# 제 1 장
# 정 보 보 호

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

# Thinking

- Cryptography ?
- Security ?

# 보안관련 국가기관, 자격증 등

- 국가정보원
- ETRI
- KISA
- 국가보안연구소
- 검찰청 사이버테러대응센터 / 사이버수사대
- 기무사
- 금융보안연구원
- 금융감독원

- CISA
- CISSP
- 정보보호기사
- 디지털 포렌식 전문가
- CCFP

# 보안의 세부 연구 분야들

- 암호학/분석
- 대칭키/공개키연구
- 시스템
- 네트워크 / 인터넷(웹)
- 임베디드 / 하드웨어
- 멀티미디어
- 디지털 포렌식
- 개인정보보호(프라이버시)
- 정보보호 법률/정책
- 보안프로토콜

1절 네트워크 사회와 정보보호

2절 정보보호란?

3절 정보의 특성

4절 정보보호의 인적 요소

# 제1절 네트워크 사회와 정보보호

1.1 업무 패턴의 변화

1.2 인터넷 환경

1.3 스마트워크

1.4 무슨 일이 벌어지는가?

1.5 무엇이 두려운가?

# 1.1 업무 패턴의 변화

- 네트워크를 통한 업무 처리
  - 이메일
  - 오디오 컨퍼런싱
  - 비디오 컨퍼런싱
  - 인스턴트 메시지
  - 소셜 미디어
  - 텍스트 메시징

# 1.2 인터넷 환경

- 한 국가의 경제개발과 복지 수준에 ICT 활용 정도를 나타내는 지표
  - E-readiness
    - 연결성과 기술적 인프라
    - 비즈니스 환경
    - 사회 문화적 환경
    - 법률적 환경
    - 정부 정책과 비전
    - 소비자와 비즈니스 분야 적용도

# Internet Penetration


그림 1-1 • Internet Penetration(인구 대비, Wikipedia 제공)

**Digital economy rankings 2010_Beyond e-readiness**

※ E-readiness : 한 국가의 경제 개발과 복지 수준에 ICT를 활용하는 정보를 나타내는 지표

# 1.3 스마트워크

- 시간과 공간 제약 탈피

- 스마트워크센터 URL LINK : Smartworkcenter
  - 생산성 향상
  - 일자리 창출
  - 교통량 감소
  - 고령화, 저출산 문제 해결

- 자료전송의 빈번화
  - 정보보호문제 대두

# 1.4 무슨 일이 벌어지는가?

- 네트워크를 통한 업무
  - 인터넷 쇼핑
  - 인터넷 뱅킹
  - 이메일 사용
  - 개인정보 제공
  - 생물학적 정보 제공
  - 유틸리티 활용
  - 프로그램 설치
  - 첨부된 파일 실행

- 위험하지 않을까?

# 1.5 무엇이 두려운가?

- 정보노출
- 정보변경
- 위장
- 정보전달의 지체
- 송신/수신 부정
- DoS 공격
- 신원 정보
- 신용카드 사용
- 온라인 송금
- 전자 상거래
- 이동전화 통신

# 제2절 정보보호란?

## 2.1 정보보호란?

## 2.2 정보보호의 역사

## 2.3 보안과 보호

# 2.1 정보보호란?

- 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단, 또는 그러한 수단으로 이루어지는 행위

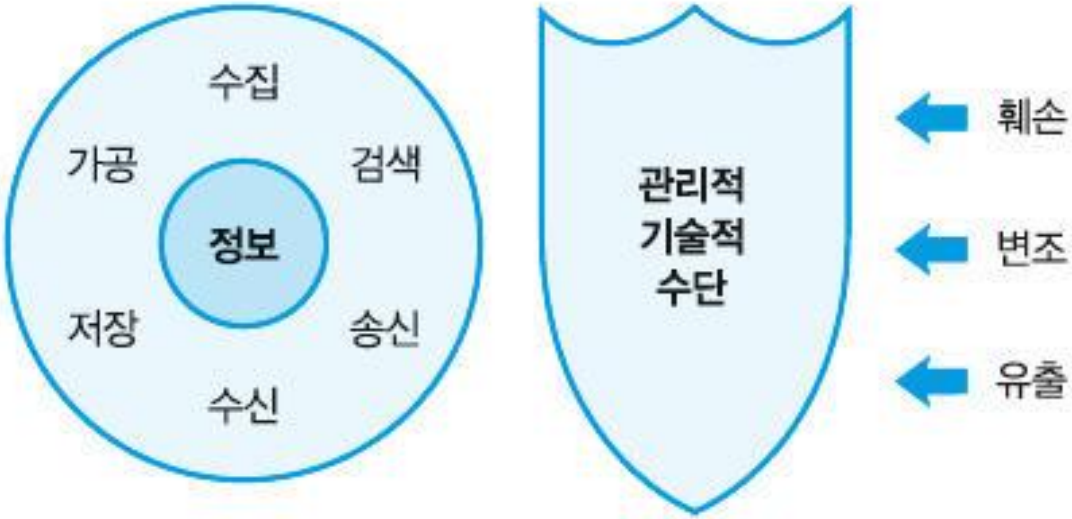


그림 1-2 • 정보보호

# 정보의 가용성과 안전성

- 정보의 활용과 정보의 통제 사이의 균형감각을 갖는 행위


그림 1-3 • 정보의 가용성과 안전성

# 2.2 정보보호의 역사

- 60년대 – 냉전 시대
- 70년대 – 네트워크 확산 시대
- 80년대 – PC와 네트워크
- 90년대 – WWW
- 2000년대 – 전자 상거래
- 현재 – 무선 네트워크와 이동성

# 60년대 – 냉전 시대

- 그물형 네트워크의 탄생
- ARPANET
- 정보보호 개념 부재
- Rand Report R-609
  - 보안 개념의 변화 계기
  - 보안 문제
    - 데이터 보안
    - 데이터 접근 제한
    - 인적 구성원에 대한 보안
- MULTICS(Multiplexed Information and computing Service) 개발 시작

# 70년대 - 네트워크 확산시대

- 4개의 노드로 시작
- 네트워크에 연결된 노드 수의 폭발적 증가
- ARPANET 의 보안문제 심각
  - 패스워드 구조와 형식의 취약성
  - 공중 전화망을 통한 접속의 안전성 결여
  - 사용자 시스템 접근 허락문제
- 암호를 이용한 전송
- 비대칭 암호의 발견

# 80년대 - PC와 네트워크

- PC 보급과 네트워크 연결
- TCP/IP 채택
- 인터넷 환경 구축
- 보안문제 급증
  - 네트워크를 통한 사기, 산업 스파이, 컴퓨터 해킹, 불법 접속
  - PC와 소규모 LAN을 대상으로 하는 공격

# 90년대 - WWW

- WWW 웹 브라우저 등장
- 인터넷 확산
- 정보보호의 산업화 표준 부족
- 물리적 보안이 주류

# 2000년대-전자상거래

- 금융거래 방식의 변화
- 인터넷을 통한 금융거래
- 온라인 금융거래 보안문제 발생
- 다양한 공격 방법과 방어 방법에 대한 연구
- 3세대 이동통신 보안 문제 대두

# 현재 - 무선 네트워크와 이동성

- 보안에 대한 개념 부족
- 유선보안에서 무선보안 문제로 진화
- 개인정보보호문제 심각
- 개인정보보호법 등 법적 제도 마련
- 정보보호는 한 컴퓨터의 안전만으로 해결되지 않는다.

# 2.3 보안과 보호

- **보안**
  - 가치 있는 유형과 무형 자산을 도난, 소실, 유출로부터 보호하는 것
- **보호**
  - 위협으로부터 안전한 정도
  - 정보를 저장하거나 유통하는 전반적인 시스템의 안정

# 다중보안시스템

- 물리적 보안(Physical Security)
- 인적 보안(Personal Security)
- 운용 보안(Operation Security)
- 통신 보안(Communication Security)
- 네트워크 보안(Network Security)
- 정보보호(Information Security)

# 정보보호시스템

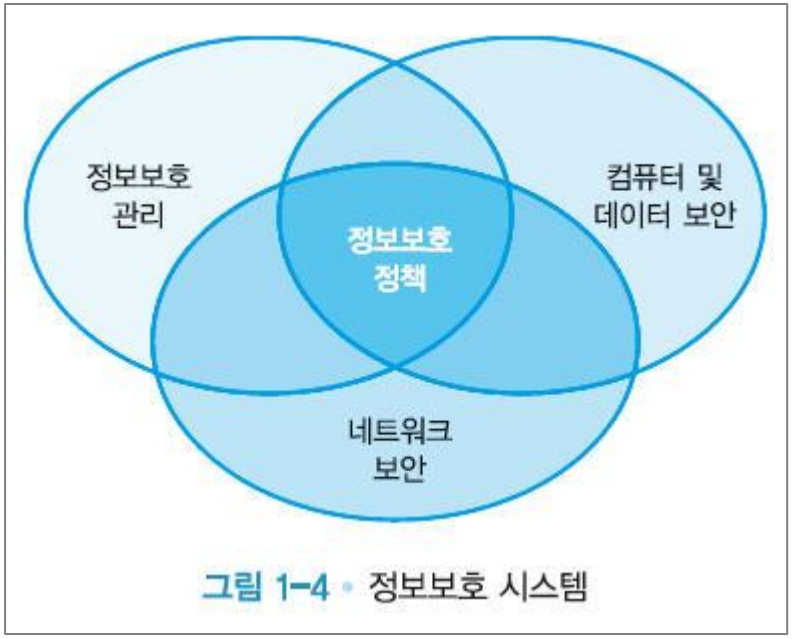


그림 1-4 • 정보보호 시스템

# CIA Triad

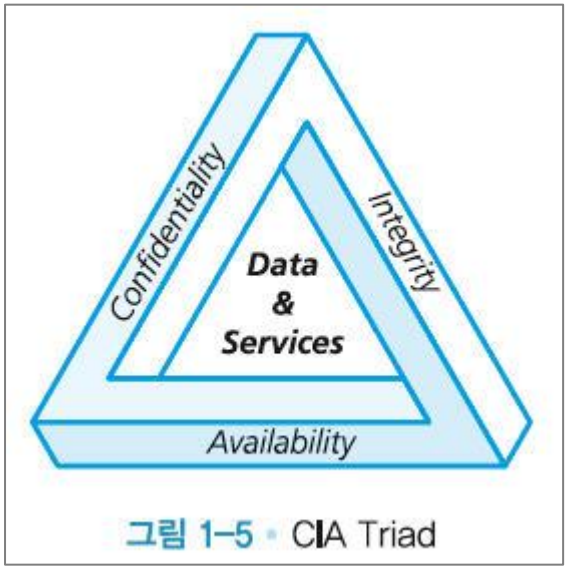

그림 1-5 • CIA Triad

- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)

# 제3절 정보의 특성

## 3.1 정보보호 서비스의 종류

## 3.2 정보보호의 대상

## 3.3 컴퓨터의 양면성

## 3.4 가용성과 보안성

# 3.1 정보보호 서비스의 종류

- 가용성(availability)
- 기밀성(confidentiality)
- 무결성(integrity)
- 인증(authentication)
- 부인방지(nonrepudiation)
- 소유권(possession)
- 정확성(accuracy)
- 활용성(utility)

# 정보보호 서비스의 종류

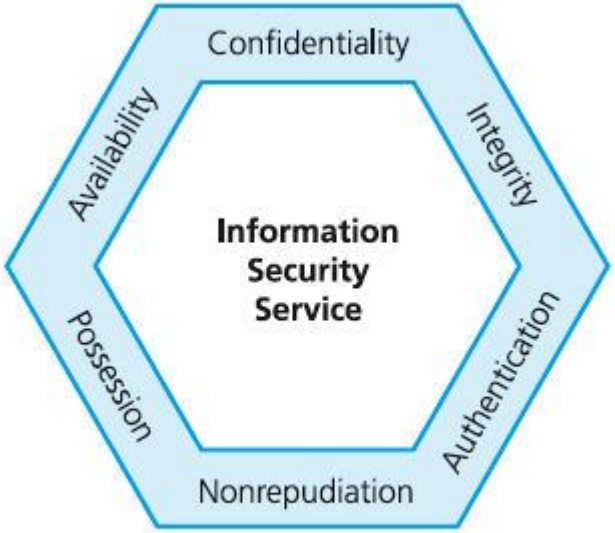


그림 1-6 • 정보보호 서비스의 종류

# 3.2 정보보호의 대상

- 소프트웨어(software)
- 하드웨어(hardware)
- 데이터(data)
- 인적 요소(personnel)
- 절차(procedure)
- 네트워크(network)

# 3.3 컴퓨터의 양면성

- 보안공격의 주체
- 공격의 대상
- 직접공격
- 간접공격

# 3.4 가용성과 보안성

- 정보보호는 보안과 가용성의 균형감을 유지하는 것
- 사용자의 요구와 보안관리자의 전문성 사이에서 균형점인 타협점 찾기

**사람이 바로 조직의 정보보호 프로그램의 링크 중에서 가장 취약한 링크**

# 4.1 정보보호의 인적요소

- 사회공학적 공격(social engineering attack)
- 사람의 심리적인 취약점을 활용하여 정보를 취득하거나 컴퓨터 접근권한을 얻거나 정보제공을 재정적 이득과 연결하여 시스템을 공격하는 방법

# 정보보호의 인적요소

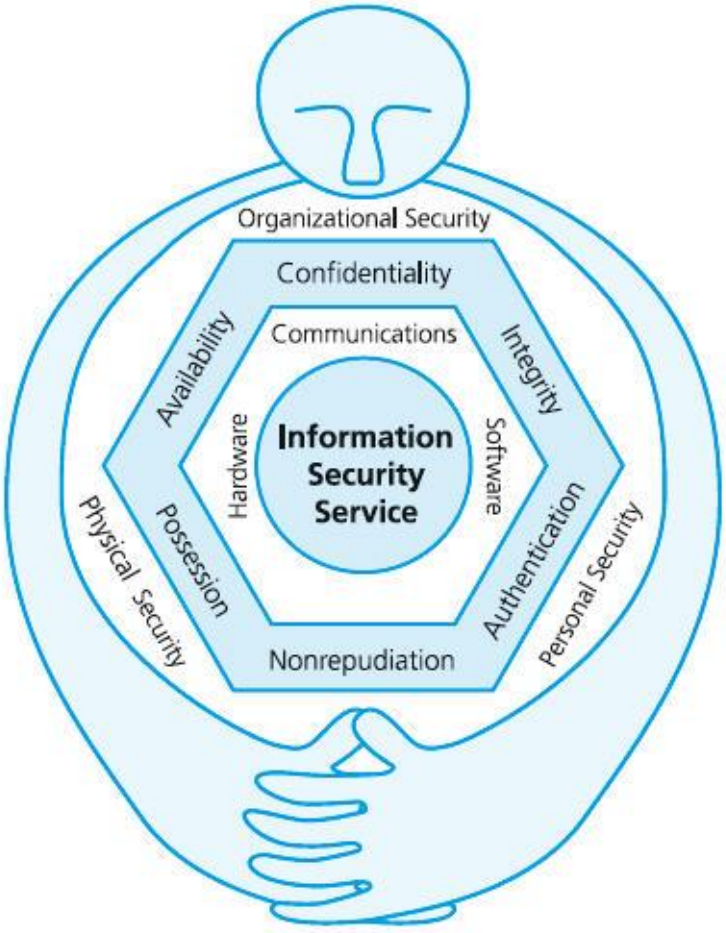


그림 1-7 • 정보보호의 인적 요소

# Q & A

# Thank You!