정보전에 대비한 정보통신기반 구축용 보안 운영체제 기술

한국전자통신연구원 김정녀
경산대학교 하경주
한국전자통신연구원 윤이중 · 조현숙

1. 서 론

산업 사회를 거쳐 고도의 정보화 사회로 진입하면서, 고도의 각종 통신 수단이나 세계 각국에서 경쟁적으로 구축하고 있는 국가정보통신기반 구조 등이 전략적인 위험에 노출되기 시작하였다. 이에 따라 무기나 시설에 의한 종래의 전쟁 개념이 정보통신 요소 기술을 이용한 비트나 바이트 단위의 정보전 개념으로 변경되고 있다. 즉 기존의 육·해·공군 중심의 대량 파괴, 살상의 전쟁 형태에서 점차 전쟁 수행 능력 대신 상대방의 전투 능력을 무력화 시키는 관점으로 변경된다는 것이다.

또한 기존에는 탱크나 미사일, 그리고 군함과 같은 무기를 이용한 전쟁이 였다면 정보전은 무기, 시설, 네트워크, 그리고 전자파 등 다양한 요소들이 전쟁 도구로 사용이 가능하다. 이에 따라 미래의 전쟁은 바이트 또는 비트 단위의 전자전으로 이어져, 통합 전자전이나 정보전 개념이 급부상하게 되었다. 이는 미래의 전장에서는 통합 전자전 또는 정보전 기술의 확보 유무가 전쟁 수행 능력 및 국력의 우위를 나타내는 지표가 될 수 있다는 것이다.

위에서 말한 바와 같이 정보전이란 기존의 전쟁에 쓰였던 무기나 시설 대신에 정보통신망을 비롯한 정보통신 요소 기술을 이용하여 자국의 정보를 보호하고 적국의 주요 정보자원을 빼내거나 마비 시킴으로써 국가적 위협을 가하는 미래의 가상 전쟁을 말한다. 이에 의하면 정보통신 요소 기술을 이용하여 자국의 정보를 보호하는 측면에서 보안 운영체제는 정보전의 중요한 기반 기술이 됨을 알 수 있다. 또한, 응용 프로그램 수준의 보안으로는 정보 시스템의 완벽한 보안이 될 수 없음으로 운영체제 자체의 결함을 해결하고 시스템 차원의 정보보호 기능을 제공하는 보안 운영체제 기술이 필요함을 인식하여야 할 것이다.

정보시스템에 대한 보안은 기본적으로 구조를 변경하지 않고 여러 가지 방법으로 개선될 수 있으나 아주 민감한 정보를 보호하고자 한다면, 강력한 개발 전략과 특별한 시스템 구조가 요구된다. 본 고에서 소개될 정보전의 중요 요소 기술인 보안 운영체제 커널은 일반 운영체제 내에 내재되어 있는 보안 문제점을 해결하기 위하여 운영체제를 설계하는 방법을 말한다. 기존 유닉스 시스템의 취약점을 보완하는 패치 버전이나 업그레이드를 통한 임시 방편적인 방법보다는 원천적으로 새로운 보안 운영체제 개발과 같은 근본적인 해결 방법이 바람직하다. 또한 요즈음 들어서는 공개 소프트웨어 개념에 의해 리눅스를 비롯한 FreeBSD, Open BSD 등 많은 운영체제 들이 공개되는 추세에 있어서 더 더욱 운영체제의 보안 결함을 이용하는 시스템 해킹 수법 들이 늘고 있다.

본 고에서는 이러한 운영체제 상에 내재된 보안상의 결함으로 인하여 발생할 소지가 있는 각종 해킹으로부터 시스템을 보호하기 위하여, 기

존의 운영체제 내에 보안 기능을 추가한 보안 운영체제 개념을 소개하고자 한다. 보안 운영체제는 시스템 사용자에 대한 다중 수준의 식별 및 인증, 강제적 접근 통제, 임의적 접근 통제, 역할 기반 접근 통제의 최소 권한 분리 기능 등의 보안 기능 요소들을 갖추어야 한다. 더 나아가서는 사용자의 시스템 사용 현황을 파악하기 위한 감사 추적 기능이나 실시간 전장 정보를 다각적으로 제공하고 이에 대하여 실시간으로 대응할 수 있는 실시간 처리 기능과 생존권 보장을 위한 고장 감내 기능까지 확장될 수 있다.

정보전에서의 보안 운영체제의 개념과 필요성을 살펴보고, 이에 따라 미국을 비롯한 선진국에서의 보안 운영체제 개발 현황을 알아보며 정보전을 대비한 보안 운영체제 개발의 앞으로 방향을 제시해 보고자 한다.

2. 보안 운영체제 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.보안 운영체제는 기존의 운영체제 내에 내재되어 있는 문제점을 해결하기 위하여 운영체제를 설계하는 기술로 운영체제 내에 보안 기능을 추가하여 운영체제의 결함을 이용한 시스템 해킹을 방지하기 위한 것이다. 정보전에서의 방어적인 기술인 보안 운영체제는 개념적으로 그림 1과 같이 나타낸다.

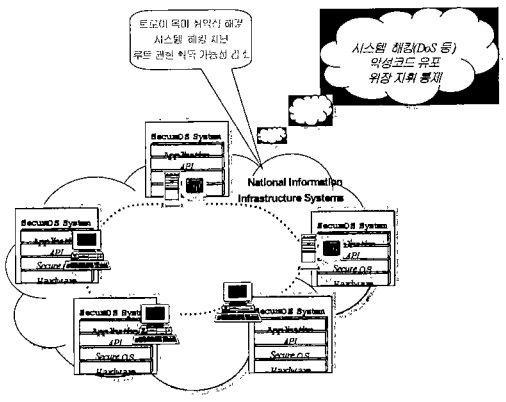

그림 1 보안 운영체제 개념도

2.1 정보전에서의 필요 기술

• 시스템 자원 보호 기술 : 시스템 내의 모든 자원을 보호 하는 기술로 접근 제어, 암호, 인증 기술 등 보안 운영체제 기본 기능에 해당하는 기술

• 시스템 모니터링 기술 : 시스템의 동작이나 운영 상태를 탐지하는 기술

• 실시간 처리 기술 : 상대에게서 공격을 당하였을 때 사이버 공격 받은 사실을 즉시 감지하거나 실시간으로 분석이 가능하도록 하는 기술

• 고장 감내, 고가용성 기술 : 특정 호스트에 고장이 발생한 경우, 국방망 전체의 신뢰성에 큰 영향을 끼침으로 이중화 또는 삼중화에 의하여 다운이 되더라도 계속적으로 기능 수행이 가능하도록 하는 기술

위와 같은 필요 기술들은 모두 보안 운영체제에서 제공하여 줄 수 있는 기술들이다. 그들을 위주로 보안 운영체제 기능들을 기술한다.

2.2 보안 운영체제 기본 기능 요구사항

보안 운영체제의 기본 기능은 시스템 내의 자원을 보호하기 위한 기술로 다음과 같이 크게 두 가지로 나누어 볼 수 있다.

• 강제적인 접근 제어(Mandatory Access Control)

- 접근 제어 정책(Access Control Policy) : 주체가 객체를 어떻게 접근할 것인지를 지정하는 운영체제 정책

- 인증 정책(Authentication Policy) : 사용자 인증에 사용되는 인증 메커니즘

- 암호 정책(Cryptographic Policy) : 데이터를 보호하는데 사용되는 암호 메커니즘

- 추가 사용 정책 : 커널 내의 각 서브시스템이 특정하게 사용하는 정책으로 예를 들자면 라우터를 위한 네트워크 사용 정책이 있다. 이는 외부 네트워크로 보내지기 전에 터널링 모드에서 IPSEC ESP를 이용하여 보호되는 Sensitive Network Traffic을 지정하는 것으로 말하면, 그 이외에도 IPSEC ESP를 위한 암호 알고리즘도 들 수 있다.

• 신뢰할 수 있는 경로와 보안 경로(Trusted

Path와 Protected Path)

- 신뢰할 수 있는 경로(Trusted Path) : 신뢰할 수 있는 소프트웨어와 함께 상호 동작하는 사용자를 허가하는 메커니즘으로 운영체제의 제어하에서 주체가 객체를 어떻게 접근할 것인가를 지정한다. 이는 사용자에 대해 신뢰할 수 있는 소프트웨어를 속이는 악의적인 응용 프로그램을 막을 수 있다. 예를 들면, 패스워드를 변경하거나, 접근 권한을 변경하는 등의 보안 관리 기능을 수행할 경우에는 신뢰성 있는 경로가 설정되어야 한다.

- 보안 경로(Protected Path) : 소프트웨어 요소 사이의 상호 보증적인 채널을 말하는 것으로 중요한 시스템 기능을 보호하기 위해 필요하며 운영체제에서 직접적으로 더욱 간단하게 제공이 가능하다.

2.3 보안 운영체제 기본 기능의 효과

위의 보안 운영체제의 기본 기능에 의해 얻어지는 효과는 다음과 같다.

• 강제적인 접근 제어

- 응용 프로그램의 우회를 방지하고 부정 변경을 막을 수 있다.

- 허가되지 않은 암호 요소의 사용에 대한 보호가 가능하다.

- 다른 사용자 응용 프로그램으로부터 암호 사용을 막거나 허가된 사용자에 의해 실행되는 신뢰할 수 없는 응용 프로그램의 실행을 막을 수 있다.

- 초기 키와 암호 요소의 코드 및 데이터 보호가 가능하다.

• 신뢰할 수 있는 경로(Trusted Path)

- 초기키의 설정을 보호할 수 있다.

- 암호의 오용을 막을 수 있다.

• 보안 경로(Protected Path)

- 악의있는 소프트웨어가 암호를 흉내낼 수 없게 한다.

- 암호 요소를 실행하여 클라이언트를 식별할 수 있다.

2.4 확장 기능 요구사항

시스템 내의 자원을 보호하는 기본 기능 외에 정보전을 위하여 더 확장되어야 할 운영체제 기능은 다음과 같다.

• 시스템 모니터링 기능

- 감사 추적 : 시스템 모니터링을 위하여 시스템 호출 수준에서 프로세스의 동작 및 운영 상태를 추적하는 기능

• 실시간 처리 기능

- 실시간 감지 : 실시간으로 공격상황을 감지하는 기능

- 실시간 분석 : 감지된 상황을 수집하여 공격을 분석하는 기능

• 고장 감내 기능

- 고장 감내 : 고장을 감지하여 이중화된 노드에 시스템의 컨텍스트를 이전하고 계속 처리되도록 하는 기능

- 고가용성 : 시스템 내의 한 노드가 다운이 되더라도 처리에는 아무런 영향이 미치지 않고 다만 성능만이 조금 줄어들게 처리하는 기능 (Gracefully Degradation)

3. 보안 운영체제 개발 현황

미국의 경우 국가정보 기반구조 구축과 국방용으로 정부기관과 군사기관들이 사용하기 위해 정부 차원에서 기술 개발을 진행 중이며 NSA(National Security Agency) 주도 하에 1994년까지 보안 운영체제 개발 타당성 조사를 마치고, 1995년부터 보안 운영체제를 개발하고 있다. 주로 국가 정보 기반 구조 구축과 국방용으로 정부기관과 군사기관 들이 사용하기 위한 것이다. 1995년부터 보안 운영체제 개발을 시작하여 DT Mach, DTOS, Flask[2] 커널에 이어 작년 9월부터는 Secure Linux[5] 커널을 지속적으로 개발 하고 있다. 또한 보안 운영체제는 정부 기관이나 국방 관련 기관뿐만 아니라 국방 기관, 정부 기관, 병원, 정보통신 회사 등 정보보호가 중요시 되는 기관을 주요 시장으로 하고 있으며, 각급 기관들이 인터넷 등을 통한 외부 사이트와의 접속으로 인한 보안 위협 때문에 운영체제의 필요성이 대두되고 있다. 미국 같은 경우에는 차별화하여 개발하고 사용하는 경향이 있었다. 국방 정보시스템 과 금융, 정부 및 공공 기관의 정보시스템에는 TCSEC[6] B3 등급 이상의 보안 운영체제를, 기업 정보 시스템에는 보안 등급 B2

급 이하의 운영체제를 사용하였다.

또한 유럽을 비롯한 많은 선진국에서도 TCSEC, ITSEC 등과 같은 시스템 보안 평가 기준에 해당하는 높은 보안 등급의 보안 운영체제를 개발하여 인증을 획득하고 상용화하는 등의 작업을 하여왔다. 민간 업체의 시큐어 운영체제 개발 현황을 주요 업체별로 살펴보면 표 1과 같다.

위와 같이 많은 민간 업체에서 보안 운영체제를 개발하여 상용화 하였으나 미국의 경우 TCSEC B3 급 이상의 보안 운영체제는 수출을 규제하고 있으므로 우리도 정보전에 대비하여 독자적으로 보안 운영체제를 개발하여야 할 것이다.

표 1 민간 업체의 제품 개발 현황

업체	제품명	특징
IBM	- MVS/SP Ver. 5 - ES/9000 PM/SM - AIX 4.1	- B1 - ITSEC E4 - C2
DEC	- VMS V5.4 - ULTRIX MLS	- C2 - B1
HP	- HP-UX BLS - HP-UX V10 - MPE/iX G.02.04	- B1 (HP9000) - U.S DoD C2 - C2
SGI	- Trusted IRIX	- B1
ICL	- VME/HSO	- B1(39시리즈)
Unisys	- OS 1100	- B1(2200)
TIS	- TMach - Trusted XENIX	- B2/E5 - B2
SCO	- SCO UNIX	- B1
OSF	- OSF/1	- B1
BullHN	- Multics System - Securics B1	- B1 - B1
Sun	- Sun Soraris2.4	- E2
Micro	- Win NT V 3.5	- C2

4. 보안 운영체제 구조

위와 같은 보안 운영체제의 기본 기능에 따라 보안 운영체제가 가져야 할 운영체제 구조를 기능 별로 구분한 것은 다음 그림 2와 같다. 보안 운영체제가 실행되는 정보시스템은 크게 인터넷 서버와 데이터 운용 서버 용도로 사용될 수 있다. 인터넷 서버의 경우는 웹서버, FTP 서버, DNS 서버, Proxy 서버, Mail 서버 등을 들 수 있고, 데이터 운용 서버의 경우에는 DB 서버나 파일 서버로 쓰이는 경우이다.

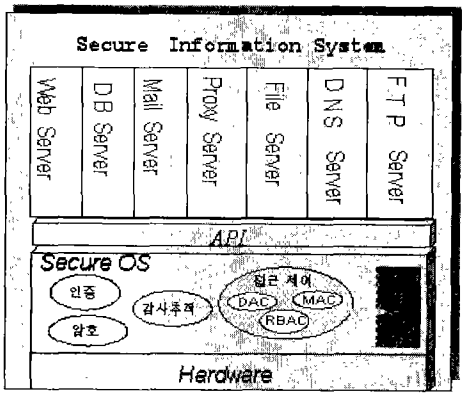

그림 2 보안 운영체제 구조도

4.1 사용자 인증

다중 수준 보안 정책의 사용자 인증 기능을 제공한다. 기존의 신분 기반 사용자 인증은 ID와 패스워드를 가지고 인증하므로 트로이 목마 취약성을 가지고 있으므로, 다중 수준 보안 등급에 의한 사용자 신분 확인 기능을 추가한다. ISO 표준 문서에 정의된 5가지 보안 등급과 객체들이 그룹화된 응용 분야의 범주로 조직의 부서를 나

타내는 범주에 의해 신분을 확인할 수 있도록 한다. 이에 덧붙인다면 원격 로그인의 경우나 보안 정책 및 접근 권한을 변경하는 보안 관리자의 로그인의 경우에는 스마트 카드에 의하여 인증을 하도록 확장할 수 있다.

4.2 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 처리 정보를 로그에 기록한다. 이는 setuid, setgid, link, read, writer, exec 등과 같은 중요 시스템 호출을 사용하는 경우에 로그에 기록하도록 한다. 또한 보안 등급이 높은 사용자의 처리 정보도 로그에 기록 할 수 있다. 이는 객체에 대한 접근 여부와 시간 등을 기록하여 이상 상태가 발생하였을 때 추적 할 수 있도록 한다. 그 이외에도 로그의 기록을 분석하여 이상 상태를 알릴 수도 있다.

4.3 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.

• 임의적 접근 제어(DAC)

- 신분기반의 접근 제어 정책
- 주체나 또는 그들이 속해 있는 그룹들의 신분 즉 ID에 근거하여 객체에 대한 접근을 제한하는 기법
- 기존의 UNIX, Linux 등이 모두 C2 등급의 DAC 기능을 제공함
- 상용 컴퓨터 시스템은 모두 DAC을 제공함
- 주체의 신분이 중요하므로 다른 사람의 신분을 이용하여 가로채기 가능
- 트로이 목마의 취약성 가짐
- 메커니즘으로는 UNIX의 파일 보호 비트, 엑세스 제어 리스트(Access Control List), 자격 리스트(Capability List) 등이 있음

• 강제적 접근 제어(MAC)

- 규칙 기반의 접근 제어 정책
- 다중 수준의 보안 정책을 사용
- 보안등급과 범주에 의한 강제적인 접근 제어 방식
- BLP 접근 제어 모델을 적용하여, 다음 그림 3과 같이 해당 등급의 자료만 접근 하도록 하고, 상위 등급의 자료는 읽기를 막고, 하위 등급의 자료는 쓰기를 금지함

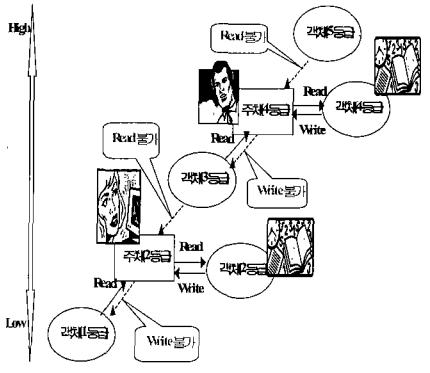

그림 3 보안 등급에 의한 접근 제어

• 직무기반 접근 제어(RBAC)

- DAC과 MAC의 혼합 형태의 접근 제어
- 직무 또는 역할 기반의 접근 제어 방식
- 자원에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내에서의 개인 직무에 따라 결정하는 것으로 이는 보안 관리의 유연성 및 효율성을 제공

4.4 암호

암호 기능은 정보의 비밀성을 제공하기 위하여 사용되는 것으로 암호화와 복호화에 쓰이는 키의 상이 여부에 따라 암호 방식도 나뉘어 진다.

암호 기술은 인증 과정이나, 데이터를 보호하기 위하여 사용될 수 있다. 예를 들자면 인증 과정 중 가로 채기 공격으로 재생 공격(Replay Attack)을 방지 하기 위한 일회용 패스워드(One Time Passwd) 등을 사용할 수도 있으며, 하드디스크를 가로채 가도 파일을 읽을 수 없도록 암호화된 파일 및 파일 시스템에 사용할 수 있다.

5. 보안 운영체제 확장 기능

정보전에서는 보안 운영체제의 기본 기능이 외에도 확장 기능이 필요하다. 그 중 고장 감내 기능이나, 실시간 처리 기능은 아주 중요하다.

• 고장 감내 기능

고장 감내 기능을 하드웨어와 소프트웨어가 지원하느냐에 따라 다르다.

- 소프트웨어 기법 : primary-backup 기법으로 주 모듈과 백업 모듈이 동시에 수행되다가 주 모듈이 잘못되는 경우 백업이 주 모듈이 되어 수행되는 것을 말한다. 물론 이 두 모듈은 실행 도중에 서로의 상태를 갖게 하는 체크포인트 시점을 가지고 있다. 또한 서로 살아 있다는 신호로 메시지를 서로 주고 받다가 그 메시지가 타임아웃내에 오지 않으면 주 모듈이 다운 되었음으로 감지한다. 대표적인 소프트웨어 기법의 고장 감내 시스템은 Tandem 시스템이다.
- 하드웨어 기법 : 하드웨어 중복에 의하여 고장 감내 기능을 한다. 예를 들자면 하드웨어 사중화 방식(Quadraple Redundancy) 인 Stratus 시스템은 하드웨어 사중화에 의하여 pair-and-spare 기법을 사용한다. self-checking 기법에

의해 하드웨어의 고장을 알아내며 모두 실행 중이므로 복구가 불필요하다는 특징이 있다. 또 다른 방식 중에 하나는 Sequoia 시스템과 같은 하드웨어 이중화 방식이다. Tightly -coupled 구조의 시스템으로 고장의 감지는 운영체제가 하며, 주기적으로 체크포인팅을 하여 상태의 일관성을 유지한다.

• 실시간 처리 기능

실시간 처리 기능은 운영체제 자체에서 그 기능을 제공하여야 한다. 실시간 처리 기능도 크게 두가지로 나누어 볼 수 있다.

- 하드 실시간 처리(Hard Real Time) : 처리가 반드시 정해진 시간 안에 이루어져야 하는 것으로 정해진 시간 안에 처리가 되지 않으면 실패한 것으로 보는 것을 말한다. 위성 등에서는 정해진 시간 안에 처리가 되지 않으면 아주 심각한 문제를 발생하므로 하드 실시간 처리가 되어야 한다.

- 소프트 실시간 처리(Soft Real Time) : 정해진 시간 안에 처리되어야 하는 것은 아니지만 빠른 응답 시간을 요구하는 것을 나타낸다. 기존의 유닉스에서는 실시간 프로세스클래스를 두어 시스템 프로세스 보다 우선 순위를 높게 하여 먼저 처리되도록 하는 스케줄링 방식으로 실시간 처리 기능을 제공한다.

6. 결론 및 향후 연구 방향

본 고에서는 정보전에서의 보안 운영체제의 개념과 보안 운영체제의 필요성을 기술하고 미국을 비롯한 정보보호 기술 선진국에서의 정보전을 대비하여 개발 중인 보안 운영체제 개발 현황을 소개하였다. 또한 보안 운영체제 개발을 위한 운영체제 기능 요구사항과 개발하기 위하여 필요한 기술 내용을 기술하였다. 미국을 비롯한 정보보호 기술 선진국의 경우 단일 시스템 내부에서의 보안성 강화는 물론 네트워크, 데이터베이스 등의 정보 자원 보호에 대한 총체적인 솔루션을 제공하기 위해 노력하고 있으며 그 노력은 일반 기업체는 물론 정부 차원에서도 활발하게 진행되고 있다. 이러한 동향에 힘입어 우리 나라에서도 정보전을 대비한 보안 운영체제 기술을 점차 단계적으로 연구와 개발을 하여야 할 것이다.

먼저 기본 기능을 갖는 보안 운영체제 기술을 개발하고, 단계적으로 확장 기능을 접목하도록 하고 더 나아가서 네트워크 보안 기술도 개발하여야 할 것이다. 무엇보다도 미래 정보전에 대비한 보안 운영체제 기술에 대한 적극적인 연구와 개발이 필요하며, 끊임없는 관심도 더해가야 할 것이다.

참고문헌

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

[2] 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.

[3] 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

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

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

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

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

[8] S. Garfinkel. "Web Security and Commerce". OReilly & Associates, Cambridge, 1997.

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

Conference, 1992.
[10] M. Harrison et al. "Protection in Operating Systems". Communications of ACM 19(8), August 1976.
[11] Secure Computing Corporation, "Assurance in the Fluke Microkernel:: Formal Security Policy Model", Technical report MD A904-97-C-3047 CDRL A003, March 1998.
[12] Dorothy E, Denning, 'Information Warefare and Security',Addison-wesley, April 1999.

김 정 녀

1987. 2 전남대학교 전산통계학과(학사)
1995~1996 Open Software Foundation Research Institute 공동 연구 파견(미국)
1998. 3~2000. 2 충남대학교대학원 컴퓨터공학과(석사)
2000. 3~현재 충남대학교대학원 컴퓨터공학과(박사 과정)
1988. 2~현재 한국전자통신연구원 보안운영체제연구팀장(선임연구원)
관심분야:OS, Secure OS, Distributed Processing, Fault Tolerant System,
E-mail:jnkim@etri.re.kr

하 경 주

1987~1991 경북대학교 공과대학 컴퓨터공학과(공학사)
1991~1993 경북대학교 공과대학 대학원 컴퓨터공학과(공학석사)
1993~1996 경북대학교 공과대학 대학원 컴퓨터공학과(공학박사)
1996~1999 한국전자통신연구원 선임연구원
1999~현재 경산대학교 정보과학부 전임강사
E-mail:kjha@kyungsan.ac.kr

윤 이 중

1988. 2 인하대학교 전산학과(학사)
1990. 2 인하대학교 전산학과(석사)
1997. 3~현재 충남대학교 컴퓨터과학과(박사과정)
1990. 2~현재 한국전자통신연구원, 정보보호시스템연구부장
관심분야:유무선 PKI, Secure OS, 인터넷정보보호
E-mail:yej@etri.re.kr

조 현 숙

1979. 2 전남대학교 수학과(학사)
1991. 2 충북대학교 전산학과(석사)
2000 충북대학교 전산학과(박사과정 수료)
1982. 3~현재 한국전자통신연구원 책임연구원 정보보호기술연구본부장
관심분야:Network Security, Conditional Access System
E-mail:hscho@etri.re.kr