11주차 1차시 정보보호 개요

【학습목표】

1. 정보보호의 개요를 설명할 수 있다.
2. 정보보호의 기법, 영역을 설명할 수 있다.

학습내용1 : 정보보호의 개념

1. 자원 보호

하드웨어 적인 보호
  - CPU, 메모리 세그먼트, 프린터, 보조기억장치 등
소프트웨어 적인 보호
  - 파일, 프로그램, 세마포어 등
불법적인 접근 제어
물리적인 손상을 예방

2. 사용자 접근에 의한 파일 보호

다수의 사용자로부터 접근제어
접근 권한이 허가된 사용자만 접근허용
사용자의 권한 정도에 따라 부분 접근 허용

3. 데이터 접근에 의한 파일 보호

다수의 프로그램의 접근 권한 제어
접근 권한이 허가된 집합체/프로그램 만 접근 허용
프로그램의 권한 정도에 따라 부분 접근 허용

4. 보호정책

무엇이 행해질 것인가를 결정하는 것

보호정책 설정
시스템 설계 시에 설정
시스템 관리 중에 설정
자신의 파일이나 프로그램을 보호하기 위한 각 사용자로부터 정의

5. 보호영역의 개념

한 프로세스는 한 개의 보호 영역 내에서 동작
각 영역은 프로세스가 접근할 수 있는 객체(자원)의 집합과 그 객체에서 취할 수 있는 조작의 형태를 정의

6. 접근권한

객체에 대한 조작을 수행할 수 있는 능력
한 영역은 접근 권한의 집합이고, 그 각각은 (객체이름, 권한집합)의 순서쌍으로 구성
영역은 서로 분리될 필요가 없고, 접근 권한을 공유

학습내용2 : 정보보호의 기법

접근 제어 행렬(Access Control Matrix)
전역 테이블(Access Control Matrix)
접근 제어 리스트(Access Control List)
권한 리스트(Capability List)
록-키(Lock-Key)

1. 접근 제어 행렬(Access Control Matrix)

일반적인 모델
객체 접근 권한을 행렬로 표시한 기법
행 : 주체(사용자, 프로세스)
열 : 객체(파일, 프로그램, 스캐너, 프린터)
각 항 : 접근 권한 집합
각 항은 영역 내에서 실행중인 프로세스가 객체에 대해서 호출 가능한 연산의 집합을 정의한다.

	File 1	File 2	스캐너	프린터
영역1	기록	판독		
영역2	판독	기록		
영역3			판독	프린트
영역4	판독,기록	판독,기록		

2. 전역 테이블(Global Table)

가장 단순한 기법
세 개의 순서쌍으로 표현
- 영역
- 객체
- 접근권한의 집합

테이블 사이즈가 큼
- 가상기억장치 기법 사용

단점
테이블 때문에 기억공간을 낭비한다.
보조기억장치에 저장할 경우 추가적인 입출력이 필요하다.
어떤 객체 또는 영역을 특별한 그룹으로 분류하여 이용하기가 어렵다.

영역	객체	권한
영역1	파일1	기록
영역1	파일2	판독
...	...	...
영역n	파일n	기록, 판독

3. 접근 제어 리스트(Access Control List)

접근 제어 행렬에 있는 각 열/객체를 중심으로 접근 리스트 구성
각 객체 리스트는 (영역, 접근권한)의 순서쌍으로 구성
각 영역은 (사용자명, 사용자 그룹명)의 쌍으로 지정
접근 권한이 없는 영역은 제외

객체	접근 제어 리스트
파일1	영역1:기록, 영역2:판독, 영역4:판독,기록
파일2	영역1:판독, 영역2:기록, 영역4:판독,기록
스캐너	영역3:판독
프린터	영역3:프린트

4. 권한 리스트(Capability List)

접근 제어 행렬에 있는 각 행/영역을 중심으로 권한 리스트 구성
한 영역에 대한 권한 리스트는 객체와 그 객체에 허용된 조작의 리스트이다.
객체는 권한이라는 물리적 이름이나 주소로 표현되기도 한다.
권한의 소유는 접근을 허용한다는 뜻이다.
권한 리스트는 객체와 객체에 허용된 제어/조작 리스트로 구성
권한 리스트는 운영체제에 의해 유지되며, 사용자에 의해서 간접적으로만 접근되는 보호된 객체이다.
만일 모든 권한이 안전하다면, 그들이 보호하는 객체도 역시 권한이 없는 접근에 대하여 안전하다.

영역1	
파일1	기록
파일2	판독

영역2	
파일1	판독
파일2	기록

영역3	
스캐너	판독
프린트	프린트

영역4	
파일1	판독, 기록
파일2	판독, 기록

5. 록-키(Lock-Key)

접근 제어 리스트와 권한 리스트를 절충한 기법
Key의 길이에 따라 효율적이고 융통적이다.
객체=Lock, 영역=Key
영역과 객체가 일치하는 경우에만 해당 객체에 접근 허용
영역에 대한 Key들의 리스트는 운영체제가 관리한다.
사용자들이 직접 Key(혹은 Lock)의 리스트를 조사하거나 수정할 수 없다.
Key들을 영역 간에 자유로이 전달할 수 있다.

영역n(Key)	111
Lock	111
파일1	판독/기록

영역n(Key)	111
Lock	110
파일2	판독/기록

영역n(Key)	111
Lock	101
스캐너	판독

영역n(Key)	111
Lock	011
프린트	프린트

【학습정리】

1. 자원 보호란?
하드웨어 적인 보호
소프트웨어 적인 보호
불법적인 접근 제어
물리적인 손상을 예방

2. 자원 보호 기법
접근 제어 기법
전역 테이블
접근 제어 리스트
권한 리스트
록-키(Lock-Key)