2021/07/07, 2021 보안 기초 세미나

# Network Security Essentials

## - Chapter_1 개요 -

발표자 : 이 태 양(taeyang2.lee@gmail.com)

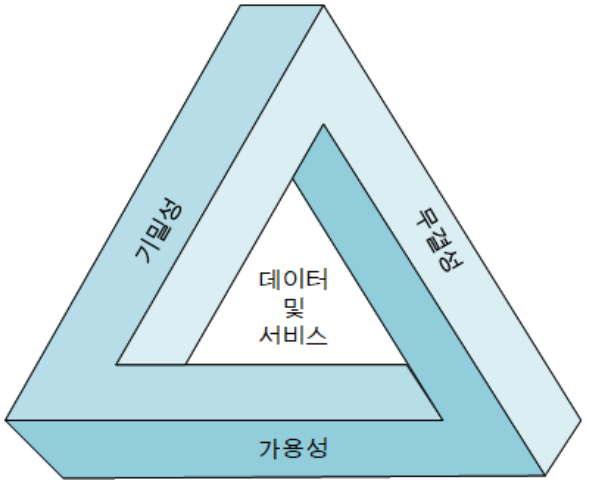
세종대학교 프로토콜공학연구실

# 목 차

- 컴퓨터 보안 개념
- OSI 보안 구조
- 보안 공격
- 보안 서비스
- 보안 메커니즘
- 네트워크 보안 모델

# 컴퓨터 보안 개념

- 컴퓨터 보안
  - 정의
    - 정보시스템 자원의 무결성, 가용성, 기밀성 보전을 위해 제공되는 보호
      - 정보시스템 자원
        - e.g., 하드웨어, 소프트웨어, 펌웨어, 정보/데이터, 통신
      - CIA 트라이어드
        - 기밀성(Confidentiality)
        - 무결성(Integrity)
        - 가용성(Availability)




<CIA 트라이어드>

# 컴퓨터 보안 개념

- 컴퓨터 보안
  - 3가지 주요 목표 (1/3)
    - 기밀성 (Confidentiality)
      - 허락되지 않은 사용자, 개체에게 정보의 내용이 노출되지 않도록 하는 것
        - 데이터 기밀성 (Data Confidentiality)
          - 인가되지 않은 사용자나 개체에게 개인정보나 기밀정보를 노출되지 않도록 하는 것
        - 프라이버시 (Privacy)
          - 사용자와 관련된 데이터를 수집하고 배포하는 방식에 대한 보안
      - 특징
        - 정보 접근과 공개에 대한 제한조건을 지키는 것
        - 기밀성을 상실하게 되면 정보가 부정하게 공개됨

# 컴퓨터 보안 개념

- 컴퓨터 보안
  - 3가지 주요 목표 (2/3)
    - 무결성 (Integrity)
      - 허락되지 않은 사용자, 개체로 인해 정보가 변경되거나 삭제되지 않도록 하는 것
        - 데이터 무결성 (Data integrity)
          - 허가된 방식으로만 정보나 프로그램을 변경할 수 있도록 하는 것
        - 시스템 무결성 (System integrity)
          - 허가되지 않은 조작을 방지하여 허가된 접근자만 시스템의 동작을 조작할 수 있도록 하는 것
      - 특징
        - 부적절한 정보 수정이나 파괴를 막을 수 있도록 함
        - 무결성을 상실하게 되면 정보가 무단으로 수정되거나 파괴됨

# 컴퓨터 보안 개념

- 컴퓨터 보안
  - 3가지 주요 목표 (3/3)
    - 가용성 (Availability)
      - 허락된 사용자, 개체가 정보에 접근하려고 할 때 방해받지 않도록 하는 것
      - 시스템이 신속히 동작하도록 하고 인가된 사용자의 요구라면 언제든지 요구를 처리할 수 있도록 하는 것
        - e.g., 랜섬웨어는 개인의 파일을 잠궈서 개인이 본인의 파일 사용을 방해함
      - 특징
        - 정보사용에 있어서 시간성과 신뢰성 있는 접근을 할 수 있도록 함
        - 가용성을 상실하게 되면 정보나 정보 시스템을 사용하거나 접근이 불가능함

# 컴퓨터 보안 개념

- 컴퓨터 보안
  - 추가적 목표
    - 인증 (Authentication)
      - 어떤 실체가 정말 주장하는 실체가 맞는지 확인하는 것
      - 메시지 또는 자료가 정말로 신뢰할 수 있는 출처에서부터 온 것인지 확인하는 것
    - 책임 (Accountability)
      - 보안이 미치는 범위에서는 보안 침해에 대한 정보를 기록, 분석, 추적하고 관련된 분쟁을 해결할 수 있다는 것
        - e.g., 부인봉쇄, 억제, 결함 분리, 침입 탐지 및 예방, 사후 복구, 법적 조치

# 컴퓨터 보안 개념

- 보안 침해의 3가지 수준
  - 저급 위험
    - 경미한 금전적 손실, 개인에게 경미한 손해 등
  - 중급 위험
    - 중대한 금전적 손실, 인명 손실을 제외한 중대한 개인적 손해 등
  - 고급 위험
    - 치명적 금전적 손실, 인명 손실을 포함한 치명적인 개인적 손해 등

# 컴퓨터 보안 개념

- 보안 침해의 3가지 수준
  - 기밀성의 예시

| 수준 | 예시 |
|---|---|
| 저급 위험 | 학생 목록, 교수 목록, 학과 목록정보 유출 및 조회 |
| 중급 위험 | 학생 재학 정보 유출 및 조회 |
| 고급 위험 | 학생 성적 정보 유출 및 조회 |

  - 무결성의 예시

| 수준 | 예시 |
|---|---|
| 저급 위험 | 뉴스 사이트의 익명 온라인 투표 결과 조작 |
| 중급 위험 | 포럼 웹사이트 정보 훼손 |
| 고급 위험 | 환자의 알레르기 정보 훼손 |

# 컴퓨터 보안 개념

- 보안 침해의 3가지 수준
  - 가용성의 예시

| 수준 | 예시 |
|---|---|
| 저급 위험 | 온라인 전화번호부 검색 응용 시스템 |
| 중급 위험 | 신입생 모집 시기에 대학 웹사이트 서비스 중단 |
| 고급 위험 | 로그인 시스템의 인증 서버 서비스 중단 |

# OSI 보안 구조

- OSI (Open System Interconnection)
  - 정의
    - 서로 다른 정보처리시스템 사이를 접속하여 정보교환과 데이터처리를 할 수 있도록 표준화한 컴퓨터 네트워크 구조
  - 특징
    - 물리, 데이터 링크, 네트워크, 전송, 세션, 표현, 응용의 순으로 7계층을 이룸

# OSI 보안 구조

- 정의
  - 관리자가 효과적으로 보안 문제를 조직화할 수 있는 유용한 방법
  - OSI 보안 구조의 핵심
    - 보안 공격 (Security attack)
      - 정보의 안전성을 침해하는 것과 관련된 모든 행위
    - 보안 메커니즘 (Security mechanism)
      - 보안 공격을 탐지, 예방하거나 공격으로 인한 침해를 복구하는 절차
    - 보안 서비스 (Security service)
      - 정보처리 시스템의 보안을 보장하기 위한 제반 서비스
      - 하나 이상의 보안 메커니즘을 사용하여 서비스를 제공

# 보안 공격

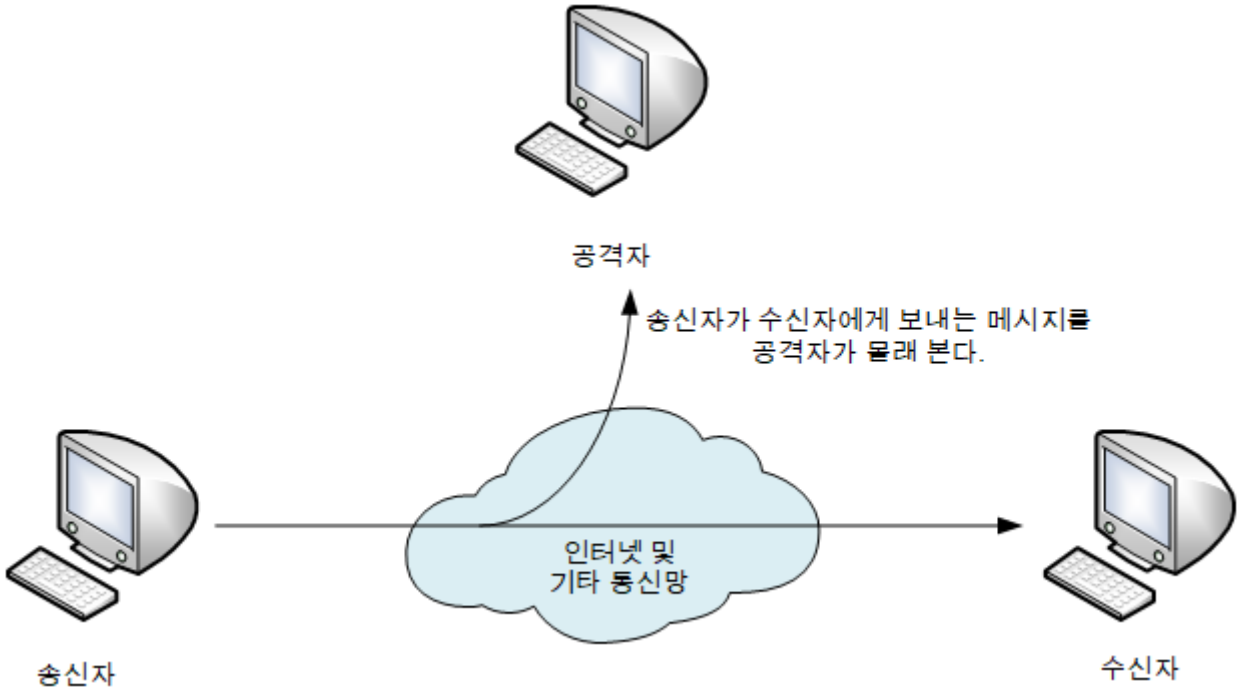
- 위협과 공격
  - 위협 (Threat)
    - 보안을 침해하고 손해를 가져올 수 있는 상황 또는 행위
  - 공격 (Attack)
    - 공격자가 정보를 누출, 변조, 파괴하는 행위

# 보안 공격

- 분류 (1/2)
  - 소극적 공격 (Passive attack)
    - 정의
      - 시스템으로부터 정보를 획득하거나 사용하려는 시도
    - 특징
      - 시스템 자원에 영향을 끼치지 않는 공격 형태
      - 전송 정보에 대한 도청이나 감시
      - 전송 중인 정보를 취득하는 것이 목표
      - 공격을 탐지하기 어려워 예방에 더 신경을 써야 함
    - 유형
      - 메시지 내용 갈취
      - 트래픽 분석

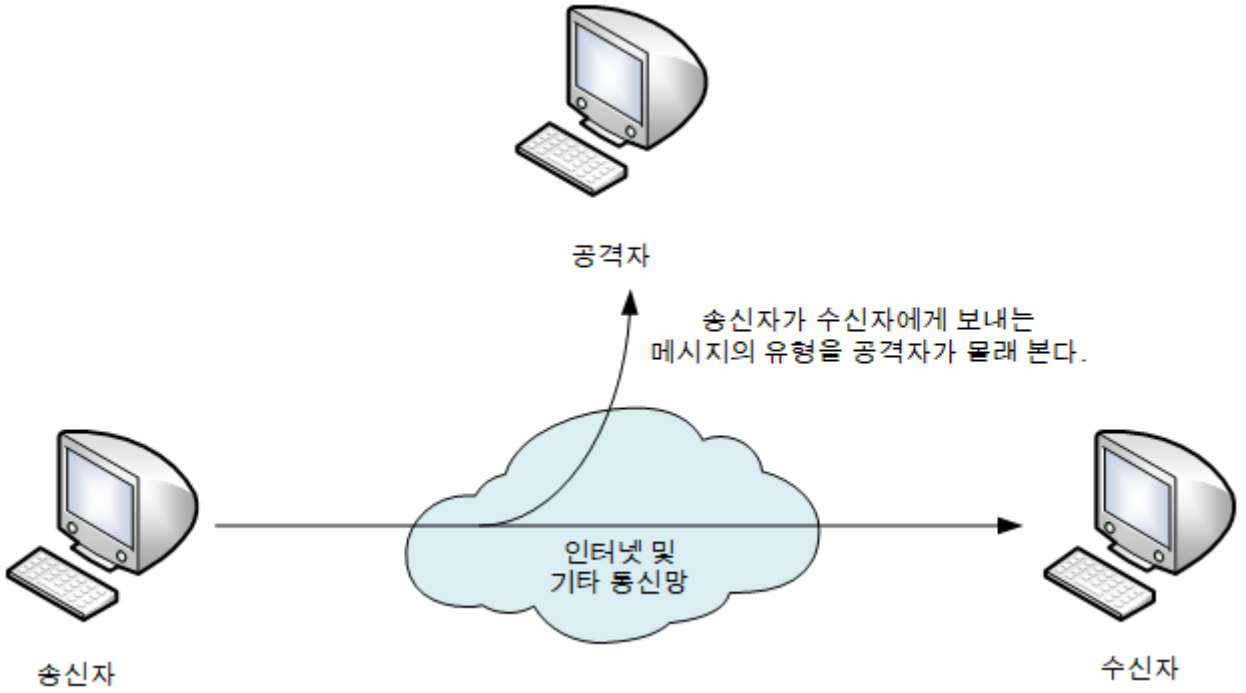
# 보안 공격

- 분류 (1/2)
  - 소극적 공격 (Passive attack) (1/2)
    - 메시지 내용 갈취 (Release of message contents)
      - 공격자가 전달되는 정보와 내용을 몰래 취득하거나 보는 것



# 보안 공격

- 분류 (1/2)
  - 소극적 공격 (Passive attack) (2/2)
    - 트래픽 분석 (Traffic analysis)
      - 메시지의 유형을 관찰하여 통신자의 통신 특성을 추측하는 것
      - e.g., 통신자의 접속위치, 신원파악, 교환되는 메시지의 빈도, 메시지 길이 등을 관찰

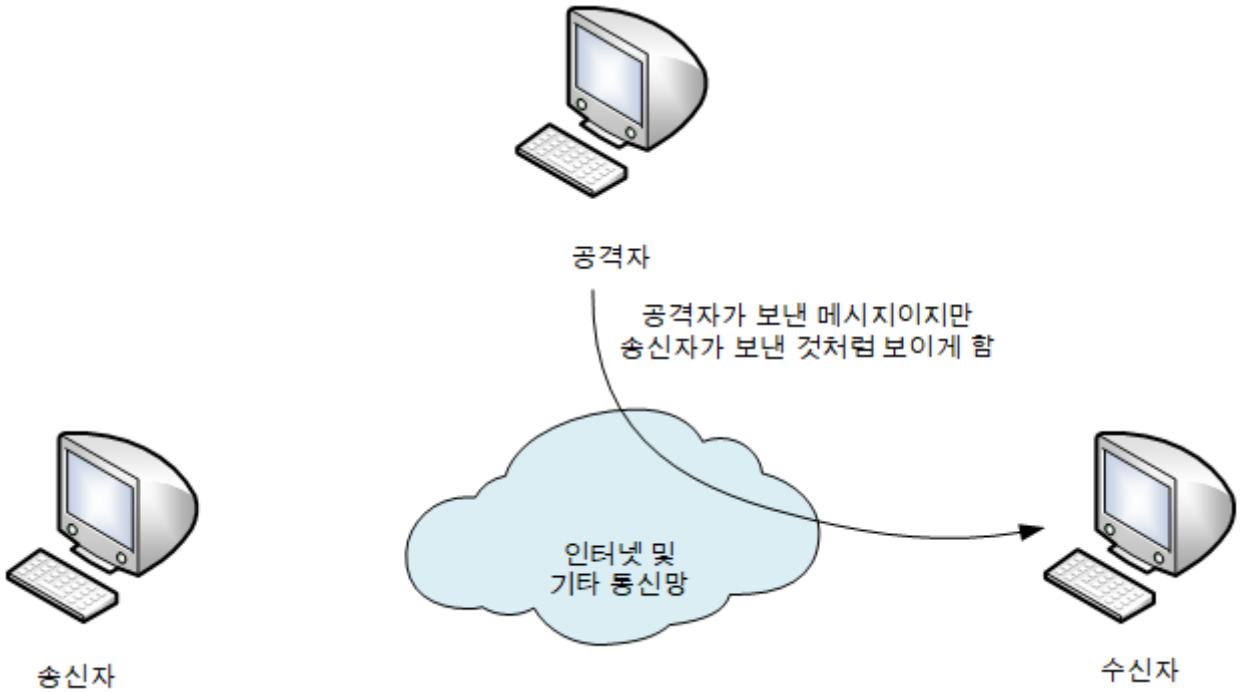


# 보안 공격

- 분류 (2/2)
  - 적극적 공격 (Active attack)
    - 정의
      - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격
    - 특징
      - 공격자가 다양한 방법으로 공격하므로 방어보다는 탐지가 쉬움
    - 유형
      - 신분위장
      - 재전송
      - 메시지 수정
      - 서비스 거부

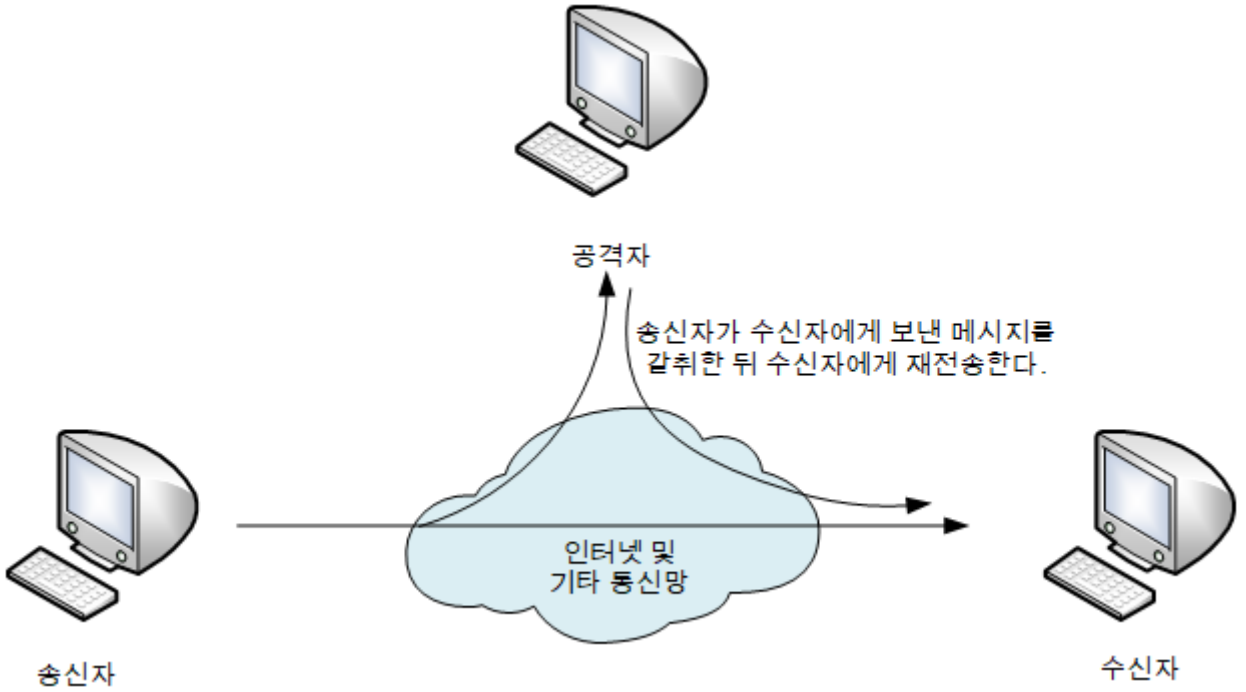
# 보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (1/4)
    - 신분 위장 (Masquerade)
      - 권한을 가진 개체처럼 가장하여 공격을 행사하는 것
      - 다른 형태의 적극적 공격과 병행해서 수행됨
        - e.g., 성적입력 시스템 접근에 권한을 가진자로 위장하여 데이터 변경



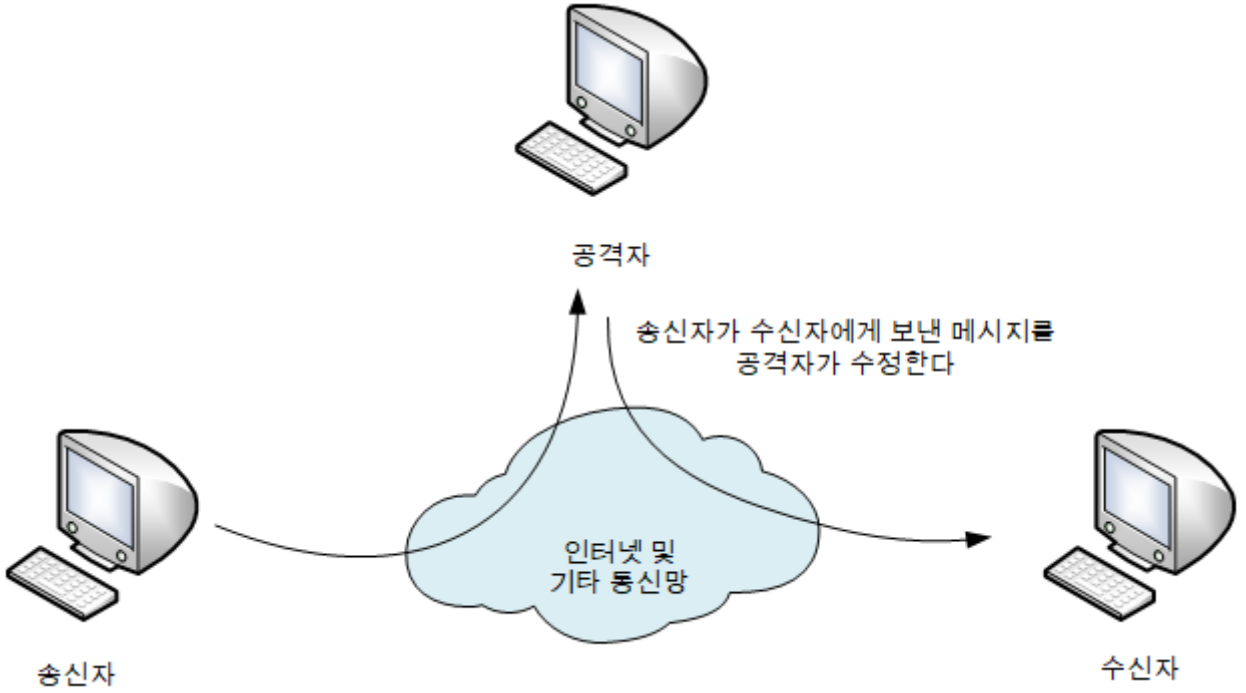
# 보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (2/4)
    - 재전송 (Replay)
      - 획득한 데이터 단위를 보관하고 있다가 시간이 경과한 후 재전송하여 인가되지 않은 사항에 접근하는 공격 형태
        - e.g., 금융 기관에 거래 메시지를 재전송하여 중복 거래를 시도



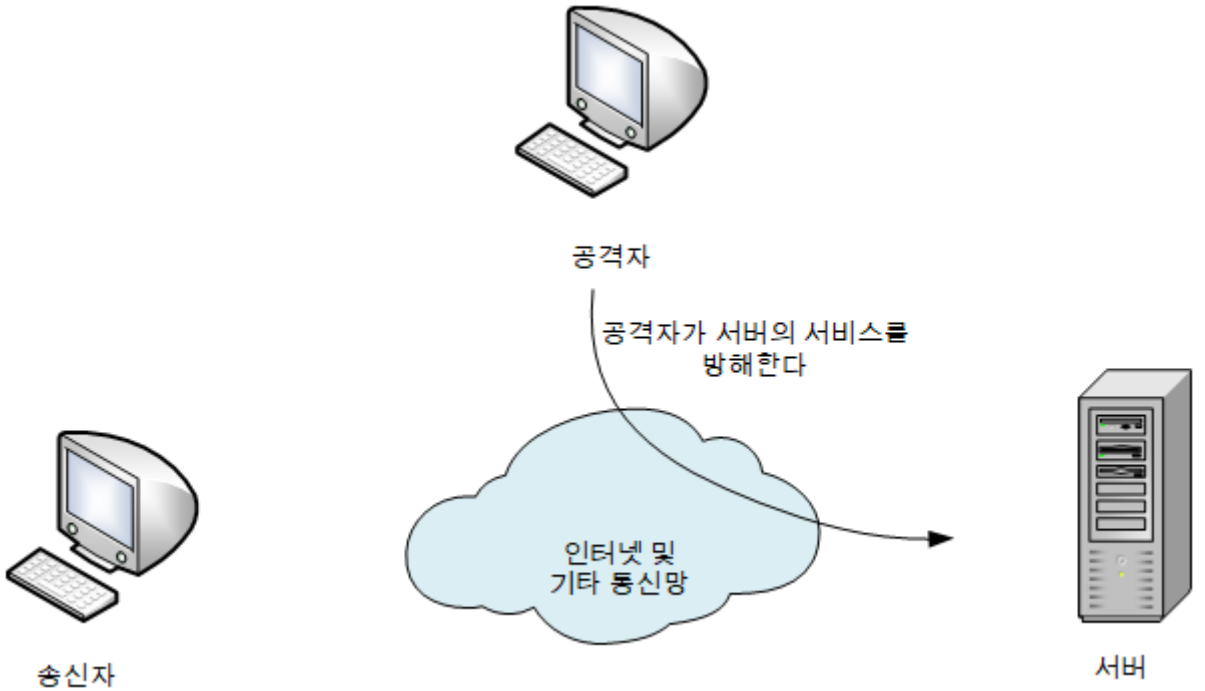
# 보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (3/4)
    - 메시지 수정 (Modification of Message)
      - 메시지의 일부를 불법으로 변경하거나 순서를 뒤바꾸어 인가되지 않은 효과를 노리는 공격 행태
        - e.g., 이메일 메시지에 악의적인 컨텐츠를 주입



# 보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (4/4)
    - 서비스 거부 (Denial of service)
      - 시스템이 정상적으로 운용되거나 관리되지 못하도록 방해하는 공격
      - 특정 목표물을 대상으로 할 수 있음
        - e.g., 대량의 메시지를 유발하여 과부하를 일으킴



# 보안 서비스

- 정의
  - 시스템의 보안이나 데이터 전송의 보안을 보장하기 위해 제공되는 서비스
  - 보안 메커니즘은 보안 서비스를 구현하고 보안 서비스는 보안 정책을 구현함

# 보안 서비스

- 분류 (1/3)
  - 기밀성 서비스 (Confidentiality Service)
    - 인가된 개체만 데이터를 읽을 수 있도록 보호하는 서비스
    - 메시지 내용 공개, 트래픽 흐름 분석, 도청으로부터 전송 메시지를 보호
  - 무결성 서비스 (Integrity Service)
    - 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신을 제공하는 서비스
    - 연결형 무결성 서비스
      - 보낸 메시지가 변경 없이 송신되는 것을 보장
    - 비연결형 무결성 서비스
      - 작은 단위 메시지 수정에 대해서만 보호 서비스를 제공

# 보안 서비스

- 분류 (2/3)
  - 가용성 서비스 (Availability Service)
    - 시스템 가용성 보장을 위해 시스템을 보호하는 서비스
  - 인증 서비스 (Authentication service)
    - 통신이 검증되었다는 것을 확인해주는 서비스
    - 대등 개체 인증 (Peer Entity Authentication)
      - 연결하고 있는 개체의 신분을 확신 시켜 줌
    - 데이터-출처 인증 (Data-Origin Authentication)
      - 비연결 전송에서 수신된 데이터의 출처를 확인해 줌

# 보안 서비스

- 분류 (3/3)
  - 접근 제어 (Access Control)
    - 인가되지 않은 정보 자원의 사용을 방지하는 서비스
      - 누가, 어떤 조건에 어떤 자원을 사용하도록 하는지 등, 자원에 대한 접근을 제한
  - 부인봉쇄 (Nonrepudiation)
    - 통신의 주체가 통신에 참여했던 사실을 부인하는 것을 방지
      - 수신자가 송신자로부터 온 메시지라는 것을 확신함
      - 송신자가 메시지를 받은 주체가 수신자라는 것을 확신함
        - e.g., 주식거래 위탁 메시지 발송을 부인

# 보안 메커니즘

- 분류
  - 특정 보안 메커니즘 (Specific Security Mechanism)
    - 통신 개체가 주장하는 것처럼 정말로 그 당사자인지를 확인해주는 것
  - 일반 보안 메커니즘 (Pervasive Security Mechanism)
    - 임의의 특정 OSI 보안 서비스나 프로토콜 계층에 구애받지 않는 메커니즘

# 보안 메커니즘

- 특정 보안 메커니즘 (Specific Security Mechanism)
  - 종류 (1/2)
    - 암호화 (Encipherment)
      - 수학적 알고리즘을 사용하여 데이터를 읽을 수 없는 형태로 변환하는 것
      - 데이터의 변환과 복구는 알고리즘과 사용되는 키에 따라 달라짐
    - 디지털 서명 (Digital Signature)
      - 데이터 수신자가 데이터의 발신자와 무결성을 입증하기 위한 기술
      - 위조를 막도록 데이터에 붙이는 데이터의 암호적 변경
        - e.g., 은행지점의 계좌 잔고 변경 요청
    - 접근 제어 (Access Control)
      - 자원에 접근할 권한을 제한하는 다양한 메커니즘
        - e.g., 인증정보, 접근이 시도된 시간 및 경로, 접근지속시간 등
    - 데이터 무결성 (Data Integrity)
      - 데이터 무결성을 확신하는데 사용되는 메커니즘

# 보안 메커니즘

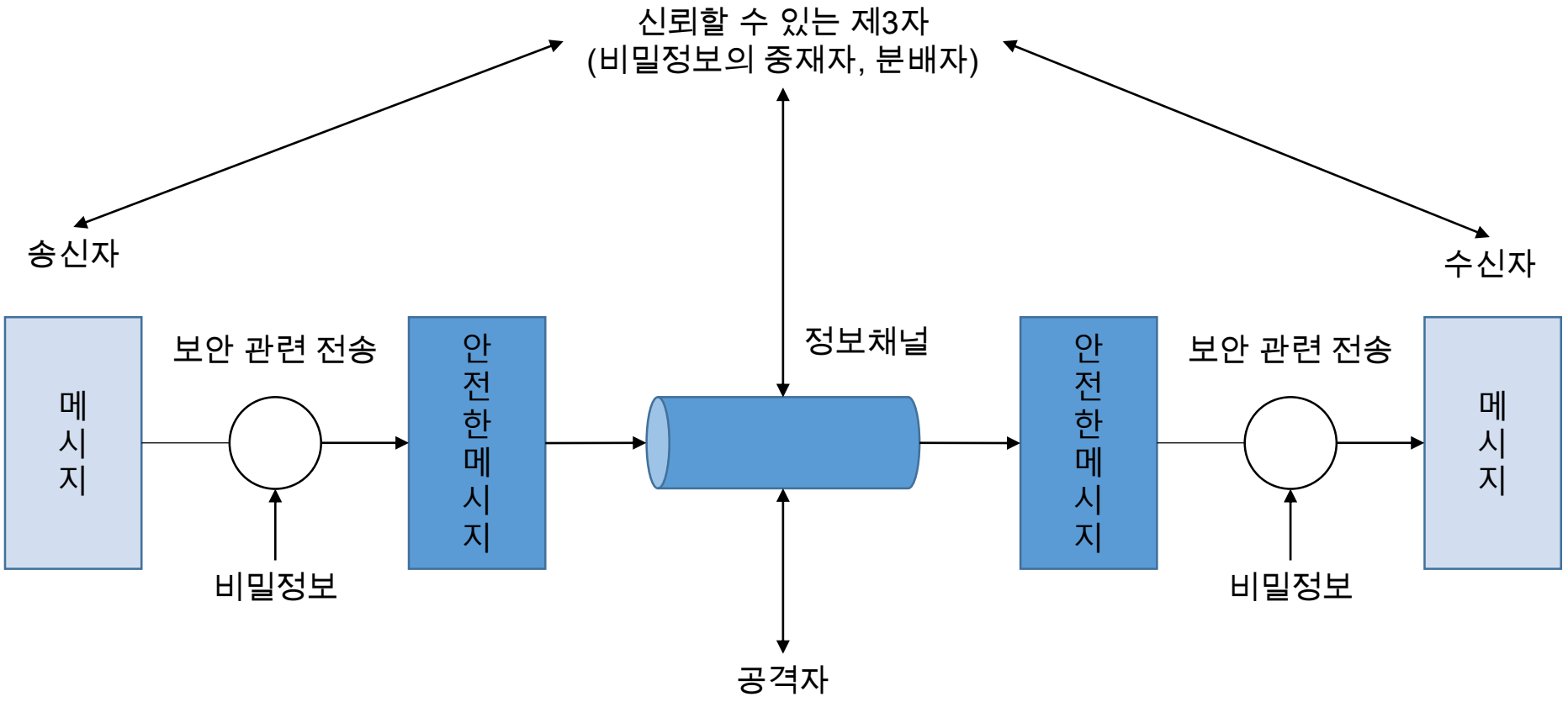
- 특정 보안 메커니즘 (Specific Security Mechanism)
  - 종류 (2/2)
    - 인증교환 (Authentication Exchange)
      - 정보교환을 통해 개체의 신원을 확인하는 데 사용하는 것
    - 트래픽 패딩 (Traffic Padding)
      - 트래픽 분석 시도를 방해하기 위해 데이터 스트림 안의 빈 곳에 비트를 채워 넣는 것
    - 경로 제어 (Routing Control)
      - 특정 데이터에 대해 물리적으로 안전한 경로를 선택할 수 있도록 하는 것
    - 공증 (Notarization)
      - 신뢰할 수 있는 제3자를 통해 데이터 교환의 무결성, 출처, 목적지 등의 특성들을 보증하는 것

# 보안 메커니즘

- 일반 보안 메커니즘 (Pervasive Security Mechanism)
  - 종류
    - 신뢰 기능 (Trusted Functionality)
      - 보안 메커니즘에 대한 정보를 제공하며 다른 메커니즘의 범위를 확장하거나 효과를 확고히하는 데 사용되는 메커니즘
    - 보안 레이블 (Security Label)
      - 자원에 대한 보안속성을 표시하는 메커니즘
        - e.g., 민감도 수준
    - 사건 탐지 (Event Detection)
      - 보안 관련 사건을 탐지하는 메커니즘
    - 보안 감사 추적 (Security Audit Trail)
      - 보안 감사를 하기 위해 수집하거나 이용되는 데이터로써 시스템 기록과 동작을 독립적으로 조사하고 검토하는 메커니즘
    - 보안 복구 (Security Recovery)
      - 사건처리와 관리기능 같은 메커니즘의 요구사항을 다루고 복구 동작을 수행하는 메커니즘

# 네트워크 보안 모델

- 일반적인 모델
  - 정의
    - 네트워크를 통해 통신주체 사이에 메시지가 안전하게 공유되도록 설계된 모델



# 네트워크 보안 모델

- 정보 채널
  - 양 통신주체는 통신 프로토콜(TCP/IP)을 사용하기로 협의하여 논리적 정보 채널을 구성해야 함

- 보안 관련 전송
  - 보안을 위해 전송될 정보를 변환하여 암호화, 신원 확인을 위한 코드를 메시지에 첨부
  - 양 통신주체는 비밀정보를 공유함

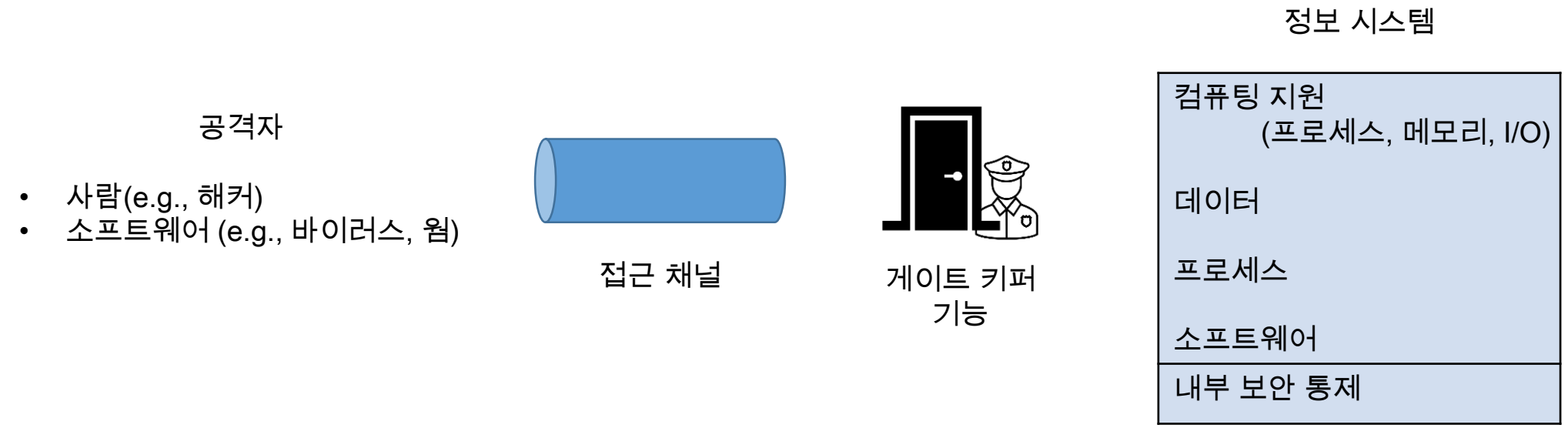
# 네트워크 보안 모델

- 신뢰할 수 있는 제3자
  - 공격자가 모르는 비밀정보를 두 송신 주체에게 책임지고 전달하는 임무를 가짐
  - 메시지 전송의 인증에 있어서 양쪽 통신 주체 간 분쟁이 발생할 경우 조정자 역할을 함

- 보안 모델 사용을 위한 4가지 기초적인 임무
  - 보안을 위해 변환을 수행할 알고리즘 설계
  - 알고리즘에서 사용할 비밀 정보(key)를 생성
  - 비밀 정보를 공유하고 배분할 수 있는 방법을 개발
  - 보안 알고리즘 및 비밀 정보를 사용할 수 있도록 양쪽 통신 주체가 사용할 프로토콜 지정

# 네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 정의
    - 공격자의 접근 가능성이 있는 정보 시스템을 보호하도록 설계된 모델



# 네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 공격자 유형
    - 해커 (Hacker)
      - 시스템에 침투하는 데에만 목적을 둔 개체
    - 침입자(Intruder)
      - 시스템에 손상을 입히거나 악의적 목적 달성을 위해 정보를 시스템에서 취득하려는 개체
    - 위협의 유형
      - 정보 접근 위협 (Information Access Threats)
        - 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정해서 그 사용자 자신에게 유리하도록 만드는 위협
      - 서비스 위협 (Service Threats)
        - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협

# 네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 소프트웨어 공격의 사례
    - 바이러스 (Virus)
      - 정상 파일을 감염시키는 형태로 실행됨
      - 감염시킬 대상이 존재하지 않을 때에는 실행되지 않음
      - 네트워크를 통해 전파되지 않음
    - 웜 (Worm)
      - 감염시킬 대상이 존재하지 않아도 스스로 실행됨
      - 자가 복제 및 네트워크를 통한 전파 가능성이 있음

# 네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 불법 침입 문제의 보안 방법
    - 케이트키퍼 (Gate Keeper)
      - 로그인 과정을 이용해서 인가되지 않은 사용자를 가려내고 접근을 통제하는 것
      - 감독 및 심사 구조를 통해 웜, 바이러스 등을 검출하는 것
    - 모니터링 (Monitoring)
      - 침입자 검출하기 위한 내부적 보안 제어
        - e.g., 컴퓨터 동작 모니터링, 저장된 정보분석

# Thanks!

이 태 양 (taeyang2.lee@gmail.com)