리눅스 기반 PC의 보안성 평가기준에 관한 연구

김기환, 남길현

국방대학교, 전산정보학과

A Study on the Linux based PC Security Evaluation Criteria

Ki-hwan Kim, Kil-hyun Nam

Department of Computer & Information Science, National Defense Univ.

요 약

국외의 경우엔 일찍부터 컴퓨터 시스템 평가기준이 제정되어 활용중이나 국내의 경우엔 아직 평가기준이 없는 상태이다. 본 논문에서는 국내외 정보시스템의 보안 요구사항과 보증 요구사항을 바탕으로 리눅스 기반 PC의 보안성 평가기준을 제안하고자 한다. 평가등급은 KL(Korea Linux)1, KL2, KL3 등의 3등급으로 분류하였다. 제안된 평가기준은 오픈 소스기반의 리눅스를 이용하여 보안기능을 강화한 운영체제 개발방향을 제시하였고, 보안 시스템 구축의 방향 및 보안표준에 대한 복잡한 문제를 줄였다. 또한 국제공통평가기준(CC : Common Criteria)의 보안기능부분과 보증부분을 거의 수용함으로써, 외국의 보안성 평가기준과 상호 운용이 가능하다.

I. 서론

컴퓨터와 정보통신 기술의 발전은 21세기 지식정보사회를 이끌어 가는 주도적 역할을 수행 중이다. 반면에 주요 정보의 누출, 오용, 파괴 및 개인의 프라이버시 침해, 컴퓨터 범죄의 증가 등 정보화의 역기능적 폐해도 기하급수적으로 늘고 있다. 이의 대책으로 방화벽이나 침입탐지시스템 등과 같은 응용프로그램 차원의 보안활동이 이루어지고 있으나 보다 근본적 취약성에대한 보안대책으로는 미흡한 실정이다. 이에 중요 데이터와 시스템을 보호하기 위하여 보안 운영체제의 개발 필요성이 대두되었다. 그러나 국내에서는 보안 운영체제 개발을 위해 필요한 보안성 평가기준이 없는 실정이다. 만약 외국제도 하에서의 평가 시에는 많은 비용 지출과 국내 보안 기술의 유출 문제가 야기 될 가능성이 있다. 본 논문에서는 오픈소스개념의 리눅스를 활용하여 보안 커널이 강화된 보안 운영체제의 평가기준을 제안하고자 한다.

II. 국내외 정보보호시스템 평가체계

1. 국외 정보보호시스템 평가체계

보안성 평가기준의 개발 노력은 주로 미국 국방성(DoD)내의 NCSC(National Computer Security Center)에 의해 주도되어 왔다. NCSC에서는 1983년에 오렌지 북으로 불리는 안전한 컴퓨터 시스템 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria) 초안을 제정하였으며, 이를 약간 수정하여 1985년에 미 국방성의 표준(DoD STD 5200.28)으로 채택하였다.

유럽의 ITSEC(Information Technology Security Evaluation Criteria)은 영국, 독일, 프랑스 및 네델란드가 주도가 되어 소위 "일치된 평가체계(Harmonized Criteria)"를 작성하기로 합의하고 1991년에 ITSEC 버전 1.2를 제정하였다. ITSEC은 TCSEC과는 달리 단일 기준으로 모든 정보보호 제품을 평가한다. 따라서 보안 기능은 개발자가 제품이 사용될 환경을 고려하여 보안 기능을 설정하거나 미리 정의한 보안 기능을 사용토록 하였으며, 제품에 대한 평가는 보증 부분만 가지고 수행이 된다.

국제공통평가기준(CC : Common Criteria)은 하나의 기준으로 다양한 정보보호제품을 평가할 수 있는 것으로 1998년 버전 2.0이 개발되었으며, 표준문서 양식에 맞게 수정되어 버전 2.1이 국제표준(ISO/IEC 15408)으로 제정되었다. 정보보호제품 평가·인증 제도를 운영하고 있는 국가들은 자

국의 평가체계를 국제공통평가기준을 이용한 평가·인증 제도로 재정비하고 있는 상황이다[1].

2. 국내 정보보호시스템 평가체계

국내에서는 1995년 정보화 촉진 기본법의 제정을 통해 정보보호시스템 평가·인증제도 구축의 기반을 구축하였으며, 현재는 침입차단시스템과 침입탐지시스템 평가기준이 고시되어 활용 중에 있다[2][3].

3. 컴퓨터 보안성 평가기준을 위한 요구사항

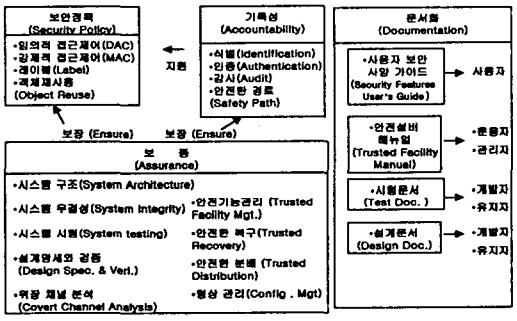
컴퓨터 보안성 평가기준을 위한 요구사항에는 [그림 1]에서와 같이 보안정책, 기록성, 보증, 문서화 등이 있다.

첫째, 보안정책의 목표는 사람, 자원, 정보에 대한 비밀성, 무결성, 가용성 등을 보장하기 위한 것으로서 정보보호를 위해 조직이 기본적으로 구비해야할 사항이다.

둘째, 기록성은 접근제어정책 지원을 위해 식별, 인증, 감사, 안전한 경로 등의 기능을 제공한다.

셋째, 보증이라 함은 시스템의 정확성과 효율성을 보장하는 것이다.

넷째, 문서화는 전체적인 네트워크 시스템과 각 구성요소가 사용자 인터페이스에서 이용 가능하도록 보호체계의 상호작용 방법이 기술된다.



[그림 1] 컴퓨터 시스템 평가기준 개념

Ⅲ. 리눅스와 보안 운영체제

1. 리눅스 현황

리눅스는 1991년 10월 5일 핀란드의 헬싱키 대학에 다니던 리누스 토발즈가 발표한 유닉스와 유사한 운영체제를 말한다. 리눅스는 소스가 개방되어 있는 운영체제이기 때문에 소스 코드의 허점을 공격하는 취약성 공격에 약하다. 반면에 정보보호 전문가들에 의한 코드 정밀진단 과정을 통해 기존의 운영체제보다 더욱 안전한 운영체제 개발방법을 제시할 가능성도 있다[4][5].

리눅스 보안측면에서 TCSEC 기준 C2급 이하 보안기능에는 사용자 계정, 임의적 접근제어, 네트워크 접근제어, 암호화, logging, 침입 탐지, 침입 차단 기능이 있다[6].

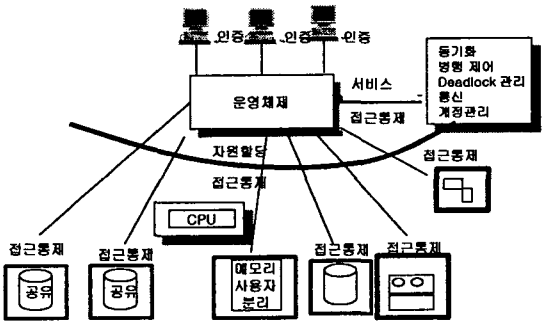
2. 리눅스 보안의 문제점

하나의 운영체제로서 리눅스는 기본적인 보안 이슈를 가지고 있다. 리눅스는 단일 사용자를 위한 데스크탑으로서 로그인 아이디와 패스워드, 적절한 백업 및 부적절한 사용으로부터 데이터를 보호하는 등의 기본적인 보안기능을 요구한다. 그러나 리눅스는 일반적으로 단일 사용자 시스템으로 쓰이지 않고 다중사용자 시스템으로 쓰이기 때문에 관리자는 개인 및 그룹의 액세스 허가를 관리해야 하는 것은 물론이고, 네트워크 보안 문제도 고려해야 한다[7].

3. 보안 운영체제(Secure OS)

보안 운영체제란 컴퓨터 운영체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안기능을 통합시킨 보안 커널(Security Kernel)을 추가로 이식한 운영체제를 말한다[8].

보안 커널이 이식된 운영체제는 [그림 2]에서와 같이 컴퓨터 사용자에 대한 식별 및 인증, 강제적 접근통제, 임의적 접근통제, 재사용 방지, 침입 탐지 등의 보안 기능 요소를 갖추어야 한다.



[그림 2] 운영체제 보안기능

Ⅳ. 리눅스 기반 PC의 보안성 평가 기준 제안

1. 정보보호체계 보안 요구사항

정보보호체계에서 안전한 정보보안을 위한 보안 요구사항에는 비밀성(Confidentiality) 유지, 무결성(Integrity) 유지, 가용성(Availability) 유지, 인증성(Authenticity) 제공, 책임추적성(Accountability) 유지, 효율성(Efficiency) 제고 등이 있다[9].

2. 리눅스 기반 PC의 보안 요구사항

보안 운영체제를 설계할 때 고려해야 할 것은 어떤 하나의 기술적 보안 해결책이 전체 시스템 보안을 제공할 수 없다는 점이다. 이와 같은 문제점을 보완하기 위해서는 다음과 같은 방법이 이용된다.

첫째, 보안 메커니즘의 적절한 균형을 이루도록 한다.

둘째, 각 보안 메커니즘은 특정한 보안 기능을 제공하도록 한다.

셋째, 각각의 보안 메커니즘은 보안 서비스 지원을 위해 다른 메커니즘에 의존하도록 한다.

넷째, 안전한 시스템에 있어서 보안 메커니즘들은 완전한 보안 패키지를 공통적으로 제공하도록 한다. 왜냐하면 이러한 균형을 이루지 못하는 시스템들은 취약할 수 있기 때문이다.

이상의 내용을 바탕으로 리눅스 운영체제 기반 PC의 보안 요구사항에 대해 알아보기로 한다.

1) 비밀성(Confidentiality) 유지

① 암호화 및 복호화
② 커널 모드 암호화 : 사용자 모드 파일지정
③ 응용계층의 암호화 : DES, 3-DES, SEED
④ 암호화 전송 : 암호화키, 파일별 개별 키

2) 무결성(Integrity) 유지

무결성은 데이터에 부당한 변조가 발생 시에 이를 감지해내는 기능이다.

① 신분확인 관련 데이터
② 전송데이터 무결성
③ 임의적 접근제어(DAC)
④ 강제적 접근제어(MAC)
⑤ 보안레이블

3) 가용성(Availability) 유지

① 자료 백업 : 중요 상세 정보 주기적 저장
② 중복성 유지 : 자료 중복성 유지를 통한 전송 데이터 보호

4) 인증성(Authenticity) 제공

① 사용자 식별 : User ID, 스마트 카드
② 인증 : 패스워드, 사용자 상호 인증

5) 책임 추적성(Accountability) 유지

① 감사·추적(audit trail) : 감사기록 레코드, 통계데이터, 통보기능
② 보안 표시 정보의 강제적 출력

6) 효율성(Efficiency) 제고

① 응용 프로그래밍 인터페이스(Application Programming Interface) : 다중등급보안 통제
② 시스템 호출 및 명령 : 보안 등급, 보호범주

3. 리눅스 기반 PC의 보안성 평가기준 제안

본 평가기준은 보안기능 요구사항 및 보증 요구사항으로 구분된다. 평가등급은 실질적 사용 목적에 따라 간단히 KL(Korea Linux)1, KL2, KL3등급으로 분류된다. KL1 PC는 일반 사무실에서 행정작업 및 인터넷 PC용으로 활용하고, KL2 PC는 보안을 요하는 대외비급의 문서작업용으로 활용하며, 마지막 KL3 PC는 3급 비밀 이상의 기밀서류를 다루는 중요한 작업에 활용토록 한다. 여기서 각 등급별로 하위등급의 내용은 상위등급 PC로 자동 계승된다. 본 평가기준의 구조 및 요구사항과 각 등급별 평가기준은 다음과 같다.

1) 평가기준 구조 및 요구사항

① 보안기능 요구사항
보안기능 요구사항은 비밀성, 무결성, 가용성, 인증성, 효율성, 유지보수성 등 여섯 가지 요구사항으로 이루어진다.

② 보증 요구사항
보증 평가는 평가신청인이 제출한 자료 및 평가자의 시험을 통하여 이루어지는 부분이다. 정보보호시스템 보안기능의 신뢰성을 확인하기 위한 보증요구사항은 개발과정, 시험과정, 형상관리, 운영환경, 설명서, 취약성 등의 여섯 가지 요구사항으로 구성된다.

2) 평가등급별 요구사항

각 평가등급별로 세부 요구사항은 다음 [표 1]

[표 2][표 3]과 같다.

[표 1] KL1등급 요구사항

항 목			등급별 특성요약	비고
기능부분	비밀성	암호화·복호화	저장장치의 Dump로 인한 정보유출 방지기능 필요	선택
		커널모드 암호화	해당없음	
		응용계층 암호화	해당 없음	
		암호화 전송	해당 없음	
	무결성	신분확인 데이터	해당없음	
		전송데이터 무결성	해당 없음	
		임의적 접근제어	시스템에 접근하는 모든 주체, 객체 접근제어	
		강제적 접근제어	해당 없음	
		보안 레이블	해당 없음	
	가용성	자료백업	중요 상세 정보 주기적 저장	
		중복성 유지	디스크 저장 시 자료의 중복성 유지	
	인증성	사용자 식별	User ID 또는 스마트 카드 사용	
			User ID 삭제 및 재사용	
		인증	사용자 상호 인증	
			패스워드 변경 시 사용자 신원 확인	
			패스워드 최소 길이 지정	
	책임추적성	감사기록 및 추적	감사기록 레코드 저장 기억장소 소진 시 관리자에게 통보 기능	
			감사기록 파일 조회 및 출력	
		보안표시 강제적 출력	해당 없음	
	효율성		해당 없음	
보증부분	개발과정	기능 명세	비정형화된 보안목표명세서 및 기능명세서	
		기본 설계	비정형화된 기본설계서(기본구조 및 인터페이스 서술)	
		상세 설계	해당 없음	
		구 현	해당 없음	
	시험과정		개발 각 단계별 보안기능 시험 및 결과 제시	
	형상관리		시험서에 기술된 시험의 일부 직접 수행	
	운영환경	설치과정	시스템 설치절차의 보안에 미치는 영향 서술	
		운용절차	안전한 시동, 백업, 유지보수, 운영에 대한 절차 서술	
	설명서	사용자설명서	보안기능의 사용 방법 및 경고사항 서술	
		관리자설명서	보안관리방법	
			보안기능 운용방법	
			설치 및 구성 선택사항	
	취약성	취약성분석	시스템의 설치, 시동, 운영, 관리 및 사용에 관한 문서	
		오용분석	해당 없음	

[표 2] KL2등급 요구사항

항 목			등급별 특성요약	비고
기능부분	비밀성	암호화·복호화	비밀 객체의 저장, 저장장치와 메모리간 전송 기능	선택
		커널모드 암호화	사용자 모드에서 선택적 파일 지정 후 암호화	
		응용계층 암호화	DES 이용 암호화	
		암호화 전송	비밀 객체 저장매체 저장 시, 인터넷을 통한 원격지 전송 시 암호화	
	무결성	신분확인 데이터	관리자 및 사용자 데이터 변경여부 확인	
		전송데이터 무결성	전송데이터 변경 여부 확인	
		임의적 접근제어	KL1과 동일	
		강제적 접근제어	시스템에 접근하는 모든 주체, 객체 접근 통제	
		보안 레이블	해당 없음	
	가용성	자료백업	KL1과 동일	
		중복성 유지	KL1과 동일	
	인증성	사용자 식별	동일 User ID로 복수 로그인 금지	
			필요 시 인원 수 제한	
		인증	인증수단의 최소길이, 조합규칙, 변경주기 제공	
			사용자, 관리자 인증 위해 사용된 정보에 사용 공격에 대한 대처 수단 제공	
			응용서비스 접속 후 일정시간 무응답 시 재 인증 제공	
			패스워드 생성 후 선택기능 제공	
	책임추적성	감사기록 및 추적	강제적 접근제어 규칙 설정, 변경, 삭제	
			속성별 감사기록 레코드 검색	
		보안표시 강제적 출력	보안등급 표시정보 용지에 강제적 출력	
	효율성		응용 프로그램을 위한 인터페이스 제공	
보증부분	개발과정	기능 명세	KL1과 동일	
		기본 설계	보안기능 제공방법 및 시스템의 보안, 비보안 구성요소의 분리 및 분리방법 기술	
		상세 설계	보안메커니즘 명시, 보안모듈 인터페이스의 목적 및 매개변수, 보안메커니즘 및 모듈간의 상관관계, 보안메커니즘의 보안기능 제공방법	
		구 현	원시프로그램 또는 모든 하드웨어 도면과 상세설계서 사이의 일치성 검증명세서	
	시험과정		KL1과 동일	
	형상관리		개발과정에 적용된 형상관리 체계기술	
			제공된 모든 문서는 유일한 식별자 가짐	
			형상변경 통제 방법	
	운영환경	설치과정	시스템 재구성 시 설치 선택사항 및 변경에 대한 감사기록	
		운용절차	시동 및 운용과정 동안 기록되는 감사기록 예시	
	설명서	사용자설명서	KL1과 동일	
		관리자설명서	KL1과 동일	
	취약성	취약성분석	명백히 알려진 취약성 분석 결과 서술	
		오용분석	평가자 분석에 의한 침투시험	
			문서내에 기술된 임의의 절차 반복 수행	

[표 3] KL3등급 요구사항

항 목			등급별 특성요약	비고
기능부분	비밀성	암호화·복호화	Kernel 모드로 강제적 수행, 사용자 투명성, 자동처리, 고속처리 제공	선택
		커널모드 암호화	사용자 모드에서 암호화 및 복호화 키 입력 후에 파일단위 암호화	
		응용계층 암호화	3-DES, SEED 이용 암호화	
		암호화 전송	KL2와 동일 파일별 개별 키 사용 암호화 전송	
	무결성	신분확인 데이터	KL2와 동일	
		전송데이터 무결성	KL2와 동일	
		임의적 접근제어	KL2와 동일	
		강제적 접근제어	KL2와 동일	
		보안 레이블	모든 주체, 객체에 대한 보안레이블 유지	
	가용성	자료백업	KL2와 동일	
		중복성 유지	KL2와 동일	
	인증성	사용자 식별	User ID 외 다른 정보(소속 등)의 관리를 통한 식별	
		인증	비밀번호 변경간 시간(기본 30일)초과 시 자동 사용 불가능	
			OTP(One Time Password) 방식 인증	
			패스워드 에이징	
	책임추적성	감사기록 및 추적	보안 레이블 정보의 설정, 변경, 삭제	
			통계 데이터 제공, 무결성 위반 시 통보	
		보안표시 강제적출력	KL2와 동일	
	효율성		보안등급, 보안범주 부여 후 시스템 호출 및 명령 제공	
보증부분	개발과정	기능 명세	보안정책의 정형화된 모델을 기술한 보안 모델 명세서 작성 및 해석	
			준 정형화된 기능명세서	
		기본 설계	준 정형화된 기본설계서, 독립적 기본 모듈로 구조화	
		상세 설계	준 정형화된 상세설계서, 독립적 기본 모듈로 구조화	
			인터페이스, 모듈변수 목적, 추가내용, 포함이유 서술	
		구 현	개발단계에서 생성되는 각 문서사이의 일치성	
	시험과정		시험서의 전부를 직접 수행	
	형상관리		원시프로그램 및 하드웨어 도면에 대한 식별자 부여	
			형상관리 도구기반 형상변경 통제	
	운영환경	설치과정	KL2와 동일	
		운영절차	시스템의 고장 또는 오류 발생 시 복구절차	
	설명서	사용자설명서	KL2와 동일	
		관리자설명서	KL2와 동일	
	취약성	취약성분석	제출물 분석에 근거한 침투시험 수행	
		오용분석	관련문서 내에 기술된 모든 절차 수행 점검	

V. 결 론

본 논문에서는 오픈소스개념의 리눅스를 활용하여 보안 커널이 강화된 보안 운영체제의 평가기준을 제안하였다. 제안된 평가기준은 정보보호체계에 적합한 보안 요구사항을 수용토록 함으로써 보안기능을 강화한 운영체제 개발방향을 제시하였고, 리눅스 기반 PC의 보안성 평가기준을 제시함으로써 장차 리눅스를 기반으로 하는 보안 시스템 구축 및 보안표준 방향 정립에 도움을 주었다. 또한 미국의 TCSEC과 보호 프로파일을 강화한 CC의 보안기능 및 보증 요구사항을 수용함으로써 외국의 평가체계와 상호 운용이 가능하도록 하였다. 향후 본 논문에서 제안한 평가기준을 보완 발전시켜 CC와 연동되는 보안성 평가기준을 제정한다면, 국내 자체 보안 운영체제의 보안기능과 설계 요구사항, 기술개발 방향 등을 확립할 수 있을 것이다.

참고문헌

[1] 정보통신부, 정보보호 평가기준 개발, 한국정보보호진흥원, 1999. 12.

[2] 한국정보보호진흥원, 정보통신망 침입차단시스템 평가기준, 한국정보보호진흥원, 2000. 2.

[3] 한국정보보호진흥원, 정보통신망 침입탐지시스템 평가기준, 한국정보보호진흥원, 2000. 7.

[4] 김혜진, "데스크탑 운영체제로서 리눅스 연구 방향", 정보과학회지, 2000. 2.

[5] 손성훈, "리눅스 커널의 특징", 정보과학회지, 2000. 2.

[6] 한국정보보호진흥원, 국산 주전산기 OS 보안기능 개발방향 및 활용방안 연구, 한국정보보호진흥원, 1998. 12.

[7] Scott Mann 외 2인, Linux System Security, Prentice Hall PTR , 2001. 2.

[8] 박태규 외 1인, "다중등급 보안 리눅스 운영체제 개발", 정보보호와 암호에 관한 학술대회 논문집, 2001. 9.

[9] 남길현, "정보사회에서의 정보보안," 정보보안 대책연구 및 토론회, 1996.