알기 쉬운

정보보호개론 3판

흥미로운 암호 기술의 세계

INFORMATION SECURITY and CRYPTOGRAPHY

INFINITYBOOKS
인피니티북스

INFORMATION SECURITY and CRYPTOGRAPHY

PART I 암호

PART I 암호

PART II 인증

PART III 키, 난수, 응용 기술

INFORMATION SECURITY and CRYPTOGRAPHY

CHAPTER 1 정보보호

Section 01
스마트시대와 정보보호

1.1 스마트 환경

1.2 인터넷 환경과 보안

1.3 스마트워크

1.4 네트워크 보안

1.5 정보보호 위협 환경

1.1 스마트 환경

- 스마트 환경
  - 시간 장소에 구애됨 없이 저비용 고성능 컴퓨팅 기능을 사용해 인간의 삶을 편리하고 즐겁게 영위하도록 만드는 환경
- 스마트 환경 요소
  - 수월한 원격 장치 제어
  - 원활한 네트워크
  - 원활한 정보수집 및 배분
  - 편리한 서비스 제공
  - 정확한 예측 및 의사결정이 가능한 시스템

스마트 환경을 구축하는 ICT 기술

- 무선통신
- 알고리즘 디자인
- 신호처리 기술
- 정보 기술
- 다계층 소프트웨어 아키텍처
- 자연어 처리 기술
- 이미지 인식 및 프로세싱 기술
- 센서 디자인
- 동작감지 기술
- 온도 및 압력 센서 기술
- 컴퓨터 네트워킹 기술
- 병렬처리 기술
- 고도화 운영체제

1.2 인터넷 환경과 보안

- 인터넷 발달로 인한 정보보호 및 사생활 보호 문제 대두
- 인터넷을 악용한 범법 행위
- 안전하지 않은 정보화 생활
- 정보기술의 안전성과 정보 서비스 편리성 간 문제
- 미래의 인터넷
  - 안전하고 편리한 암호기술 및 보안 인증기술
  - 보안사고에 대한 다국적 공조
  - 국가를 초월한 인터넷 서비스
  - 정치경제, 환경 및 사회적 인종적 환경 초월한 서비스

1.3 스마트워크

- 시간과 공간 제약 탈피
- 스마트워크센터 smartworkcenter
  - 생산성 향상
  - 일자리 창출
  - 교통량 감소
  - 고령화, 저출산 문제 해결
- 자료전송의 빈번화
  - 정보보호문제 대두

1.4 네트워크 보안

- 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 정보보호 위협 환경

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

Section 02
정보보호란?

2.1 정보보호란?

2.2 시대별 정보보호

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

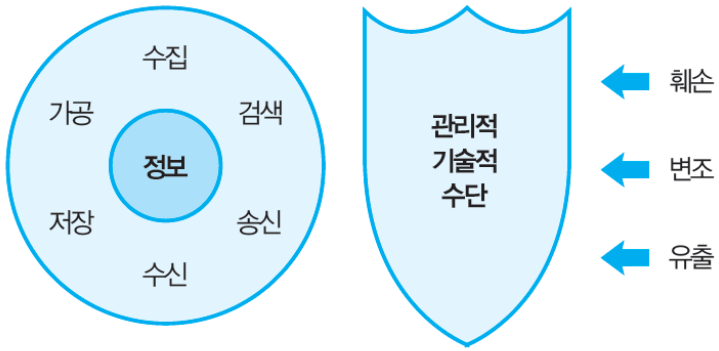

그림 1-1 • 정보보호

정보의 가용성과 안전성

- 정보의 활용과 정보의 통제 사이의 균형 감각을 갖는 행위

그림 1-2 • 정보의 가용성과 안전성

- 퀴즈 1 관대한 관리자(p10)

네트워크를 관리하는 관리자가 자신이 관리하는 컴퓨터에 유익한 자료가 많아서 많은 사용자로 하여금 쉽게 접속하고 자료를 다운로드하는 것을 쉽게 하기 위해 아이디와 패스워드를 입력하는 인증 절차를 없애고 익명 접속을 허락하였다면 관리자가 시스템의 안전성과 가용성 중에 어느 쪽에 더 비중을 두고 있는 것인가?

2.2 시대별 정보보호

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

60년대-냉전시대

- 그물형 네트워크의 탄생
- ARPANET(Advanced Research Project Agency Network)
- 정보보호 개념 부재
- Rand Report R-609
  - 보안 개념의 변화 계기
  - 보안 문제에 대한 권고 사항
    - 데이터 보안
    - 데이터 접근 제한
    - 인적 구성원에 대한 보안
- MULTICS(Multiplexed Information and computing Service) 개발 시작 : 보안에 중점을 둔 최초의 시스템

70년대-네트워크 확산시대

- 4개의 노드로 시작
- 네트워크에 연결된 노드 수의 폭발적 증가
- ARPANET의 보안문제 심각
  - 패스워드 구조와 형식의 취약성
  - 공중전화망을 통한 접속의 안전성 결여
  - 사용자 시스템 접근 허락문제
- 암호를 이용한 전송
- 공개키 암호의 등장(1976년)

80년대-PC와 네트워크

- PC 보급과 네트워크 연결
- TCP/IP 채택 :1980년대 초, 인터넷의 기초가 되는 프로토콜
- 인터넷 환경 구축
- 보안문제 급증
  - 네트워크를 통한 사기, 산업 스파이, 컴퓨터 해킹, 불법 접속
  - PC와 소규모 LAN을 대상으로 하는 공격

90년대-WWW

- WWW 웹브라우저 등장
- 인터넷 확산
- 인터넷 개발 당시 보안 문제는 고려 대상의 후순위, 보안의 개념이 제대로 설정되지 못함
- 정보보호의 산업화 표준 부족
- 물리적 보안이 주류 : 컴퓨터가 설치된 데이터 센터의 물리적 환경 보안

2000년대-전자상거래

- 금융거래 방식의 변화
- 인터넷을 통한 금융거래
- 온라인 금융거래 보안문제 발생
- 다양한 공격 및 방어 방법 연구
- 3세대 이동통신 보안 문제 대두

현재-무선 네트워크와 이동성

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

2.3 보안과 보호

- 보안
  - 가치 있는 유형과 무형 자산을 도난, 소실, 유출로 부터 보호하는 것
- 보호
  - 위협으로부터 안전한 정도
  - 정보를 저장하거나 유통하는 전반적인 시스템의 안정
  - 보안보다 광의의 의미

다중보안시스템

- 물리적 보안(Physical Security) : 불법적인 접근과 오용으로부터 물리적인 대상, 물체 또는 영역을 보호하는 것
- 인적 보안(Personal Security) : 한 조직과 조직의 활동에 합법적으로 접속할 수 있는 개인 혹은 집단을 보호하는 것
- 운용 보안(Operation Security) : 특정 운용이나 일련의 동작의 세밀한 사항을 보호하는 것
- 통신 보안(Communication Security) : 통신 미디어, 기술, 통신 내용을 보호하는 것
- 네트워크 보안(Network Security) : 네트워킹 요소, 연결 상태, 통신 내용을 보호하는 것
- 정보보호(Information Security) : 정보 자산을 보호하는 것

정보보호시스템

- 미국의 CNSS(Committee on National Security Systems)의 정보보호에 대한 정의
  - 정보를 사용하고 저장하고 전송하는 시스템과 하드웨어 및 정보와 중요한 요소를 보호하는 것

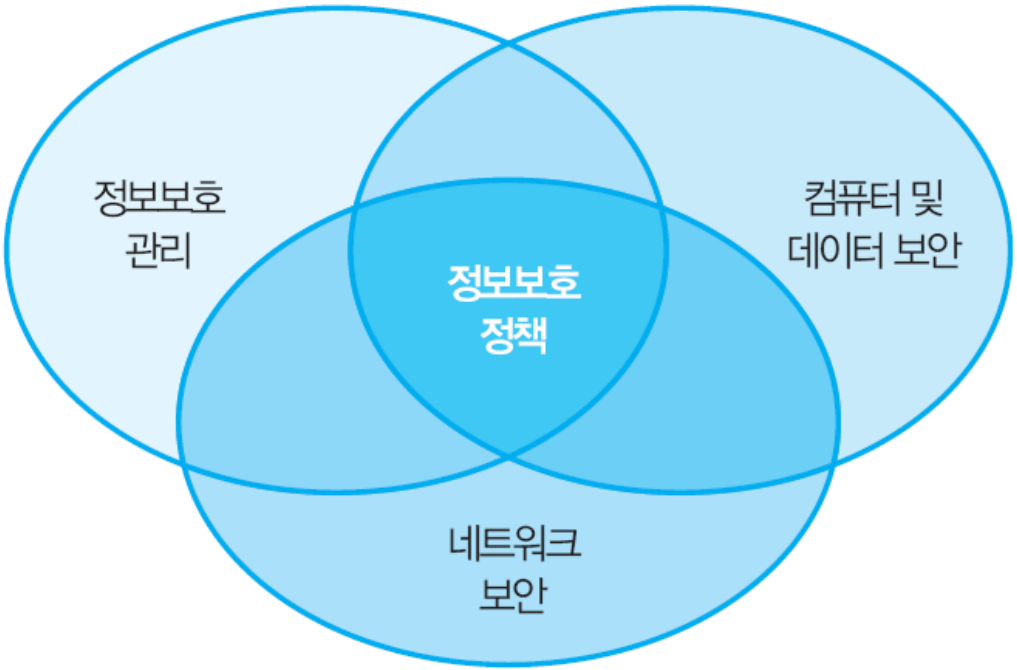

그림 1-3 • 정보보호시스템

CIA Triad 정보보호 모델

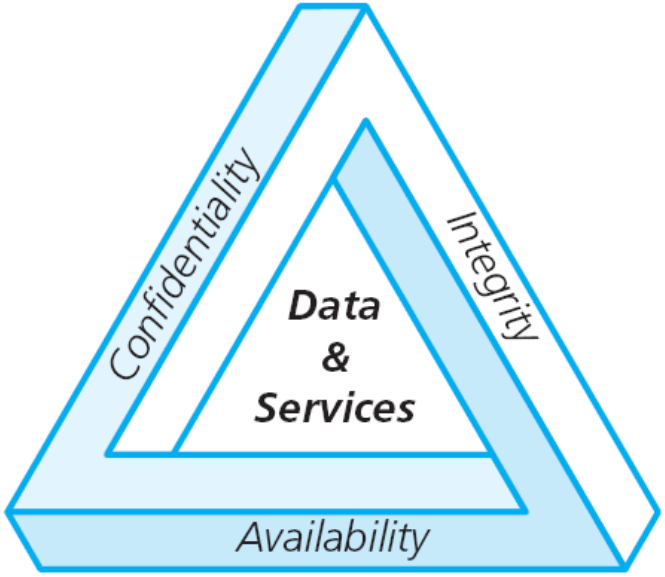

그림 1-4 • CIA Triad

- 기밀성(**C**onfidentiality)
- 무결성(**I**ntegrity)
- 가용성(**A**vailability)

- NSTISSC (National Security Telecommunications and Information Systems Security Committee) 에서 개발한 정보보호모델

Section 03
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

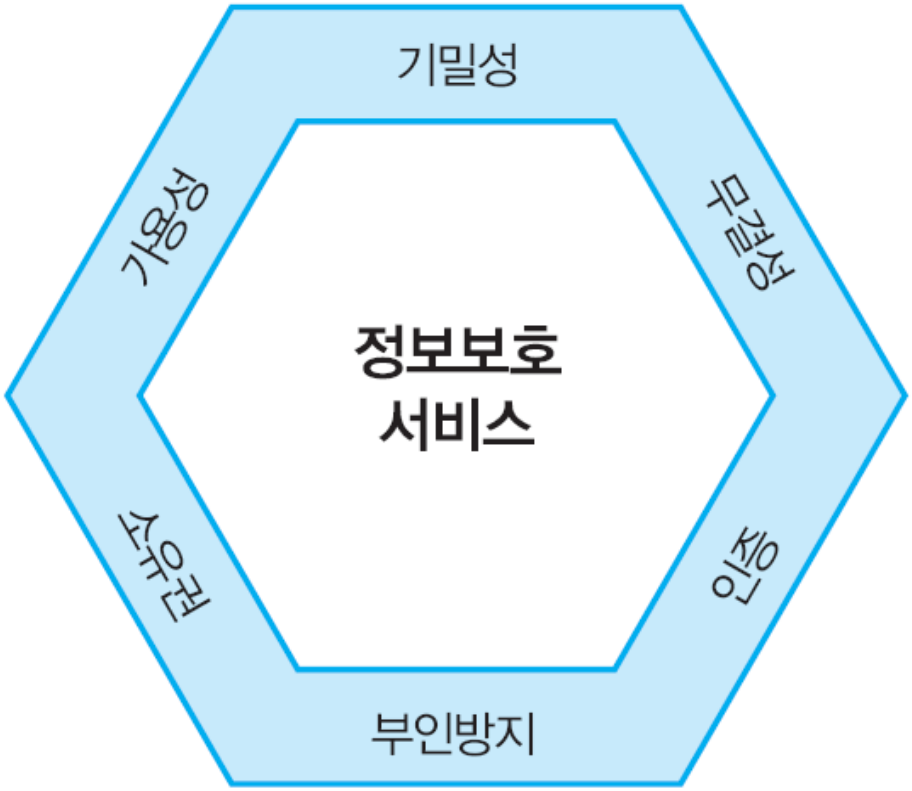

그림 1-5 • 정보보호 서비스의 종류

3.2 정보보호의 대상

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

3.3 컴퓨터의 양면성

- 정보보호를 위해서 불법과 편법적인 사용자를 제거하여야 함
- 컴퓨터 : 보안 공격의 주체이자 공격의 대상
- 직접공격
- 간접공격 : 한번 공격받은 시스템이나 자원에 의해 이루어짐(예 DDoS 공격)

- 퀴즈 2 선량한 사람 (p19)

어떤 사람이 있는데 그는 선량한 사람으로서 남에게 해를 끼치지 않고 사는 것이 인생 철학이다. 그래서 그가 사용하는 컴퓨터는 언제나 가장 최신의 보안 업데이트를 하고 안티바이러스 프로그램도 최신으로 업데이트 하였고 모든 소프트웨어도 정품으로 설치하였다고 한다. 그리고 인터넷을 사용할 때에도 남에게 해를 끼치는 행위를 하지 않았다고 한다. 그럼 이 컴퓨터가 다른 컴퓨터에게 위협적이지 않고 안전하다고 말할 수 있는가?

3.4 가용성과 보안성

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

Section 04
정보보호의 인적 요소

- 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

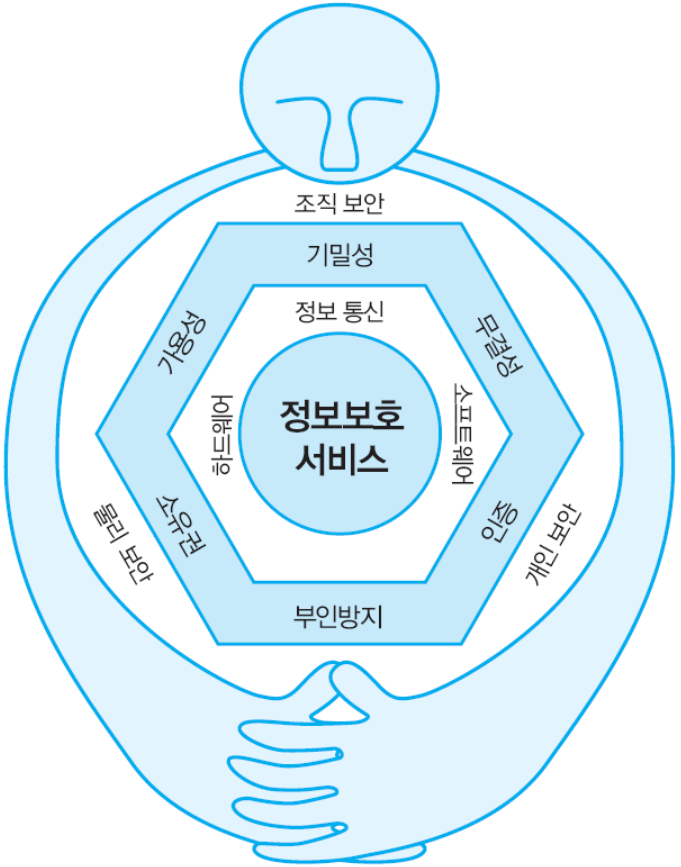

그림 1-6 • 정보보호의 인적 요소