11주차 2차시 보안 기법

【학습목표】

1. 보안의 정의를 설명할 수 있다.
2. 보안유지 기법 등을 설명할 수 있다.

학습내용1 : 보안의 정의

1. 보안

컴퓨터 시스템 내부의 프로그램과 데이터를 보호하기 위하여, 내부로 접근하는 사용자와 정보의 흐름을 권한부여와 암호를 이용하여 제어하는 통제 기법이다.
시스템 내부의 프로그램과 시스템 데이터에 오류가 없도록 무결성을 유지해야 한다.
컴퓨터 시스템에서 허용된 자원에 대해서만 프로그램, 프로세스, 사용자의 허용된 접근만 허락한다.
데이터의 유출과 손상을 방지한다.
외부보안, 내부보안, 사용자 인터페이스 보안, 컴퓨터 보안, 네트워크 보안, 인터넷 보안.

학습내용2 : 보안의 범위

1. 보안 범위

기술적 보안
물리적 보안
관리적 보안

① 기술적 보안
불법공격으로부터의 보호를 위한 접근제어 기술, 정책, 절차
대상 : 컴퓨터, 통신회로, DB, 등
통신회로
  - 네트워크 접근제어, 암호화 정보유출 방지
시스템 접근제어
  - 사용자인증, 암호화, 접근제어, 침입차단 및 탐지

② 물리적 보안
물리적인 시설 시스템에 대한 허가되지 않은 사람 혹은 물체에 대한 접근 제어, 감시
물리적인 시설 출입 제어
접근이력감시, 침입탐지 관리, 감시 추적

③ 관리적 보안
내부 조직에 대한 정보보호 체계 확립
접근절차, 감시, 사고 대책, 사후관리

2. 보안 요구 사항

비밀성/기밀성(Security, Confidentiality) : 인가된 사용자만 접근 허용
무결성(Integrity) : 인가된 사용자만 정보 수정
가용성(Availability) : 인가된 사용자만 정보 이용
인증 : 사용자 확인 절차
액세스 제어 : 사용자 접근 권한 여부 판단
권한부여 : 사용자 접근 범위 설정
자격증명 : 사용자 정보를 포함한 신분 증명으로 정보 접근

3. 보안 위협

중단(차단) : 컴퓨터 시스템에 대한 공격으로 컴퓨터 시스템 이용불가 상태
도청(가로채기) : 컴퓨터 시스템에 불법 접근하여 정보 획득, 복사
변조(수정) : 컴퓨터 시스템에 불법 접근하여 정보의 내용 변경
위조(조작) : 컴퓨터 시스템에 불법 접근하여 정보의 내용 일부 교체, 제거, 데이터 블록 순서 변경
사칭(가장) : 인가되지 않은 사용자가 인가된 사용자인척 하여 컴퓨터 시스템에 접근

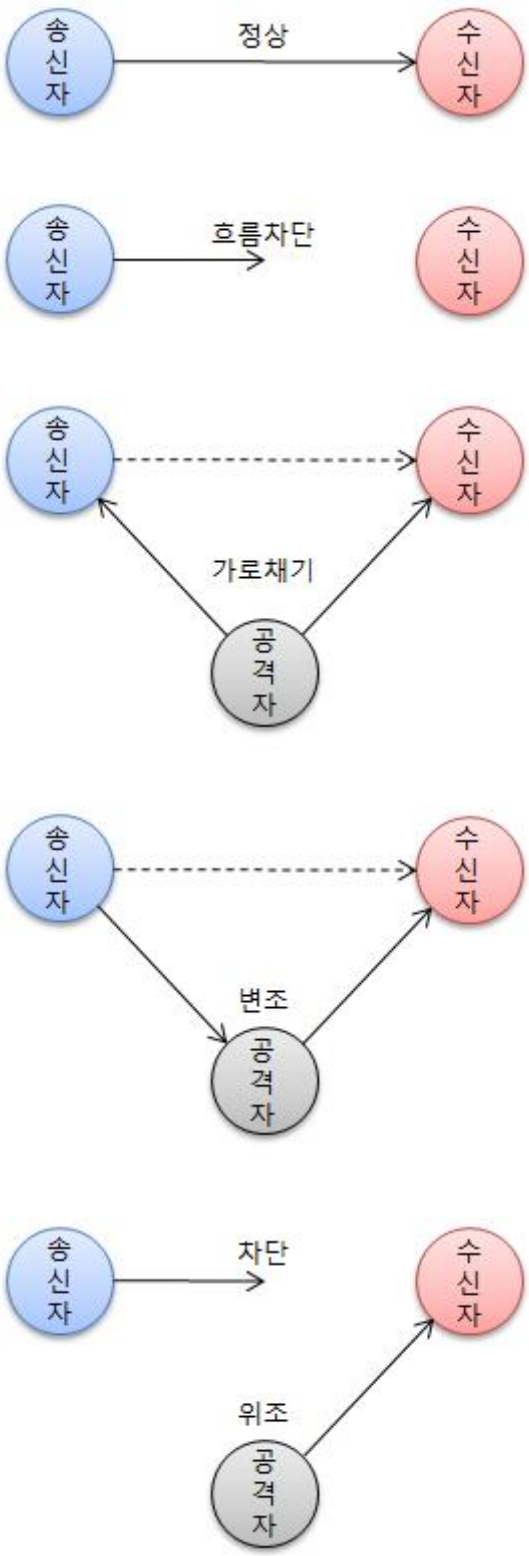
4. 소프트웨어 위협

사이버 테러 : 이메일 폭탄, 논리폭탄, 시한폭탄(트로이목마 운송)
백도어(Back Door), 트랩도어(Trap Door)

5. 컴퓨터 바이러스

트로이 목마(Trojan Horse)
자기 복제/증식
은폐, 파괴
웜(Worm) 바이러스

보안 위협 유형


송신자
정상
수신자
송신자
흐름차단
수신자
송신자
수신자
가로채기
공격자
송신자
수신자
변조
공격자
송신자
차단
수신자
위조
공격자

학습내용3 : 보안유지 기법

1. 외부 보안(External Security)

시설보안
- 외부로부터 침입 제한
- 화재, 홍수등과 같은 천재지변으로부터의 보안을 유지

운용보안
- 컴퓨터 관리자에 의한 사용자 접근 제한

2. 사용자 인터페이스 보안(User Interface Security)

운영체제가 사용자의 신원을 확인 후 접근 제한

3. 내부 보안(Internal Security)

컴퓨터 내부에 저장된 보안 기능을 이용하여 시스템의 무결성, 신뢰성 유지
외부 침입자로부터 보호하기 위하여 프로그램, 데이터로 접근하는 것을 방지하기 위한 권한사항을 하드웨어나 운영체제가 내장하고 있도록 하는 기능

학습내용4 : 보안위험 감소 기법

1. 사용자 감시(Surveillance)

권한이 부여된 사람만 접근할 수 있도록 허가하는 기법
지문, 음성, 얼굴, 홍채, 신분증, Key

2. 위험 탐지

컴퓨터 시스템으로의 접근 권한을 사용자가 아닌 운영체제가 갖도록 하는 기법
감시프로그램에 의해서 접근 여부 결정

3. 확충(Amplification)

일반 사용자보다 더 많은 권한을 컴퓨터 감시 프로그램이 갖도록 하는 기법
불법 사용에 대한 정보를 시스템 관리자에게 보고

4. 패스워드 보호

컴퓨터 시스템에 접근하기 위한 이름과 비밀번호를 이용하여 컴퓨터 시스템에 접근하는 기법
가장 많이 사용하는 인증 기법

【학습정리】

1. 보안이란!
컴퓨터 시스템 내부의 프로그램과 데이터를 보호하기 위하여, 내부로 접근하는 사용자와 정보의 흐름을 권한부여와 암호를 이용하여 제어하는 통제 기법
시스템 내부의 프로그램과 시스템 데이터에 오류가 없도록 무결성을 유지해야 한다.

2. 보안 범위
기술적 보안, 물리적 보안, 관리적 보안,

3. 보안 요구사항
비밀성/기밀성, 무결성, 가용성, 인증, 액세스 제어, 권한부여, 자격증명.

4. 보안 위협
중단, 도청, 변조, 위조, 사칭 , 소프트웨어 위협, 컴퓨터 바이러스.

5. 보안 유지 기법
외부보안 : 시설보안, 운용보안
사용자 인터페이스 보안
내부보안

6. 보안 위험 감소 기법
사용자 감시
위험 탐지
확충
패스워드