通信情報保護學會誌
第1卷, 第2號, 1991. 8

컴퓨터 시스템의 보안평가를 위한 기술적 기준

申 壯 均*

1. 서 론

컴퓨터 시스템의 안정성, 신뢰성 등을 확보하는 목적으로 하는 컴퓨터 보안은 고도 정보화 사회의 필수조건이다. 컴퓨터 보안문제는 정보를 어떻게 통제하여 보호할 것인가라는 보호 메카니즘의 설계와 구현, 그리고 보호 메카니즘을 어느정도 신뢰할 수 있는가라는 보안에 대한 평가 및 검증으로 분류할 수 있다.

컴퓨터 보안은 기본적으로 다음 3가지의 원칙을 가정하고 있다. 첫째로 신뢰(trust)는 절대적일 수 없으며, 절대적일 필요도 없다. 이 원칙은 신뢰 수준에 따라 여러 등급의 시스템이 존재함을 의미한다. 가장 높은 수준의 시스템은 기술적으로 매우 복잡한 공격에도 보호될 수 있으며, 가장 낮은 수준의 시스템은 안전한 환경에서 작동될 때에만 신뢰할 수 있다. 두번째 원칙은 보안정책을 실현하는 컴퓨터 시스템의 능력에 대한 신뢰는 최소한 완전 조정(complete mediation) 조건을 요구한다는 점이다. 완전 조정은 각 객체에 대한 주체의 모든 엑세스는 적법한 권한을 받은 것인지 확인되어야 한다는 조건이다. 마지막 원칙은 컴퓨터 시스템의 신뢰성에 대한 믿음은 각각의 보안규칙에 적용되었는지 여부가 아니라 보안구조가 어떻게 설계되고 구현되었는가에 근거한다는 것이다. 이와 같이 신뢰의 수준이 다양하게 증가함에 따라 컴퓨터 보안 기능을 수준에 따라 분류하고 평가하여 검증하는 방법에 관한 연구가 활발하게 진행되고 있다[6,8].

본고에서는 미국의 컴퓨터 보안평가 지침서인 TCSEC의 보안 요구사항과 평가등급 내용을 살펴보고 유럽 4개국이 공동으로 추진하고 있는 정보기술 보안평가 지침서인 ITSEC의 보안 요구사항과 평가 등급을 조사하였으며, TCSEC과 ITSEC을 비교하여 국내에서 적용할 수 있는 컴퓨터 보안평가 기준을 제시하고자 한다.

2. TCSEC(Trusted Computer Security Evaluation Criteria)

미국의 NCSC(National Computer Security Center)는 1985년에 안전한 컴퓨터 시스템을 위한 평가 지침서인 TCSEC(일명 "Orange Book")을 발간하였다. 안전한 컴퓨터 시스템은 인가된 사용자나 사용자 그룹을 식별하고, 정보에 대한 읽기, 쓰기, 삭제 등에 대한 엑세스 요구를 통제한다. 컴퓨터 보안의 절대적인 보증을 기대하는 것은 비 효율적이기 때문에 어떤 종류의 보안측정 도구들이 컴퓨터 시스템의 보안을 평가하는데 적절한지 식별되어야

* 종신회원, 육군사관학교 수학과 부교수

한다. TCSEC은 컴퓨터 시스템의 보안을 효과적으로 평가하기 위해 6개의 기본 요구사항을 정의하였으며 그 기본 요구사항을 만족시키는 수준에 따라 7가지의 평가등급을 제시하고 있다[2].

2.1 보안 요구사항

기본적인 보안 요구사항은 보안정책(security policy), 표시(marking), 식별(identification), 기록성(accountability), 보증(assurance), 연속적 보호(continuous protection)이다. 이러한 요구사항 중에서 보안정책, 표시, 식별, 기록성은 정보에 대한 엑세스를 통제하기 위한 사항이고, 보증과 연속적 보호는 신뢰성 있는 컴퓨터를 제공하기 위한 보안 검증에 관한 사항이다.

1) 보안정책

컴퓨터 시스템에는 명시적이고 잘 정의된 보안정책이 있어서 주체와 객체가 식별되고 주체에 의한 객체에 대한 엑세스 요구를 인가해 줄 것인가에 대한 보안규칙을 적용해야 한다.

2) 표 시

모든 객체는 그 객체의 보안 등급을 나타내는 "레이블"을 갖고 있어야 하는데 객체와 보안 레이블의 연관을 표시(marking)라고 한다. 이러한 레이블들은 객체에 대한 엑세스 요구시마다 비교를 위해 사용 가능해야 한다.

3) 식 별

모든 주체들은 유일하고 분명하게 식별되어야 한다. 컴퓨터 시스템은 엑세스 요구시마다 엑세스하는 주체가 누구인지 식별 가능해야 하며, 이와 관련된 인증 정보는 안전하게 관리되어야 한다.

4) 기록성

시스템 보안에 영향을 미치는 동작에는 새로운 사용자 가입, 주체나 객체의 보안 등급변화, 새로운 주체나 객체에 대한 보안 등급부여, 비인가된 엑세스 요구 등이 있는데 시스템은 이러한 동작들에 대한 안전하고 완벽한 기록들을 유지해야 한다.

5) 보 증

보안정책, 표시, 식별, 기록성이 시스템에 의해 적용된다는 것을 보증하기 위한 메카니즘을 포함해야 하며, 메카니즘의 효율성을 평가할 수 있어야 한다.

6) 연속적 보호

보안을 구현한 메카니즘은 비인가된 변화나 침투에 의한 방해로부터 계속적으로 보호되어야 한다.

2.2 보안 평가등급

NCSC는 6개의 기본 요구사항을 만족하는 정도에 따라 크게 D분류, C분류, B분류, A분류를 구분한 다음 각 분류에 대해 세분하여 7가지 보안 등급을 제시하였는데 낮은 보안수준으로부터 높은 보안수준으로 각 등급을 나열하면, C, C1, C2, B1, B2, B3, A1이다. 우선 각 분류에 대한 정의를 살펴보면 다음과 같다.

D 분류 : Minimal Protection

기본 요구사항이 없는 것으로 평가는 되었지만 상위 평가등급을 위한 요구사항들을 충족시키지 못한 시스템들이 포함된다.

C 분류 : Discretionary Protection

이 분류에 포함되는 등급들은 discretionary (need-to-know) 보호를 제공하며 감사기능(audit capability)을 수행하여 모든 주체들의 동작을 기록 유지하는 기록성을 제공한다. DAC(Discretionary Access Control)은 주체의 식별(identification)에 근거하여 객체에 대한 엑세스 요구를 통제하는 방법으로 한 주체가 다른 주체에게 자신이 갖고 있는 엑세스 권한을 넘겨주는 것을 허용한다.

B 분류 : Mandatory Protection

이 분류의 주요한 요구사항은 보안 레이블의 무결성을 유지하고 MAC(Mandatory Access Control)을 수행하는 TCB(Trusted Computing Base) 개념이다. MAC는 객체에 포함된 정보의 기밀성(sensitivity)과 주체에게 부여된 보안인가(clearance)에 근거하여 수학적인 보안 모델을 사용하여 보안정책을 적용함으로써 주체의 객체에 대한 엑세스를 강제로 통제하는 방법이다. 이 분류를 만족하는 시스템들은 TCB를 기반으로 하는 보안정책 모델을

제공해야 하며, 조회 모니터(reference monitor) 개념이 구현되었다는 것을 증명하는 증거를 제공해야 한다.

A 분류 : Verified Protection

이 분류의 주요한 특징은 공식적인 보안 검증(formal security verification)이다. 시스템에 도입된 Mandatory 보안제어와 Discretionary 보안제어가 시스템에 저장되어 처리되는 모든 기밀정보를 효과적으로 보호할 수 있는지를 확신할 수 있는 공식적인 보안 검증방법이 사용되어 시스템 보안을 보증해야 한다. 또한 TCB가 시스템의 모든 설계, 개발, 구현에서 제시된 보안 요구사항을 충족시키는지를 증명하는 확장된 문서가 요구된다.

이러한 분류에서 평가등급은 D, C1, C2, B1, B2, B3, A1으로 구분된다. 각 등급은 서로 독립적인 것이 아니고 서로 연관되어 있으며 상위 등급은 하위 등급에 보다 많은 보안 요구사항들을 추가시킨 것으로 정의된다. 실제로 이 등급들은 D, C, B, A의 4가지 분류와는 다른 4개의 집합으로 구분할 수 있다 : 집합 D는 요구사항이 없는 등급이다 ; 집합 C1/C2/B1은 많은 상업적 운영체제에 대한 일반적인 보안특성을 요구하는 등급들이다 ; 집합 B2는 사용하고 있는 모델의 보안에 대한 정확한 증명과 TCB의 서술적인 명세서를 요구하는 등급들이다 ; 집합 B3/A1은 TCB에 대해 더욱 정확하게 증명된 명세서와 공식 설계를 요구하는 등급들이다. 이와 같은 각 보안등급에서 요구하는 보안특성들은 다음과 같다.

1) 등급 D : Minimal Protection

요구되는 보안특성이 없는 등급으로 보안평가가 실패한 시스템이 포함된다.

2) 등급 C1 : Discretionary Security Protection

C1 등급은 동일 수준의 기밀성을 갖는 데이타를 처리하는 사용자들의 환경을 위한 등급으로 시스템은 데이타로부터 사용자들의 격리(separation)를 제공한다.

사용자들이 그들 자신의 데이타를 보호할 수 있는 엑세스 제한을 구현하기에 충분한 엑세스 제어 메카니즘이 있어야 한다. C1 등급으로 분류되기 위해서는 시스템은 보안기능을 포함하는 보안 영역(domain)을 가져야 하는데 이 영역들은 비인가된 변경(tampering)로부터 보호되어야 한다.

C1 등급에서의 가장 중요한 개념은 "discretionary" 제어이다. 모든 사용자 그룹은 확인되어야 하며, 각 사용자 그룹은 다른 사용자 그룹의 엑세스 요구를 허락 또는 거부할 수 있는 권한을 갖는다. 즉 사용자 그룹의 식별에 근거하여 객체에 대한 엑세스 요구를 통제하게 된다. 또한 시스템 보안을 보증하기 위해서는 침투시험(penetration testing)과 같은 방법을 수행하여 비 인가된 사용자 그룹이 보호 메카니즘을 우회하거나 파괴하는 방법이 없다는 것을 보여야 한다. 이러한 C1 등급에 요구되는 보안기준은 다음과 같다.

- 보안정책(Security policy)
  - Discretionary 엑세스 제어
- 기록성(Accountability)
  - 식별(identification)과 인증(authentication)
- 보증(Assurance)
  - 시스템 구조(system architecture)
  - 시스템 무결성(system integrity)
  - 시스템 시험(system testing)
- 문서화(Documentation)
  - 사용자 보안 가이드(security features user's guide)
  - 신뢰기능 메뉴얼(trusted facility manual)
  - 시험문서(test documentation)
  - 설계문서(design documentation)

3) 등급 C2 : Controlled Access Protection

C2 등급은 보호기능이 개인 사용자 수준으로 구현되는 discretionary 엑세스 제어를 제공한다. 시스템의 감사추적(audit trail)은 각 객체에 대한 각 개인들의 엑세스를 추적할 수 있어야 한다. C2 등급에 부과된 추가의 규제는 잔여정보(residue) 노출의 제거이다. 잔여정보란 한 프로세스가 실행이 종료된 후 레지스터, 메모리, 디스크에 남아 있는 데이타이다. 즉 프로세스 종료시에 기억장소에 남아있는 것 뿐아니라 보조기억 장치에 쓰여진

데이타를 포함한다. C2 등급은 잔여정보인 한 객체(object)가 다른 사용자에 의해 재사용될 수 있기 전에 0으로 쓰기를 하는 등의 방법으로 제거되어야 하는 요구사항을 포함한다.

C2 등급의 시스템을 예를들어 보면 IBM MVS 운영체제와 DEC VAX/VMS 운영체제가 있다.

4) 등급 B1 : Labeled Security Protection

모든 B 등급은 nondiscretionary 즉, 강제적인 엑세스 제어인 mandatory 엑세스 제어(MAC)를 포함한다. B1 등급에서 제어되는 모든 주체와 객체들은 각각 하나의 보안수준(security level)을 할당받아야 한다. 제어되는 각 객체는 개별적으로 보안수준에 의해 레이블이 붙여지고 이 레이블들이 기본적으로 엑세스 제어 결정에 사용된다.

엑세스 제어는 계층적 등급(hierachical levels)과 비계층적 범주(nonhierachical categories)를 모두 포함하는 보안 모델(security model)에 기초로 하고 있다. 계층적 등급을 갖는 시스템의 예로는 unclassified, classified, secret, top secret의 계층적 등급을 갖는 군사적 모델을 들수 있고 비계층적 범주는 최소 권한(need-to-know) 범주 집합을 의미한다. 이러한 mandatory 엑세스 제어 정책을 포함하고 있는 대표적인 보안 모델은 Bell-Lapadula 모델이다.

Bell-Lapadula 모델은 보호시스템을 유한 상태 기계(finite state machine)으로 나타내는데 현재 상태는 신원허가(clearance)를 갖는 주체들의 집합, 비밀등급(classification)을 갖는 객체들의 집합, 그리고 엑세스 행렬(access matrix)로 표현되며, DAC에 관해 다음과 같은 중요한 특성을 갖는 보호 모델이다[7].

i) SS-특성(simple-security property)

주체 S는 자신의 신원허가보다 작거나 같은 비밀등급을 갖는 객체에 대해서만 판독을 수행할 수 있다.

ii) *-특성(star property)

주체 S는 자신의 신원허가 보다 크거나 같은 비밀등급을 갖는 객체에 대해서만 기록을 수행할 수 있다. 이 특성은 주체가 자신의 비밀수준 보다 더 낮은 비밀수준으로 정보를 복사하는 것을 금지한다.

따라서 B1 등급은 DAC 통제를 포함하며, 나아가 Bell-Lpadula 모델의 모든 통제를 포함해야 한다.

5) 등급 B2 : Structured Protection

B2 등급의 주요한 개선은 설계 요구사항이다 : B2 시스템의 설계와 구현은 더욱 철저한 테스트와 조사가 가능해야 한다. 검증 가능한 설계가 제시되어야 하며, 테스트는 시스템이 제시된 설계를 구현했음을 확인할 수 있어야 한다. 따라서 시스템의 모든 주체와 객체들에게 적용되는 DAC와 MAC 통제가 명확하게 정의되고 문서화된 공식적인 보안모델을 기초로 구성되어야 한다.

B2 등급의 또 다른 특성은 Covert 채널의 분석이 요구되는 점이다. Covert 채널은 서로 통신할 수 없는 프로세스들이 비정상적인 방법으로 정보를 누출시키는 채널이다. 즉 직접적으로 통신을 하는 것이 아니라 제 3 의 객체를 통해 간접적으로 통신을 하거나, 또는 한 프로세스의 실행동작으로부터 다른 프로세스가 정보를 획득하는 방법을 사용하는 가상적인 채널이다.

이러한 Covert 채널을 모두 찾아내어 봉쇄하는 일은 매우 어려운 일이므로 채널의 bandwidth를 줄이는 방안이 연구되고 있다[7].

6) 등급 B3 : Security Domains

B2 등급은 주체의 객체에 대한 모든 엑세스를 통제하는 조회 모니터(reference monitor) 요구사항을 만족해야 한다. 조회 모니터는 시스템의 모든 엑세스 메카니즘을 포함하고 있는 부분으로 엑세스 권한집합이 데이타베이스로 구성되어 있으며, 활동중인 모든 주체가 객체에 대한 엑세스 권한을 얻기 위해서나 엑세스 권한을 변경하기 위해서는 반드시 조회 모니터에 요구하여 승인을 받아야 하는 규칙이 적용된다. 이러한 조회 모니터는 분석과 테스트가 용이하도록 충분히 작아야 하며, 침투로부터 완전히 보호(tamperproof) 되어야 한다. 이러한 tamperproof 시스템은 침투에 대해 매우 민감하게 저항하는 시스템이다. 따라서 시스템 보안

에 관한 위반사건이 발생했을 때 즉시 식별할 수 있는 감사(audit) 능력과 시스템 회복능력이 요구된다.

7) 등급 A1 : Verified Design

A1 등급은 공식적으로 검증된 시스템 설계를 요구한다. A1 시스템의 보안능력은 B3 등급의 능력과 같다. A1 등급은 trusted computing base가 정확하게 구현되었다는 높은 수준의 보증(assurance)을 요구하는데 A1 등급 검증(certification)을 위한 5가지 중요한 기준이 제시되고 있다.

i) 보호 시스템의 공식적인 모델과 그 모델의 일관성 및 적절성에 대한 증명

ii) 보호 시스템의 공식적인 최상위 명세(top-level specification)

iii) 최상위 명세가 보호 모델과 일치한다는 것을 증명

iv) 명세와 일치하는 구현

v) Covert 채널의 공식적인 분석

이러한 A1 등급으로 분류된 시스템에는 Honeywell SCOMP가 있으며 SRI의 PSOS(Provably Secure Operating System), IBM의 KVM/370(Kernelized VM/370), 그리고 Ford Aerospace의 KSOS(Kernelized Secue Operating System)이 A1 등급을 목표로 연구 개발되고 있다.

3. ITSEC(Information Technology Security Evaluation Criteria)

정보시스템은 기업활동의 효과적 수행을 위한 필수조건이 되고 있으며, 상업적인 사용자들은 그들이 구매하려고 하는 시스템들의 보안능력을 평가할 수 있는 방법을 요구하고 있다. 이러한 요구사항에 기초로 하는 IT(Information Technology) 생산물에 대한 추정과 비교가 가능한 표준의 제정은 분류된 데이타를 보호하고, 시스템 개발에 필요한 여러 작업의 중복성을 배제하며, 자국의 정보에 대한 비인가된 엑세스에 의한 파괴로 국가의 이익에 피해를 가져오는 것을 막자는데 그 목적이 있다.

미국의 TCSEC의 발간은 유럽 공동체 국가들에게 상당한 자극을 주어 자국의 보안 평가 지침서에 대한 연구를 시작하게 하였다. 유럽 공동체 국가들의 보안 평가 지침서 연구는 미국의 TCSEC이 보안의 기술적인 요소중에서 confidentiality만 강조한 평가기준이라고 비판하고 confidentiality외의 보안요소인 integrity, availability까지 포함하는 더 포괄적인 표준안을 제시하고 있다[4].

본장에서는 먼저 유럽 2개 국가(영국, 독일)의 자체 보안 평가 지침서를 살펴보고, 1990년 5월에 발표된 유럽국가들의 공동 보안 지침서인 ITSEC의 성격과 내용을 살펴본다.

3.1 영국 지침서(U.K. Technical Criteria for Security Evaluation)

1989년 2월에 Department of Trade & Industry Commercial Computer Security Center에 의해 제정된 영국 지침서는 Security Prerequests와 claims language를 요구사항으로 하여 6개의 평가등급으로 정의하고 있다[5].

1) 요구사항

Security prerequests는 보안 시스템의 요구된 성질에 대한 공리적인 문장들의 모임으로 보안관리를 위해 제공되는 사항이다. 이 요구사항에는 강제 규정인 Security control(X1-X6)와 비강제 규정인 Security objectives(Y1-Y5)가 있으며 그 내용은 다음과 같다.

X1 :	Accountability	Y1 :	No Addition
X2 :	Authenticatiojn	Y2 :	No Loss
X3 :	Permission	Y3 :	Confinement
X4 :	Object Protection	Y4 :	Timeliness
X5 :	Object Reuse	Y5 :	No Denial of Resource
X6 :	No Repudiation		

한편 Claims language는 보안특성을 사용하기에 적절한 형태로 서술하는데 이용되는 언어로 판매자에 의해 작성되고 보안평가의 기초가 되며, 고객에 의해 이용된다.

2) 평가등급

보안 요구수준이 높아지는 순으로 L1-L6의 6등급으로 분류된다. 각 보안등급은 claim의 주체인 보안특성이 정확히 구현되었는가에 대한 상대적 신뢰수준과 vulnerability에 대한 상대적 신뢰성에 의해 구분된다.

3.2 독일 지침서(German IT-Security Criteria)

1989년 7월 독일 Information Security Agency는 "Criteria for the Evaluation of Trustworthiness of Information Technology Systems"를 발간하였다. 이 지침서는 8개의 보증수준(Q0-Q7)과 10개의 기능등급(F1-F10)을 정의하고 사용자 보안정책은 기능등급중 하나를 사용하거나 그들의 조합에 의해 강화될 수 있음을 제시하고 있다. 이 지침서는 기능등급과 보증수준에 대한 정의 뿐 아니라 기본적인 보안기능들의 개별적인 특성과 그들의 보안시스템 상에 구현되는 방법에 대한 상세한 설명을 포함하고 있다[5].

1) 요구사항

보안기능(Security functionality)에 관한 요구는 다음 10개 등급으로 분류된다.

F1 : Discretionary Security Protection
F2 : Controlled Access Protection
F3 : Labeled Security Protection
F4 : Structured Protection
F5 : Security Domains
F6 : High Integrity for Data & Programs
F7 : High Availability
F8 : High Integrity during Data Communication
F9 : High Confidentiality during Data Communication
F10 : Networks with high demands on Confidentiality

한편 보증수준(assurance levels)에 관한 요구는 다음 7개 등급으로 구분된다.

Q0 : Inadequate Assurance
Q1 : Tested
Q2 : Methodically tested
Q3 : Methodically tested partially analysed
Q4 : Informally analysed
Q5 : Semi-Formally analysed
Q6 : Formally analysed
Q7 : Formally verified

2) 평가등급

보안 요구사항인 보안기능과 보증수준의 조합으로 분류되는데 보안 요구수준이 높아지는 순으로 다음 7개 등급을 제시하고 있다.

(, Q0), (F1, Q1), (F2, Q2), (F3, Q3), (F4, Q4), (F5, Q5), (F5, Q6)

따라서 보안기능 F6-F10은 평가등급과 무관하다.

3.3 ITSEC(Information Technology Security Evaluation Criteria)

1991년 5월에 프랑스, 독일, 네델란드, 영국은 하나의 보안 평가기준인 ITSEC을 발표하였는데 이들 국가들의 노력은 다음 사항들의 성취를 목표로 하고 있다[3].

- 유럽국가간 무역에 대한 장벽을 피하기 위한 공통 지침서
- 기본적인 표준안과 시험에 관한 출판된 지침서
- 재평가, 생산, 향상, 새로운 version, 평가과정의 신뢰성 문제를 해결할 수 있는 지침서
- 새로운 것과 개선된 생산물 사이의 충돌을 최소화하고, 기대효과를 최대화하는 지침서
- 다국적 개발과 이질 시스템인 경우 평가과정에서의 중복된 노력을 최소화하는 지침서

그러나 이러한 이유보다 ITSEC을 유럽 4개국이 공동으로 발표한 더 큰 이유는 세계 IT(Information Technology) 시스템에 대한 보안평가 지침서로서 주도적 역할을 수행하기 위한 것이다.

ITSEC은 유럽 4개국의 공통된 보안기준과 보안

평가과정에 대한 내용과 IT 생산물이나 시스템의 보안기능을 서술할 수 있는 방법을 설명하는 내용으로 구성되어 있다. 평가등급은 7개의 수준으로 정의되어 각 등급별로 여러가지 정확한 요구사항을 제시하고 있으며, 각 수준에 적용할 수 있는 효용성 기준(effectiveness criteria)도 제시하고 있다. 이 지침서에 포함되어 있는 보안은 confidentiality, integrity, availability의 기술적 요소를 모두 포함하고 있어서 정보는 엑세스 권한을 가진 사용자에게만 노출되며 수정할 수 있는 권한을 가진 사용자에 의해서만 수정될 수 있고, 정보와 다른 기술적 자원을 적법한 사용자가 필요시에는 항상 엑세스 할 수 있는 보안 시스템을 의미한다. 이와 같은 ITSEC은 보안기능(functionality), 보증(assurance), 정확성(correctness), 효용성(effectiveness) 기준에 따라 보안 요구사항을 분석하고 평가등급을 제시하고 있다.

1) 보안기능(functionality)

보안평가의 목적은 평가시스템에 대해서 보안에 관한 보증등급을 부여하는 것이다. 이 목적을 달성하기 위해 평가자는 시스템이 보안측면에 기여하는 기능을 정확하게 구분하고 정의할 수 있어야 한다. ITSEC은 보안기능에 대한 다음 3가지 추상화 수준을 제시하고 있다.

- 보안목표(security objectives) :
  가장 추상화된 수준으로, 시스템이 달성하려고 하는 보안에 대한 기여로서 왜 보안기능이 요구되는가를 정의한다.
- 보안기능(security functions) :
  보안에 기여하는 생산물이나 서비스의 특성으로 실제 무엇이 수행되는가를 나타낸다.
- 보안 메카니즘(security mechanisms) :
  보안기능을 구현한 논리 및 알고리즘으로 보안기능이 어떻게 수행되는지를 나타낸다.

한편 이 지침서는 보안기준의 가장 중요한 부분을 이루고 있는 보안기능을 제시하고 있는데 보안기능은 다음과 같은 8개의 기본적인 기능으로 그룹화되어 있다.

- 식별(identification)과 인증(authentication) :
  요구된 사용자의 신원을 식별하고 인증한다.
- 엑세스 제어(access control) :
  사용자나 프로세스에 의한 객체에 대한 사용을 제어하고, 사용자나 프로세스간의 정보흐름을 제어하며, 엑세스 권한을 관리하고 검증한다.
- 기록성(accountability) :
  보안에 관련된 행위를 수행할 수 있는 권한의 변화를 기록한다.
- 감사(audit) :
  보안에 대한 위협이 될수 있는 모든 사건을 추적하고 조사한다.
- 객체 재사용(object reuse) :
  데이타 객체의 재사용을 제어한다.
- 정확성(accuracy)
  보안에 관련된 정보의 정확성과 일치성을 보장한다.
- 서비스의 신뢰성(reliability) :
  보안 서비스의 가용성과 신뢰성을 보장한다.
- 데이타 교환(data exchange) :
  통신채널을 통한 전송중의 데이타 보안을 보장한다.

이러한 보안기능에 근거를 두고 평가등급을 F1-F10의 10개 등급으로 분류하였는데 F1-F5까지의 5개 등급은 미국의 TCSEC으로부터 유도되어 그 기능들을 포함하고 있으며, F6-F10까지의 5개 등급은 시스템의 운영체제와는 별도로 다양한 형태의 생산물 또는 시스템이 상기의 8개 보안기능으로 정의될 수 있음을 나타내고 있다.

따라서 시스템의 보안기능은 미리 정의되어 있는 등급과는 관계없이 발표된 표준기능으로부터 유도될 수 있어서 특정 시스템의 보안기능이 또다른 표준을 나타내는 지침서가 될 수도 있다.

2) 보 증(assurance)

보증기준은 2개의 상이한 내용으로 구성되어 있는데 첫번째는 시스템에서 규정된 보안기능의 정확한 구현에 관한 모든 기준을 포함하고 있으며, 다른 내용은 시스템 평가과정에서 발견된 보안기능, 보안 메카니즘의 효용성(effectiveness)를 나타내는 기준을 포함하고 있다. 효용성이란 보안

생산물이 사용될 가상적인 환경이나 실제 환경에서 일어날 수 있는 가정된 또는 실제 위협에 대응하는 능력을 말한다. 이와 같이 보증에 관한 평가는 정확성과 효용성에 관한 기준이 만족되었다는 증거를 제시해 준다.

3) 정확성(correctness)

이 기준은 평가 시스템의 정확성에 관한 신뢰에 따라 7개의 평가 등급을 제시하고 있는데 E0가 가장 낮은 레벨이고 E6가 가장 높은 레벨이다. E1으로부터 E6에 이르는 평가등급은 점진적으로 요구사항이 증가하는데 개발과정, 개발환경, 운영 지침서, 평가를 위한 운영결과 등이 어떻게 만족되어야 하는지를 나타내고 있다.

- E0 등급 : 부적절한 보증을 나타낸다.
- E1 등급 : 비공식적으로 규정된 보안목표와 보안구조에 대한 비공식적인 설명을 요구하고 있으며, 보안시험(testing)으로 시스템이 보안목표를 만족하는가를 나타낼 수 있어야 한다.
- E2 등급 : E1 등급에 부가하여 상세 설계의 비공식적인 서술을 요구하고 있으며, 보안시험의 증거가 제시되어야 한다.
- E3 등급 : E2 등급에 부가하여 보안기능에 대한 상세 설계와 원시코드를 요구한다.
- E4 등급 : E3 등급에 부가하여 보안정책에 대한 공식모형(formal model)을 요구하고 있으며, 구조적 설계와 상세 설계를 사용하여 침투분석(vulnerability analysis)이 수행된다.
- E5 등급 : E4 등급에 부가하여 상세 설계와 원시코드를 사용하여 침투분석이 수행된다.
- E6 등급 : E5 등급에 부가하여 구조적 설계의 공식적인 기술과 보안정책 공식모형의 일치성을 요구하고 있다.

4) 효용성(effectiveness)

효용성 평가를 위한 지침은 평가등급별로 구분되지 않고 전체로서 적용되도록 제시하고 있는데 효용성 평가는 시스템이 사용될 환경에서의 제안된 사용에 관한 사항으로 다음과 같은 기준을 포함하고 있다.

- 기능의 적합성(suitability) : 시스템의 보안기능이 보안목표에 규정된 위협에 대응할 수 있는지 여부
- 기능의 결합성(binding) : 각각의 보안기능과 메카니즘이 함께 수행되어 통합될 수 있는지 여부
- 메카니즘의 강도(strength) : 보안 메카니즘이 직접 공격에 견딜수 있는지 여부
- 사용의 편리성(ease) : 보안기능과 메카니즘을 실제 운영시의 편리성
- 운영침투에 대한 보호 : 시스템 운영시 보안목표에 규정된 보안이 유지되지 않는 침투 허점이 발견될 수 있는지 여부

이러한 기준에 근거하여 효용성 평가는 시스템의 보안 메카니즘에 대한 강도를 기본(basic), 중급(medium), 고급(high)으로 분류하고 있다. 기본등급은 모든 중요한 메카니즘이 비록 시스템에 관한 정보를 알고 있는 공격자로부터는 침투당할 수 있지만 그외의 우연한 침투공격(subversion)으로부터는 보호되는 수준이고, 중급 등급은 모든 중요한 메카니즘이 제한된 기회와 자원을 갖고 있는 공격자로부터 보호되는 수준이며, 고급 등급은 모든 중요한 메카니즘이 고급 수준의 기술, 기회, 자원을 갖고 있는 공격자에 의해서만 침투될 수 있는 수준이다.

5) 종합 등급(rating)

보안평가 후에 종합 등급은 효용성과 보증기준을 제외한 보안기능과 정확성 기준에 의해 보안요구가 더 엄격한 순서로 다음과 같이 분류된다.

(E0), (F1, E1), (F2, E2), (F3, E3), (F4, E4), (F5, E5), (F5, E6)

정확성 기준을 만족하지 못하는 모든 시스템은 E0 등급인 부적절한 보증 등급을 부여받으며, 정확성 기준을 만족한 경우에도 효용성 측면에서 실패한 모든 시스템도 역시 E0 등급을 부여받는다. 효용성 기준에 대한 등급은 별도로 부여하지 않는다.

4. 보안평가 기준

4.1 TCSEC과 ITSEC의 비교

ITSEC에서 보안 기능측면에서 분류된 F1-F5 등급은 TCSEC의 5개 등급과 일치하도록 설계되었다. 그러나 ITSEC의 평가등급은 integrity와 availability의 다양한 기준을 통합하려고 노력하여 TCSEC에는 없는 여러 요구사항을 포함하고 있다. ITSEC의 평가등급과 TCSEC의 평가등급 사이에는 직접적인 일치성은 존재하지 않으나 두 지침서 사이의 의도된 동질성은 다음과 같다.

TCSEC	ITSEC
D ←	E0
C1 ←	F1, E1
C2 ←	F2, E2
B1 ←	F3, E3
B2 ←	F4, E4
B3 ←	F5, E5
A ←	F5, E6

ITSEC에서 평가된 보안 생산물이나 시스템은 해당 행의 TCSEC 요구사항을 충족하지만 그 반대는 성립하지 않는다. 왜냐하면 ITSEC의 요구사항들이 TCSEC의 요구사항보다 더 광범위하고 구체적이기 때문이다. ITSEC은 심지어 엑세스 제어 정책을 갖고 있지 않는 시스템까지도 평가 범주에 포함시켜 그 평가대상이 광범위 하기 때문에 TCSEC의 TCB (Trusted Computing Base)와 조회 모니터(reference monitor)의 개념을 포함하고 있지 않다.

4.2 KCSEC(Korea Computer System Evaluation Criteria)

이 절에서는 미국의 TCSEC과 유럽의 ITSEC을 기초로 국내에서 적용할 수 있는 간단하면서도 명확한 컴퓨터 보안평가 기준인 KCSEC을 제시하고자 한다. 컴퓨터 시스템의 보호 메카니즘은 크게 나누어 객체에 대한 주체의 엑세스를 통제하여 적절한 권한을 갖는 주체만이 객체를 엑세스 할수 있게 하는 엑세스 제어(access control)와 컴퓨터 시스템에서의 정보흐름에서 보안등급상 안전한 채널만을 허용함으로써 정보누출을 방지하려는 흐름제어(flow control)로 분류할 수 있다. 엑세스 제어의 기본 개념은 DAC(Discretionary Access Control)에 의해 구현되며, 흐름제어의 기본 개념은 MAC(Mandatory Access Control)에 의해 구현된다. 이와 같은 보안기능을 갖는 등급을 2개의 가장 낮은 수준으로, 병렬로 분류할 수 있다.

등급 가 : 엑세스 제어, 등급 A : 흐름제어

다음 단계의 등급은 TCSEC의 B등급과 마찬가지로 등급 가(엑세스 제어)에 등급 A(흐름제어)의 기능이 부가된 등급과 역으로 등급 A(흐름제어)에 등급 가(엑세스 제어)의 기능이 부가된 등급으로 제시한다.

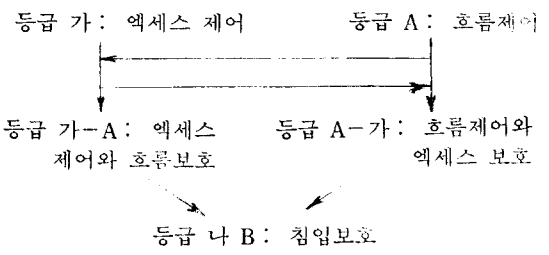
등급 가-A : 엑세스 제어와 흐름보호 (flow protection)
등급 A-가 : 흐름제어와 엑세스 보호 (access protection)

등급 A-가(흐름제어와 엑세스 보호)는 시스템내의 모든 정보흐름은 MAC 정책에 의해 통제되는데 정보흐름이 허용된 경우에는 자원의 소유권을 보유하고 있는 주체에게 이중으로 정보흐름 요구를 하여 허용/거부의 통제를 받게 하는 새로운 보호 방법이다[10].

보호등급의 마지막 단계는 외부 침입을 탐지하여 보호할 수 있는 수준으로 보호 메카니즘을 우회한 경우에도 정보의 confidentiality, integrity, availability를 보장해야 한다.

등급 나 B : 침입보호(Intrusion Protection)

침입보호는 암호기술을 사용하여 정보의 비밀성을 보장하는 수동적 보호와 침입을 탐지하여 경보함으로써 정보의 무결성을 달성하려는 능동적인 보호를 포함한다. 이와 같은 컴퓨터 시스템의 보안평가 기준을 요약하면 다음과 같다.



5. 결 론

컴퓨터 시스템의 보안평가는 컴퓨터내의 정보를 어떻게 보호하는가 라는 문제를 입증할 수 있다는 면에서 매우 중요한 문제이다. 미국은 NCSC(National Computer Security Center)를 설립하고 보안평가 지침서인 TCSEC을 발표하였으며 프랑스, 독일, 네델란드, 영국의 4개국은 유럽의 보안평가 지침서인 ITSEC을 발표하였다. TCSEC과 ITSEC은 각기 보안의 기술적 요소인 Confidentiality, integrity, availability를 보증하기 위해 다양한 보안 요구사항과 여러 수준의 보안 평가등급을 제시하고 있다.

컴퓨터 보안에 대한 국내의 요구가 증대되고 있는 현재 컴퓨터 시스템을 보안측면에서 분류하고 평가할 수 있는 국가 표준의 제정은 시급한 실정이다. 본고에서는 컴퓨터 보안 평가기준을 주도하고 있는 미국의 TCSEC과 ITSEC을 분석하고 비교하였으며, 국내의 컴퓨터 보안에 적용할 수 있는 새로운 보안 평가기준을 제시하였다. 제시된 보안 평가기준에 관한 세부적인 요구사항과 각 등급별 검증방법은 계속 연구될 과제이다.

참 고 문 헌

1. Bell, D.E. and L.J. Lapadula, Secure Computer Systems : Mathematical Foundations and Model, M 74-244, Vol. 3, MITRE Corp., 1974.

2. DoD, Trusted Computer System Evaluation Criteria, Dod 5200.28 STD, Dec., 1985.

3. GIM, Information Technology Security Evaluation Criteria, German Interior Ministry(for the Four Nation Group) Version 1, May, 1990.

4. Jahr, C., "Europe Pursues Different Computer Security Approach," Signal, AFCEA, pp.45-50, Jan., 1991.

5. Le Roux Y., "Technical Criteria for Security Evaluation of Information Technology Products," 90 IFIPS TC-11 Conference, May, 1990.

6. Lee, T.M., "Security Criteria Evolves to Meet a Changing World," Signal, AFCEA, pp.29-34, Jan., 1991.

7. Millen, J.K., "Covert Channel Capacity," Proceedings Symposium on Security and Privacy, IEEE, pp.60-67, 1987.

8. Pfleeger C.P., Security in Computing, Prentice-Hall, 1989.

9. 박태규외 2인, "컴퓨터/네트워크 시스템 보안 표준화 동향분석," 제 2 회 정보보호와 암호에 관한 워크숍 논문집, 한국전자통신 연구소, pp.95-113, 1990.

10. 신광균, 황종선, "소유권에 의한 화일 액세스 제어," 제 2 회 정보보호와 암호에 관한 워크숍 논문집, 한국전자통신 연구소, pp.45-59, 1990.

□ 著者紹介

申 壯 均(종신회원)

1974年 陸軍士官學校 卒業
1979年 서울大 産業工學科 卒業
1983年 美 Wisconsin大(電算學 碩士)
1989年 高麗大 大學院(電算學 博士)
現 陸軍士官學校 副教授

관심분야 : 운영체제 보안, 분산 시스템