국가기관용 안전커널 정보보호 요구사항 분석

김현희*, 남길현*, 강정민**, 김은영**, 이진석**, 홍순좌**

*국방대학교 전산정보학과, **국가보안기술연구소

A Study on Analysis for Secure Kernel Requirements of Governmental Organization

H.H. Kim * , K.H. Nam * ,

J.M. Kang * * . E.Y. Kim * * , J.S. Lee * * , S.J. Hong * *

* Department of Computer & Information Science, National Defence Univ.

* * National Security Research Institue

요 약

네트워크로 연결된 국가기관의 중요한 정보시스템에 대한 보안위협에 대해 기존의 침입차단/탐지시스템을 중심으로 하는 보안솔루션은 잠재적인 보안위협의 처리 한계와 우회하는 새로운 해킹기법 등의 발달로 인해 시스템의 정보보증을 위한 대응책이 떨어지고 있는 것으로 판단된다. 따라서 이에 대한 대안으로 TCSEC B5급(CC EAL5) 이상의 국가기관용 보안운영체제 개발의 필요성이 부각되고 있다. 본 논문은 국가기관용 보안운영체제 개발을 위해 선행되어야 할 안전커널 요구사항에 관한 연구로 이를 위해 먼저 적용될 보안환경과 목적, TCSEC 요구사항, CC 기반 보호프로파일, CC 요구사항을 분석 적용하였다. 이를 기반으로 정보의 중요도에 따라 두개의 등급으로 분류된 국가기관에 적합한 안전커널 요구사항을 제안하고자 한다.

I. 서론

최근 컴퓨터 환경은 개방적인 구조로 변화되었고 동시에 정보통신기반의 급속한 성장으로 정보에 대한 접근이 용이하게 되었다. 이에 따라 정보시스템은 바이러스, 해킹 등으로부터 위협이 더욱 높아지고 있으며 시스템 운영체제에 대한 취약점을 이용한 공격이 빈번하게 이뤄지고 있다. 특히, Firewall, IDS 등 보안솔루션의 취약점을 이용한 공격으로 인해 새로운 해결책이 요구되고 있다. 이러한 공격으로부터 시스템을 보호하기 위해서 기존의 운영체제 수준에 보안기능을 일부 추가하거나 새로운 보안운영체제를 개발하는 것이 보안위협에 대한 대안으로 제시되고 있다.

미국을 비롯한 유럽, 중국, 일본 등 선진국에서는 국가 정보통신기반시스템의 정보 처리를 위한 정보시스템의 필요성을 인식하여 이를 보호할 수 있는 정보보호시스템의 신뢰성을 평가할 수 있는 기준을 제정하고 보안운영체제의 연구 및 개발에 많은 투자를 하고 있다. 국내의 보안운영체제는 TCSEC B1등급 기준의 보안운영체제가 개발되고 있지만 국가기관 적용을 위한 보안운영체제는 상용 보안운영체제와는 다른 보안환경이 요구하기 때문에 이에 적합한 보안기능을 지원할 수 있는 안전커널 요구사항에 대한 연구가 필요하다.

본 논문에서는 안전커널 요구사항을 정보시스템의 평가기준인 TCSEC과 CC 기반 보호프로파일, CC 요구사항중 적합한 요구사항을 분석한 후 비밀은 아니지만 민감한 정보를 다루는 시스템과 비밀정보를 다루는 시스템에 적용 가능한 요구사항으로 분류해서 제안한다. Ⅱ장에서는 보안운영체제의 개념, 기능 및 구조, Ⅲ장에서 TCSEC과 CC 기반의 보안운영체제 보호프로파일 분석한다. Ⅳ장에서는 Ⅲ장의 분석내용과 CC 요구사항을 기반으로 안전커널 요구사항을 제시한다.

II. 보안운영체제의 기능과 구조

보안운영체제는 안전커널이 추가로 이식된 운영체제로써 내·외부의 침입로부터 운영체제의 통제권한을 획득하는 것을 방지한다. 그리고 운영체제 접근통제 대상을 정보영역의 분리, 직무영역 분리, 최소권한 유지, 강제적 접근통제 등을 사용하여 보호한다. 이러한 보안운영체제는 1970년대부터 미국, 유럽 등에 의해 시도되어 상용제품으로 출시되고 있다. 초기에 유닉스시스템을 기반으로 하였고 현재는 리눅스 시스템을 기반으로 하는 보안운영체제에 관한 연구가 활발히 진행되고 있다

현재 보안운영체제에서 구현하고 있는 보안기능은 식별 및 인증, 임의적/강제적 접근통제, 암호화, 잔여 정보 재사용 방지, 완전한 중재 및 조정, 책임성 및 감사로그, 안전한 경로, 침입탐지, 해킹방지, 통합보안관리 등이 있다.

보안운영체제 구조의 핵심인 안전커널은 객체에 대한 접근통제를 수행하고 다른 보안메커니즘과 데이터를 교환하면서 상호 작용하는 참조모니터와 보안정책의 시행을 책임지는 하드웨어, 펌웨어, 소프트웨어의 조합인 TCB에 의해 보호된다. 안전커널의 역할은 기존의 운영체제에 내재된 보안상의 결함으로 인한 각종 침해로부터 시스템을 보호하고 사용자의 모든 접근에 대한 행위를 안전하게 통제하는 것이다. 그리고 대부분의 취약성들은 설계 및 개발과정에서 발생하므로 해결하기 더욱 어렵게 만들고 있다. 따라서 설계, 개발, 배포 등의 과정에서 반드시 정보보증이 요구된다..

국내·외 기술 개발 현황을 살펴보면 미국은 국가정보기반구조의 구축과 국가기관용으로 사용하기 위해서 NSA 주도하에 지난 1995년부터 정부차원의 보안운영체제 개발을 시작하여 ETMach, DTOS, Flask, SE-Linux를 지속적으로 개발하고 있으며 서버관련 기업들이 주축으로 자사의 독자적인 운영체제로 시스템의 안전성과 무결성을 강화한 운영체제를 개발하여 상용화하고 있다. 중국은 국가 운영체제로 리눅스를 지정하고 현재 GB 17859-1999의 3등급(TCSEC B1등급에 해당)을 통과한 CAS-ACCESS(리눅스 기반)와 CS&S 안전한 운영체제 두 개의 자체 운영체제를 개발하여 보유하고 있으며 4등급(TCSEC B2등급에 해당) 보안운영체제를 개발하기 위해 연구하고 있다.

국내는 정보통신부에서 국가보안기술연구소와 함께 "보안운영체제" 및 "국산 주전산기용 운영체제 보호기능" 등의 보안운영체제 관련 기술을 개발하고 있으며 소수의 민간업체에 의해서 연구 및 개발된 제품이 상용화되어 있다. 그러나 아직까지 국가기관에서 사용하기에 적합한 보안운영체제의 사용자 요구사항이 확실하지 않은 상태이다.

III. TCSEC 분석과 CC 기반의 보안운영체제 보호프로파일 분석

1. TCSEC 요구사항 분석

TCSEC은 미 국방부 보안요구사항에 대해서 소프트웨어 생명주기 관리 접근, 운영체제, 프로세스, 그리고 컴퓨터의 계층적 장치와 소프트웨어를 포함하는 자동화된 정보처리시스템에 적용할 목적으로 제공한다[3,4]. 특히, 시스템 무결성과 정보무결성의 보장을 위해서 높은 등급으로부터 낮은 등급으로 비밀정보 변질을 방지, 참조모니터의 의한 비밀정보 노출 방지를 제시하고 있다. 그리고 TCSEC Interpretation에서 객체의 실행, 수정, 조작 및 임무 분리를 시행하도록 강제적 무결성 통제정책, 서비스거부 공격 방지, 데이터 변조 방지, 실시간 감사분석, 프로그램 영역분리(사용자 프로그램과 시스템 프로그램) 등을 제시하고 있다[5].

TCSEC은 현재까지 미국에서 자국의 정보보호와 중요한 정보를 처리하는 시스템의 평가기준을 사용하고 있으며 B2등급 이상의 정보시스템을 국가기반용 시스템에 적용하고 있다. 그리고 민감하거나 비밀등급으로 분류된 정보를 처리하는 시스템을 최소 C2등급을 요구하지만 민감한 정보를 처리하는데 있어서 B1등급의 강제적 접근과 보증사항이 요구되며 비밀등급으로 분류되거나 범주화된 정보를 처리하고 두개 이상의 범주화된 정보를 처리하는 경우 최소 B2등급을 제시하고 있다[4]. 따라서 국가기관용 운영체제의 보안요구사항에서 민감한 정보(비밀로 분류되지 않은)에는 B1등급에 준하는 내용을 적용하며 비밀등급으로 분류되고 범주화된 정보를 처리하는데 있어서 B2등급 이상의 요구사항과 강제적 무결성 통제정책을 적용한다. [표 1]은 B등급에서 국가용 보안운영체제에 적용할 수 있는 보안기능을 나타낸 것이다.

2.보안운영체제 보호프로파일

현재 미국의 NSA에서 개발된 보호프로파일로는 RBACPP, CAPP, LSPP, SLOSPP,MLSOSPP가 있으며 보증등급은 각각 EAL2, EAL3, EAL3, EAL4+, EAL4+등급으로 평가 및 개발을 완료한 상태이다.

Labeled Security 보호프로파일은 DoD TCSEC B1등급의 보안기능요구사항을 기술한 것이며 TCSEC에 의해 제공된 요구사항과 동등한 보안기능과 보증요구사항을 제공한다[1].

MLSOSPP는 민감한 정보을 포함하는 네트워크 환경에서 제공되는 다중등급 운영체제에 적용하기 위해 개발된 보호프로파일이며 강제적 무결성 접근통제, 암호서비스, TCSEC B2등급의 보안기능을 포함하고 있다[2].

[표 1] 보안기능요구사항 클래스

보안기능	등급		
	B1	B2	B3
식별 및 인증	인증데이터 유지, 비인가된 사용자의 접근 제한	사용자 인증/초기 로그인 인증 시 안전한 경로 제공	안전한 경로를 통한 사용자와 연결시 주체 비밀등급 변경 제공
임의적 접근통제	C2등급과 동일		객체에 대한 개인/그룹의 접근 목록 유지
강제적 접근통제	모든 주체와 저장 객체들에 정책 적용, 계층적 분류등급 및 비계층적 범주 할당, 두개이상의 보안등급 제공	직접적/간접적으로 접근 가능한 모든 자원에 정책 적용	
레이블 및 레이블 무결성	주체와 저장 객체에 대한 보안 레이블 유지, 정보유출시 보안 레이블 표시, 기본값 표시가 무시됐을 시 감사 기록	외부 주체에 의한 직접/간접적으로 접근 가능한 자원의 보안레이블 유지	
감사	감사기록 시 신분과 보안등급 포함, 사건 선택가능, 출력시 보안레이블 표시유 무시하는 사건도 감사기록	비밀 저장채널에 악용되는 사건 감사 가능해야 함	보안정책 위반시 즉시 지적하고 사건의 증적 및 감시하는 메커니즘 포함, 보안관련 사건 위반 발생빈도 초과시 인가된 관리자에게 즉시 통보하거나 사건 종료시킴
레이블된 정보 유출 및 장치로 정보 유출	단일/다중 등급으로 분류된 각각의 통신채널과 입출력 장치 지정 그리고 수동적 변경가능, 다중등급 장치로 유출시 연관된 보안등급과 동일한 레이블 유출, 단일 등급 통신채널과 입출력 장치 경유시 단일 등급을 지정할 수 있어야 함, 출력시 보안등급 표시(상 · 하 부분)		
주체 보안등급	해당사항 없음	상호 세션 시 주체의 보안등급 변경사항을 즉시 통보하고 디스플레이를 요구	
장치 레이블		모든 연결된 물리적 장치에 최소와 최대의 보안등급이 할당할 수 있어야 함	

3. CC 기반 보호프로파일 보안요구사항 분석

본 논문에서 분석한 보안요구사항은 PP의 보안기능과 보증부분을 분석한 것이다. 보안기능요구사항은 통신클래스와 프라이버시클래스를 제외한 9개 클래스의 컴포넌트에 대해서 분석하였다. 분석한 PP은 국가기관의 보안환경 및 목적에 부합되도록 적합하게 운영체제의 보안기능을 기술, 인가된 관리자의 직무를 명확히 분리, 암호/암호모듈과 키관리의 생명주기의 국가 정보보호 표준 요구사항 준수, 정보흐름의 강제적 무결성 통제정책을 제공한다. 그리고 안전한 경로, TCSEC B3등급의 안전한 복구(수동적 복구), 보안감사 자동대응, 잠재적인 위반 분석, 감사기록 손실 방지 등의 보안기능을 제시하고 있다[4.5]. 분석한 LSPP는 TCSEC B1등급, MLSOSPP는 B2등급 이상에 준하는 보안기능을 제시하고 있다. [표 2]는 보안운영체제 PP의 기반으로 B1/B2등급에 준하는 보안기능요구사항의 패밀리와 컴포넌트 내용을 분석한 것이며 _EXP는 미국의 CC 해석(암호모듈 기준선 및 암호 저장 및 파기 등)을 사용한 패밀리와 컴포넌트를 식별하기 위해서 표시한 것이다.

CC 기반의 보증요구사항은 TCSEC과 같이 각 등급의 보안기능에 요구되는 보증요구사항을 제시하는 것이 아니라 보증만이 평가의 기준이 된다.

[표 2] 보안기능요구사항 클래스

클래스명	패밀리	컴포넌트
FAU 보안감사	FAU_ARP, FAU_GEN, FAU_SAA,FAU_SAR, FAU_SEL, FAU_STG	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1,FAU_STG.4
FCS 암호지원	FCS_BCM_EXP, FCS_CKM, FCS_CKM_EXP, FCS_COP.1	FCS_BCM_EXP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_CKM_EXP.1,FCS_CKM_EXP.2, FCS_CKM_EXP.3 FCS_CKM_EXP.4, FCS_COP.1
FDP 사용자 데이터 보호	FDP_ACC, FDP_ACF_EXP, FDP_ETC, FDP_IFC_EXP, FDP_IFF, FDP_ITC, FDP_ITT, FDP_RIP	FDP_ACC.2, FDP_ACF_EXP.1, FDP_ETC.2, FDP_IFC.2(1), FDP_IFC.2(2), FDP_IFF_EXP.2(1), FDP_IFC_EXP.2(2), FDP_IFC.3, FDP_ITC.1, FDP_JTC.2, FDP_ITT.1, FDP_RIP.2
FIA 식별 및 인증	FIA_AFL, FIA_ATD, FIA_SOS, FIA_UAU, FIA_UID, FIA_USB	FIA_AFL_EXP.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1
FMT 보안관리	FMT_MOF, FMT_MSA FMT_MSA_EXP, FMT_MTD FMT_REV, FMT_SAE, FMT_SMR, FMT_MSA,	FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2, FMT_MSA.3, FMT_MSA.EXP.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FMT_REV.1(1), FMT_REV.1(2) FMT_SAE.1, FMT_SMR.1, FMT_SMR.3,
FPT TOE 보안기능의 보호	FPT_AMT, FPT_ITT, FPT_RCV, FPT_RVM, FPT_SEP, FPT_STM, FPT_TDC, FPT_TRC, FPT_TST, FPT_RSA	FPT_AMT.1, FPT_ITT.1, FPT_ITT.3, FPT_RCV.1, FPT_RVM.1, FPT_SEP.2, FPT_STM.1, FPT_TDC.1, FPT_TRC.1, FPT_TST.1(1), FPT_TST.1(2), FPT_TST.1(3), FPT_RSA.1(1), FPT_RSA.1(2)
FTA TOE 접근	FTA_SSL, FTA_TAB, FTA_TAH,.	FTA_SSL.1, FTA_SSL.2, FTA_TAB.1, FTA_TAH.1
FTP 안전한 경로	FTP_TRP	FTP_TRP.1

[표 3]은 CEM의 EAL4등급과 미 국방 및 정부기관에서 요구하는 엄격한 중간 수준의 시스템의 보증설계 EAL4+등급으로 평가된 MLSOSPP에 대한 보증요구사항이다. 결함검사를 강화하기 위해서 EAL4+등급의 보증요구사항에 추가된 사항으로 오류수정(ALC_FLR.2) 요구사항, EAL5급에서 요구되는 개발사항의 구현과 모듈화, 시험사항의 깊이, 그리고 중간의 내성을 평가를 위한 취약성 평가의 평가/침투시험을 요구하고 있으며 EAL6등급의 모듈, 기타 모듈에 대한 체계적인 비밀채널 분석을 내포하고 있다[5,6]. 따라서 보증요구사항은 국가기관용은 일반환경과 달리 시스템의 오류에 대한 내성. 안전성, 무결성에 비중을 두므로 이

러한 요구사항에 부합하기 위해서는 EAL4+등급 이상의 요구사항을 적용해야 한다. 또한 CEM의 경우 EAL5등급 평가방법론에 대해서는 자국이 개발하여 사용하고 NSA에 의해서 Wing Gerverment Service사의 XTS-400(B3등급)이 운영체제 중 EAL5등급으로 평가되었고 EAL5+등급을 평가 중이다. 이를 고려할 때 국가기관용 운영체제의 안전성을 보장하기 위해서는 보증부분은 EAL5등급 이상이 필요하다.

[표 3] 보증요구사항 클래스와 문서

클래스명	패밀리	컴포넌트	문 서
ACM 형상관리	ACM_AUT, ACM_CAP, ACM_SCP	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	형상관리 지침서
ADO 배포와 운영	ADO_DEL, ADO_IGS	ADO_DEL.2 ADO_IGS.1	기술이전(배포) 절차서 사용자 설명서
ADV 개발	ADV_FSP, ADV_HLD, ADV_IMP, ADV_INT, ADV_LLD, ADV_RCR, ADV.SPM	ADV_FSP.2 ADV_HLD.2 ADV_IMP.2 ADV_INT.1 ADV_LLD.1 ADV_RCR.1 ADV.SPM.1	비정형화된 개발기능 규격서 비정형화된 상위시스템 설계서/ 하위시스템 설계서 보안기능설계서 모듈(블록/단위) 설계서 비정형화된 검증 명세서 비정형화된 보안정책모델서
AGD 설명서	AGM_ADM, AGM_USR	AGM_ADM.1 AGM_USR.1	관리자 설명서 사용자 설명서
ALC 생명주기지원	ALC_DVS, ALC_FLR, ALC_LCD, ALC_TAT	ALC_DVS.1 ALC_FLR.2 ALC_LCD.1 ALC_TAT.1	개발 보안지침서 결함교정 지침서 생명주기관리 지침서 개발도구 선정 보고서
ATE 시험	ATE_COV, ATE_DPT, ATE_FUN, ATE_IND	ATE_COV.2 ATE_DPT.2 ATE_FUN.1 ATE_IND.2	기능규격 일치성 분석서 시스템 설계 일치성 분석서 시험 절차서 및 시험결과서 시험환경 구축 계획서
AVA 취약점 분석	AVA_CCA, AVA_MSU, AVA_SOF, AVA_ALA	AVA_CCA.2 AVA_MSU.2 AVA_SOF.1 AVA_ALA.3	비밀채널 분석서 오용분석서 보안기능강도 분석서 취약성 분석서

IV. 국가기관용 안전커널 요구사항 분석

1. 보안환경 및 목적

분석한 PP의 보안환경과 목적은 안전커널 요구사항 분석에 적용할 수 있는 보안환경과 목적에 대한 내용을 포함하고 있다.

보환환경은 민감한 정보와 비밀정보를 처리하는 정보시스템 환경에서 발생하는 위협으로서 전송 데이터의 변조, 위장, 삽입, 악성코드에 의한 데이터 유출, 서비스거부 공격 등이 발생하며 잘못된 설계 및 구현으로 TOE에 잠재적인 위협을 제공한다. 추가적으로 가정사항의 설치 시 담당부서의 보안대책 수립을 기술하였다.

보안목적은 비인가된 사용자의 시스템 작동 및 사용에 대한 접근으로부터 보호, 저장된 자원에 대한 변조, 간섭, 위장, 삽입 등 위협으로부터 보호, 시스템 내·외부전송 자원에 대해서 비인가된 수정 및 탐지되지 않은 변조로부터 보호, 소프트웨어가 안전하게 작동하는지 작동상태 감시 및 사용자 요구에 대한 서비스에 대한 책임 추적을 제공, 결함검사, 취약성 분석, 제공되는 악성코드 등을 내포한 어플리케이션과 소프트웨어에 의한 자원 누출로부터 보호하는 것 등에 기반을 둔다.

2. 안전커널 요구사항 제안

안전커널요구사항는 Ⅲ장에서 분석한 내용과, CC의 내용 중 적용될 수 있는 보안요구사항을 분석(자원할용, 세션설정 및 통제, 신분확인 및 인증, 보안기능 보호, 보증)하여 적용하였다[5,8]

안전커널 요구사항은 편의상 비밀정보가 아닌 민감한 정보를 처리하는데 요구되는 금강급과 기밀정보를 처리하는데 요구되는 백두급으로 분류하여 요구사항을 기술한다. 대부분의 평가기준은 6~7개 등급으로 구분하고 있으나 실제 국가기관에서 운영할 수 있는 것은 두 가지 정도로 구분하는 것이 현실적인 것으로 판단되기 때문이다.

금강급은 비밀로 분류되지 않은 민감한 정보를 처리 및 관리하는 시스템에 적용한다. [표 4]와 같이 운영환경 기본 요구사항으로서 시스템에 의해 전송 및 저장되는 모든 정보에 접근인가를 획득하고 명확한 Need-to-Know와 역할에 부합하도록 한다.[7]. TCSEC B1등급에 준하는 보안기능요구사항을 적용한다[4]. 그리고 국가 정보보호 표준의 암호모듈(알고리즘. 키길이 포함), 키관리, 인증기반 접근통제를 적용한다[9]. 보증요구사항은 [표 5]와 같이EAL4+등급을 적용한다.

백두급은 [표 4]와 같이 금강급의 보안요구사항을 포함하며 한 단계 높은 수준으로 비밀등급으로 분류된 정보를 처리하는 시스템에 적용하며 B2등급이상의 보안기능요구사항 적용하며[4] 모든 정보에 접근하는 사용자는 보안허가를 획득하고 Need-to-Know와 역할에 부합하도록 하여야 한다[7]. 여기서는 절차와 수준이 한 단계 볼 수 있다. 그리고 국가 정보보호보호 표준의 암호모듈, 키관리, 인증기반 접근통제를 적용한다[9].보증요구사항은 EAL5등급을 적용한다.

분석한 보안요구사항은 Ⅲ장에서 분석한 내용과 CC Part 2/3의 보안기능 및 보증요구사항에서 보안운영체제에 적용 가능한 클래스의 컴포넌트를 적용하였으며 정보보증의 구현을 목적으로 비밀성, 무결성, 가용성, 책임성을 보장하도록 구성하였다. 금강급의 보안기능요구사항은 악성적인 프로그램에 의한 자원의 탈취로부터 보호하기 위해서 강제적 접근통제를 요구하며, 비밀로 분류되지 않은 민감한 정보를 처리하므로 계층적 보안속성을 적용하지 않는다. 안전한 복구 시 데이터의 손

실을 방지하기 위해서 수동적 방법을 적용하며

[표 4] 안전커널 보안기능요구사항

보안기능	균강급	백두급
보안감사 및 추적	감사자료 생성, 감사검토, 감사사건 선택, 감사사건 저장, 감사 자료 손실 방지	감사자동대응 잠재적인 보안 위반 탐지
신분확인 및 인증	식별시기, 인증시기, 보호된 인증 피드백, 인증시도 실패처리, 사용자 속성 정의, 비밀정보 검증, 사용자와 주체의 연결	비밀정보 생성
사용자 데이터 보호	임의적 접근통제, 강제적 접근통제, 보안속성없이 데이터 유출, 보안속성 포함한 데이터 유출, 내부 전송 보호	임의적 접근통제(부정 사용자로부터 객체 보호), 강제적 접근통제(보안속성 비교), 잔치 보안속성 상세적 무결성 접근통제 보안속성없이 데이터 유입 보안속성 포함한 데이터 유입 보안속성 포함한 데이터 유출(MIC 정책 적용) 보안속성에 의한 데이터 전송 분리 내부전송 보호(MIC 정책 적용)
잔여 정보 재사용	잔여 객체 정보 보호(전체 적용)	
비밀성	암호모듈, 암호키 관리, 암호연산, 자동화된 파일 암호화, 전송 데이터 암호화	암호모듈 (하드웨어 모듈 적용)
보안기능 보호	하부 추상기계 시험, 안전한 복구, 내부 보안기능 데이터 전송,, 보안기능영역 분리, 보안정책의 우회 불가성, 신뢰성 있는 시간 스탬프, 보안기능 데이터의 일관성	자동복구(최소한의 손실 보장) 보안기능 정책의 영역 분리
자체시험	보안기능, 암호, 키 생성요소에 대한 자체 시험	
보안관리	객체 보안 속성 관리, 안전한 보안속성, 정적 속성 초기화, 보안기능 데이터 관리, 보안속성 폐지, 보안속성 유효기간 만료, 보안관리 역할 제한	객체 보안 속성관리(계층적 보안속성), 주체 보안 속성관리 정적 속성 초기화(MIC 정책 적용) 보안관리 역할 제한(MIC 정책 적용)
자원활용	오류에 대한 내성: 전체적용, 자원 최대할당치	부분 자원 사용 우선순위
세션 설정 및 통제	보안기능과 사용자에 의한 세션 잠금, 접근경고, 접근이력	동시 세션수 제한(사용자 보안속성 적용)
안전한 경로	안전한 경로(신분확인 및 인증)	안전한 경로 (주체 보안 속성 변경 통보)

[표 5] 안전커널 보증요구사항

보증	균강급	백두급	문서
형상관리	부분적인 형상관리 자동화, 생성지원, 문제추적 형상관리 범위	개발도구 형상관리 범위	형상관리 문서
배포/운영	변경 탐지, 설치/생성/시동절차		기술이전절차서, 사용자 설명서
개발과정	비정형화된 기능명세, 분리된 설계, 보안기능 구현, 보안기능 모듈화, 설명적인 상세설계, 비정형화된 일차성검증, 비정형화된 보안정책 모델	준정형화된 기능명세, 준정형화된 기본설계 복잡도 감소, 상세설계 수준, 준정형화된 일치성 검증, 준정형화된 보안정책 모델	개발기능 규격서, 상위시스템 설계서, 하위시스템 설계서, 보안기능설계서, 모듈(블록/단위)설계서, 검증 명세서, 보안정책모델서
설명서	관리자 설명서, 사용자 설명서		관리자 설명서, 사용자 설명서
생명주기 지원	보안정책 식별, 기본적인 결함 교정, 개발자 생명주기 모델, 정의된 개발도구	충분한 보안대책, 결함보고절차, 표준화된 생명주기 모델, 구현표현 적용	개발 보안지침서, 결함교정 지침서, 생명주기 관리 지침서, 개발도구 선정 보고서
시험	시험범위 분석, 상세한 설계 시험, 기본시험, 독립적인 표본시험	상세한 시험범위 분석, 기능시험 순서화	기능규격 일치성 분석서, 시스템 설계 일치성 분석서, 시험절차서 및 시험결과서, 시험환경 구축 계획서
취약성 평가	체계적인 비밀채널 분석, 분석한 보안설명서 검증, 보안기능강도 검증, 독립적인 취약성 분석	체계적인 취약성 분석	비밀채널 분석서, 오용분석서, 보안기능강도 분석서, 취약성 분석서

보안기능영역 분리(FPT_SEP.1) 적용 시 NIAP CCEVS의 해석[NIAP Interpretation I-0380]에 따라서 내부 보안기능 데이터 전송(FPT_ITT.1), 보안기능 데이터의 일관성(FPT_TRC.1)과 함께 적용한다. 국가기관용 시스템은 다른 환경에서 보다 자원 활용에 대한 가용성을 보장해야 하므로 오류에 대한 내성(전체 적용)을 적용한다. 신분확인 및 인증기능에서 접근통제정책에 의하여 악의적인 소프트웨어에 의한 권한정보를 획득하지 못하도록 안전한 경로로 로그인을 수행하도록 한다. 비밀성은 아직까지 적용할 수 있는 암호모듈, 암호알고리즘, 키 길이가 국가 정보보호 표준목록이 없으므로 정립할 필요가 있다. 그래서 암호모듈 요구사항과 암호에 적용하는 알고리즘과 키 길이는 국가 정보보호 표준목록을 참조함으로써 신뢰성을 제공한다.

보증요구사항은 CC EAL4등급에 준하는 요구사항을 적용하고 비정형화된 방법으로 문서를 기술한다. 추가적으로 다음과 같은 보증사항을 적용하였다. 개발사항 중 구현에 대한 결함은 시스템의 잠재적인 취약성을 제공하므로 개발자가 작성한 코드의 결함 여부를 검사하고 이러한 결함이 내부 구성요소에 미치는 영향이 있는지 검사가 요구되므로 보안기능에 대한 구현의 표현(ADV_IMP.2)과 상세설계시험(ATE_DPT.2)이 요구된다. 그리고 구현 시 결함으로 인한 시스템에 영향을 감소시키도록 모듈화(ADV_INT.1)가 요구되며 모듈(암호모듈, 기타 모듈)에 대한 비밀채널을 체계적으로 분석할 수 있도록 비밀채널 분석(AVA_CCA.2)이 요구된다. 개발자에 의한 취약성 분석을 하며 공격자의 침투공격에 대한 TOE가 내성을 가지도록 독립적인 취약성 분석(AVA_VLA.2)이 요구된다.

백두급은 감사에서 알려진 보안위반뿐만 아니라 잠재적인 보안위반을 탐지하는 기능과 자동적으로 대응행동을 취할 수 있도록 한다. 신분확인 및 인증에서 정의된 허용기준에 부합되는 비밀정보 생성 메커니즘 적용한다. 계층적 보안속성은 주체와 객체에 대하여 비밀등급으로 분류된 정보를 처리하므로 적용하며 정보의 변질을 방지하기 위해서 모든 주체와 객체에 무결성 등급을 부여한다. 그리고 내부 전송 보호, 정적속성 초기화, 보안역할 관리 제한에 강제적 무결성 통제를 적용한다. 장치보안속성에서 연결된 장치에 보안속성을 부여하여 이를 기반으로 정보의 유출을 방지한다. 비밀성에서 암호모듈은 안정성 측면에서 국가 정보보호 표준목록에 요구되는 하드웨어를 적용한다. 안전한 복구 시 손실을 최소화한 자동 복구를 적용한다. 세션 설정 및 통제에서 사용자의 보안속성에 기반하여 정보의 시현을 통제하도록 동시 세션 수를 제한하는 기능을 제공한다. 안전한 경로에서 주체의 보안속성 변경을 안전한 경로로 통해서 제공한다.

보증요구사항은 EAL5등급의 요구사항을 적용한다. 모든 문서는 준정형화된 방법(객체지향적 및 구조적 방법 기술, 도구 등)을 사용하여 작성한다. 그리고 구현 시 접근통제정책을 수행하는 기능모

들의 복잡도를 최소화 하도록 복잡성 감소(ADV_INT.2)가 요구되며, 시험 절차로 인해서 실패를 할 수 있도록 시험의 적절성을 제공하도록 기능시험 순서화(ATE_FUN.2)가 요구되며, 개발자에 의해 체계적인 취약성 분석을 하며 공격자의 침투공격에 대한 TOE가 중간의 내성이 가지도록 체계적인 취약성 분석(AVA_VLA.3)이 요구된다.

3. 국가기관용 안전커널 개발방향

국가기관용 운영체제의 개발을 가속화시키기 위해서는 TCSEC B2(CC EAL5)등급의 보안운영체제를 구현하는 것이 중요하며 이를 뒷받침 할 수 있도록 국내 보안운영체제를 평가할 수 있는 보안기술과 평가 제도를 마련하는 것이 시급하다. 특히 정형화된(신뢰성 ,무결성 그리고 정보흐름 모델이 결합된) 보안모델 설계와 이에 대한 분석과 관련된 비밀 채널에서 저장 채널은 어느 정도 도구로써 식별이 가능하지만 타이밍 채널은 아직까지 매우 어려운 작업이므로 분석방법 연구에 초점을 두어야 한다. 또한 국가기관용으로 사용하기 위한 독자적인 안전한 운영체제의 평가기준에 대한 연구가 필요하다.

V. 결론

본 논문은 국가기관에서 민감한 정보를 처리하는 시스템과 비밀로 분류된 정보를 안전하게 처리하는 시스템을 위한 안전커널 요구사항을 금강급과 백두급으로 분류하여 제안하였지만 제시한 내용은 PP수준은 아니며 평가기준과 PP 개발 시 참고할 만한 내용으로 구성하였다. 국가차원의 정보보호를 위해서는 보안운영체제를 자체 개발하여 사용하는 것이 다른 보안솔루션 개발보다 우선적으로 수행되어야만 현재의 사이버 공간의 위협에 대비하고 어플리케이션 자체의 취약점에 대처할 수 있으며, 네트워크의 보안 취약점으로부터 발생하는 피해를 최소화시킬 수 있을 것이다. 따라서 고수준의 국가기관용 보안운영체제를 개발하는데 기준이 될 수 있는 자체 평가기준을 국가차원의 지원과 민간업체의 협력으로 개발되어야 한다.

참고문헌

[1] NSA, Labeled Security Protection Profile, Version 1.a, National Security Agency, Jan. 1999.

[2] NSA, Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness, Version 1.22, National Security Agency, May. 2001.

[3] Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria, Dec. 1985.

[4]Department of Defense Directive 5200.28, Security Requirements for Automated Information Systems(AISs), March 21, 1988.

[5]Trusted Product Evaluation Program Trusted Computer System Evaluation Criteria Interpretations.

[6] NSA. Common Methodology for Information Technology Security Evaluation, Part 2 Evaluation Methodology, CEM-99/045, Version 1.0, August 1999.

[7] Department of Defense, DOD Instruction 8500.2 Information Assurance Implemention, Februay 2003.

[8] Common Criteria Implementaion Board, Common Criteria for Information Technology Security Evaluation, CCIB-98-026, Version 2.1. Aug. 1999.

[9]National Security Agency, Information Assurance Techical Frame work(IATF), Version 3.1, Appendix E, Setemper 2002.