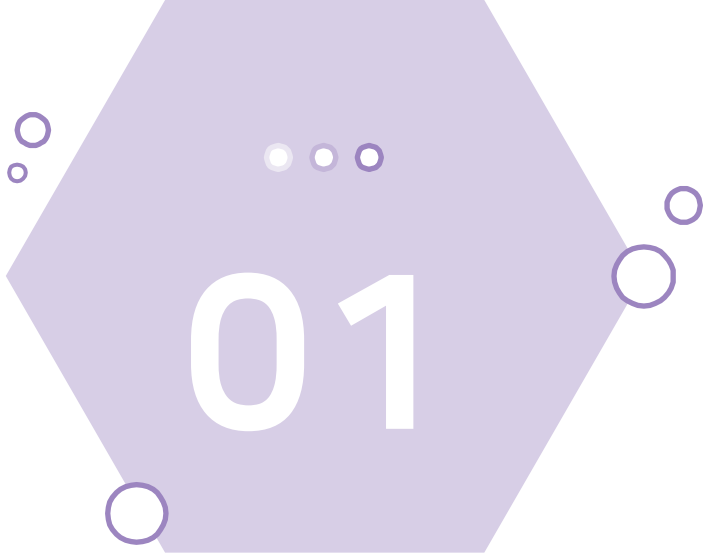
14강. 운영체제 보안

방송대 컴퓨터과학과
김진욱 교수

목차



보안의 개요

보안의 개요

컴퓨터 시스템 보호

- 컴퓨터 시스템 내부 자원 각각의 영역을 보장해 주는 것
- 각 프로세스가 CPU를 점유하는 시간, 사용하는 자료, 자료를 관리하는 작업, 점유하는 장치 등

컴퓨터 시스템 보안

- 시스템과 그 시스템 내의 자료가 결함이 없도록 보존시키고 신뢰성을 유지하는 기법
- 인증, 암호화 등을 통한 합법적인 처리만이 이루어지도록 보장

보안의 개요

보호 및 보안의 목적

- 사용자가 자원에 대한 접근 제한을 의도적으로 위반하는 것을 방지
- 주변 시스템 간의 인터페이스에서 잠재적인 오류를 검출함으로써 시스템의 신뢰도를 증가
- 시스템의 자원들이 무자격 사용자에 의하여 잘못 사용되는 것을 방지
- 권한이 있는 사용자와 권한이 없는 사용자를 구별하는 수단을 제공

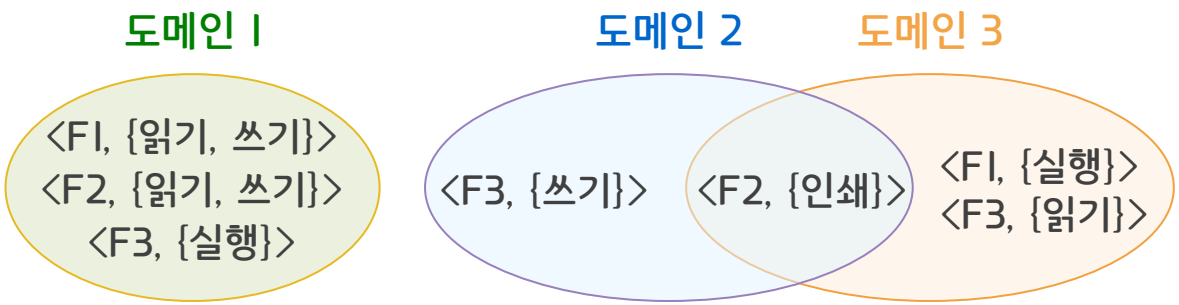
- 시스템 프로세스와 사용자 프로세스 간의 관계 규정
- 시스템 관리 자료와 사용자 관리 자료에 대한 접근제어 규정

보호영역

- 한 프로세스가 접근할 수 있는 자원
- 각 영역은 객체의 집합과 그 객체에 대해 취할 수 있는 조작의 유형을 정의
- 하나의 영역(도메인)은 접근권한의 집합

접근권한

- 프로세스가 객체에 대한 조작을 수행할 수 있는 능력
- <객체 이름, 권한 집합>

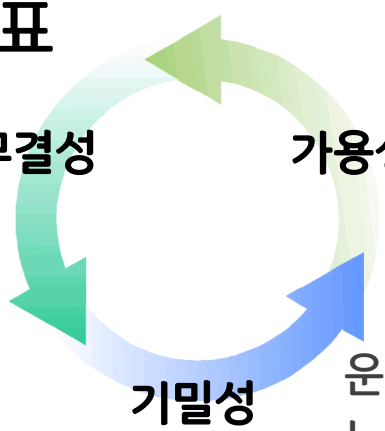


운영체제 보안

운영체제 보안의 개요

- 공격으로부터 운영체제상의 자원에 대한 불법적인 수정이나 참조를 방지하는 정책과 기법
- 분산된 다수의 사용자 시스템 및 통신망을 통해 접근되는 자원들에 대한 안정성을 보장

운영체제 보안의 기본 목표



비 인가 주체에 의한 자원의 생성, 변경, 삭제 등으로부터 자원을 보호

모든 주체는 합법적인 경우에는 항상 객체에 접근이 가능해야 함

운영체제 자원의 부적절한 노출을 예방하고 감지

운영체제 보안

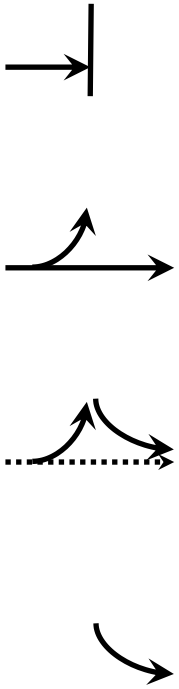
정보 침해

- 안전하게 유지되어야 할 정보에 대해서 불법적인 참조나 변조가 가해지는 것
- 고의적 침해
  - » 운영체제의 사용자 신분 확인 기능이 미약하여 고의적으로 다른 사용자의 사용권한을 도용하는 경우
- 우연한 상황의 침해
  - » 운영체제 내부의 결함이나 기능 부족으로 인하여 보호영역의 통제가 정확하게 되지 못하여 우연히 다른 사용자의 영역을 침범하게 되는 경우

운영체제 보안

정보 침해 위협 요소

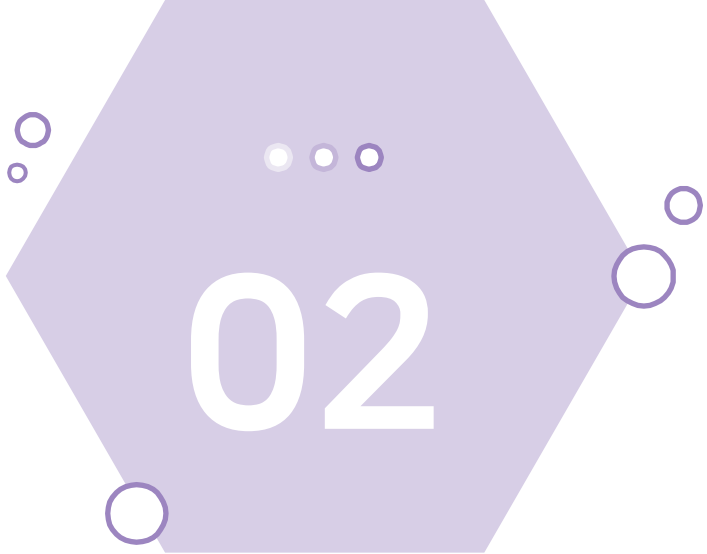
- 흐름 차단
  - » 시스템의 일부가 파괴되거나 사용할 수 없게 된 상태 (가용성 위협)
- 가로채기
  - » 인가받지 않은 제3자가 컴퓨터 자원에 접근하는 경우 (기밀성 위협)
- 변조
  - » 인가받지 않은 제3자가 자원에 접근하여 내용을 변경하는 경우 (무결성 위협)
- 위조
  - » 인가받지 않은 제3자가 운영체제 내에 위조물을 삽입하는 경우 (무결성 위협)



운영체제 보안

정보 침해 유형

트로이 목마	사용자가 감염된 프로그램을 실행하게 함으로써 사용자가 가지고 있는 합법적 권한을 사용하여 시스템 방어체제에 침입
트랩 도어	고의로 만들어 놓은 시스템의 보안이 제거된 비밀 통로 정상적인 인증 절차를 우회하거나 원격 접속 등의 행동을 할 수 있게 함
비밀 채널	중요한 정보나 자료를 얻어내기 위해 정상적인 데이터 전송 메커니즘이 아닌 비밀 통로를 만드는 것
웜	스스로 복제를 함으로써 다른 컴퓨터로 자신의 복사본을 널리 퍼뜨리는 악성코드
바이러스	다른 프로그램에 감염이 되어 전파되는 악성코드



보안 정책 및 보안 메커니즘

보안 정책 및 보안 메커니즘

- 보안 정책
  - 보안을 어떠한 관점에서 무엇을 행할 것인가를 결정
  - 권한부여, 접근제어, 최소권한, 감사 등

- 보안 메커니즘
  - 보안을 어떠한 방법으로 할 것인가를 결정
  - 암호, 인증, 보안등급 관리 등

보안 정책

- 권한부여(authorization)
  - 어떤 객체를 어떻게 액세스 할 수 있는가를 결정
  - 주체의 자원에 대한 접근제어 및 보안등급 부여를 가능하게 함

- 임의적 접근제어
  - 개별 소유자의 자율적 판단에 따라 자원의 접근권한을 다른 사용자에게 부여
  - 자원의 공동 활용에 유용하나 자원 유출 가능성 내포

보안 정책

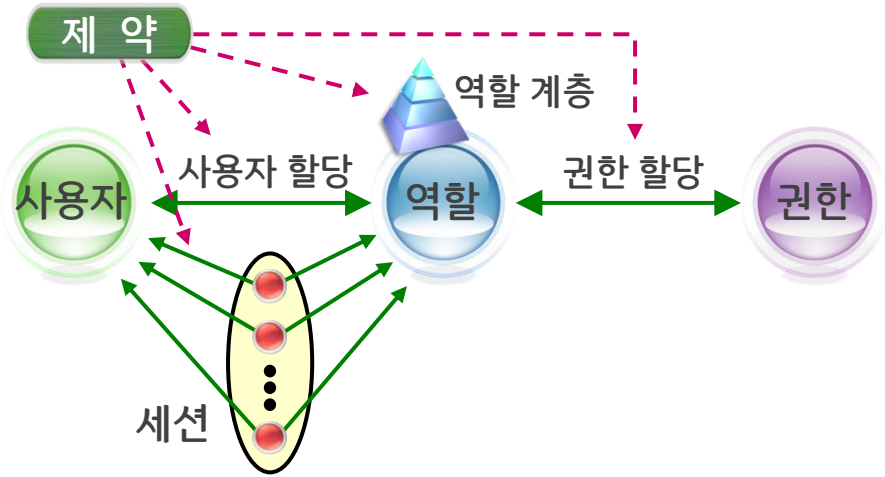
강제적 접근제어

- 개별 객체에는 비밀등급을, 사용자에게는 허가등급을 부여
- 각 주체가 객체에 접근할 때마다 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 주체에게만 권한을 부여
- 규칙의 적용은 모든 주체 및 객체에 대해 일정함

보안 정책

역할 기반 접근제어(Role-Based Access Control, RBAC)

- 권한은 역할과 관계가 있음
- 사용자는 역할의 멤버가 됨으로써 권한을 배정받음
- RBAC의 4 요소: 사용자, 역할, 권한, 세션



보안 정책

- 최소권한
  - 사용자는 특정 임무를 수행하는데 필요한 최소한의 제한적 권한만 할당받아야 함
  - 이 권한은 임무를 수행하는 동안만 할당됨

- 감사(auditing)
  - 컴퓨터 시스템에 중요한 사건이 발생하면 즉시 시스템의 안전한 곳에 자동적으로 기록

보안 메커니즘

- **주체 및 객체의 레이블 부여 메커니즘**
  - 강제적 접근제어를 위해 필요한 메커니즘
  - 시스템의 자원에 식별자 및 보안 등급 레이블 부여
  - 낮은 등급을 갖는 주체가 높은 등급을 갖는 객체에 접근하지 못하게 함
  - 체계적이고 안전한 등급의 관리를 위해 보안 등급 관리 메커니즘 사용

- **임의적 접근제어를 위한 메커니즘**
  - 모드 비트, 접근제어 리스트(ACL)를 이용

보안 메커니즘

- 안전한 암호 메커니즘
  - 비밀키 암호 및 공개키 암호 알고리즘
- 안전한 인증 메커니즘
  - 사용자 식별을 위한 ID 및 패스워드
  - 패스워드는 암호를 이용하여 안전하게 관리

보안 메커니즘

운영자 권한의 분산 메커니즘

- 시스템 관리자의 권한을 세분화하여 각각 다른 사용자에게 부여
- 최소권한 정책을 위한 방법

기록 파일 관리 메커니즘

- 사용자의 사용 기록을 안전하게 보관 및 불법적 수정 금지
- 기록 파일에 대해 접근제어 및 암호화 적용

하드웨어 보호를 위한 방법

- 하드웨어 보호를 위해 사용되는 방법
  - 모드 비트를 이용한 이중 모드(슈퍼바이저 모드, 보호 모드) 연산
  - 2개의 레지스터(기준 레지스터, 한계 레지스터)를 이용한 메모리 보호
  - 타이머를 이용한 CPU 보호

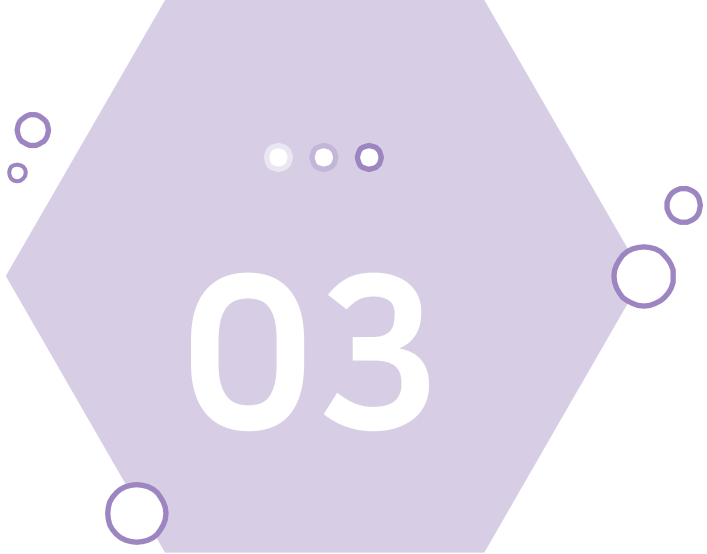
암호 알고리즘

비밀키 암호 알고리즘

- 암호화 키와 복호화 키가 동일한 암호방식
- 공개키 방식보다 빠름

공개키 암호 알고리즘

- 암호화 키와 복호화 키가 서로 다른 암호방식
- 전자서명에 응용

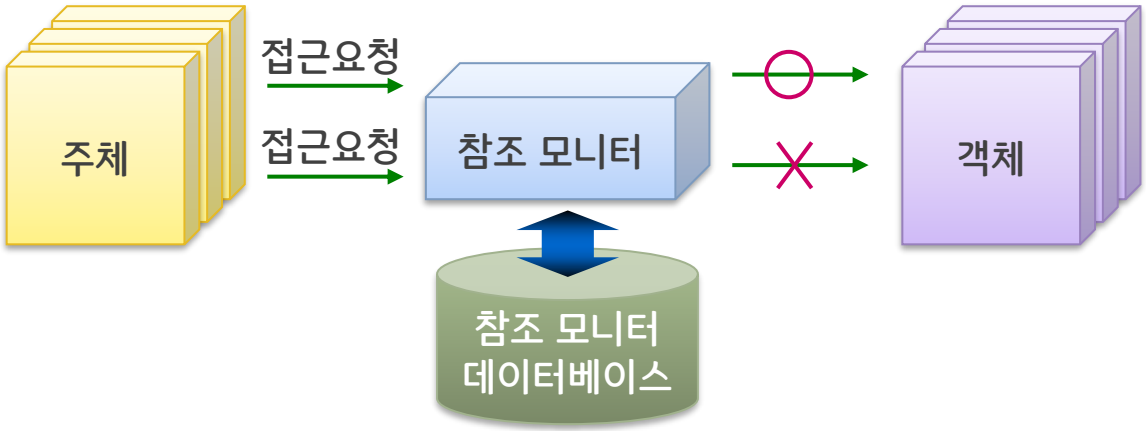


운영체제 보안 모델

운영체제 보안 모델

참조 모니터 모델

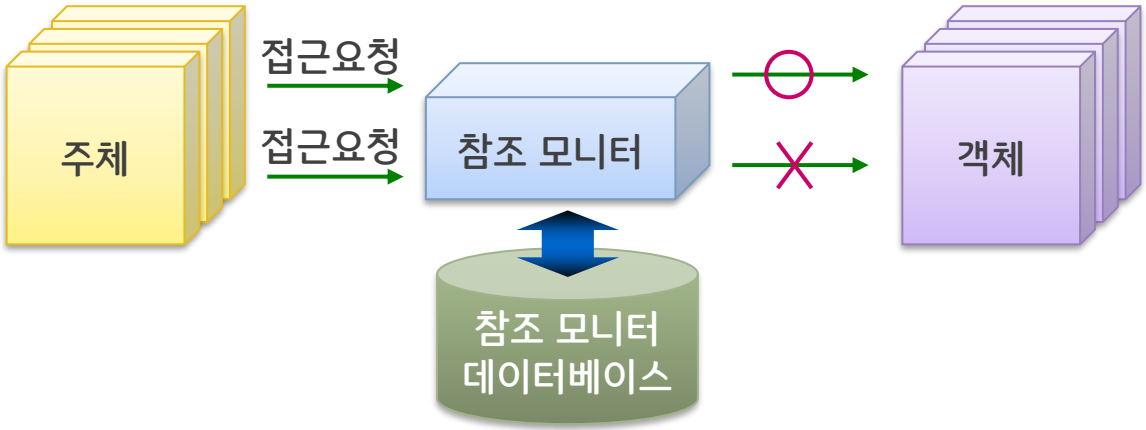
- 프로세스와 파일의 정보 흐름을 감시하는 보안 모델
- 참조 모니터는 주체와 객체의 접근 권한을 정의한 데이터베이스를 참조하여 보안 정책을 수행



운영체제 보안 모델

참조 모니터 모델

- 단순 접근의 허용 여부만을 결정하는 단일 레벨의 보안 모델
- 각 주체는 자신이 소유하거나 접근한 정보의 확산에만 책임
- 문제점: 시스템에서 정보의 안전한 흐름을 보장할 수는 없음



운영체제 보안 모델

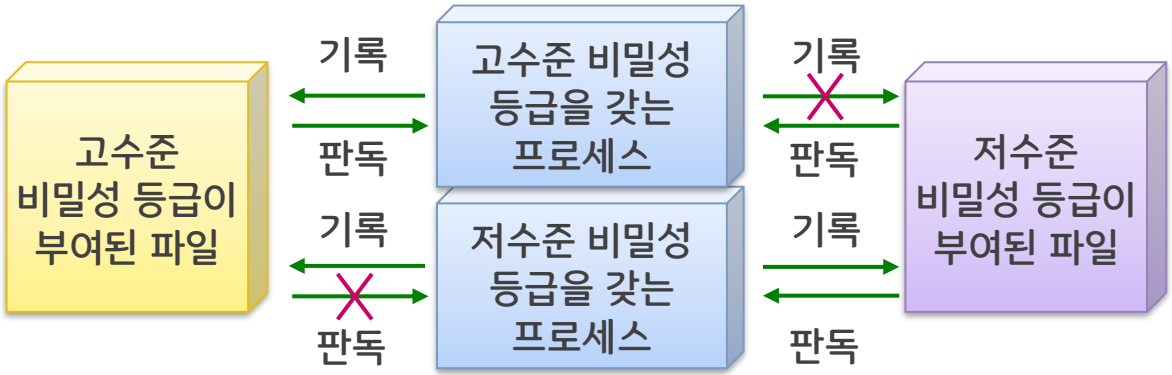
정보 흐름 모델

- 허가 받지 않았거나 안전하지 않은 정보 흐름을 방지하는 보안 모델
- 벨-라파듈라(BLP) 모델
  - » 상위 보안 수준에서 하위 보안 수준으로 정보가 흐르는 것을 방지하는 것에 관심을 둠
- 비바(Biba) 모델
  - » 하위 보안 수준에서 상위 보안 수준으로 정보가 흐르는 것을 방지하는 것이 관심을 둠

정보 흐름 모델

벨-라파듈라(BLP, Bell-LaPadula) 모델

- 기밀성 유지에 초점
- 시스템 보안을 위한 규칙 준수 규정과 주체의 객체 접근 허용 범위를 규정
- 문제점: 낮은 등급을 갖는 주체가 높은 등급을 갖는 객체에 대한 수정을 허용



✪ 쓰기 접근

객체의 보안 수준이 주체의 보안 수준 이상이어야 가능

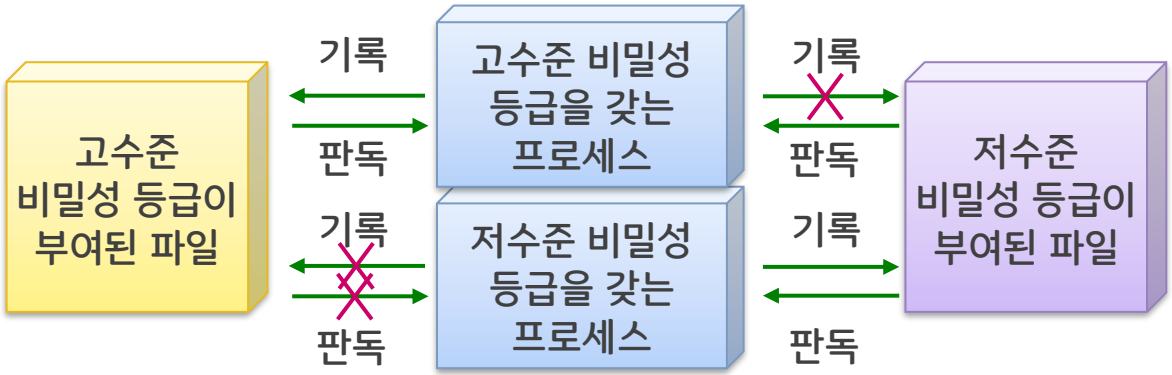
✪ 읽기 접근

주체의 보안 수준이 객체의 보안 수준 이상이어야 가능

정보 흐름 모델

비바(Biba) 모델

- BLP 모델에 불법 수정 방지를 추가로 정의한 무결성을 중요시하는 모델
- 낮은 등급의 주체가 높은 등급의 객체로 쓰기 접근을 금지



보안 커널

- 운영체제 커널에 보안기능을 통합시킨 것
- 안전한 운영체제: 보안 커널을 이식한 운영체제
- 사용자에 대한 식별 및 인증, 접근통제, 재사용 방지, 침입 탐지 등의 보안기능을 갖춤

강의를 마쳤습니다.

다음시간에는

15강. 운영체제 사례