컴퓨터 보안

컴퓨터 소프트웨어공학과

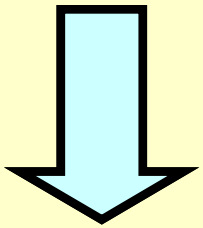
이 임영

서론

- 정보보호에 대한 초기의 대응
  - 물리적 수단(자물쇠) 및 행정적 수단(직원채용)

◆정보보호에 대한 필요성의 변화(2가지)

1. 컴퓨터의 등장 : 컴퓨터에 저장된 파일 및 기타 정보를 보호하기 위한 도구 필요
   특히 시분할 시스템이나 공중전화나 데이터 네트워크를 통해서 접근하는 시스템



컴퓨터 보안 (Computer security)
데이터를 보호하고 해커를 막기 위한 도구의 집합을 총칭

2. 분산 시스템의 등장

- 사용자와 컴퓨터간의 데이터전송을 위한 네트워크 및 통신시설의 이용

네트워크 보안 (Network security)

네트워크를 이용하여 전송중인 자료를 보호

인터네트워크 보안 (Internetwork security)

상호연결된 네트워크 집합을 보호

- 정보 보안 **(Information Security)**
- 컴퓨터 보안 **(Computer Security)**
- 네트워크 보안 **(Network Security)**
- 인터네트워크 보안 **(Internetwork security)**
- 인터넷 보안 **(Internet Security)**
- 보안
- 정보보호

보안 공격, 서비스 및 기법

보안 공격 (Security Attack)

- 조직에 의하여 소유된 정보의 안전성을 위태롭게 하는 어떠한 행위

보안 메커니즘 (Security Mechanism)

- 보안 공격을 예방, 탐지, 복구하기 위하여 설계된 메커니즘

보안 서비스 (Security Service)

- 조직의 데이터 처리 시스템과 정보의 전송에 대한 안전성을 수행하기 위한 서비스
- 보안 공격을 방어하기 위함
- 하나 혹은 그이상의 보안 메카니즘을 이용

❑ 자연적 위협 요소

- ❖ 자연적 재앙, 에러 및 손실, 정보관리 부실
- ❖ 네트워크 장애, 시스템 장애

❑ 고의적 위협 요소

- ❖ 내부의 적, 컴퓨터 해킹, 위장(Masquerade)
- ❖ 메시지 순서 변조 (Modification of Message Sequence)
- ❖ 정보 변조 (Modification of Information)
- ❖ 서비스 거부 (Denial of Service), 부인 (Repudiation)
- ❖ 정보노출 (Leakage of Information)
- ❖ 신분 레이블 변조 (Modification of Identification Label)

보안 공격

❑ 보안 공격 (Security Attack)

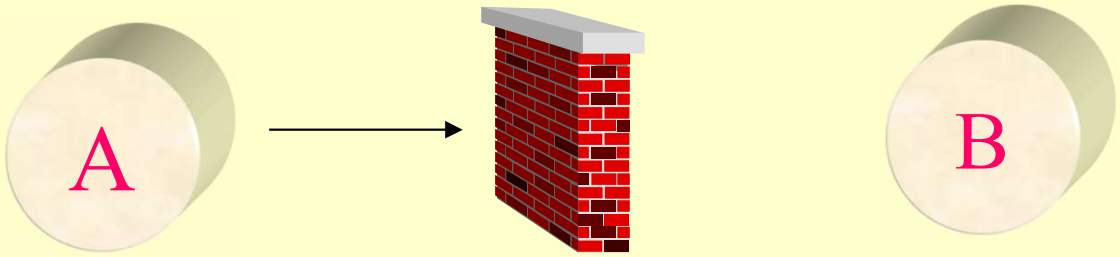
❖ 조직의 정보보호를 저해하는 제반행위

❑ 보안 공격의 유형

❖ 방해 (Interruption)

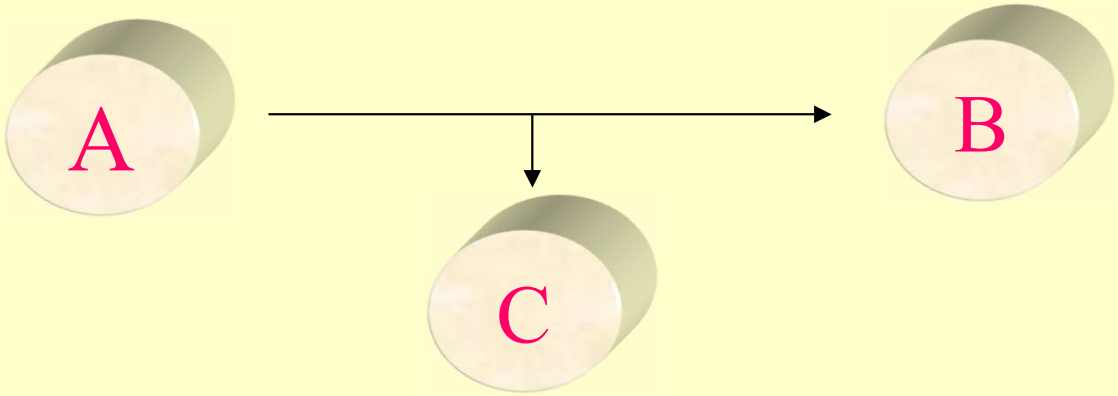
➢ 시스템의 일부가 파괴되거나 사용할 수 없는 경우로 가용성(availability)에 대한 공격

➢ 하드웨어 파괴, 통신회선 절단, 파일관리시스템의 무력화



❖ 가로채기 (Interception)

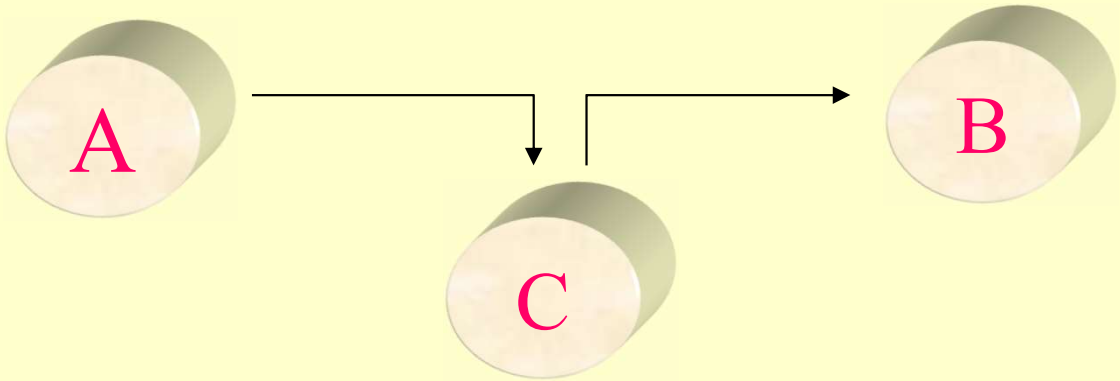
- 비인가자들의 불법적인 접근에 의한 기밀성(confidentiality)에 대한 공격
- 도청, 파일의 불법 복제



- 사용자 A가 사용자 B에게 하나의 파일을 전송한다. 그 파일은 노출되지 않도록 보호돼야 할 기밀정보(예: 봉급기록)가 들어 있다. 그 파일을 읽을 수 있는 권한이 없는 사용자 C는 그 파일의 전송 중에 전송 상황을 지켜보고 복사할 수 있다.

❖ 불법수정 (Modification)

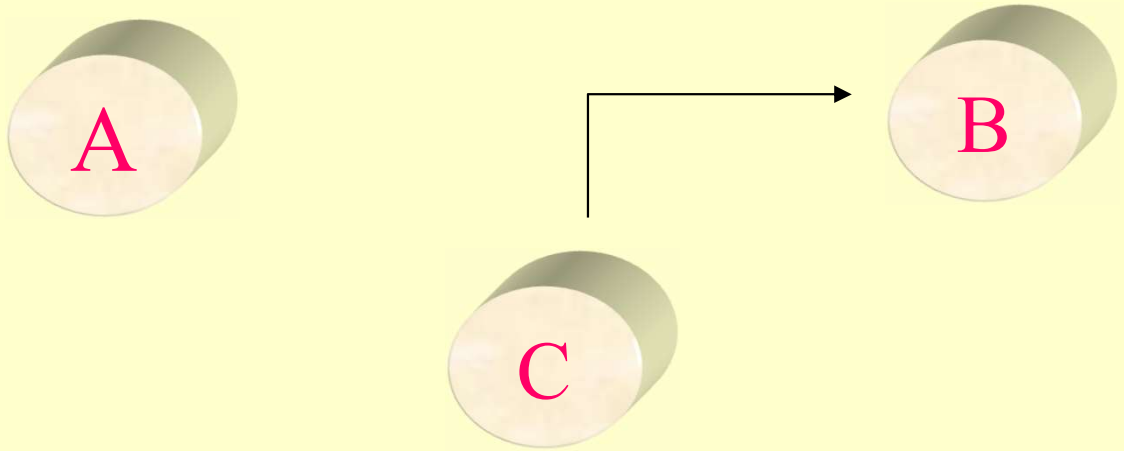
- 비인가자들의 불법적인 접근 뿐만 아니라 불법적인 변경에 의한 무결성(integrity)에 대한 공격
- 파일 값 변경, 변조, 메시지 내용 수정



- 네트워크 관리자 A는 컴퓨터 B에게 하나의 메시지를 전송한다. 그 메시지는 컴퓨터 B에게 그 컴퓨터를 접근할 수 있는 새로운 사용자를 계정인가 파일에 포함하도록 지시하고 있다. 사용자 C는 그 메시지를 가로채서 사용자를 추가 또는 삭제하라는 내용을 변경하여 B에게 보낸다. B는 메시지가 관리자 A로부터 오는 것으로 알고 접수하여 인가 파일을 갱신한다.

❖ 위조 (Fabrication)

- 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증(authentication)에 대한 공격
- 위조된 메시지 삽입, 파일에 레코드 추가

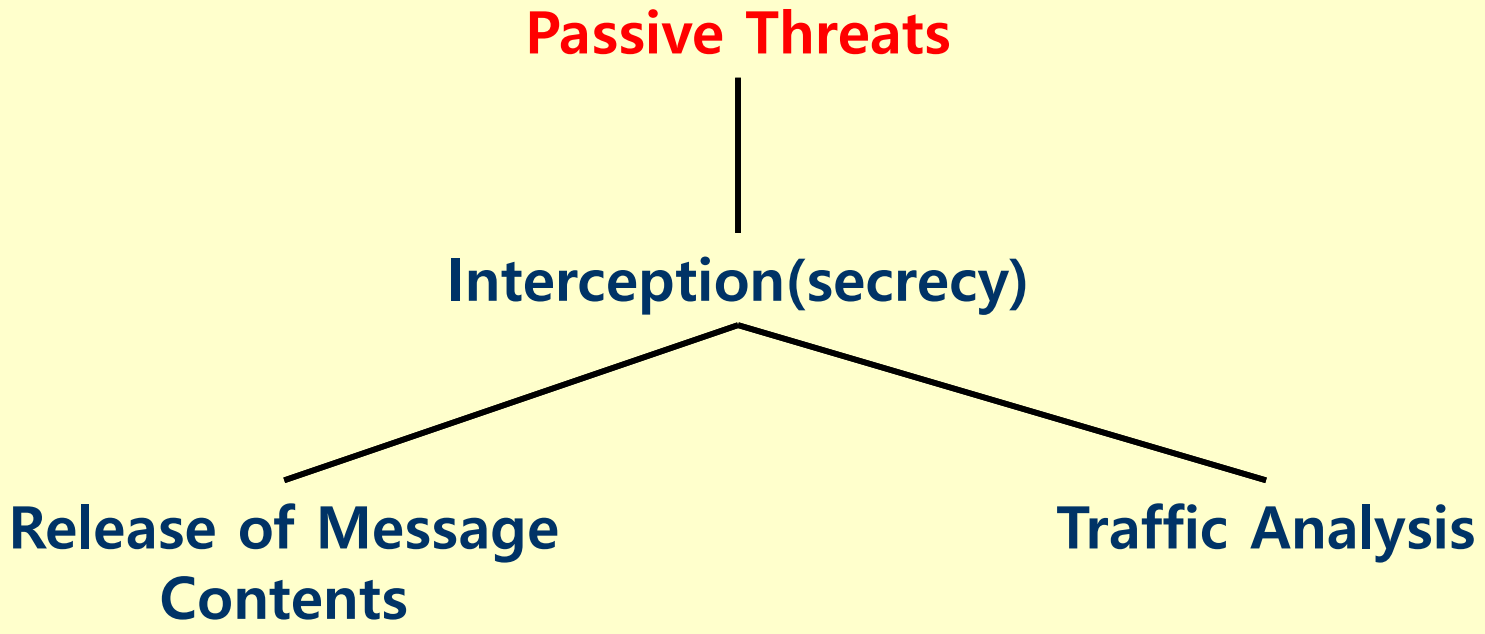


- 사용자 C는 메시지를 중간에서 가로채는 대신 자신의 의도대로 메시지를 작성하여 마치 관리자 A가 보낸 것처럼 컴퓨터 B에게 보낸다. 컴퓨터 B는 C가 보낸 메시지를 관리자 A로부터 온 것처럼 접수하여 그 메시지대로 인가 파일을 갱신한다.

❖ **부인 방지 (non-repudiation)**

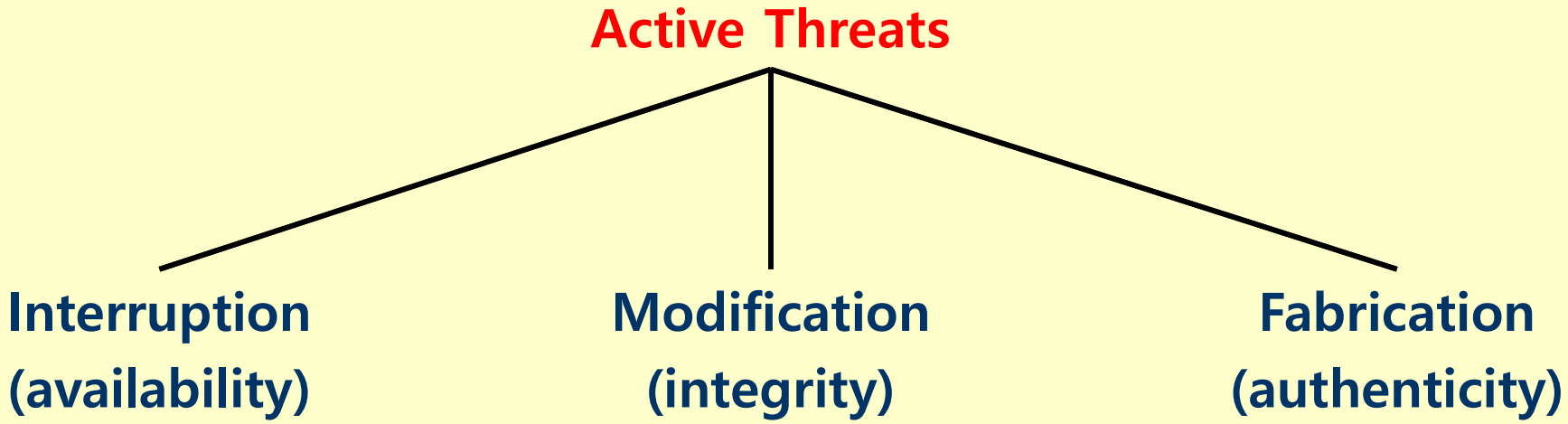
- 어느 고객이 여러 가지 거래지시사항을 담은 메시지를 증권 중개인에게 보낸다. 결과적으로 투자된 증권이 손실을 보게 되면, 그 고객은 메시지 전송 사실을 부인한다.

보안에 대한 적극적 및 소극적 네트워크 위협



- 소극적 공격 (passive attack)
  - 가로채기, 도청, 감시
    - 메시지 내용 공개 : 전화, 이메일, 전송파일의 정보
    - 트래픽 분석: 송수신자 신분, 통신시간, 주기관찰...통신의 성격을 파악
  - 변화가 없으므로 검출 곤란
  - 검출보다 예방 필요

보안에 대한 적극적 및 소극적 네트워크 위협



- **적극적 공격 (active attack)**
  - ❖ 신분위장
  - ❖ 재전송 : 데이터 단위 수동적 획득
  - ❖ 메시지 불법적 수정: 무결성 침해
  - ❖ 서비스 부인 (서비스 거부 공격) : 특정 목표물을 대상으로 무력화, 성능저하 유발
  - ❖ 예방하기가 대단히 어려움: 모든 자원과 시간 보호불가능(모든 통신설비 및 경로를 항상 물리적으로 보호)
  - ❖ 공격을 탐지, 공격으로 부터의 와해나 지연으로 부터 복구 필요

보안 서비스

❑ 보안 서비스 (Security Service)

❖ 조직의 데이터 처리 시스템 및 정보 전송에 대한 보안을 강화하기 위한 제반 서비스

❑ 보안 서비스의 종류

❖ 기밀성 서비스 (confidentiality, 비밀성, 비밀유지)

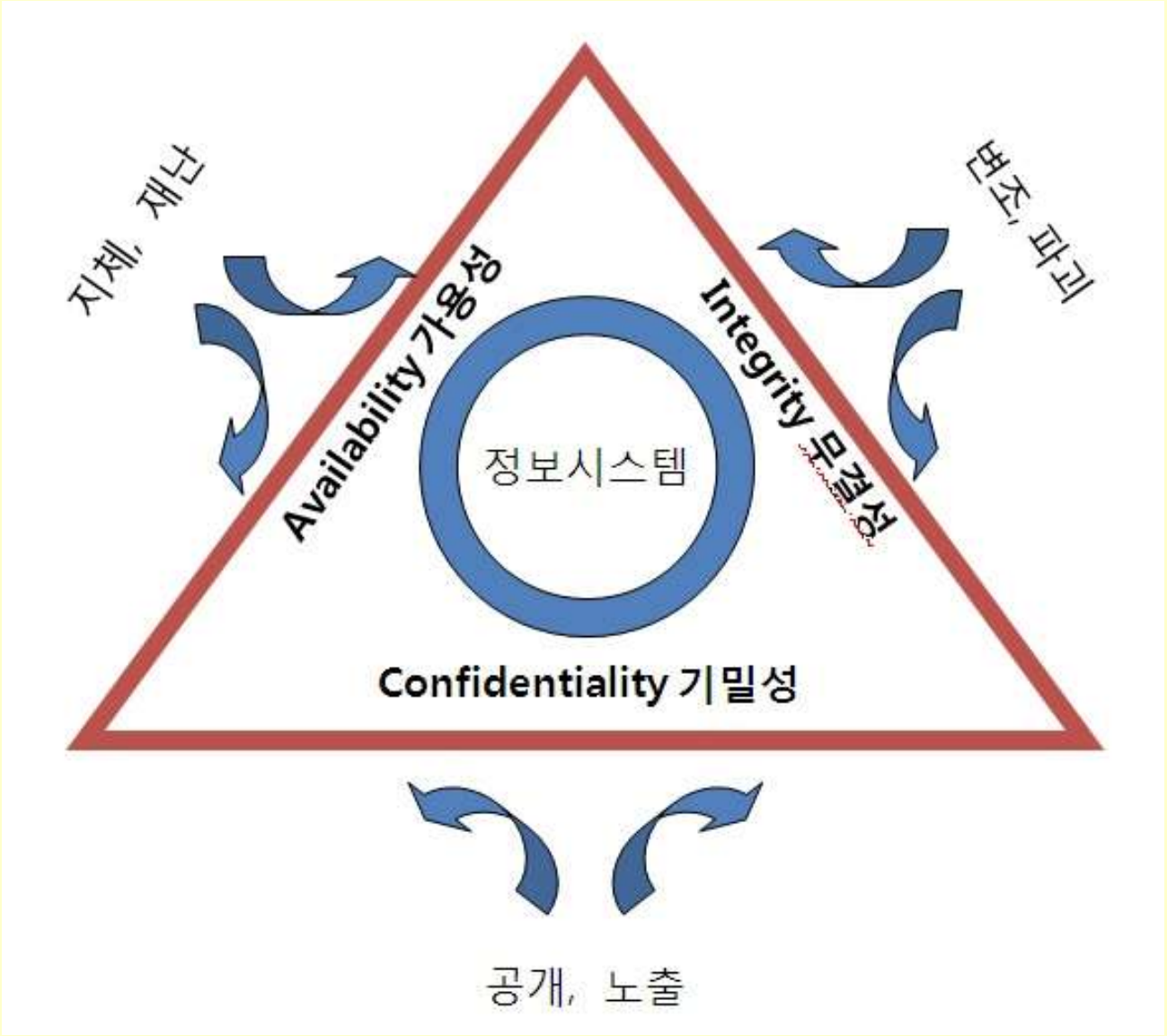
- 합법적인 실체만 읽을 수 있도록 보호하는 서비스
- 메시지 내용 공개, 트래픽 흐름 분석, 도청으로부터 전송 메시지 보호
- 접속 구간 기밀성, 내용 기밀성, 메시지 흐름 기밀성
- 암호 알고리즘 이용

❖ 무결성 서비스 (integrity, 온전성)

- 합법적인 실체만 수정할 수 있도록 보호하는 서비스
- 연결형 무결성 서비스, 비연결형 무결성 서비스
  - 연결형 : 원래 송신대로 복사, 추가, 수정, 순서변경, 재전송되지 않고 수신되었음을 확인
    - » 메시지 스트림을 대상, 불법변경 보호와 서비스 부인 방지
  - 비연결형 : 개별 메시지들만을 대상, 불법변경 보호
- 해쉬 함수, 디지털 서명, 암호 알고리즘 이용

❖ 가용성 서비스 (availability)

- 컴퓨터 시스템이 인가 당사자가 필요로 할 때 이용할 수 있게 보호하는 서비스


지체, 재난
변조, 파괴
Availability 가용성
Integrity 무결성
정보시스템
Confidentiality 기밀성
공개, 노출

❖ 인증 서비스 (authentication, 인증)

- 정보 및 시스템의 자원을 사용하는 정당한 사용자임을 확인할 수 있도록 보호하는 서비스
- 연결된 송수신자 확인, 제 3자의 위장 확인
- 발신처 인증, 메시지 인증, 실체 인증

❖ 부인봉쇄 서비스 (non-repudiation, 부인방지)

- 송수신자가 송수신 사실에 대한 부인을 하지 못하게 하는 것
- 송신자 부인 봉쇄, 수신자 부인봉쇄, 배달증명, 의뢰증명

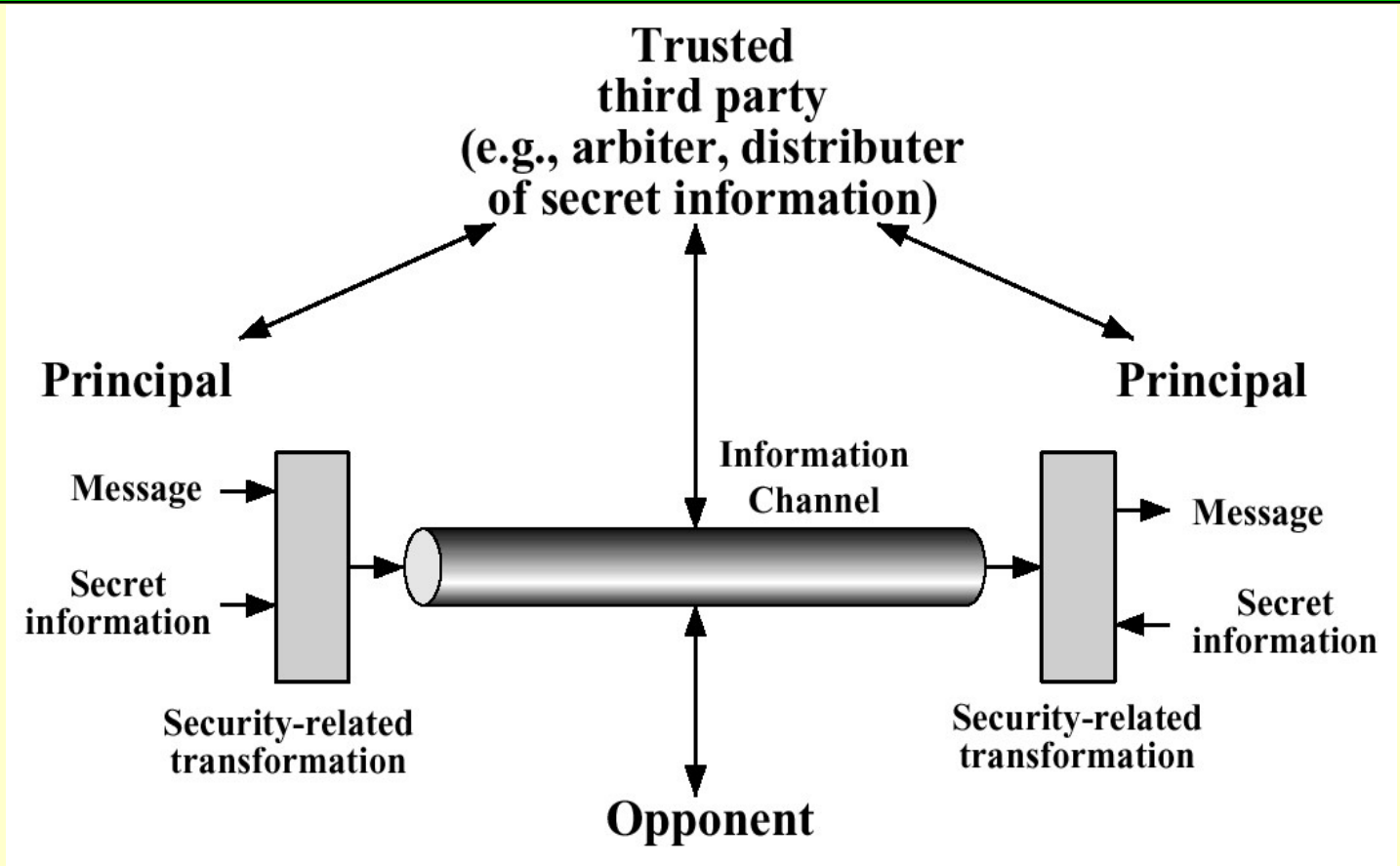
❖ 접근 제어 서비스 (access control, 접근통제)

- 사용자가 시스템 혹은 특정 자원에 접근 하고자 할 때 인가 받은 사용자만 접근을 허락하도록 제어하는 서비스

보안 서비스

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

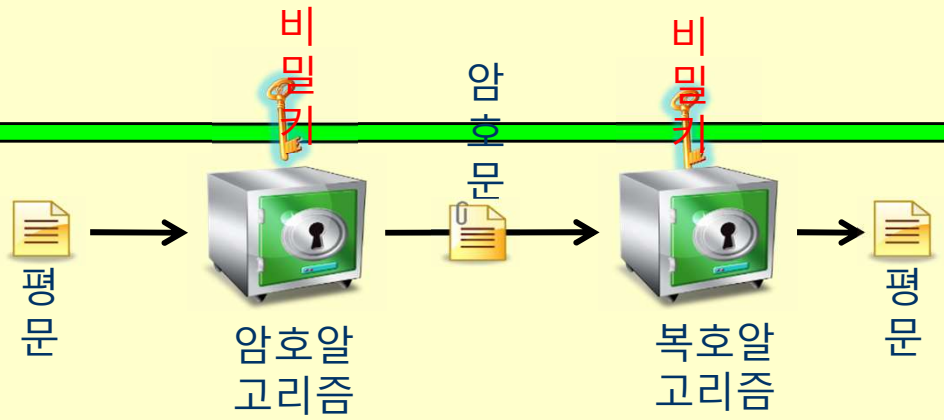
네트워크 보안 모델



- 보안을 위한 기본 기법
  - ❖ 전송될 정보에 대한 보안 관련 변환(암호화)
  - ❖ 공격자가 알지 못할 양쪽 통신주체간의 비밀 정보 공유(키)
  - ❖ 신뢰할수 있는 제3자(TTP)

❑ 암호 방식

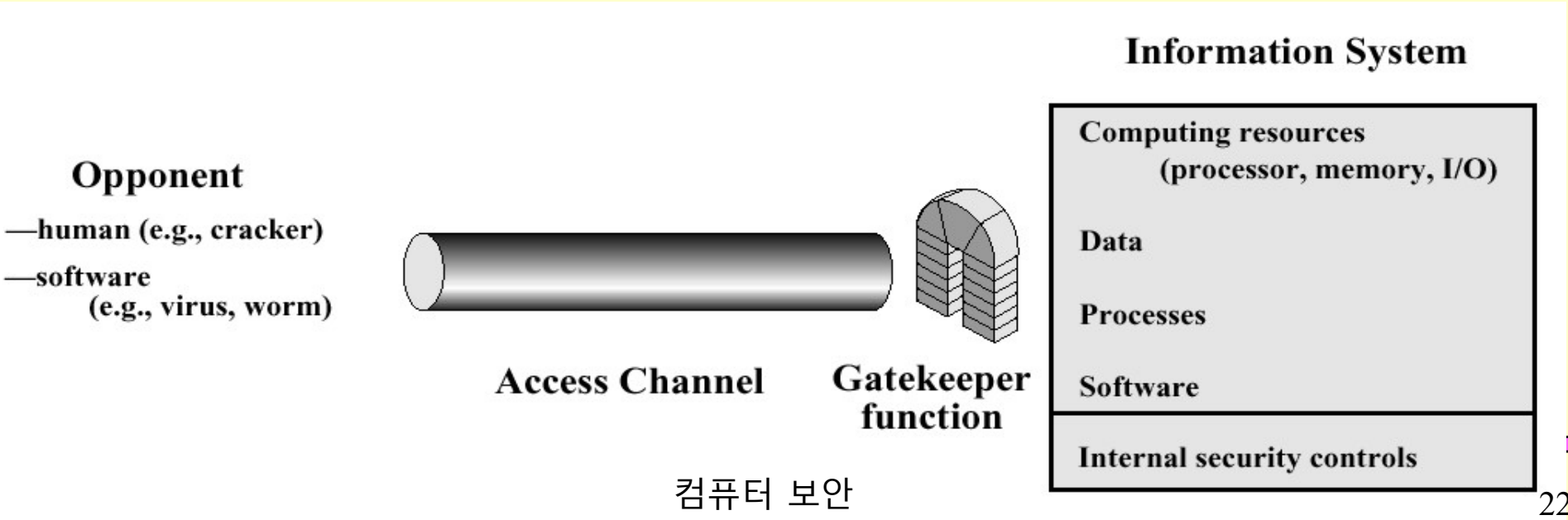
보안 서비스 설계



- 보안을 위한 모든 기술의 2가지 요소
  - 보안을 위한 암호화(Algorithm)
  - 암호화 키와 같은 어떤 비밀 정보(Key)
- 일반 모델로부터 특정 보안 서비스 설계의 기본 사항
  - 보안 관련 변환 알고리즘의 설계
    - 공격자가 변환을 파악할 수 없는 것이어야 함
  - 변환 알고리즘과 병용될 비밀 정보의 생성
  - 비밀정보의 분배 및 공유 방법의 개발
  - 특정 보안 서비스를 위한 보안 알고리즘 및 비밀정보를 사용할 통신주체간의 프로토콜 지정

네트워크 접근 보안모델

- **1차 방어: gatekeeper function**
  - ❖ 패스워드 기반 로그인 절차: 사용자 인증, 접근 통제
  - ❖ 감독 및 심사 구조: 웜, 바이러스 등의 검출과 거부
- **2차 방어: monitoring function**
  - ❖ 원하지 않는 침입자를 검출하기 위한 내부적 보안 제어
  - ❖ 내부적 활동을 감독
  - ❖ 침입자 존재 발견을 위한 저장된 정보의 분석



시대별 정보보호

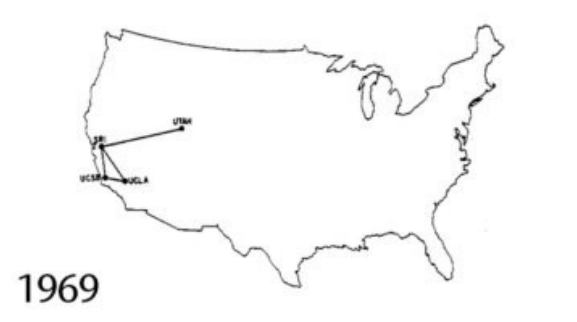
- 60년대-냉전시대
- 70년대-네트워크 확산 시대
- 80년대-PC와 네트워크
- 90년대-WWW
- 2000년대-전자 상거래
- 현재-무선 네트워크와 이동성

60년대-냉전시대

- 그물형 네트워크의 탄생
- 정보보호 개념 부재에 대하여 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 ; 보안에 중점을 둔 최초의 시스템

70년대-네트워크 확산시대

- 미국방부의 ARPANET(Advanced Reserch Project Agency Network)
- 4개의 노드로 시작
- 네트워크에 연결된 노드 수의 폭발적 증가
- ARPANET 의 보안문제 심각
  - 원격서버에 저장된 자료의 안정성 결여
  - 패스워드 구조와 형식의 취약성
  - 공중전화망을 통한 접속의 안전성 결여
  - 사용자 시스템 접근 허락문제
- 개인용 컴퓨터 등장 : 네트워크공동체 형성
  - 보안 문제 심각 ➔ 암호를 이용한 전송
  - 공개키 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 웹브라우저 등장
- 인터넷 확산
- 정보보호의 산업화 표준 부족
- 물리적 보안이 주류

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
- 개인정보보호법 등 법적 제도 마련
- 정보보호는 한 컴퓨터의 안전만으로 해결되지 않는다

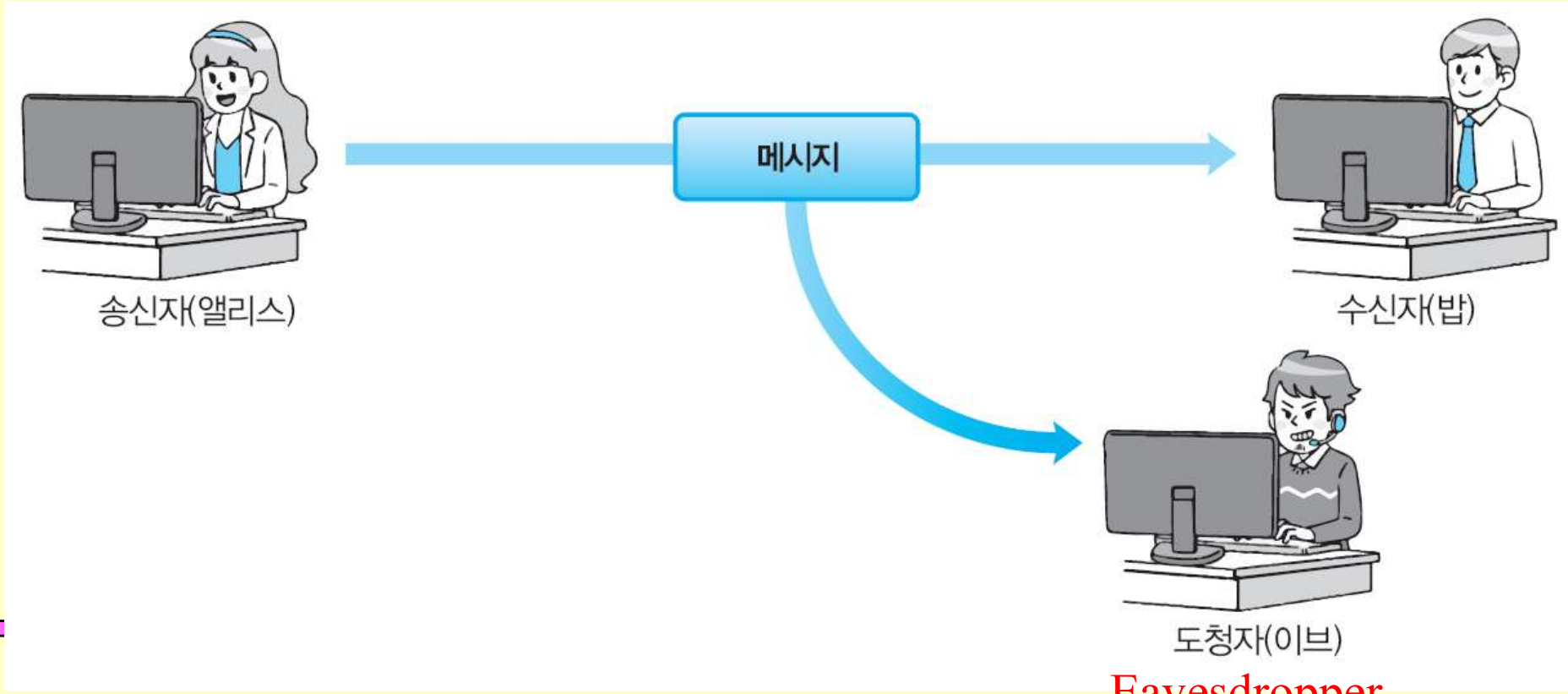
다중보안시스템

- 물리적 보안(Physical Security) : 절도, 파괴, 화재
- 인적 보안(Personal Security) : 민감한 정보에 접근, 신원 인가
- 운용 보안(Operation Security) : 기능,성능
- 통신 보안(Communication Security) : 안전한 송수신
- 네트워크 보안(Network Security) : 공용네트워크에 대한 안전
- 정보보호(Information Security) : 훼손/변조/유출 방지

송신자 · 수신자 · 도청자

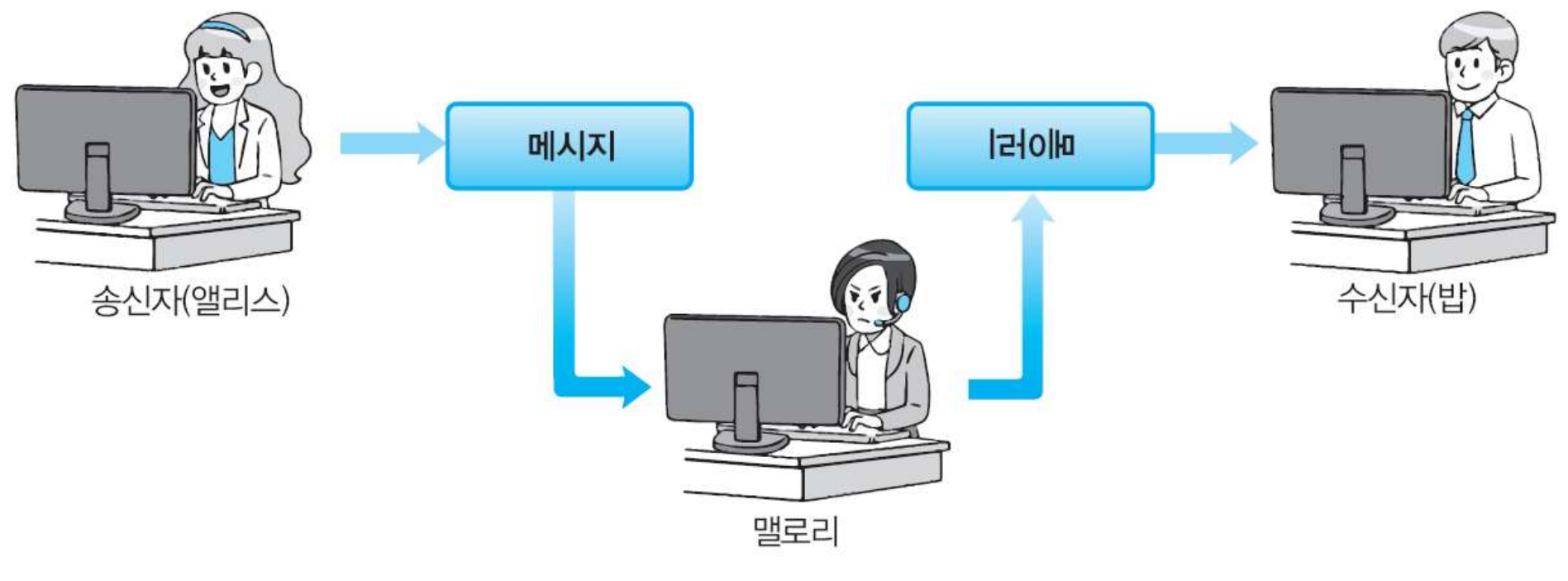
Sender

Message



Eavesdropper

송신자 · 수신자 · 도청자



암호화와 복호화

- 평문(plaintext)
  - 암호화하기 전의 메시지
- 암호문(ciphertext)
  - 암호화한 후의 메시지
- 암호기술
  - 중간에서 도청자가 암호문을 가로채어 갖게 된다고 하더라고 특정 비밀값을 모른다면 암호문을 평문으로 복호화 할 수 없도록 하는 기술

해독

- 복호화
  - 정당한 수신자가 암호문을 평문으로 바꾸는 것
- 암호 해독(cryptanalysis)
  - 수신자 이외의 사람이 암호문으로부터 평문을 복원하려고 시도하는 것
- 암호 해독자(cryptanalyst)
  - 암호 해독을 하는 사람
    - 나쁜 의도를 가진 자
    - 암호 연구자