한 리스트(Capability List) 등이 있는데, 액세스 제어 리스트를 이용하여 구현하였다.

o 강제적 접근 제어(MAC)
- 규칙 기반의 접근 제어 정책으로 보안라벨이라고 하는 보안등급과 범주에 의한 강제적인 접근제어 방식으로 계급 체계가 있는 군 또는 공공기관에서 사용될 수 있다. BLP 접근 제어 모델을 적용하여, 해당 등급의 자료만 접근 하도록하며, 상위 등급의 자료는 읽기를 막고(No Read Up), 하위 등급의 자료는 쓰기를 금지하는(No Write Down) 형태의 등급별 접근 제어와 해당되는 부서와 같은 범주에 따라 접근을 제어하는 방식이다.

o 직무기반 접근 제어(RBAC)
- DAC과 MAC 혼합 형태의 접근 제어 정책으로 DAC과 MAC 방식의 단점을 해결하기 위해 직무 또는 역할 기반의 접근 제어 방식으로 상업적인 환경에 적합하다. 자원에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내에서의 개인 직무에 따라 결정하는 것으로 이는 보안 관리의 유연성 및 효율성을 제공하는 장점을 갖는다.

2.4 암호

암호 기능은 정보의 비밀성을 제공하기 위하여 사용되는 것으로 암호화와 복호화에 쓰이는 키의 상이 여부에 따라 암호 방식도 나뉘어 진다. 본 시스템에서는 DES, Blowfish 등과 같이 널리 사용되는 암호화 방식을 이용한다. 능동형 Secure OS에서 암호 기술은 인증 과정이나, 데이터를 보호하기 위하여 사용될 수 있으며, 그 이외에도 하드디스크를 가로채 가도 파일을 읽을 수 없도록 하는 디스크에 암호화해서 저장하는 암호화 파일 시스템용 암호화나 네트워크상의 패킷 가로채기에 의한 정보 유출을 막기 위한 데이터 전송을 위한 암호화에 사용된다.

2.5 암호화 파일 시스템

시스템내의 백업 관리자와 같은 경우 시스템내의 모든 객체들을 읽을 수 있어야 백업을 할 수 있을 것이나, 시스템내의 중요 데이터나 백업 관리자가 보면 안되는 중요한 파일들도 있을 것이다. 이를 위하여 백업 관리자는 시스템내의 모든 객체를 읽기는 가능하나 쓰기는 할 수 없도록 하며 인가되지 않은 사용자 이면 파일이 암호화 된 채로 보이도록 하는 암호화 파일 시스템 기능이 필요하다. 그 이외에도 하드디스크 분실 시에도 해당되는 데이터가 암호화 되어 저장되어 있으므로 암호 키 값이 없는 경우에는 데이터를 읽을 수 없으므로 하드디스크 분실 시에도 정보 유출이 되지 않는다는 장점이 있다.

2.6 신뢰 경로

신뢰 경로 기술은 크게 두가지로 나누어 볼 수 있다. 사용자와 시스템간의 신뢰 경로 기술로 사용자가 시스템에 로그인할 때 또는 특정 사용자가 패스워드를 변경할 때 사용자가 입력하는 패스워드 등을 가로채기 할 수 있다. 이때는 신뢰할 수 있는 경로를 제공하여야 하므로 본 시스템에서는 사용자에게 로그인 역할을 주어 로그인역할이 아닌 사용자는 접근을 허가 하지 않는 형태로 신뢰 경로 기술을 제공한다. 둘째는 시스템과 시스템간의 신뢰 경로 기술로 이는 Telnet이나 Ftp 등과 네트워크를 이용하는 경우 로그인 시나 데이터전송 시에 데이터를 가로채기 할

수가 있다. 이때는 신뢰할 수 있는 신뢰 채널 기능을 제공하여야 하므로 암호화하여 전송하고 복호화하여 받아들일 수 있는 능동형 Secure OS 시스템 간의 암호화된 신뢰 채널 기능을 제공한다.

2.7 동적 구성(Dynamic Configuration)

동적 구성 기술은 시스템 상태를 모니터링 하는 감사 추적 기술과 연동하여 시스템의 보안 수준을 조절할 수 있는 기술이다. 보안의 수준이 높아지면 시스템의 성능이 떨어지므로 시스템이 이상 상태를 감지하였을 때나 시스템 보안 관리자의 요구에 의해서 시스템의 보안 수준을 정하여 줄 수 있는 기술이다. 능동형 Secure OS 시스템에서는 각 기능의 보안 수준을 Low, Middle, High로 정하여, 해당 시스템의 기능을 동적으로 구성 할 수 있도록 한다.

Ⅲ. 핵심 기술 설계 및 구현

1. 접근제어 설계 및 구현

능동형 Secure OS 시스템에서의 접근 제어 기능은 크게 세가지로 구현하였다. 그 중 DAC과 MAC은 TCSEC 기준[10]을 만족하기 위하여 구현하였으며, RBAC은 상업적인 환경에 적합하므로 구현하였다. 이 세가지의 접근제어 정책을 조합하여 낮은 보안성부터 높은 보안성까지를 제공할 수 있다.

1.1 DAC

DAC은 신분기반의 접근 제어 정책으로 ID/Passwd 기반의 인증을 거쳐서 해당 ID의 사용자 접근을 객체의 접근제어 리스트의 permission에 의하여 통제하는 기법으로 기존의 유닉스 보다는 좀더 fine-grain하게 접근을 통제할 수 있다.

DAC 메커니즘의 경우에는 기존의 리눅스에서 처럼 객체의 소유자, 소유 그룹, 다른 사용자들로 지정된 해당 객체의 접근제어 리스트를 좀더 정밀하게 나누어 접근을 통제하는 것으로 소유자 이외의 개별적인 사용자별로, 소유 그룹 이외의 특정 그룹에 따라 정해진 접근을 통제하는 형태로 확장을 시켰다. 이는 기본 IEEE POSIX P1003.1e, 2c인 Security Extension 표준 규격에 따라 정의된 DAC 기능을 제공한다. 능동형Secure OS에서 제공하는 DAC은 [그림 3]과 같다.

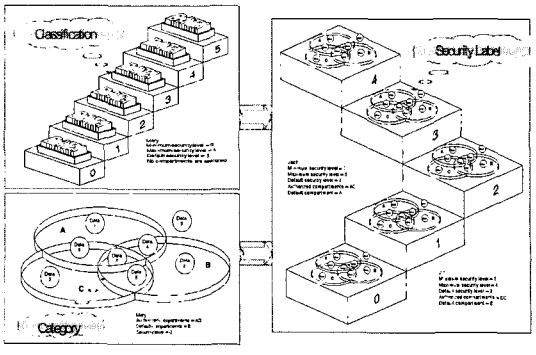
```
• Linux permission
rwxr--r--  1john   research   89  Oct 6 22:30  demo
• Access Control List of file demo
ACL_USER_OBJ::rwx                 == the owner of file
ACL_USER:bob:rwx
ACL_USER:fred:r-x
ACL_GROUP_OBJ::r--                == the group of file
ACL_GROUP:manager:rw-
ACL_GROUP:staff:r-x
ACL_OTHER::r--                    == the other
ACL_MASK::rwx
```

[그림 3] DAC 구현

1.2 MAC

MAC은 규칙을 기반으로 한 강제적인 접근제어 정책으로 시스템 내의 사용자각각에 등급과 범주를 두어서 해당 등급이나 범주에 따라 접근을 통제하는 기법이다. BLP(Bell & LaPadula) 모델을 기반으로 커널 내에 구현하였으며 시스템 내의 등급은 크게 5가지, 범주는 64개까지 구분하여 사용 가능하다.

MAC 메커니즘의 경우는 실생활에 비유하면 비밀 취급인가를 갖는 것을 구현하는 것으로 사용자의 등급을 나누어 등급별 트로이 목마 문제를 해결한 것을 말한다. 등급은 다음과 같이 사용자의 등급에 따라 동일한 등급의 주체는 동일한 등급의 객체를 읽기/쓰기 할 수 있도록 하는 것을 기본 원칙으로 하여 해당 등급의 주체가 본인이 가진 등급 보다 높은 등급의 객체를 읽을 수 없고(No Read Up), 해당 등급의 주체가 본인이 가진 등급보다 낮은 등급의 객체를 쓸 수 없는(No Write Down) 규칙에 의한 접근을 통제하는 방식이다. 이는 BLP(Bell & Lapadula) 모델을 준수하는 것으로 계층적인 관계의 접근은 통제가 가능하나 동일한 등급내의 다른 그룹간의 상호 관계에 의한 접근 통제가 필요하므로, 부서 또는 범주라 하여 해당되는 범주에 속한 주체만이 해당 객체를 접근할 수 있도록 하는 범주

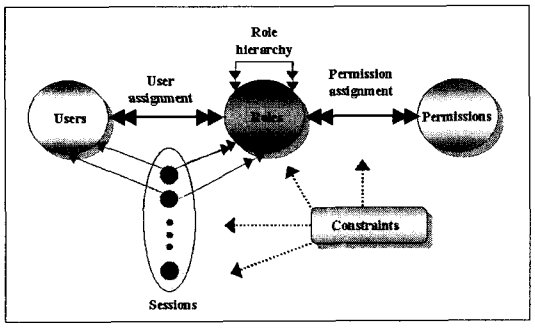


[그림 4] MAC 구현

에 의하여 접근 통제까지 한다. 능동형 Secure OS에서 제공하는 MAC은 [그림 4]와 같다.

1.3 RBAC

직무 기반의 접근 제어 정책인 RBAC은 상업적인 환경에서 가장 좋은 접근제어 정책으로 이는 Rabi Sandu 교수가 제안한 RBAC96 모델을 기반으로 커널 수준에서 구현하였다. RBAC 메커니즘의 경우는 위의 DAC과 MAC의 혼합된 형태로 상업적인 환경에 가장 적합한 접근제어 방식으로 해당 주체의 권한을 최소화한 최소 권한(Minimum Privilege) 분리 원칙으로 사용자의 역할이나 직무에 최소화된 권한을 부여하고 그 역할이나 직무에 따라 접근을 통제하는 방식을 말한다. RBAC기반의 접근 제어는 다음 [그림 5]와 같다.



[그림 5] RBAC 구현

2. 인증 설계 및 구현

인증의 타입은 크게 세가지로 구분한다. 첫번째 타입은 기존의ID/Passwd와 같은 지식을 기반으로 한 인증 기법이고, 두번째 타입은 전자 Key와 같은 소유에 의한 인증 기법이다. 세번째 타입은 사용자 생체 정보와 같은 특징에 의한 인증 기법이다. 능동형 Secure OS 시스템에서는 지식 기반 인증과 소유 기반의 인증을 제공하므로 이 두 가지 인증 정책을 조합하여 낮은 보안성부터 높은 보안성까지를 제공할 수 있다.

2.1 지식 기반 인증(Knowledge Mechanism)

지식 기반은 인증은 사용자가 알고 있는 것이 무엇인가를 가지고 인증하는 방법이다. 그 예로서는 Passwords, Pass phrases, 그리고 PIN(Personal Identification Number) 등이 있다. 본 시스템에서는 사용자 ID에 대한 Password에 의해 인증한다.

2.2 소유 기반 인증(Ownership Mechanism)

소유 기반 인증은 사용자가 가지고 있는 것을 가지고 인증하는 방법이다. 그 종류에는Real Key 또는 Electronic Key, Magnetic strip Card 등이 있다. 본 시스템에서는 스마트카드를 기반으로 한 사용자 인증 메커니즘을 제공한다.

2.3 특징 기반 인증(Characteristic Mechanism)

특징 기반 인증은 사용자의 특징을 가지고 인증하는 방법으로 사용자가 가지는 생체적인 특징을 가지고 인증하는 것이다. 그 종류에는 지문, 망막, DNS 패턴, 그리고 손금을 이용한 인증 등이 있을 수 있다.

3. 감사 추적 설계 및 구현

능동형 Secure OS 시스템에서의 감사추적은 크게 두가지로 나누어서 구현이 되었다. 첫째는 시스템의 상태를 로그하고 기록하는 부분으로 이는 크게 Low, Middle, High로 하여 로그 정도를 구분하였다. 둘째는 이렇게 로깅된 감사 로그나 시스템의 이상상태 감지에 의하여 조치하는 부분이다.

3.1 감사 로그 기록

시스템의 상태를 로그에 기록하는 기능으로 크게 세가지 보안 수준으로 로그를 할 수 있다. Low 수준은 일부시스템 호출만 감사 로그에 기록하는 것으로 사용자 인증/식별 시의 이벤트에 해당하는 시스템 호출이나 setuid, setgid 등과 같은 시스템 호출의 경우에 기록하는 것을 말한다. Middle 수준에는 중요 시스템 호출을 감사로그에 기록하는 것으로 사용자 주소 공간으로의 객체 추가와 객체 삭제 등과 같은 시스템 호출 들을 모두 포함한다. High 수준은 시스템 호출에 추가로 보안 이벤트들을 감사로그에 기록한다. 추가 보안 이벤트들은 시스템 관리자 또는 보안 관리자 등과 같은 동작에 해당하는 이벤트 들이 포함된다. 예를 들면 시스템 내의 보안 관련 형상의 추가/삭제/변경 등의 동작이 이에 해당한다.

3.2 이상 상태 감지

시스템의 이상 상태 감지는 시스템감사 로그의 내용이나 시스템 해킹의 징후를 감지하여 시스템의 이상 상태를 감지하는 것이다. 이는 주로 감사 로그

파일 내용에 있는 시스템 호출 들을 이용하여 시스템 내부 사용자의 활동을 감시한다. 감사 로그에 의한 이상 상태 감지는 시스템내의 프로세스나 TTY 단위의 모니터링으로 로그 분석에 의한 이상 상태를 감지한다. 이에 덧붙여 버퍼 오버플로나 포맷 스트링 어택 등과 같은 경우에는 시스템 예외 처리(Exception)를 감지하여 시스템 보안 관리자에게 알려주거나, 관리자가 지정해 놓은 경우에는 자동으로 시스템의 보안 수준을 높여 줄 수 있다.

4. 데이터 암호화 설계 및 구현

능동형 Secure OS 시스템에서의 데이터 암호화 기능은 크게 두가지로 구현하였다. 첫째는 데이터의 안전한 저장을 위한 암호화이다. 둘째는 데이터의 안전한 전송을 위한암호화 기법이다. 이 데이터 암호화 기법을 조합하여 낮은 보안성부터 높은 보안성까지를 제공할 수 있다.

4.1 암호화 파일 시스템

암호화 파일 시스템은 시스템내의 데이터를 암호화하여 저장하며 인가된 사용자에게는 텍스트 형태로 보이게 하고 비인가 된 사용자에게는 암호화된 형태로 보이게 하여 불법 정보 유출을 막을 수 있다. 이는 하드디스크 분실 시에라도 하드디스크의 데이터를 보호하기 위하여 키값을 가지고 있지 않으면 하드디스크 내의 데이터를 읽을 수 없도록 한다. 시스템 내부 사용자라도 인가된 사용자가 아니면 파일내의 데이터를 읽을 수 없다.

4.1 신뢰 채널

신뢰 채널 기법은 신뢰 경로 기능 중에 하나로 네트워크로 전송되는 데이터에 대한 안전성을 보장하여 주는 기법이다. 이는 네트워크 데이터의 암호화 전송에 의해 기밀성과 무결성을 제공하므로 네트워크 데이터의 가로채기를 막을 수 있다.

5. 동적 구성

능동형 Secure OS 시스템에서의 동적 구성은 시스템내의 기능을 동적으로 구성하여 시스템의 성능과 효율성을 보장하기 위한 기능이다. 시스템의 동적 구성은 감사 추적에서 감지되는 시스템의 이상 상태에 따라 바로 연동되어 시스템에 적용될 수도 있으나, 보통은 이상 상태를 보안 관리자에게 알려 조치를 취할 수 있도록 한다. 본 시스템에서의 동적 구성은 크게 세가지 수준으로 나누어서 제공된다. 이에 관련하여서는 4장에서 자세히 기술한다.

Ⅳ. 동적 구성 및 동작 시나리오

시스템 동적 구성을 위하여 기본적으로는 Low 수준을 유지한다. 시스템의 동작 상태에 따라 보안 수준을 정하여 시스템의 보안성을 줄 수 있다. 시스템의 보안성은 Low, Middle, High 로 그 보안성의 정도는 각 기능 별로 다음 〔표 1〕과 같다.

〔표 1〕 능동형 Secure OS의 보안 수준

보안수준 / 기능	Low	Middle	High
접근제어	Fine-grained DAC	DAC+RBAC	DAC+RBAC+MAC
사용자 인증	기본ID/Passwd	ID/Passwd+RBAC	ID/Passwd+DAC+RBAC+MAC+Smart Card
감사추적	Low	Middle	High
데이터암호화	None	암호화파일시스템	암호화파일시스템+신뢰채널
동적구성	Static	Static	Static+Automatic

능동형 Secure OS 시스템은 시스템 초기화 시에 구성된 Low 수준으로 설정되어 동작된다. 시스템이 동작되다가 감사추적 모듈에서 분석되는 감사 내용에 따라 시스템내의 보안 관리자에게 Alert 이 보내지고, 이에 따라 보안 관리자가 조치를 취할 수 있도록 하는 것이다. 감사 내용에 setuid, setgid 의 내용이나 사용자 인증 및 식별 등과 같은 특별 이벤트가 발생한 경우에 보안 관리자에게 Alert 이 보내진다. 보안 관리자는 보내진 Alert 내용을 보고 프로세스를 Kill 하는 등과 같은 조치를 취하고 그 심각성에 따라 시스템을 좀더 강화된 상태인 Middle 로 설정할 수 있다. 또한 버퍼 오버플로나 포맷 스트링 어택 등이 발생한 경우에도 예외 처리에 따라 시스템 내의 보안 관리자에게 Alert 이 보내지고, 이에 따라 보안 관리자가 조치를 취한다. 이 경우에도 보안 관리자가 심각성을 고려하여 시스템내의 보안 정도를 High로 설정 할 수 있다.

Ⅴ. 결 론

본 고에서는 능동형 Secure OS의 개념과 능동형 Secure OS의 필요성을 기술하고, 핵심이 되는 기

술들을 소개하였다. 또한 능동형 Secure OS 시스템내의 동적 구성 기능은 감사 추적 기능과 연계하여 시스템내의 보안성을 조절할 수 있도록 하였다. 이는 커는 수준에서의 많은 보안 기능 수행에 따라 성능적인 오버헤드가 많고 효율성이 떨어지는 단점을 극복하고, 각 기능의 조합에 따라 성능과 효율성을 높일 수 있음을 알 수 있다.

최근 들어서는 버퍼 오버플로 뿐만 아니라 분산 서비스 거부 공격 등과 같은 해킹 기법들에 의해 시스템을 halt 상태로 만들기도 하는데, 이러한 해킹 기법을 위하여 시스템 차원의 감사 추적 기능 이나 시스템 모니터링 기능으로 탐지하고 차단할 수 있도록 연구하여야 할 것이다. 이에 덧붙여서 현재는 보안 관리자의 판단과 요구에 따라 시스템의 기능을 동적으로 구성하는 방법을 위주로 하고 있는데, 자동으로 감지하고 그 심각도에 따라 보안 수준을 정하여 시스템의 기능을 동적으로 구성하도록 하는 기법에 대한 연구도 지속적으로 해 나가야 할 것이다.

참 고 문 헌

[1] J. N. Kim, S. W. Sohn, "The Technology of Secure Operating System for Secure Networking," Proc. of NETSEC-KR 2002, 2002.

[2] J. G. Ko, J. N. Kim, & K. I. Jeong, "Access Control for Secure FreeBSD Operating System," Proc. of WISA2001, The Second International Workshop on Information Security Applications, 2001.

[3] Peter A. Loscocco, Wtephen D. Dmalley, Patric A. Muckelbauer, Ruth C. Taylor, S.Jeff Truner, JohnF. Farrel, 'The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments', National Security Agency, 1997.

[4] Bell, David Elliott, & Leonard J. La Padula, "Secure computer system: Unified exposition and multics interpretation," MITRE Technical Report 2997, MITRE Corp, Bedford, MA, 1975.

[5] David F. Ferraiolo, Ravi Sandu, & Serban Gavrila, "A Proposed Standard for Role-Based Access Control," ACM transaction on Information and System Security, Vol.4, No.3, pp.224~274, Aug. 2001.

[6] Ray Spencer, Stephen Smalley, Peter Loscocco, Mike Hibler, Dave, Anderson, and Jay Lepreau, "The Flask Security Architecture : System Support for diverse Security Policies", Proceeding of th 8th USENIX Security Symposium, 1999.

[7] UNICOS Multilevel Security(MLS) Features Users Guide, SG-21111 10.0, http://rcs21.urz.tu-dresden.de:80/ebt-bin/nph-dweb/dynaweb./@Generic__BookTextVie.

[8] http://www.hpcc.gov/pubs/blue97/nsa/secureos.html.

[9] http://www.cs.utah.edu/flux/fluke/html/linux.html.

[10] DOD 5200.28-STD. 'Department of Defense Trusted Computer System Evaluation Criteria', December 1985.

[11] D.Ferraolo and R. Kuhn, "Role-Based Access Control", Proceeding of the 15th National Computer Security Conference, 1992.

[12] R. Graubart. "Operating System Support for Trusted Applications", Proceedings of the 15th National Computer Security Conference, 1992.

[13] M. Harrison et al. "Protection in Operating Systems", Communications of ACM 19(8), August 1976.

[14] Secure Computing Corporation, "Assurance in the Fluke Microkernel: Formal Security Policy Model", Technical report MD A904-97-C-3047 CDRL A003, March 1998.

[15] Dorothy E. Denning, 'Information Warfare and Security',Addison-wesley, April 1999.

[16] J. G. Ko, S. Y. Doo, S. K. Un, & J. N. Kim, "Design and Implementation for Secure OS based on Linux", WISA2000, Vol.1 No.1, pp.175~181.

〈著 者 紹 介〉

김 정 녀 (Jeong-Nyeo Kim)
종신회원

1987년 2월 : 전남대학교 전산통계학과 졸업
1995년~1996년 : Open Software Foundation Research Institute 공동 연구 파견(미국)
2000년 2월 : 충남대학교 컴퓨터공학과 석사
2000년 3월~현재 : 충남대학교 컴퓨터공학과 박사과정
1988년~현재 : 한국전자통신연구원, 선임연구원(팀장)
관심분야 : 인터넷 정보보호, Secure OS, 네트워크 보안

손 승 원 (Sohn, Sung-Won)
정회원

1984년 2월 : 경북대학교 전자공학과 졸업
1994년 2월 : 연세대학교 컴퓨터공학과 석사
1999년 2월 : 충북대학교 컴퓨터공학과 박사
1991년~현재 : 한국전자통신연구원, 책임연구원(부장)
관심분야 : 이동인터넷 보안, 정보보호, 네트워크 보안

이 철 훈 (Cheol-hoon Lee)

1983년 2월 : 서울대학교 전자공학과 졸업
1983년~1986년 : 삼성전자 컴퓨터 개발실 연구원
1988년 2월 : 한국과학기술원 전기 및 전자공학과 석사
1992년 2월 : 한국과학기술원 전기 및 전자공학과 박사
1992년~1994년 : 삼성전자 컴퓨터 사업부 선임연구원
1995년~현재 : 충남대학교 컴퓨터공학과 부교수
관심분야 : 운영체제, 병렬처리, 결함 허용 및 실시간 시스템 등