

# Network Security Essentials

## - CHAPTER 1 개요 -

손 우 영([wooyoungson79@naver.com](mailto:wooyoungson79@naver.com))

세종대학교 프로토콜공학연구실

# 목 차

---

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

# 컴퓨터 보안 개념

- 컴퓨터 보안

- 정의

- 정보 시스템 자원의 무결성, 가용성, 기밀성을 보전하기 위해 제공된 정보 시스템 보호
  - 정보 시스템
    - 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)

- 인가된 사용자만 정보 자산에 접근할 수 있는 것

- 데이터 기밀성(Data confidentiality)

- 부정한 사용자에게 개인 정보나 기밀 정보가 노출되지 않도록 하는 것

- 프라이버시(Privacy)

- 개인이 자신과 관련된 어떤 정보가 수집되고 저장되는지, 누구에게 그 정보가 공개되는지, 누가 공개하는지 등을 통제하거나 영향을 미칠 수 있는 것

- 특성

- 정보 접근과 공개에 대해 합법적인 제한 조건을 지키는 것

- 기밀성을 상실하게 되면 정보가 부정하게 공개됨

# 컴퓨터 보안 개념

---

- 컴퓨터 보안

- 3가지 주요 목표(2/3)

- 무결성(Integrity)

- 인가되지 않은 사용자와 개체로부터 데이터의 정확성과 일관성을 보호하는 것
      - 데이터 무결성(Data integrity)
        - 허가된 상태에서만 정보나 프로그램을 변경할 수 있도록 하는 것
      - 시스템 무결성(System integrity)
        - 시스템이 부정하게 조작되지 않고 의도했던 기능이 손상되지 않은 채 그 대로 수행하는 것

- 특성

- 부적절한 정보 수정이나 정보 파괴를 막는 것
    - 무결성을 상실하게 되면 정보가 무단으로 수정되거나 파괴됨

# 컴퓨터 보안 개념

---

- 컴퓨터 보안

- 3가지 주요 목표(3/3)

- 가용성(Availability)

- 시스템이 지체 없이 동작하는 것
    - 합법적인 사용자에게 서비스를 거절하지 않도록 하는 것

- 특성

- 정보 사용에 있어서 시간성과 신뢰성 있는 접근을 할 수 있도록 함
    - 가용성을 상실하게 되면 정보나 정보 시스템을 사용하거나 접근이 불가능 함

# 컴퓨터 보안 개념

---

- 컴퓨터 보안

- 보안 실무 필드에서 필요한 개념

- 인증성(Authenticity)

- 진짜라는 성질을 확인할 수 있고 신뢰할 수 있다는 것
      - 사용자가 정말 그 사용자인지 확인하는 것
      - 메시지와 자료가 정말로 신뢰할 수 있는 출처에서 온 것인지 확인하는 것

- 책임성(Accountability)

- 보안 침해의 책임이 있는 곳까지 보안 침해의 활동 상황을 기록, 포렌식 분석, 추적하고 전송과 관련된 분쟁을 해결할 수 있다는 것
      - e.g., 부인 봉쇄, 억제, 결함 분리, 침입 탐지 및 예방, 사후 복구, 법적인 조치

# 컴퓨터 보안 개념

---

- 컴퓨터 보안

- 보안 침해의 수준

- 저급 위험

- 주요 기능을 그대로 유지할 수는 있지만 어느 기간 동안 성능이 떨어지는 제한된 부정적 효과를 줌

- 중급 위험

- 특정 기간 동안 성능이 심각하게 저하되는 심각한 부정적 효과를 줌

- 고 위험

- 수행하는 주요 기능 중 한두 가지 기능을 상실하여 특정 기간 동안 성능이 극심하게 저하되는 재난 수준의 부정적 효과를 줌

# OSI 보안 구조

---

- OSI 보안 구조

- OSI(Open System Interconnection)

- 정의

- 다른 기종 간에도 문제 없이 데이터를 송수신하고 새로운 기술을 적용하는 등과 같은 상호 호환성과 확장성을 제공하기 위한 네트워크의 기본 구조

- 특징

- 물리, 데이터 링크, 네트워크, 전송, 세션, 표현, 응용 계층 순으로 7계층을 이룸

# OSI 보안 구조

---

- 정의

- 관리자가 효과적으로 보안 문제를 조직화 할 수 있는 유용한 방법

- OSI 보안 구조의 핵심

- 보안 공격(Security attack)
  - 정보의 안전성을 침해하는 제반 행위
- 보안 메커니즘(Security mechanism)
  - 보안 공격을 탐지, 예방하거나 공격으로 인한 침해를 복구하는 절차 또는 이런 절차를 처리하는 장치
- 보안 서비스(Security service)
  - 정보 전송과 데이터 처리 시스템의 보안을 강화하기 위한 처리 서비스 또는 통신 서비스
  - 보안 공격에 대응하기 위한 것
  - 하나 이상의 보안 메커니즘을 사용하여 서비스를 제공

# 보안 공격

---

- 위협과 공격

- 위협

- 보안 취약점을 이용하려는 잠재적인 위협
  - e.g., 보안에 침해와 위해를 가할 수 있는 환경, 능력, 행동, 사건

- 공격

- 지적인 위협을 수반하는 시스템 보안에 대한 침범
  - 지적인 위협
    - 보안 서비스를 교묘히 피하는 것
    - 시스템 보안 정책을 위반하는 정교한 시도

# 보안 공격

---

- 보안 공격의 분류(1/2)

- 소극적 공격(Passive attack)

- 정의

- 시스템으로부터 정보를 획득하거나 사용하려는 시도
    - 시스템 자원에는 영향을 끼치지 않는 공격 형태

- 특징

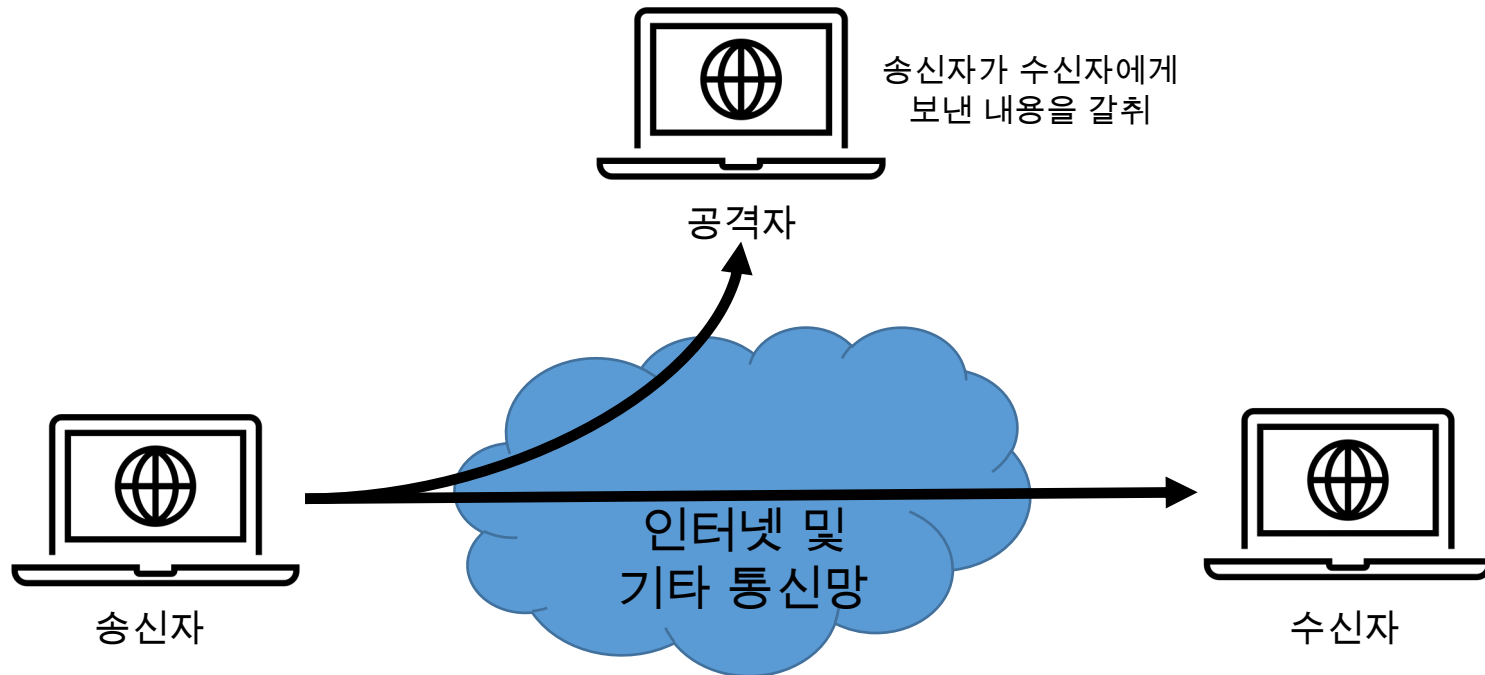
- 정보 전송에 대한 도청이나 감시
    - 전송 중인 정보를 취득하는 것이 목표
    - 공격자가 데이터를 변경하지 않기 때문에 공격을 탐지하기 어려우므로 탐지보다는 예방에 더 신경 써야 함

- 유형

- 메시지 내용 갈취(Release of message contents)
    - 트래픽 분석(Traffic analysis)

# 보안 공격

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



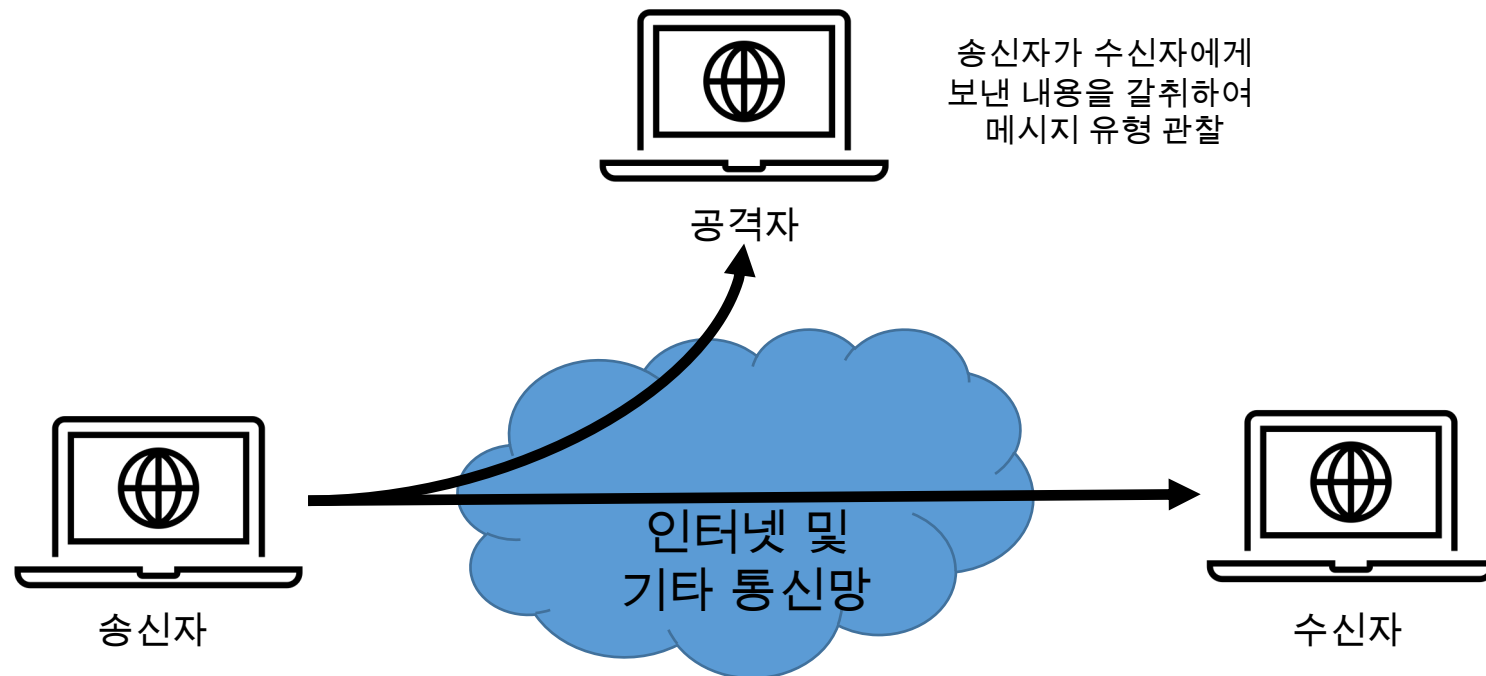
# 보안 공격

- 보안 공격의 분류(1/2)

- 소극적 공격(2/2)

- 트래픽 분석(Traffic analysis)

- 메시지 유형을 관찰하여 통신자의 통신 특성을 추측하는 것
      - 통신자의 접속 위치나 신원을 파악하거나 교환되는 메시지의 빈도와 길이 등을 관찰함



# 보안 공격

---

- 보안 공격의 분류(2/2)

- 적극적 공격(Active attack)

- 정의

- 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격

- 특징

- 적극적 공격을 완벽하게 차단하는 것은 불가능
    - 공격을 탐지하고 이로 인한 재전송이나 피해를 복구하는 것이 목표

- 유형

- 신분 위장(Masquerade)
    - 재전송(Replay)
    - 메시지 수정(Modification of message)
    - 서비스 거부(Denial of service)

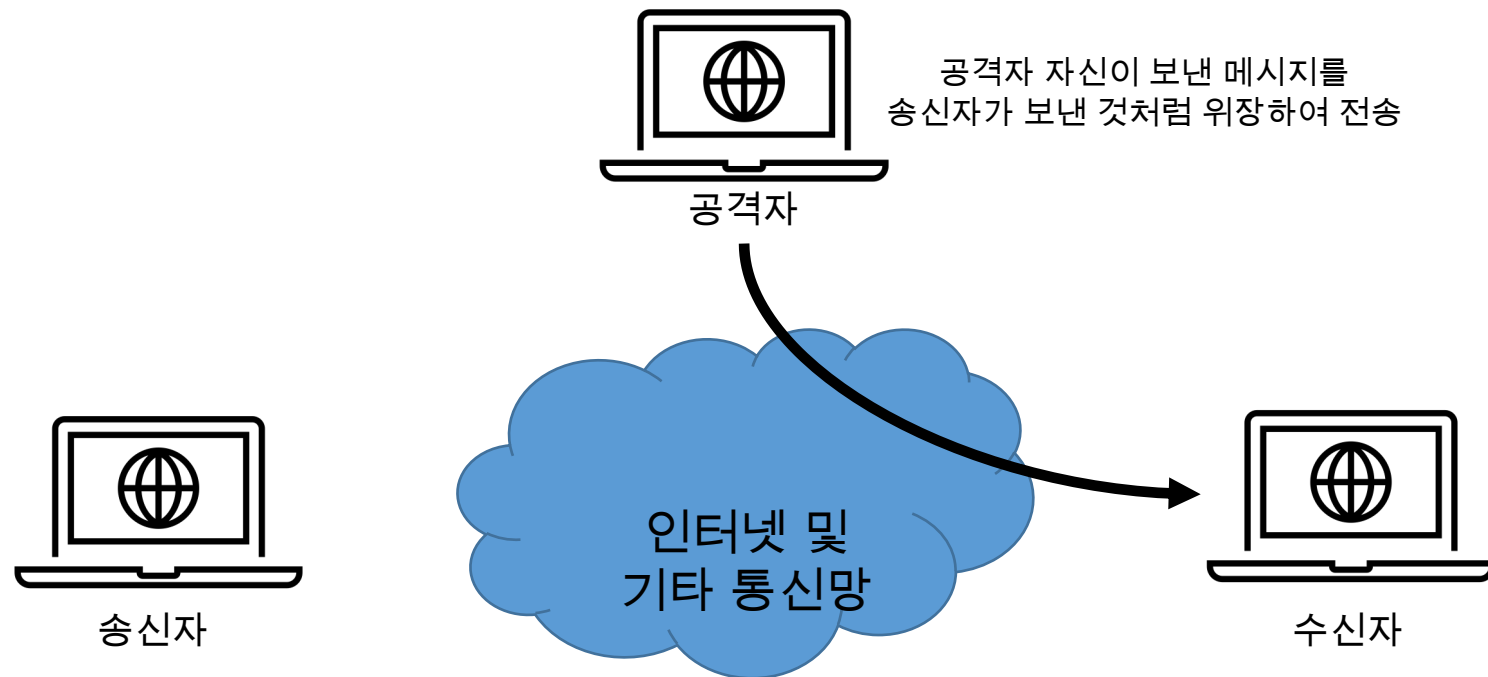
# 보안 공격

- 보안 공격의 분류(2/2)

- 적극적 공격(1/4)

- 신분 위장(Masquerade)

- 한 개체가 다른 개체의 행세를 하는 것
    - 다른 형태의 적극적 공격과 병행해서 수행됨



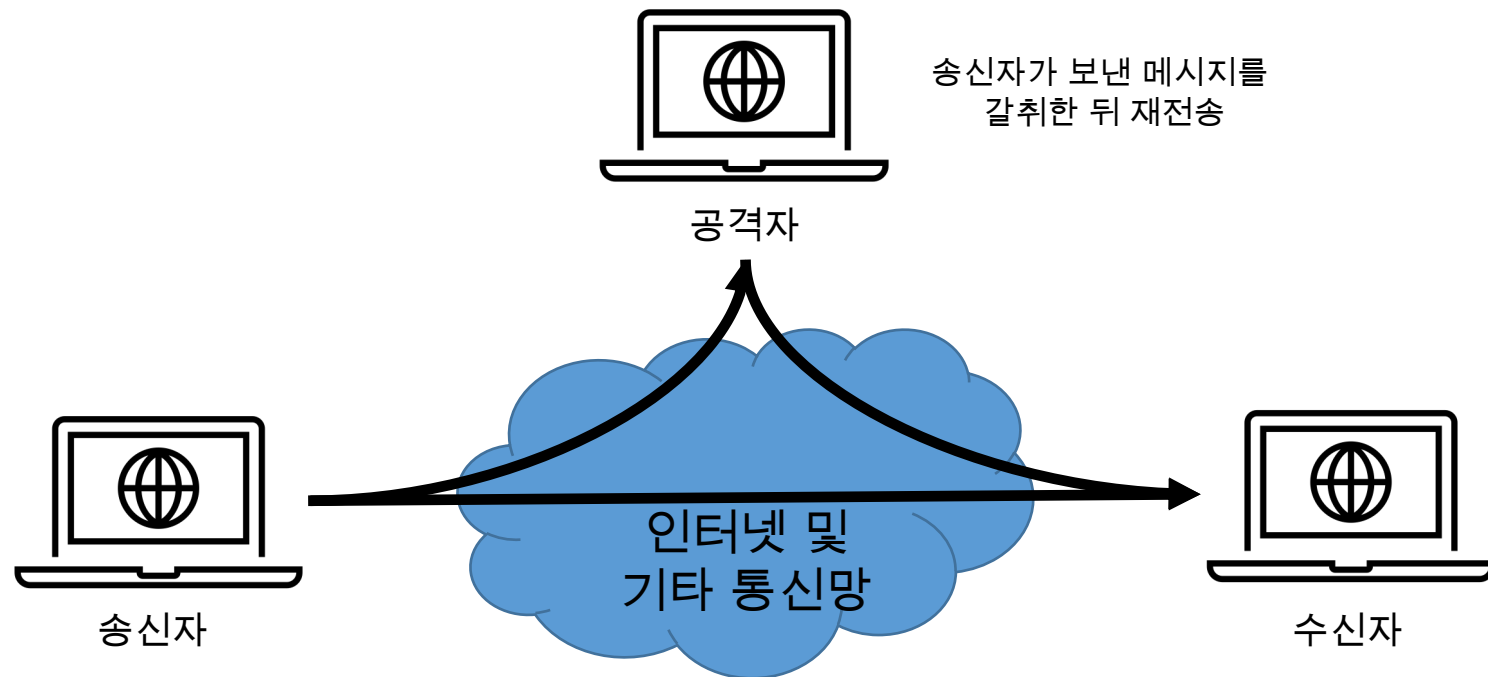
# 보안 공격

- 보안 공격의 분류(2/2)

- 적극적 공격(2/4)

- 재전송(Replay)

- 획득한 데이터 단위를 보관하고 있다가 시간이 경과한 후에 재전송을 함으로써 인가되지 않은 사항에 접근하는 행위



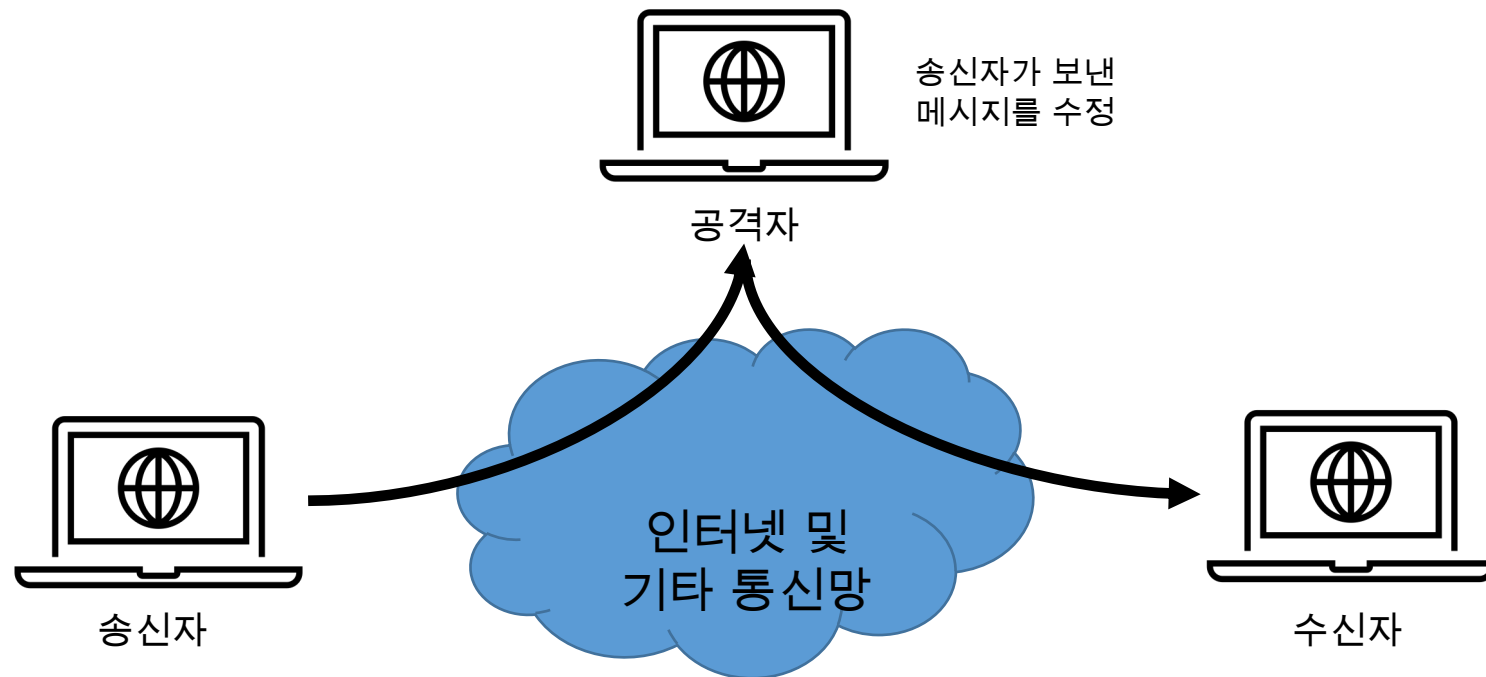
# 보안 공격

- 보안 공격의 분류(2/2)

- 적극적 공격(3/4)

- 메시지 수정(Modification of message)

- 적법한 메시지의 일부를 불법으로 수정하거나 메시지 전송을 지연시키거나 순서를 뒤바꾸어서 인가되지 않은 효과를 노리는 행위



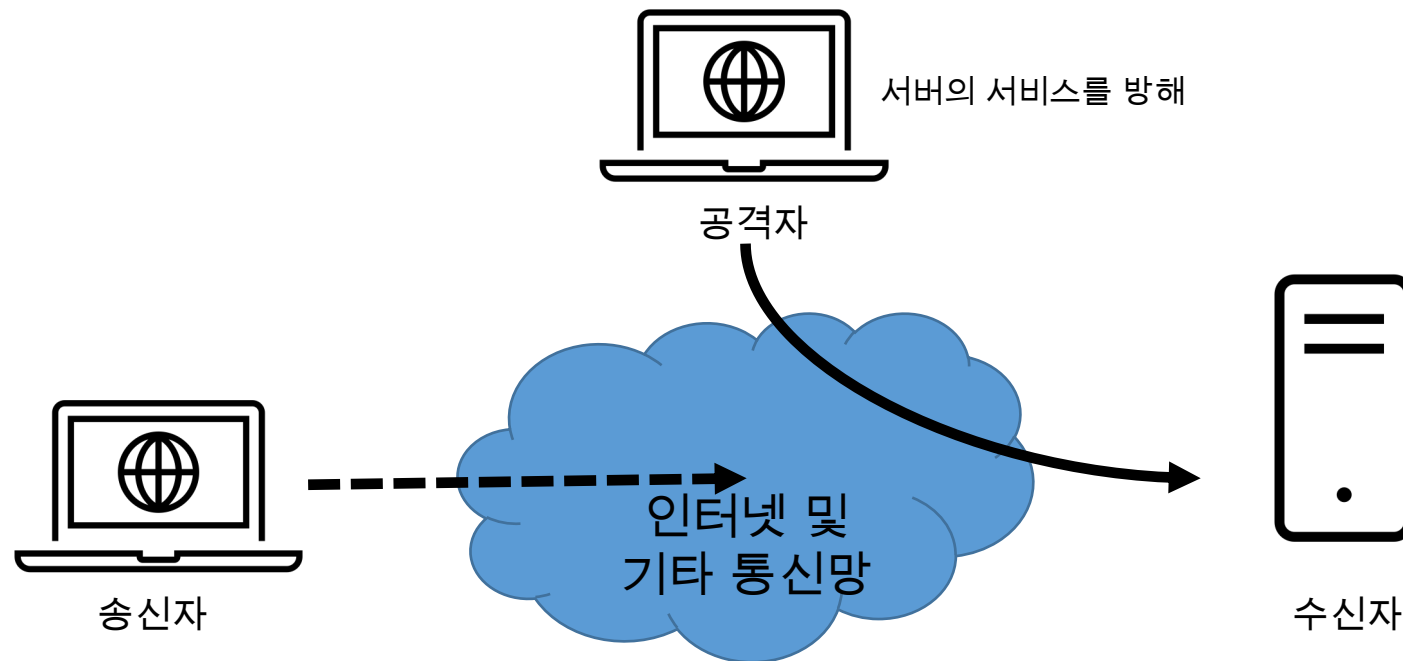
# 보안 공격

- 보안 공격의 분류(2/2)

- 적극적 공격(4/4)

- 서비스 거부(Denial of service)

- 통신 설비가 정상적으로 운용되거나 관리되지 못하도록 방해하는 행위
    - 특정 목표물을 대상으로 할 수 있음



# 보안 서비스

- 정의

- 시스템의 보안이나 데이터 전송의 보안을 보장하기 위해 제공되는 서비스
- 보안 서비스는 보안 정책을 구현하며 보안 메커니즘에 의해 구현됨



# 보안 서비스

---

- 보안 서비스의 분류(1/6)
  - 인증 서비스(Authentication service)
    - 통신이 검증되었다는 것을 확인해주는 것
    - 대등 개체 인증(Peer entity authentication)
      - 통신하는 상대방의 신원을 확인시켜 줌
      - 연결 설정 및 데이터 전송 과정에서 사용
    - 데이터 출처 인증(Data origin authentication)
      - 데이터 단위의 출처를 확인시켜 줌
      - 이메일 같은 비연결형 전송에서 사용됨

# 보안 서비스

---

- 보안 서비스의 분류(2/6)
  - 접근 통제(Access control)
    - 통신 링크를 통한 호스트 시스템과 응용 간의 접근을 제한하고 통제할 수 있는 능력
      - 누가, 어떤 조건하에, 어떤 자원을 사용하도록 하는지와 같은 자원에 대한 접근을 제한
- 보안 시스템의 분류(3/6)
  - 데이터 기밀성(Data confidentiality)
    - 소극적 공격으로부터 데이터를 보호하는 것
    - 트래픽 흐름을 보호하는 것

# 보안 서비스

---

- 보안 서비스의 분류(4/6)
  - 데이터 무결성(Data integrity)
    - 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신을 주는 것
    - 연결형 무결성 서비스
      - 연결 시 사용자의 데이터의 무결성을 제공
      - 메시지 스트림의 수정과 서비스 거부 모두에 대해서 보호 서비스를 제공
    - 비연결형 무결성 서비스
      - 작은 단위 메시지 수정에 대해서만 보호 서비스를 제공

# 보안 서비스

---

- 보안 서비스의 분류(5/6)

- 부인 봉쇄(Nonrepudiation)

- 통신의 주체가 통신에 참여했던 사실을 부인하는 것을 방지
  - 수신자는 송신자로부터 송신된 메시지임을 확신함
  - 송신자는 메시지가 수신자에 의해 수신되었음을 확신함

- 보안 서비스의 분류(6/6)

- 가용성 서비스(Availability service)

- 시스템의 가용성을 보장하기 위해 시스템을 보호하는 서비스

# 보안 메커니즘

---

- 정의

- 보안 서비스를 구현하는데 사용되는 기술적 도구
- 보안 공격을 탐지, 예방하거나 공격으로 인한 피해를 복구하는 절차나 장치

- 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
    - 암호화(Encipherment)
      - 수학적 알고리즘을 사용하여 데이터를 읽을 수 없는 형태로 변환하는 것
      - 데이터를 변환하고 복구하는 것은 알고리즘과 사용되는 키에 따라 달라짐
    - 디지털 서명(Digital signature)
      - 데이터 수신자가 데이터의 발신자와 무결성을 입증하기 위한 것
      - 위조를 막도록 데이터에 붙이는 데이터나 데이터 단위의 암호적 변경
    - 접근 통제(Access control)
      - 자원에 접근할 권한을 제한하는 다양한 메커니즘
    - 데이터 무결성(Data integrity)
      - 데이터의 무결성을 확인하는데 사용되는 다양한 메커니즘

# 보안 메커니즘

---

- 특정 보안 메커니즘(Specific Security Mechanism)

- 종류

- 인증 교환(Authentication exchange)
  - 정보 교환을 통해 개체의 신원을 확인하는 데 사용하는 메커니즘
- 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 함
- 공증(Notarization)
  - 신뢰받는 제 3자를 이용하여 데이터 교환의 성질을 확신하기 위한 것

# 보안 메커니즘

---

- 일반 보안 메커니즘(Pervasive security mechanism)

- 종류

- 신뢰받는 기능(Trusted functionality)
  - 보안정책과 같은 기준으로 볼 때 올바른 것으로 여겨지는 것
- 보안 레이블(Security label)
  - 자원에 대한 보안속성을 지정하는 것
- 사건 탐지(Event detection)
  - 보안 관련 사건을 탐지하는 것
- 보안 감사 추적(Security audit trail)
  - 보안 감사를 하기 위해 수집하거나 이용되는 데이터로서 시스템 기록과 동작을 독립적으로 조사하고 검토하는 것
- 보안 복구(Security recovery)
  - 사건 처리와 관리 기능 같은 메커니즘의 요구사항을 다루고 복구 동작을 수행하는 것

# 공격 대상과 공격 트리

---

- 공격 대상(Attack surfaces)

- 정의

- 시스템의 접근이 가능하고, 악용할 수 있는 취약점

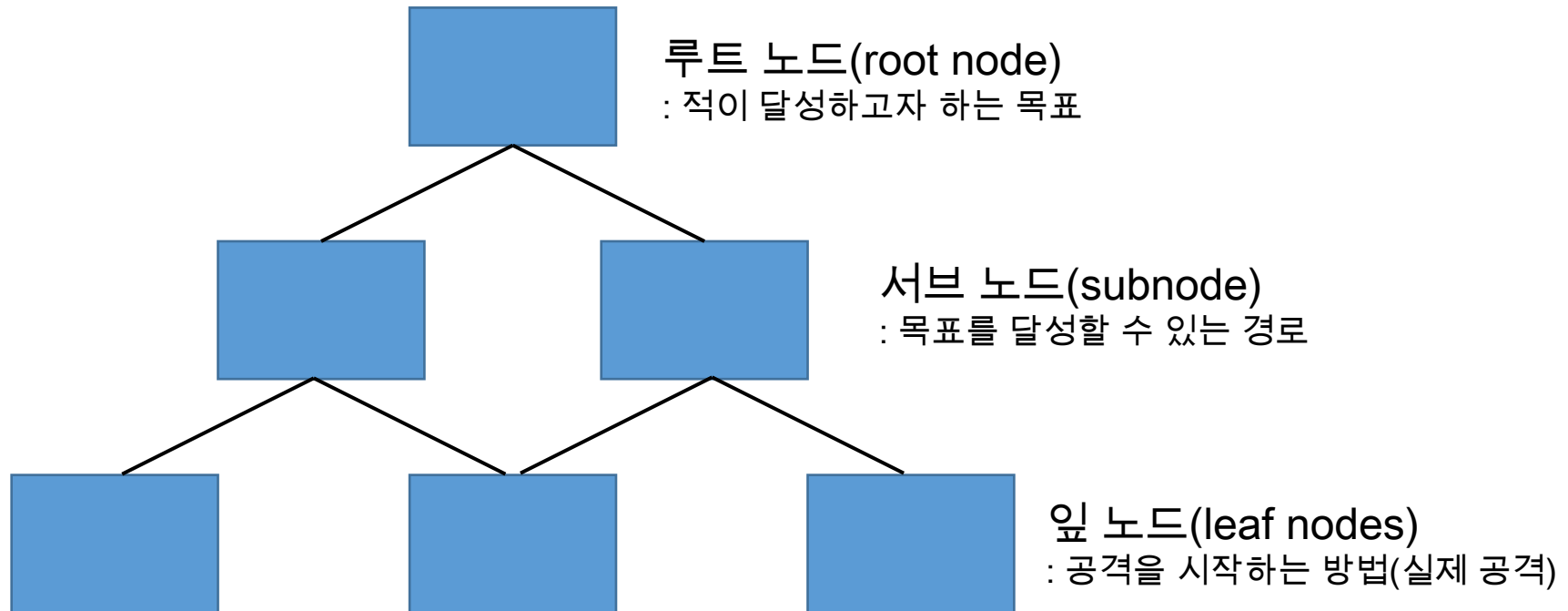
- e.g., 웹에 연결된 개방된 포트, 공격에 취약한 민감 정보에 접근 권한을 가진 직원

- 분류

- 네트워크 공격 대상(Network attack surface)
    - 소프트웨어 공격 대상(Software attack surface)
    - 인적 공격 대상(Human attack surface)

# 공격 대상과 공격 트리

- 공격 트리(Attack trees)
- 보안 취약점을 악용하는 데 사용할 수 있는 기법을 보여주기 위한 브랜치(branches) 및 계층적 데이터 구조

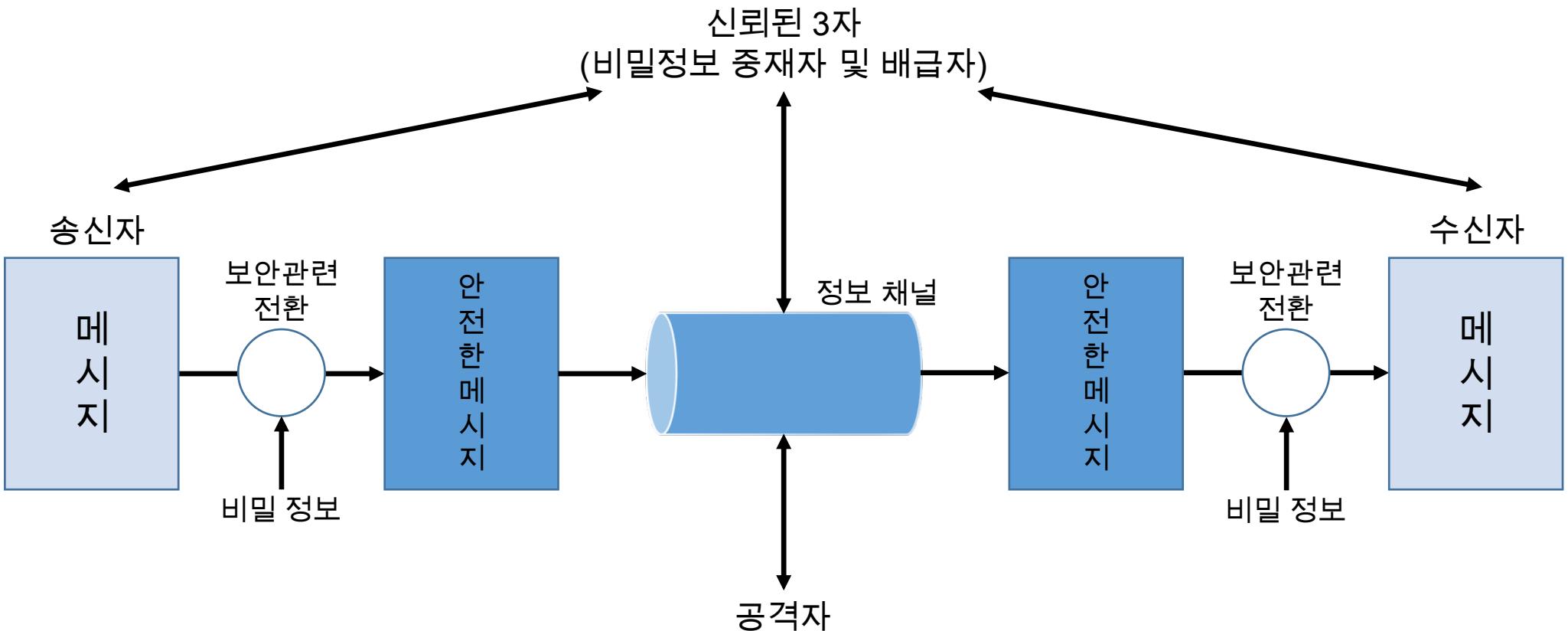


# 네트워크 보안 모델

- 일반적인 모델

- 정의

- 통신주체 사이에서 메시지가 안전하게 전송되도록 하기 위해 설계된 모델



# 네트워크 보안 모델

---

- 정보 채널

- 통신주체로서의 양쪽은 통신 프로토콜(TCP/IP)을 사용하기로 합의하여 논리적 정보 채널을 구성해야 함

- 보안 조치

- 보안을 위해서 전송될 정보를 변환해야 함
  - e.g., 메시지 암호화
  - e.g., 송신자의 신원 확인을 위해 메시지에 코드를 첨부
- 통신주체는 비밀 정보를 공유함
  - e.g., 암호 키

# 네트워크 보안 모델

---

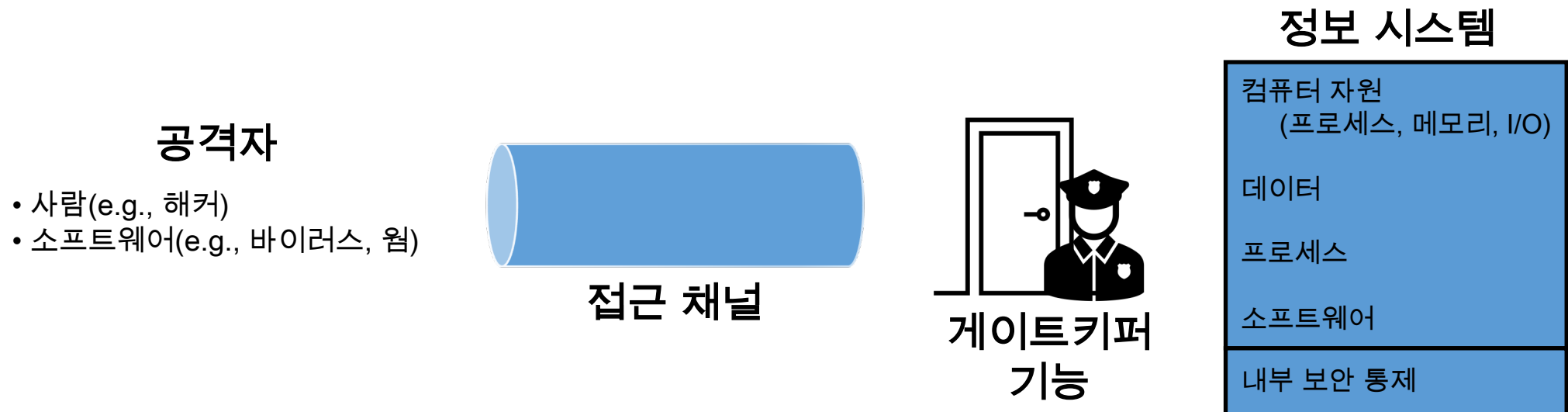
- 신뢰할 수 있는 제 3자
  - 공격자가 모르는 비밀 정보를 두 송신 주체에게 책임지고 전달하는 의무를 가짐
  - 메시지 전송의 인증에 있어서 양쪽 통신 주체 간 분쟁이 발생할 경우 조정자 역할을 함
- 네트워크 보안 모델 설계를 위한 4가지 기초 임무
  - 보안을 위한 변환을 수행할 알고리즘을 설계함
  - 알고리즘에서 사용될 비밀 정보 생성
  - 비밀 정보를 공유하고 배분할 수 있는 방법 개발
  - 보안 알고리즘 및 비밀 정보를 사용하기 위해 양쪽 통신 주체가 사용할 프로토콜 구체화

# 네트워크 보안 모델

## • 네트워크 접근 보안 모델

### • 정의

- 침입자로부터 정보 시스템을 보호할 목적으로 만들어진 모델



# 네트워크 보안 모델

---

- 네트워크 접근 보안 모델

- 공격자

- 해커(Hacker)

- 시스템을 깰 수 있다는 자기 만족을 위해서 침입을 시도하는 공격자

- 침입자(Intruder)

- 손해를 끼칠 의도가 있거나 경제적 이득을 노리는 공격자

- 프로그램의 위협 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 공격
    - 유형
      - 바이러스(Virus)
      - 웜(Worm)
    - 공격 방법
      - 유용한 소프트웨어에다 악성 로직을 잠복시켜 놓아서 그 소프트웨어를 시스템에 깔면 시스템이 감염됨

# 네트워크 보안 모델

---

- 네트워크 접근 보안 모델
  - 불법 침입 문제에서의 보안 메커니즘
    - 게이트키퍼(Gatekeeper)
      - 로그인 과정을 이용해서 인가받지 않은 사용자를 가려내고, 공격을 탐지하여 제거하는 것
    - 모니터링(Monitoring)
      - 침입자가 있었는지 탐지하기 위해 컴퓨터 동작을 모니터링하고 저장된 정보를 분석함

---

# Thanks!

손 우 영 ([wooyoungson79@naver.com](mailto:wooyoungson79@naver.com))