정보보호개론

1장. 정보보호의 개요

목포해양대 해양전자통신공학부

교재 구성(1)

- Part 1 : 정보보호
  - 정보보호의 개요
    - 정보보호의 필요성
    - 정보보호의 주요 개념
    - 정보보호의 목적
  - 정보보호 기술
    - 식별과 인증
    - 권한 부여
    - 접근통제 기술
    - 부인봉쇄
  - 정보보호 대책과 평가
    - 정보보호의 관리적 및 운영적 대책
    - 국내외 정보보호 시스템 평가 기준

교재 구성(2)

- Part 2 : 암호화
  - 암호화 기술
    - 암호의 개요
    - 암호화
    - 암호 알고리즘
  - 키 분배와 해쉬함수
    - 키 분배 및 관리
    - 해쉬함수
    - 암호화 기반 인증기술
    - 공개키 기반 구조(PKI)

교재 구성(3)

- Part 3 : 해킹 공격과 대응책
  - 해킹과 정보보호
    - 해킹의 개요
    - 해킹 수법
  - 해킹 공격과 대응책
    - 유닉스 해킹 공격
    - 윈도우 해킹 공격
    - 네트워크 해킹 공격
    - 해킹 관련 법률 적용

교재 구성(4)

- Part 4 : 시스템 보안
  - 시스템 보안
    - 유닉스 시스템 보안
    - 유닉스 파일 시스템 보안
    - 유닉스 프로세스 보안
    - 유닉스 사용자 계정 보안
  - 침입탐지시스템
    - 침입탐지 시스템
    - 침입탐지 시스템 분류
    - 침입탐지 모델
    - 침입탐지 방법론
  - 컴퓨터 바이러스
    - 컴퓨터 바이러스
    - 컴퓨터 바이러스 전파 경로
    - 컴퓨터 바이러스 감염 증상
    - 컴퓨터 바이러스 분류
    - 최근 바이러스 특징

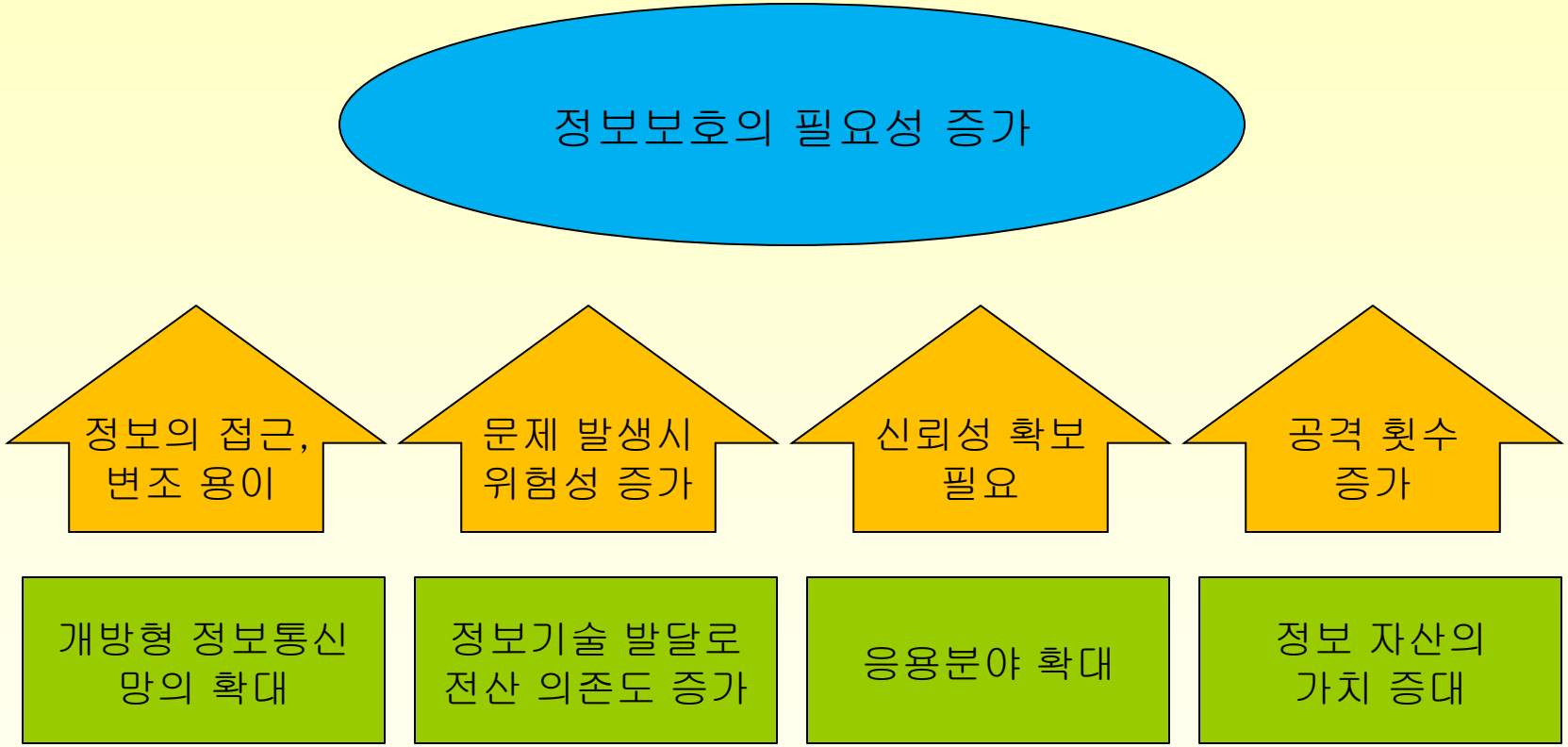
교재 구성(5)

- Part 5: 네트워크 보안
  - 통신과 네트워크 보안
    - 통신과 네트워크 보안
    - 네트워크 장비
  - 유무선 인터넷 보안
    - IPSec 보안 프로토콜
    - SSL/TLS 보안 프로토콜
    - WAP 보안 프로토콜
  - 네트워크 보안 시스템
    - 침입차단 시스템
    - 가상 사설망(VPN)

교재 구성(6)

- Part 6: 전자상거래 보안
  - 전자상거래 보안
    - 전자상거래 개요
    - 전자지불 및 전자화폐 시스템
    - 전자지불 보안 기술
  - 웹과 전자우편 보안
    - 웹 보안
    - 전자우편 보안

정보보호의 필요성


정보보호의 필요성 증가
정보의 접근, 변조 용이
문제 발생시 위험성 증가
신뢰성 확보 필요
공격 횟수 증가
개방형 정보통신 망의 확대
정보기술 발달로 전산 의존도 증가
응용분야 확대
정보 자산의 가치 증대

정보보호의 개념

- 정보보호(Information Protection)
  - 정보의 수집, 가공, 저장, 검색, 송신 그리고 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것
  - 우연히, 혹은 의도적으로 허가 받지 않은 정보의 누출, 전송, 수정, 파괴 등으로부터의 보호를 의미
- 정보보호 개념 변화
  - 1990년대까지 : 국가 안보 차원의 보안
    - 보안시설물에 대한 물리적 개념
    - 비문, 통신 보안 등
  - 1991년 ~ 1998년 : 정보시스템의 안전, 신뢰성 확보
    - 침해 방지
    - 정보 유출 방지
  - 1998년 이후 : 정보보호 개념의 확대
    - 생활 속의 정보보호
    - 인증 수단 강구
    - 개인 정보보호

보안 위협(Threat)

- 시스템 내의 정보 자원에 대한 원하지 않는 결과를 초래할 수 있는 잠재적 가능성, 악의적인 의도, 위협 요소 등
- 보안위협의 종류
  - 정보 누출(Disclosure) 위협
    - 보호되어야 할 정보가 권한이 없는 사용자에게 알려지게 되는 것
  - 무결성(Integrity) 위협
    - 보호되어야 할 정보가 불법적으로 변경, 생성, 삭제 되는 것
  - 서비스 거부(Denial of Service) 위협
    - 정보시스템을 사용할 권한이 있는 사용자에게 제공되어야 하는 서비스를 지연, 방해, 중지 시키는 것
  - 자연 재해
    - 화재, 홍수, 지진 등으로 인한 전력 차단 및 정보시스템 파괴
  - 인간에 의한 위협
    - 의도적 위협 : 바이러스, 해커, 사이버 테러, 저작권 침해 등
    - 비의도적인 위협 : 인간의 실수, 태만 (암호 공유, 백업 부재 등)

취약성(Vulnerability) (1)

- 보안위협에 원인을 제공할 수 있는 시스템의 약점
- 현존하는 정보시스템의 취약성
  - 물리적 취약성 : 건물이나 사무실 침입 등
  - 자연적 취약성 : 자연재해
    - 탐지기, 재난 예비 및 복구 대책 수립
  - 환경적 취약성 : 먼지, 습도, 온도 등의 주변 환경
    - 적정 온도(21 ~ 25도), 습도(40 ~ 60%) 유지
  - 하드웨어 취약성 : 하드웨어 오류나 오작동
    - 대체 사이트, 하드웨어 백업
  - 소프트웨어 취약성
    - 백업, 로그(log), 디스크 섀도잉(disk-shadowing), 데이터 미러링(data mirroring)

취약성(Vulnerability) (2)

- 현존하는 정보시스템의 취약성(계속)
  - 매체 취약성
    - 기록 매체(자기디스크, 출력물 등)
    - 폐기 매체에 대한 처리방안
  - 전자파 취약성
    - 전자파 유출 방지 대책
  - 통신 취약성
    - 개인 식별
  - 인적 취약성
    - 추천, 고용경력 확인, 인성평가 등을 통한 채용
    - 추가 교육
    - 고용종결 절차(계정 잠금, 패스워드 변경)

위험(Risk) (1)

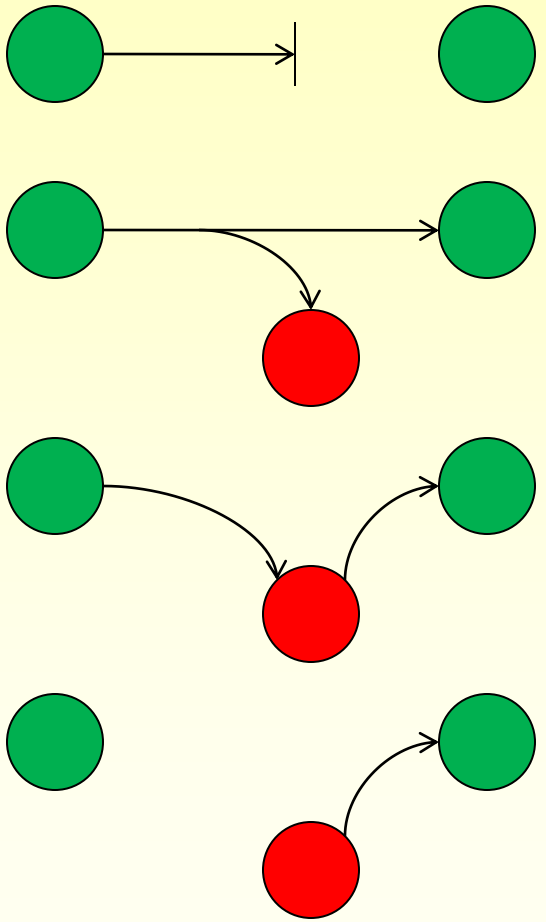
- 위협 주체가 취약성을 활용할 수 있는 가능성
- 위협요소가 컴퓨터시스템 또는 네트워크의 잠재적 취약성을 부당하게 활용할 수 있는 잠재적 손해 혹은 가능성
- 보안대책(countermeasure) 또는 안전장치(safe guard) : 잠재적 위험을 줄여줌
  - 보안대책 : 취약성을 제거하거나 위협주체가 취약성을 부당하게 활용하는 위험을 줄여주는 소프트웨어 설정 및 하드웨어 절차
  - 예: 엄격한 패스워드 관리, 보안감시, 접근제어 메커니즘, 바이오스 패스워드 설정, 보안 교육 등

위험(Risk) (2)

- 위험요소와 보안대책

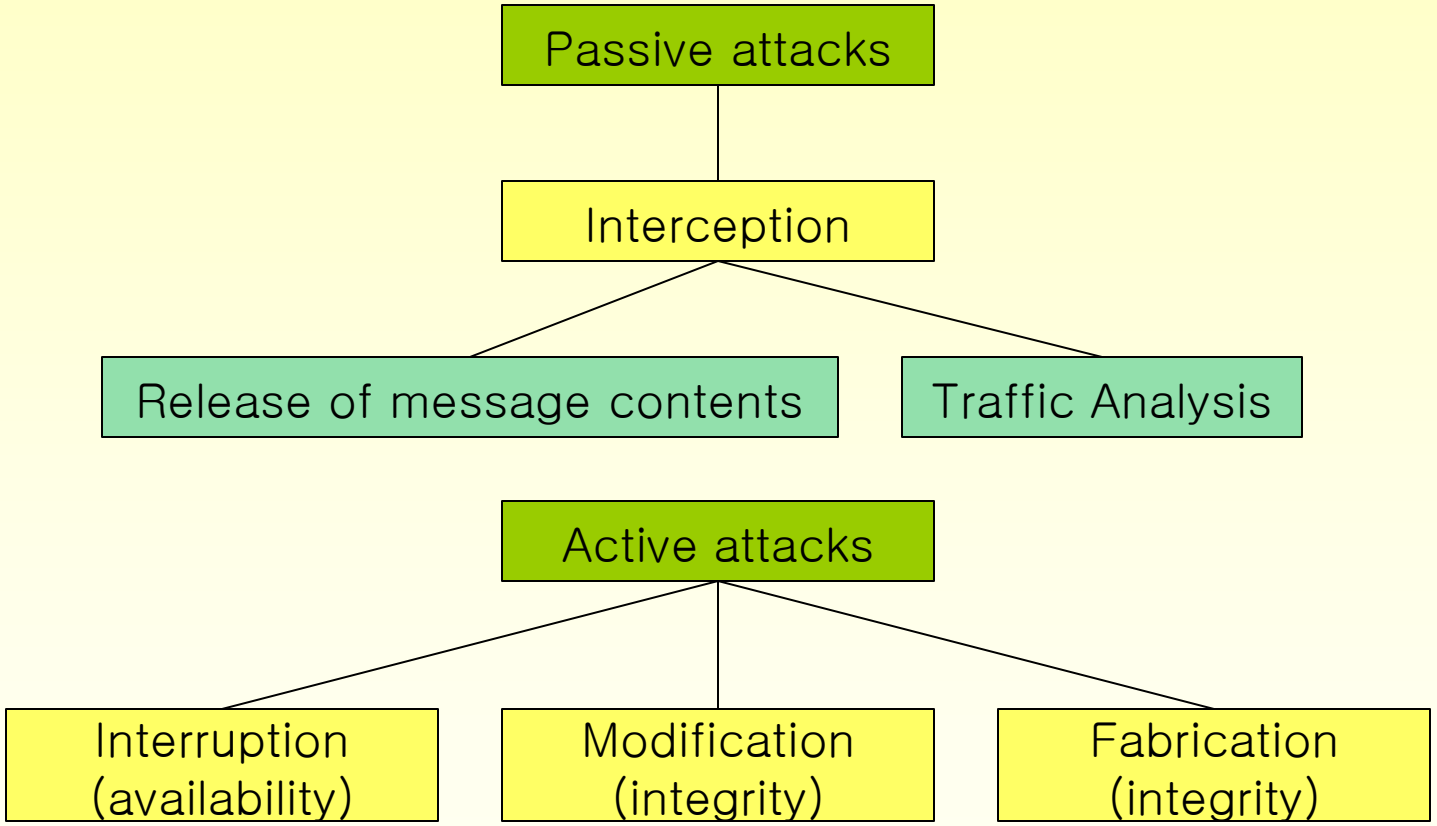
공격(Attack) (1)

- 악의적인 의도를 가진 공격자가 시스템 내의 정보를 누출, 변조, 파괴하는 행위
- 종류
  - 중단(Interruption)
  - 가로챔(Interception)
  - 변조(Modification)
  - 가공(Fabrication)



공격(Attack) (2)

- Active and Passive Attacks



정보보호의 기본 목표

- 정보보호의 3요소(CIA Triad)
  - 기밀성(Confidentiality)
  - 무결성(Integrity)
  - 가용성(Availability)

기밀성(Confidentiality)

- 보호의 대상이 되는 시스템의 자원들이 승인된 주체(사용자, 프로세스 등)들에게만 접근이 허용되는 것
- 공격 행위 :
  - 네트워크 감시,
  - 훔쳐보기(shoulder surfing)
  - 패스워드 파일 훔치기
  - 사회공학(social engineering)적인 방법으로 암호 추론
- 방지대책
  - 암호화
  - 트래픽 패딩(padding)
  - 엄격한 접근 통제
  - 데이터 분류
  - 정보 이용에 대한 올바른 절차 교육

무결성(Integrity)

- 대상이 되는 자원들이 승인된 주체에 의해서만, 그리고 승인된 방법에 의해서만 변경이 이루어지도록 하는 것
- 정보와 시스템에 대한 정확성과 신뢰도(reliability)에 대한 보장이 제공되고, 데이터에 대한 권한이 없는 사용자로 인한 수정이 방지되는 경우에만 유지
- 공격행위
  - 바이러스, 논리폭탄(logic bomb), 백도어(back door)에 의한 시스템 훼손
- 방지대책
  - 암호화
  - 엄격한 접근통제
  - 침입탐지 기술

가용성(Availability)

- 보안의 대상이 되는 컴퓨터 시스템의 자원들이 승인된 사용자들에 의해서 적시에 사용이 가능하도록 하는 것
- 가용성의 목표
  - 적절한 시간 내의 응답
  - 공평(fair)한 서비스
  - 장애극복(fault tolerance)
  - 다수의 사용자에 대한 동시적 서비스
  - 교착상태(deadlock) 관리
- 공격행위
  - 서비스 거부 공격(DoS : Denial of Service)

과제

- 인터넷 검색을 통해 다음 사항을 자세히 조사하여 보고서 제출
  - (학번 마지막 2자리) % 3을 해서 결과가 1인 학생은 1,4, 2인 학생은 2,5, 0인 학생은 3,6 수행
  - 아래아 한글로 작업하고, 최종본은 pdf로 만들어 제출
  - 내용에 참고한 문서 또는 사이트 이름 반드시 포함
  - 파일 이름은 제목(작성자 이름)
    - 예: 인터넷대란(홍길동)
  - 과제 주제
    1. 1/25 인터넷대란
    2. 777 DDoS 공격
    3. 2010년 삼일절 사이버 전쟁
    4. 인터넷진흥원
    5. 정보보호 관련 법령
    6. 디지털포렌직