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, 정책적 수단, 또는 그러한 수단으로 이루어지는 행위

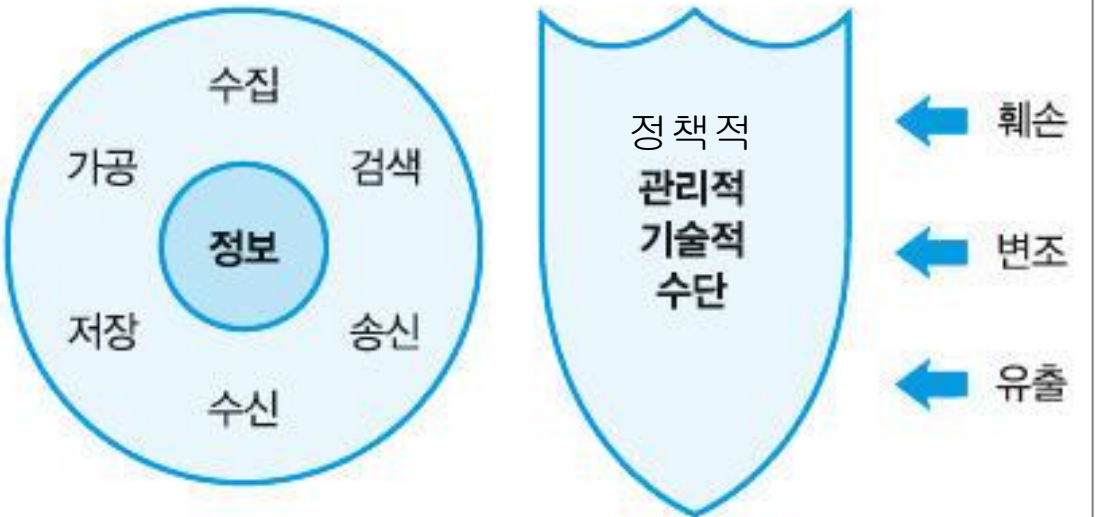

그림 1-2 • 정보보호

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.

정보 보안의 역사

- 1980~1990년대
  - 해킹 문화의 등장
    - 1983년에 개봉된 영화 〈위험한 게임〉은 해커를 소재로 한 최초의 영화
      - 핵미사일을 제어하는 프로그램을 게임으로 착각하고 동작시켜 미국과 러시아 간에 핵전쟁이 일어날 뻔한 위기 상황이 발생
    - 1984년 출간된 SF 소설 《뉴로맨서》에서 저자 윌리엄 깁슨은 사이버스페이스라는 용어를 처음으로 사용
      - 오늘날 흔히 사용하는 용어인 인공지능, 가상 세계, 유전자 공학, 다국적 기업 등에 대한 개념이 등장
    - 1985년에는 나이트 라이트닝과 타란 킹이 유명한 해커 잡지 《프랙》을 창간
      - 컴퓨터 보안, 전화 시스템과 같은 다양한 정보가 실려 있어 해커들에게 큰 인기를 모음
    - 1년 후 《프랙》에 이어 또 다른 해커 잡지 《2600》이 정기 출간
    - 1985년 7명의 미국 소년이 뉴저지 소재 국방부 컴퓨터에 침입하여 극비 군사 통신 데이터를 빼낸 사건이 발생
      - 이에 1986년 미의회는 컴퓨터 범죄와 관련된 최초의 처벌 규정인 '컴퓨터 사기와 오용에 관한 조항' 제정

그림 1-7 영화 〈위험한 게임〉(왼쪽)과 공상 과학 소설 《뉴로맨서》(오른쪽)

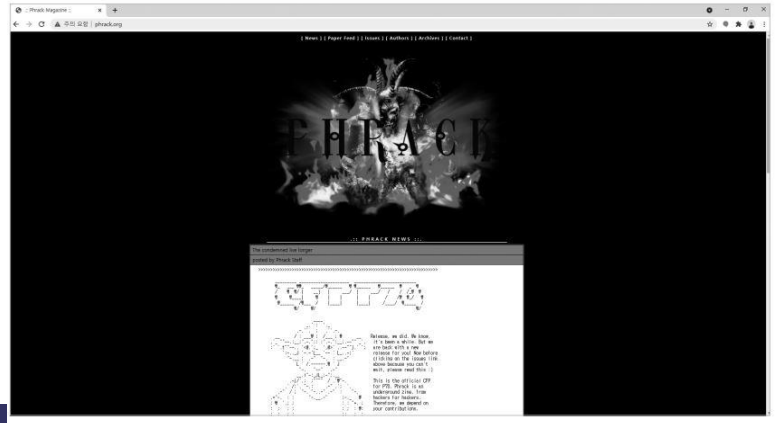

그림 1-8 《프랙》 홈페이지(http://www.phrack.org)

정보 보안의 역사

- 1980~1990년대
  - 해커의 등장
    - 1980년대에 해킹이 발전하면서 역사적으로 유명한 해커들이 본격적으로 등장
      - 1986년 구소련 KGB로부터 자금을 지원받는 서독 해커들이 300여 기관에 불법적인 접근을 시도하고 군사 기밀 정보를 탈취
      - 1987년에는 케빈 미트닉이 컴퓨터 개발·판매 회 사인 산타크루스 오퍼레이션의 시스템에 침입
      - 1988년 11월 22일 코넬대학 대학원생이었던 로버트 모리스는 웜 바이러스를 구동하여 미국 전역에 피해를 끼침
      - 로이드 블랭켄십은 사이버 갱단 MoD의 맴버로 해킹과 프리킹에 관한 문서를 주고받는 장소인 Elite 보드를 운영
      - 로터스 123을 개발한 미치 케이퍼와 존 발로는 정부의 임의적인 정보 검열에 저항해 전자프런티어 제단(EFF)를 결성
      - 전자프런티어재단은 국제 사회에서 표현의 자유, 저작물의 자유로운 이용, 개인 정보 보호, 정보 투명성을 위한 활동 수행

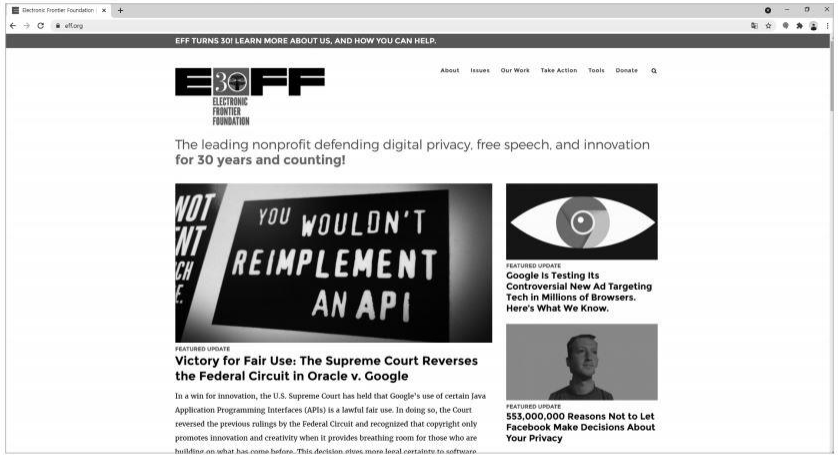

그림 1-11 전자프런티어재단 사이트(https://www.eff.org)

정보 보안의 역사

- 해커선언문
  - 로이드가 한 일 가운데 가장 유명한 것은 〈해커 선언문〉 발표

오늘 또 한 명이 잡혔다. 신문마다 난리다.
'컴퓨터 범죄 사건으로 10대 체포', '은행 컴퓨터 조작으로 해커 체포'
빌어먹을 어린놈들, 그놈들은 다 똑같아.
하지만 당신들은 싸구려 심리학이든 1950년대식 과학이든 무엇으로라도
그들을 이해해보려 한 적이 있는가?
왜 그들이 그런 장난을 하는지,
무엇이 그들을 그렇게 만들었는지,
생각해본 적이 있는가?
나는 해커다. 나의 세계로 오라.
나의 세계는 학교에서 시작한다.
나는 대다수 학우들보다 똑똑하다.
학교에서 가르치는 것은 우리를 지겹게 한다.
빌어먹을 낙제생들, 그놈들은 다 똑같아. 중·고등학교에서 분수식 계산법을 수십 번도 더 들었다.
이미 다 이해하고 있는 것들이다.
"아니요, 선생님. 계산 과정을 보여드릴 수는 없어요. 암산으로 했거든요."
빌어먹을 어린놈들, 아마 베꼈을 거야. 그놈들은 다 똑같아.
오늘 뭔가를 발견했다. 바로 컴퓨터다.
잠깐, 이거 멋진데. 내가 원하는 걸 할 수 있잖아.
만약 그것이 실수를 한다면 내가 그것을 망쳤기 때문이지.
그것이 나를 싫어해서도, 나 때문에 겁을 먹어서도,
나를 똑똑하기만 한 바보로 생각해서도 아냐.
어쨌거나 우리는 다 똑같기 때문이다.

<중략>

나는 해커다. 이것은 나의 강령이다.
당신들은 나 한 사람을 멈추게 할 수 있을지 몰라도 우리 모두를 멈추게 할 수는 없다.

정보 보안의 역사

- 1980~1990년대
  - 데프콘 해킹 대회
    - 최초의 해킹 대회인 '데프콘'이 1990년 라스베이거스에서 개최
    - 데프콘 해킹 대회는 지금도 매년 열리는데, 팀 단위로 예선을 거쳐 여덟 팀이 라스베이거스에서 본선 진행
    - 자신의 팀을 보호하면서 상대 팀을 공격하여 상대 시스템을 많이 해킹한 팀이 승리

그림 1-12 데프콘 사이트(http://www.defcon.org)

  - 해킹 도구의 개발
    - 1994년 인터넷 브라우저인 넷스케이프가 개발되어 웹 정보에 대한 접근이 가능해짐
    - 해커들은 자신의 노하우와 프로그램을 BBS에서 웹 사이트로 옮기고 해킹 정보와 해킹 툴을 웹에서 공개
    - 일부 사용자들은 해킹 툴을 사용하여 개인 정보를 캐기도 하고 은행 컴퓨터의 계좌 정보를 변조
    - 언론은 이들을 해커라 부르기 시작
    - 이때부터 해커라는 용어가 순수한 목적으로 시스템 내부를 연구하는 컴퓨터광을 지칭하지 않게 됨

정보 보안의 역사

- 1980~1990년대
  - 아메리카온라인 해킹
    - 1997년에 아메리카온라인(AOL)침입만을 목적으로 고안된 무료 해킹 툴인 AOHell이 공개
    - AOHell은 초보 해커와 스크립트 키드가 사용하도록 개발된 것
    - 이후 며칠 동안 초보 해커들이 악용하여 미국 내 수백만 명의 온라인 사용자가 대용량 메일 폭탄 공격을 받음
  - 트로이 목마, 백 오리피스
    - 1998년에는 'CDC'라는 해킹 그룹이 데프콘 해킹 대회에서 트로이 목마 프로그램인 '백 오리피스'를 발표
    - The Analyzer라는 이스라엘의 10대 해커가 미국 펜타곤의 시스템에 침투해서 소프트웨어를 훔쳐낸 사건이 발생

정보 보안의 역사

- 2000년대 이후
  - 분산 서비스 거부 공격 (DDoS)
    - 2000년 2월 인터넷에서 소통량이 많은 몇 개 사이트에 분산 서비스 거부(DDoS) 공격이 가해짐
    - 이로 인해 야후, CNN, 아마존 등의 사이트가 ICMP 패킷을 이용한 스머프 공격으로 몇 시간 동안 마비
    - 네트워크를 스캔한 후 취약한 서버에 trojans라는 클라이언트 프로그램을 설치하여 정해진 시간에 목표 사이트에 수많은 패킷을 전송함으로써 사이트가 다운되도록 하는 공격
  - 웜과 바이러스
    - 2000년에는 러브 버그바이러스가 등장하여 87억 5,000만 달러의 경제적 손실을 입힘
      - 바이러스 메일에는 “ILOVEYOU”라는 제목에 “발송드린 첨부의 LOVELETTER를 확인 부탁드립니다”라는 내용의 본문 메시지와 ‘LOVELETTER.TXT.VBS’라는 파일이 첨부
      - 첨부 파일에 접근하면 다른 이메일 계정으로 메일이 복제 및 전송
    - 2003년 1월 마이크로소프트의 MS-SQL 2000 서버를 공격하는 슬래머 웜이 전국 네트워크를 마비시킨 사건 발생
    - 2004년에는 베이글 웜, 마이둠 웜, 넷스카이 웜이라는 웜 삼총사가 등장
  - 개인 정보 유출과 도용
    - 2005년~2006년 사이에 우리나라에서 주민 등록 번호 수십만 개가 유출되어 개인 정보가 무단 도용 사건 발생
    - 사이버테러대응센터에서 접속 IP를 분석해보니 중국에서 직접 접속한 경우, 국내 사설망 등을 통해 접속한 경우, 해킹으로 중간 경유지를 이용한 경우 등이 원인으로 밝혀짐
    - 2005년 11월에는 금융 정보를 이용하여 은행 계좌에서 잔고를 인출한 사건 발생

정보 보안의 역사

- 2000년대 이후
  - 전자 상거래 교란
    - 2006년 7월에는 안심클릭의 허점을 이용한 해킹 사기 사건이 발생
      - 범인들은 해킹으로 타인의 신용카드 번호를 입수한 후, 인터넷에서 이루어지는 신용카드 결제 방식의 제도적· 기술적 취약점을 이용하여 물품을 대신 결제하고 현금을 돌려받아 수억 원을 인출
      - 대부분의 신용카드 사용자들이 일반 사이트,쇼핑몰, 카드사 사이트의 접속 아이디와 비밀 번호를 동일한 점에 착안한 범죄
    - 2006년 3월에는 국내 대형 포털 사이트의 정보 검색 순위를 조작한 인터넷 광고 대행 업체의 대표가 입건
      - 국내 4개 대형 포털 사이트의 검색 순위에 업체의 홈페이지 주소를 상위에 노출시켜 주는 조건으로 광고주를 모집
      - 자체 개발한 프로그램을 이용하여 750개 회사의 홈페이지 주소를 자동으로 클릭하게 만들어 정보 검색 순위를 조작
  - APT 공격의 등장
    - 2008년 해커 8명으로 구성된 캐시어가 영국 RBS 은행의 월드페이 시스템에 침입하여 복제 카드를제작
    - 신용카드의 한도를 올리고 12시간 동안 세계 49개 도시의 2,100개 ATM 기기에서 약 950만 달러를 인출
    - 이 해킹 사건을 최초의 APT(지능적 지속 위협) 공격으로 흔히 언급
    - APT 공격: 오랜 시간을 들여 사이트를 분석하고 취약점을 찾아내어 해킹하는 경우를 APT 공격이라고 함

정보 보안의 역사

- 2000년대 이후
  - 농협 사이버 테러
    - 2011년 4월 대규모 데이터 삭제로 농협의 전산 시스템이 멈추는 사건이 발생
    - 정부는 이를 북한의 사이버 테러라고 발표
    - 이 사건은 국내 기업의 보안 인식 자체를 바꿔 놓는 계기가 됨
  - 스마트폰 해킹
    - 대표적인 스마트폰 운영체제인 애플의 iOS와 구글의 안드로이드는 모두 유닉스(리눅스)와 유사
    - 리눅스에 기반을 둔 안드로이드에는 리눅스 해킹툴을 비교적 쉽게 설치할 수 있음
    - 스마트폰은 긴 시간 동안 전원 공급이 가능하고 와이파이, 3G 망, LTE 망도 이용 가능한 최고의 해킹 도구
      - 스마트폰에 무선 랜 해킹 도구를 설치하고 택배 상자에 넣어 공격 대상 회사로 보내 무선 네트워크를 해킹하는 방식
  - 가상 화폐 해킹
    - 현재 가상 화폐는 큰 돈이 되고 있기 때문에 관련 해킹 사건도 증가

표 1-1 가상 화폐 해킹 사례

발생 시기	거래소 명	피해 원인	피해 규모
2019년 11월	업비트	핫월렛 해킹	580억 원
2018년 6월	빗썸	이메일 악성 코드 추정	350억 원
2018년 6월	코인레일	이메일 악성 코드 추정	400억 원
2017년 12월	유빗(구 야피존)	핫월렛해킹	172억 원

- 해킹과 보안기술의 발전 (해커, 암호, 공개키, 랜섬웨어) (12m)

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

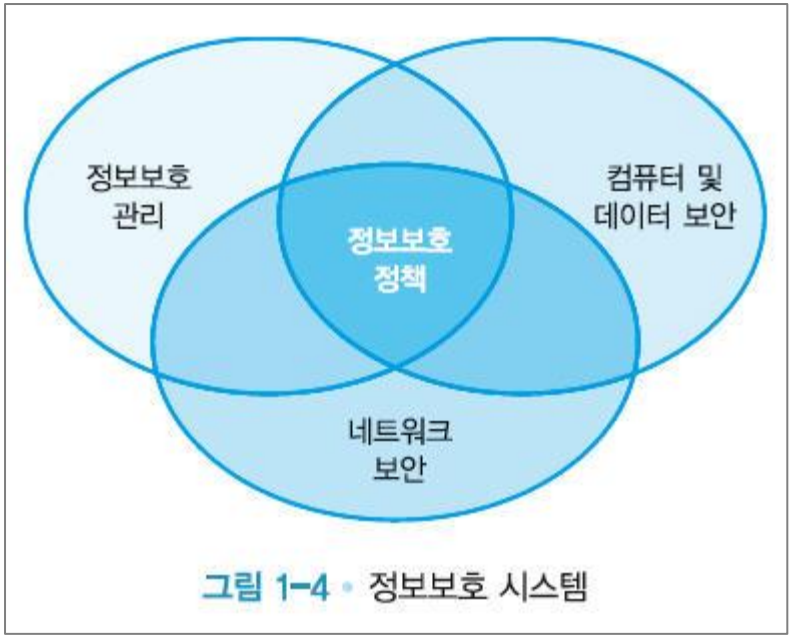

그림 1-4 • 정보보호 시스템

CIA Triad

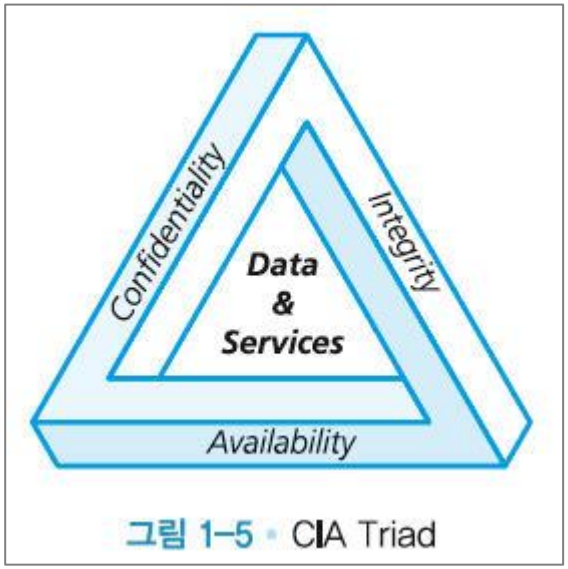

그림 1-5 • CIA Triad

- 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

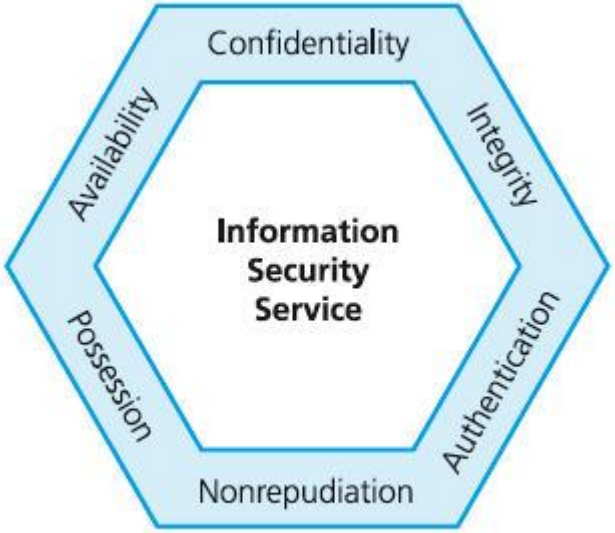

그림 1-6 • 정보보호 서비스의 종류

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

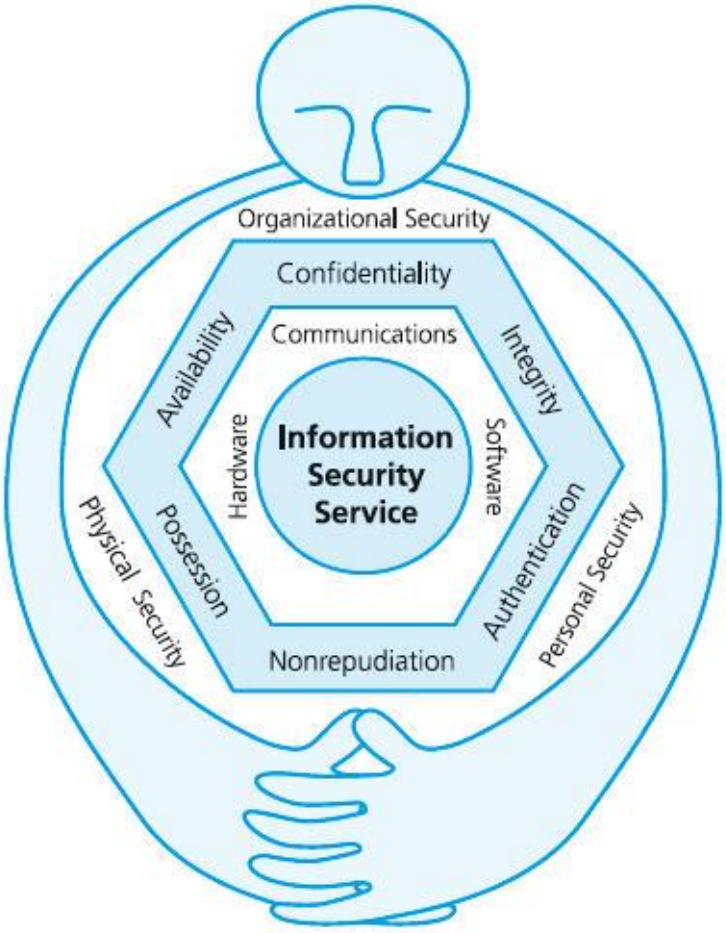

그림 1-7 • 정보보호의 인적 요소

참고문헌

- 정보 보안 개론 (4판), 양대일, 한빛아카데미 (2021)

Q & A

Thank You!