2023/01/16, 2023 겨울방학 보안기초 세미나

Network Security Essentials

- Chapter_1 개요 -

김 지 혜(jihye@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

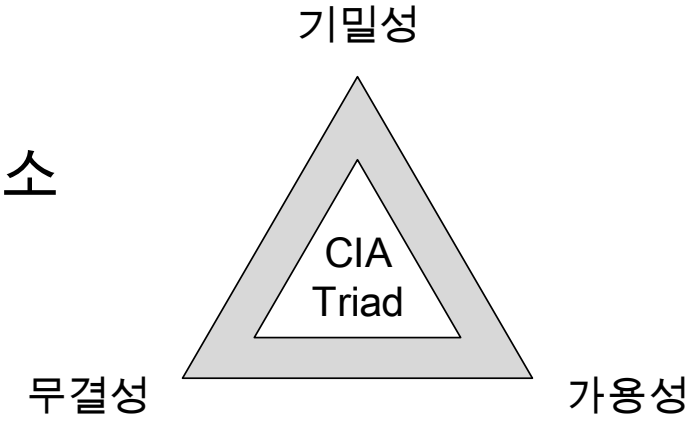
목 차

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

목 차

컴퓨터 보안 개념

- 컴퓨터 보안
  - 정의
    - 정보 시스템 자원의 기밀성, 무결성, 가용성 유지를 위해 시스템에 제공되는 보호 기능
      - e.g., 하드웨어, 소프트웨어, 펌웨어, 정보/데이터, 통신
  - CIA Triad
    - 기밀성(Confidentiality)
      - 정보의 노출 및 유출 여부를 확인하는 요소
    - 무결성(Integrity)
      - 정보의 변조 여부를 확인하는 요소
    - 가용성(Availability)
      - 정보 사용에 대한 지체 여부를 확인하는 요소



컴퓨터 보안 개념

- 컴퓨터 보안
  - 핵심 보안 요소

보안 요소	정의	특징
기밀성 (Confidentiality)	• 인가된 사용자만 정보 접근이 가능해야 함을 의미	• 접근 제어, 암호화 등의 보안 기술로 기밀성 보장 가능 • 개인 정보 및 기밀 정보가 유출되는 경우, 기밀성이 침해되었다고 함
무결성 (Integrity)	• 정보가 원본을 유지해야 함을 의미	• 접근 제어, 인증, 침입 탐지, 백업 등의 보안 기술로 무결성 보장 가능 • 비인가된 사용자로부터 정보가 위조/변조되거나 삭제되는 경우, 무결성이 침해되었다고 함
가용성 (Availability)	• 필요 시, 인가된 사용자의 접근 및 정보 사용이 가능해야 함을 의미	• 백업, 중복성 유지 등의 보안 기술로 가용성 보장 가능 • 강력한 보안으로 인해 권한이 부여된 사용자가 시스템을 사용하지 못하는 경우, 가용성이 침해되었다고 함
인증성 (Authentication)	• 접근을 위해 사용자의 신원을 검증할 수 있어야 함을 의미	• 정보 내용 및 출처의 유효성을 검증함으로써, 자료의 신뢰성 확인 가능
책임추적성 (Accountability)	• 사용자의 행동을 추적할 수 있어야 함을 의미	• 시스템은 사용자의 활동 상황을 기록하고, 포렌식 분석을 함으로써 보안 침해에 대한 추적 가능

컴퓨터 보안 개념

- 컴퓨터 보안
  - 보안 위험 수준
    - 공통 취약점 등급 시스템(Common Vulnerability Scoring System) 점수를 기반으로 보안 위험 및 심각도를 평가함
    - 저급 위험(CVSS 0.0 ~ 3.9)
      - 개인 및 조직에게 미칠 제한된 부정적 효과를 줌
      - 주요 기능을 유지하나, 일정 기간 동안 성능이 저하됨
    - 중급 위험(CVSS 4.0 ~ 6.9)
      - 개인 및 조직에게 심각한 부정적 효과를 줌
      - 주요 기능에 있어, 특정 기간 동안 성능이 심각하게 저하됨
    - 고급 위험(CVSS 7.0 ~ 10.0)
      - 개인 및 조직에게 극심한 재난 수준의 부정적 효과를 줌
      - 주요 기능 중 한두 가지 기능을 상실하여, 특정 기간 동안 성능이 극심하게 저하됨

목 차

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

OSI 보안 구조

- OSI(Open Systems Interconnection)
  - 정의
    - 시스템 간 원활한 통신을 위해 국제 표준화 기구(ISO, International Organization for Standardization)에서 개발한 개방형 시스템 상호 연결 모델
  - 계층 구조

계층		역할
1	물리(Physical)	• 장비가 직접 연결되어 데이터 전송
2	데이터 링크(Data Link)	• 데이터의 안전한 전달을 위한 오류 탐지 및 흐름 제어
3	네트워크(Network)	• IP 주소 부여 및 경로 지정
4	전송(Transport)	• 데이터의 용량, 속도, 목적지 등을 처리 및 전송
5	세션(Session)	• 장비 간 통신을 위한 세션 설정
6	표현(Presentation)	• 응용 프로그램을 위한 데이터 표현
7	응용(Application)	• 사용자와 직접 상호작용

7	응용 계층
6	표현 계층
5	세션 계층
4	전송 계층
3	네트워크 계층
2	데이터 링크 계층
1	물리 계층

OSI 보안 구조

- OSI 보안 구조
  - 정의
    - 보안에 필요한 항목을 체계적으로 정의하고, 이를 충족하는 구체적인 접근 방법을 제시하는 구조
  - 특징
    - ITU-T(International Telecommunication Union Telecommunication Standardization Sector) 권고안 X.800에서 정의하고 있는 체계적인 접근 방법
    - 관리자에게 보안 문제 조직화를 위한 효과적인 방법 제공
    - 국제적 표준이므로 제품과 서비스에 보안 규정 적용 및 발전에 활용

OSI 보안 구조

- OSI 보안 구조
  - 핵심 요소
    - 보안 공격(Security Attack)
      - 조직 및 기관 정보의 안전성을 침해하는 모든 행위
    - 보안 메커니즘(Security Mechanism)
      - 보안 공격 탐지, 예방 혹은 침해를 복구하는 절차 및 방법
    - 보안 서비스(Security Service)
      - 조직 및 기관 정보 처리 및 시스템 보안 강화를 위한 서비스
      - 보안 메커니즘을 이용하여 보안 공격에 대응하고자 제공되는 서비스

목 차

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

보안 공격

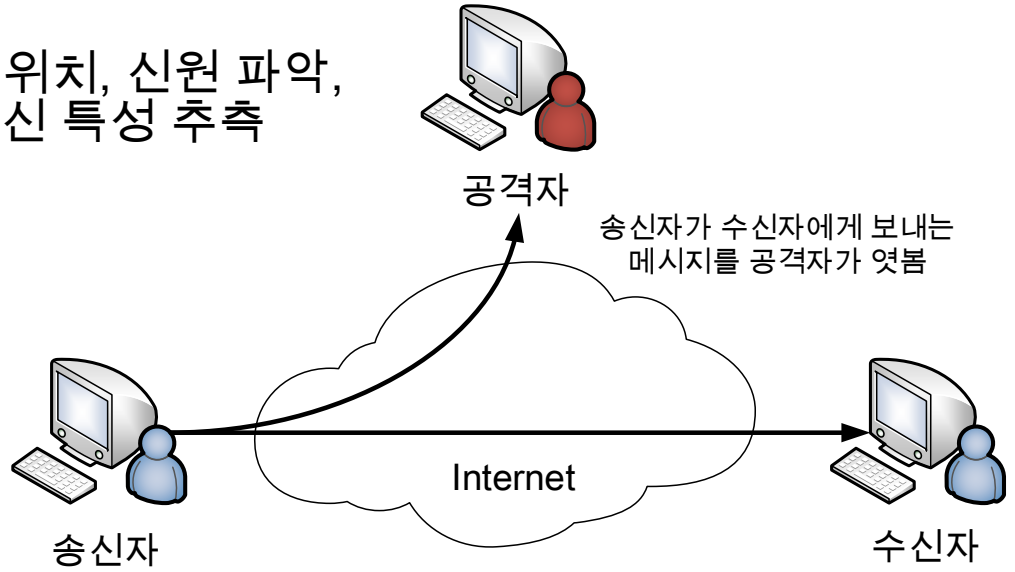
- 용어 설명
  - 위협(Threat)
    - 시스템의 손실 및 피해를 유발할 수 있는 행위
  - 공격(Attack)
    - 시스템의 손실 및 피해를 유발하는 직접적인 침해 행위

보안 공격

- 소극적 공격(Passive Attack)
  - 정의
    - 시스템으로부터 정보 획득하거나 사용하고자 하는 공격
  - 특징
    - 데이터를 변조하지 않아, 시스템 작동에 영향을 미치지 않음
      - e.g., 정보가 유출된 경우, 송수신자에게 피해를 주지만 시스템은 영향을 받지 않음
    - 기밀성을 위협하는 공격임
    - 공격에 대응하기 위하여, 예방에 초점을 두어야 함
      - 공격자가 데이터를 변조하지 않으므로 공격 탐지가 어려움

보안 공격

- 소극적 공격(Passive Attack)
  - 종류
    - 메시지 내용 갈취(Release of Message Contents)
      - 공격자가 수신자에게 전송된 메시지를 몰래 취득하거나 엿보는 공격
        - e.g., 스니핑(Sniffing)
    - 트래픽 분석(Traffic Analysis)
      - 공격자가 수신자에게 전송된 메시지의 유형을 몰래 취득하거나 엿보는 공격
        - e.g., 통신자(송수신자)의 접속 위치, 신원 파악, 메시지 길이 및 빈도를 통한 통신 특성 추측

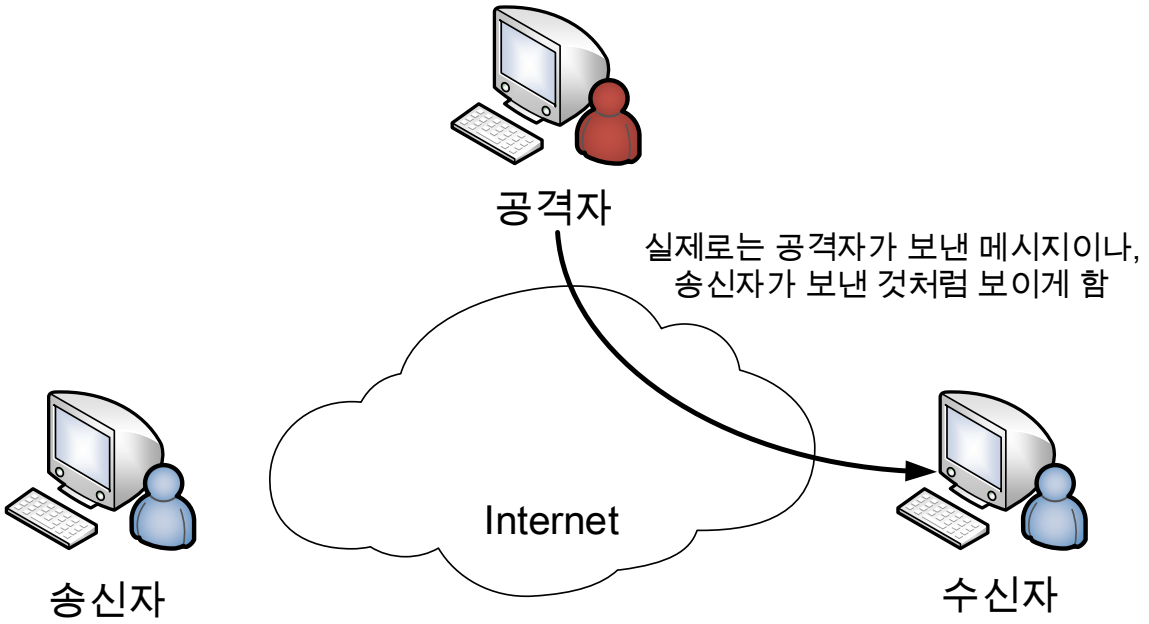


보안 공격

- 적극적 공격(Active Attack)
  - 정의
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 주는 공격
  - 특징
    - 데이터를 변조함에 따라, 시스템 작동에 영향을 미침
      - e.g., 정보가 변조된 경우, 송수신자 및 시스템에 피해를 줌
    - 무결성 및 가용성을 위협하는 공격임
    - 공격에 대응하기 위하여, 공격 탐지 및 피해 복구에 초점을 두어야 함
      - 공격자의 데이터 변조로 인해 공격을 완벽히 차단하기 어려움

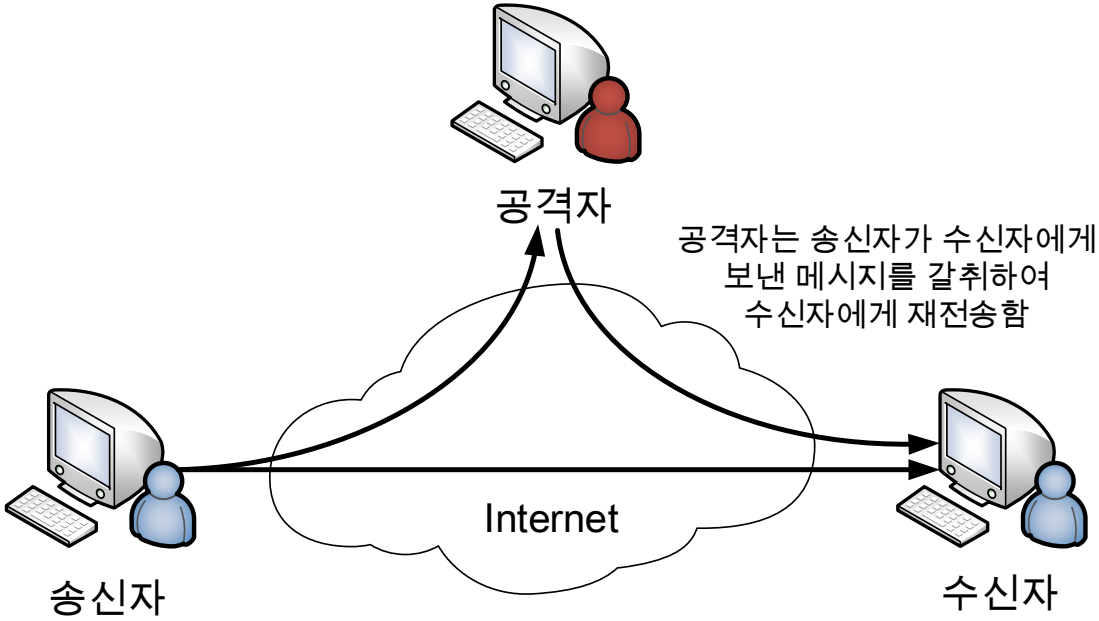
보안 공격

- 적극적 공격(Active Attack)
  - 종류(1/4)
    - 신분위장(Masquerade)
      - 공격자가 송신자로 위장하여 수신자에게 메시지를 전송하는 공격
        - e.g., 사용자가 관리자로 위장하여 기밀 정보를 유출하는 행위



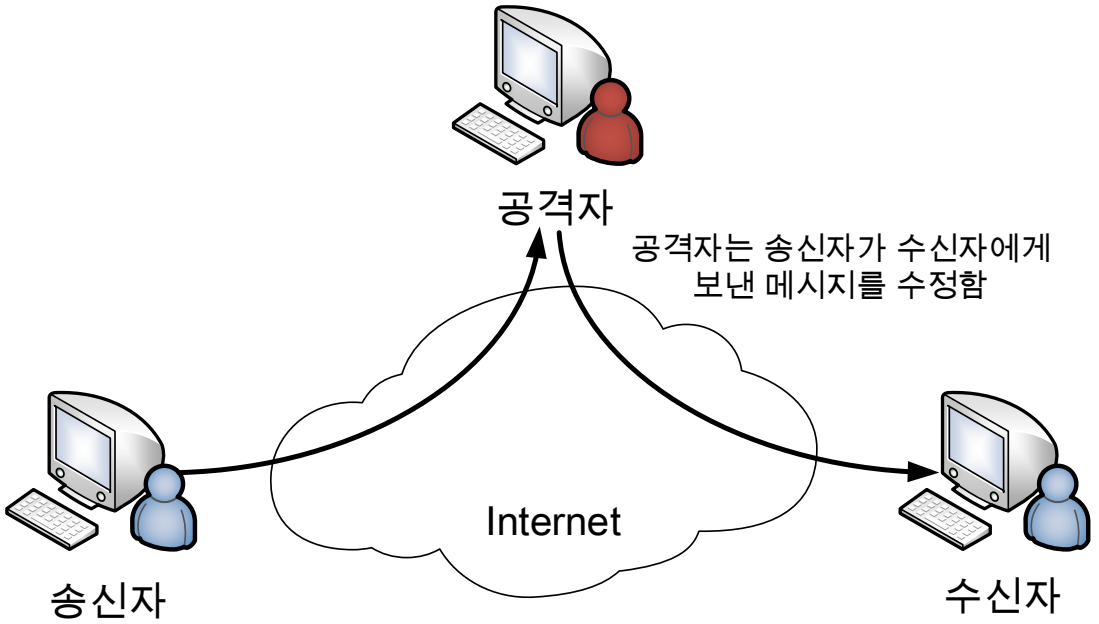
보안 공격

- 적극적 공격(Active Attack)
  - 종류(2/4)
    - 재전송(Replay)
      - 공격자가 수신자에게 전송된 메시지를 보관하고 있다가, 일정 시간 후에 재전송하는 공격
        - e.g., 송신자가 인증 요청한 후, 공격자가 일정 시간 후에 재요청하는 행위



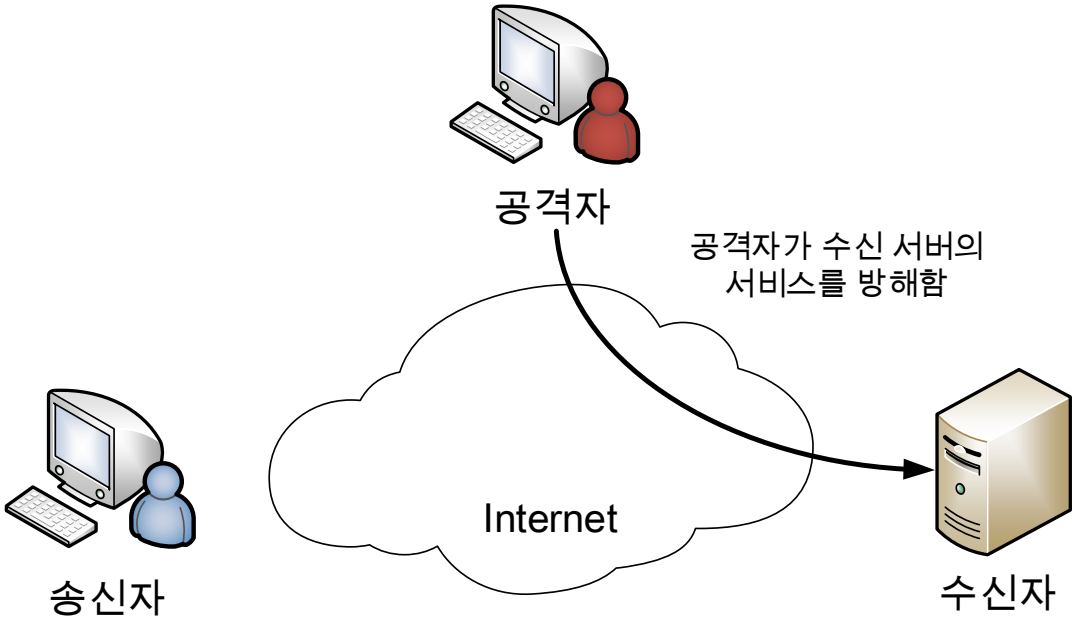
보안 공격

- 적극적 공격(Active Attack)
  - 종류(3/4)
    - 메시지 수정(Modification of Messages)
      - 공격자가 수신자에게 전송하려는 메시지의 일부 수정 및 위변조를 시도하는 공격
        - e.g., 메시지를 불법으로 수정하는 행위, 메시지 전송을 지연하거나 순서를 변경하는 행위



보안 공격

- 적극적 공격(Active Attack)
  - 종류(4/4)
    - 서비스 거부(Denial of Service)
      - 공격자가 특정 장비의 정상 운용 및 관리를 방해하는 공격
        - e.g., 특정 장비로 전송되는 모든 메시지의 전송을 방해하는 행위, 네트워크 마비 및 성능 저하를 위해 대량의 메시지를 전송하는 행위



목 차

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

보안 메커니즘

- 보안 메커니즘(Security Mechanism)
  - 정의
    - 보안 공격 탐지, 예방 혹은 침해를 복구하는 절차 및 방법
  - 종류
    - 특정 보안 메커니즘(Specific Security Mechanism)
      - 통신자의 신원 검증을 위한 보안 메커니즘
    - 일반 보안 메커니즘(Pervasive Security Mechanism)
      - 통신 탐지 및 관리를 위한 메커니즘

보안 메커니즘

- 보안 메커니즘(Security Mechanism)
  - 특정 보안 메커니즘(1/2)
    - 암호화(Encipherment)
      - 데이터를 읽을 수 없는 형태로 변환하는 메커니즘
    - 디지털 서명(Digital Signature)
      - 수신자가 무결성이 입증된 송신자의 데이터에 추가로 데이터를 삽입하는 메커니즘
    - 접근 제어(Access Control)
      - 자원에 대한 접근 권한을 확인한 후, 제어하는 메커니즘
    - 데이터 무결성(Data Integrity)
      - 데이터 변조가 일어나지 않음을 확인하는 메커니즘

보안 메커니즘

- 보안 메커니즘(Security Mechanism)
  - 특정 보안 메커니즘(2/2)
    - 인증 교환(Authentication Exchange)
      - 데이터 교환을 통해 통신자의 신원을 파악하는 메커니즘
    - 트래픽 패딩(Traffic Padding)
      - 트래픽 분석 방해를 위해 데이터 빈 곳에 비트를 채우는 메커니즘
    - 경로 제어(Routing Control)
      - 데이터의 안전한 전송 경로를 선택하는 메커니즘
    - 공증(Notarization)
      - 데이터 교환의 보안을 위해 신뢰된 제3자를 활용하여 증명하는 메커니즘

보안 메커니즘

- 보안 메커니즘(Security Mechanism)
  - 일반 보안 메커니즘
    - 신뢰받는 기능(Trusted Functionality)
      - 보안 정책 기준의 관점에서 올바르게 판단되는 메커니즘
    - 보안 레이블(Security Label)
      - 자원의 보안 속성 지정 및 해당 자원에 대해 표시하는 메커니즘
    - 사건 탐지(Event Detection)
      - 보안 관련 사건에 대해 탐지하는 메커니즘
    - 보안 감사 추적(Security Audit Trail)
      - 데이터를 수집하여 시스템 기록 및 동작에 대해 조사 및 검토하는 메커니즘
    - 보안 복구(Security Recovery)
      - 사건 처리 및 관리 기능 같은 메커니즘 요구사항을 통해 복구 동작을 수행하는 메커니즘

목 차

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

보안 서비스

- 보안 서비스(Security Service)
  - 정의
    - 시스템 및 데이터 전송의 보안을 보장하기 위해 제공되는 서비스
  - 특징
    - 조직 및 기관의 정보 전송 및 정보 처리 시스템 보안 강화를 위한 서비스
    - 보안 메커니즘을 이용하여 보안 공격에 대응하고자 제공되는 서비스

보안 서비스

- 보안 서비스(Security Service)
  - 종류(1/4)
    - 인증 서비스(Authentication Service)
      - 통신자의 신원 확인 및 통신 상태를 검증하는 서비스
        - 암호화, 디지털 서명, 인증 교환 등의 메커니즘 적용
      - 대등 개체 인증(Peer Entity Authentication)
        - 연결된 통신에서 통신자의 신분 검증을 위한 인증 서비스
          - e.g., 신분위장 및 재전송 여부 확인을 위해 사용
      - 데이터 출처 인증(Data-Origin Authentication)
        - 비연결된 통신에서 수신된 데이터의 출처 검증을 위한 인증 서비스
          - e.g., 통신자의 사전 연결 협상이 불필요한 전자메일에 사용
    - 접근 제어 서비스(Access Control Service)
      - 자원의 불법 사용이 불가능하도록 접근을 제한 및 통제하는 서비스
        - 경로 제어 등의 메커니즘 적용

보안 서비스

- 보안 서비스(Security Service)
  - 종류(2/4)
    - 부인봉쇄 서비스(Nonrepudiation Service)
      - 통신자의 데이터 전송 사실 부인을 방지하는 서비스
        - 디지털 서명, 무결성 등의 메커니즘 적용
      - 부인봉쇄, 출처(Nonrepudiation, Origin)
        - 데이터가 특정 출처로부터 송신됨을 증명하는 서비스
      - 부인봉쇄, 목적지(Nonrepudiation, Destination)
        - 특정 개체가 데이터를 수신함을 증명하는 서비스

보안 서비스

- 보안 서비스(Security Service)
  - 종류(3/4)
    - 기밀성 서비스(Confidentiality Service)
      - 데이터 노출 및 유출을 방지하는 서비스
        - 암호화, 트래픽 패딩 등의 메커니즘 적용
      - 연결 기밀성(Connection Confidentiality)
        - 연결 수립 및 유지 시, 연결된 데이터 보호 서비스
      - 비연결 기밀성(Connectionless Confidentiality)
        - 단일 데이터 블록 안의 전체 데이터 보호 서비스
      - 선별된 필드 기밀성(Selective-Field Confidentiality)
        - 선별된 데이터 필드에 대한 보호 서비스
      - 트래픽 흐름 기밀성(Traffic-Flow Confidentiality)
        - 트래픽 흐름 관찰을 통한 데이터 보호 서비스
    - 가용성 서비스(Availability Service)
      - 인가된 통신자의 요구 시, 실시간으로 데이터를 제공하는 서비스
        - 무결성, 인증 교환 등의 메커니즘 적용

보안 서비스

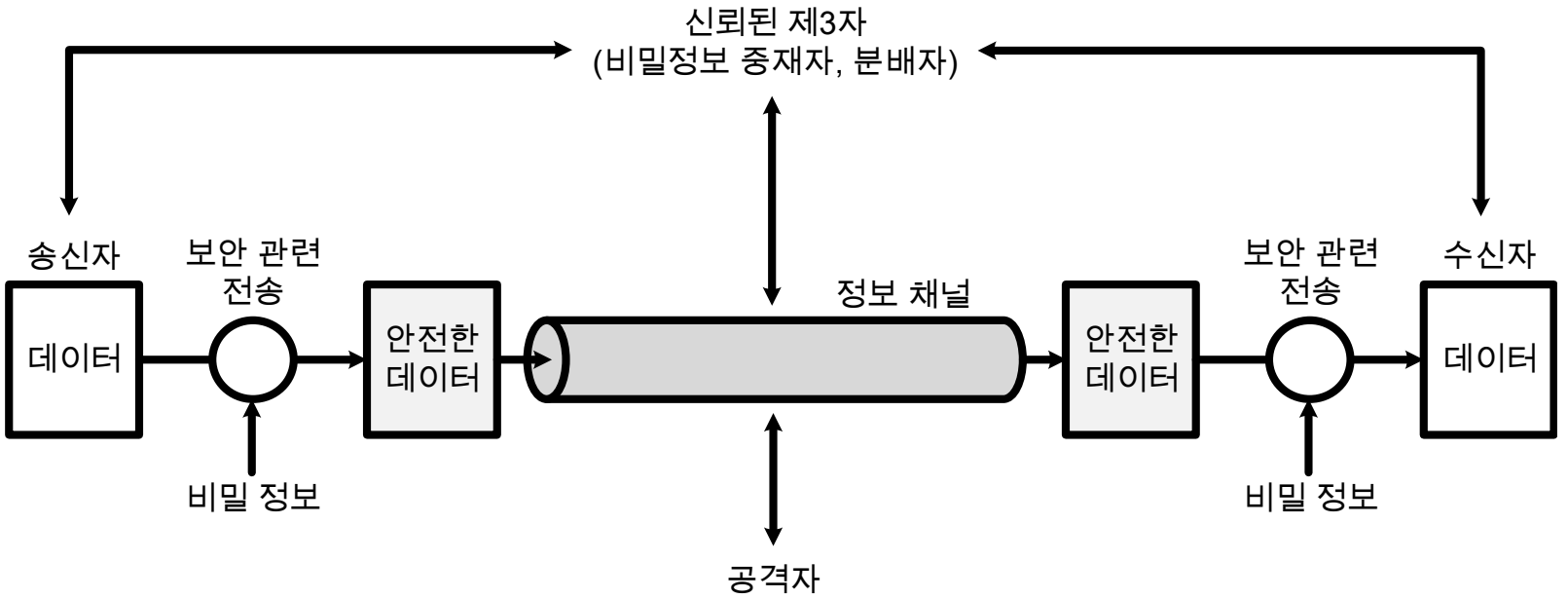
- 보안 서비스(Security Service)
  - 종류(4/4)
    - 무결성 서비스(Integrity Service)
      - 데이터의 수정, 추가, 제거, 재전송으로부터 데이터의 정확성 및 안전성을 보장하는 서비스
        - 암호화, 디지털 서명 등의 메커니즘 적용
      - 복구 가능 연결 무결성(Connection Integrity with Recovery)
        - 연결 설정 및 복구 시, 데이터 변조 및 재전송 탐지 서비스
      - 복구 없는 연결 무결성(Connectionless Integrity with Recovery)
        - 연결 설정 시, 데이터 변조 및 재전송 탐지 서비스
      - 선별된 필드 연결 무결성(Selective-Field Connection Integrity)
        - 선별된 연결 데이터 필드의 데이터 변조 및 재전송 탐지 서비스
      - 비연결 무결성(Connectionless Integrity)
        - 단일 데이터 블록 안의 전체 데이터 변조 탐지 서비스
      - 선별된 필드 비연결 무결성(Selective-Field Connectionless Integrity)
        - 선별된 비연결 데이터 필드의 데이터 변조 탐지 서비스

목 차

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

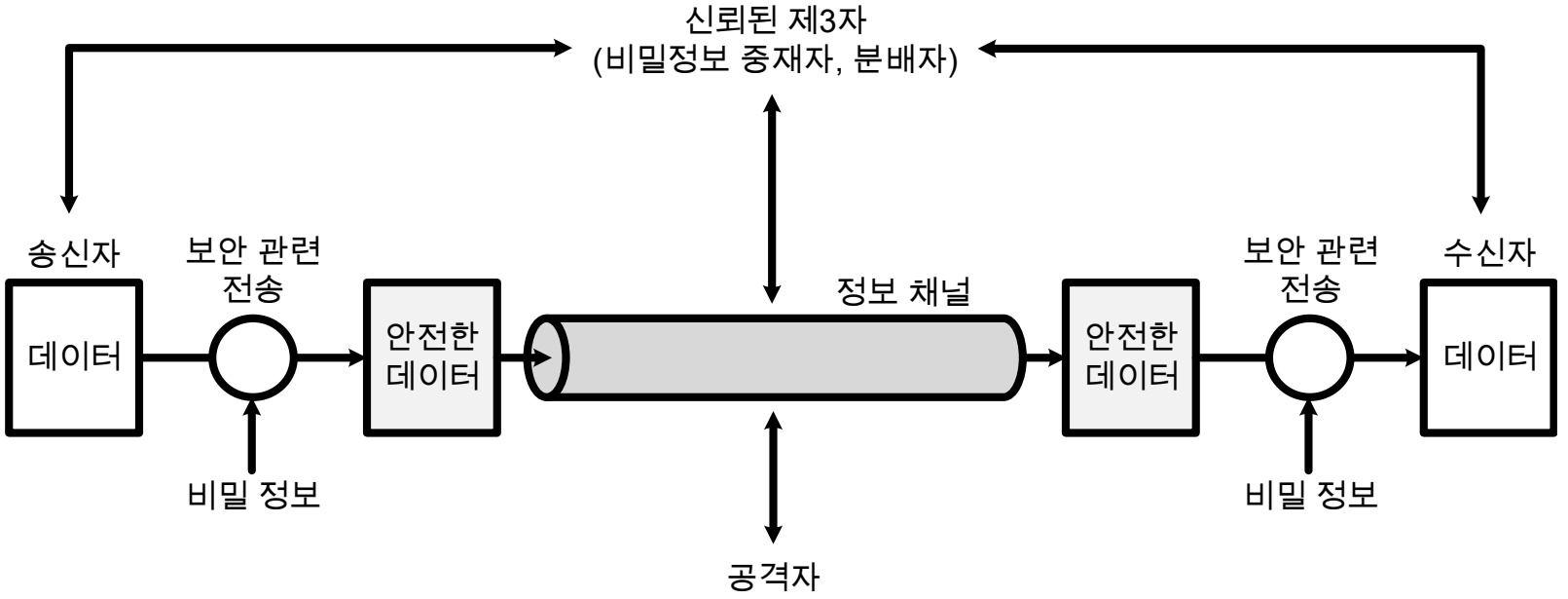
네트워크 보안 모델

- 네트워크 보안 모델
  - 보안 모델 성질
    - 전송될 데이터의 형태 변환
      - e.g., 송신자의 데이터에 데이터 추가 삽입 및 암호화
    - 공격자에게 비공개된 비밀 정보 공유
      - e.g., 수신자의 데이터 복호화를 위한 암호키



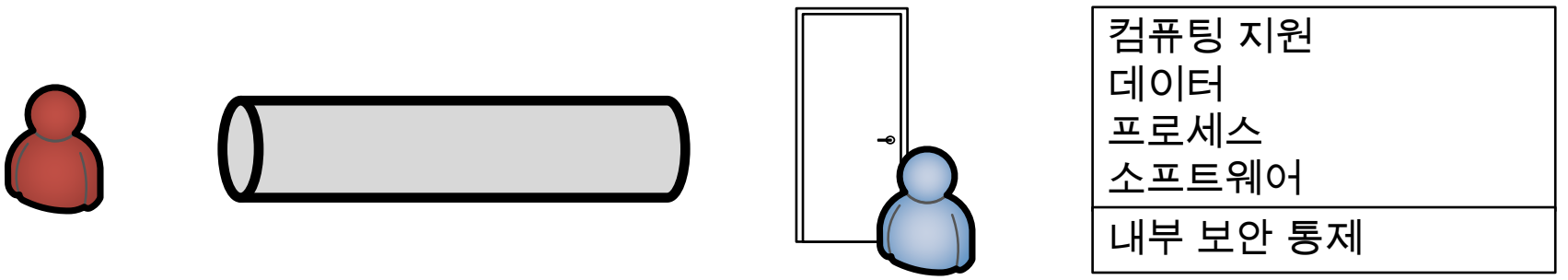
네트워크 보안 모델

- 네트워크 보안 모델
  - 보안 서비스 설계 기본 요구사항
    - 보안을 위한 변환 수행 알고리즘 설계
    - 해당 알고리즘을 위한 비밀 정보 생성
    - 비밀 정보 공유 및 배분 방법 개발
    - 양쪽 통신 주체가 사용할 프로토콜 결정



네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 네트워크 침입 방법(1/2)
    - 공격자
      - 해커(Hacker)
        - 시스템에 접근하여 데이터 및 프로그램을 다루는 사람
      - 침입자(Intruder)
        - 시스템을 파괴할 목적으로 불법 접근하여 안정성을 해치는 사람



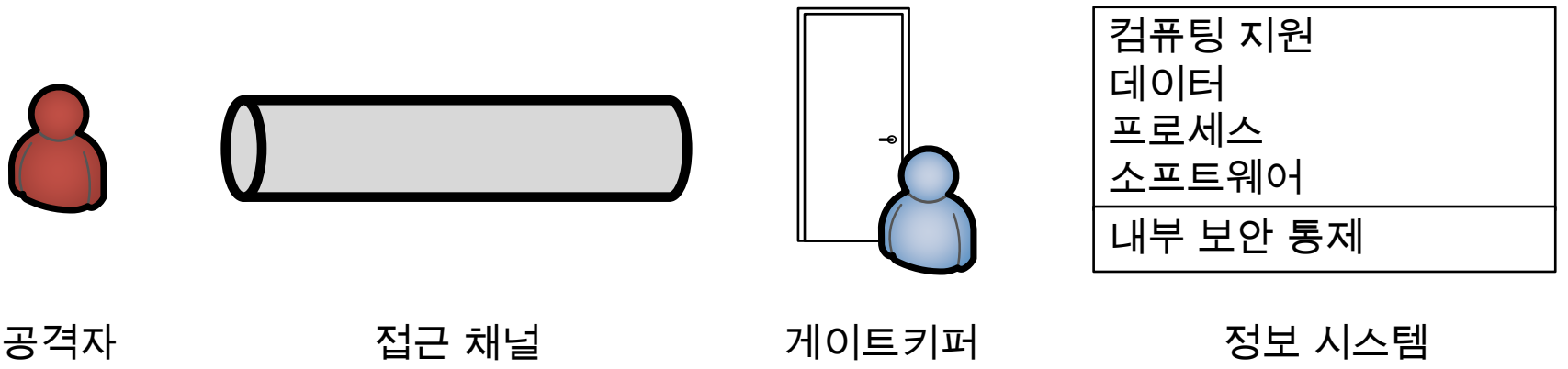
네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 네트워크 침입 방법(2/2)
    - 악성 소프트웨어
      - 악성 로직(Logic)이 잠복된 시스템 공격 방법
        - 바이러스(Virus)
          - 컴퓨터 시스템에 침입하여 프로그램에 기생하며, 시스템 변경 및 사용 불가능하도록 만드는 악성 소프트웨어
        - 웜(Worm)
          - 감염된 컴퓨터 시스템에서 스스로 복제하여 다른 컴퓨터로 복제본을 확산시킬 수 있는 악성 소프트웨어

특징	바이러스(Virus)	웜(Worm)
자가 복제 능력	O	O
자가 전파 능력	X	O
전염성 여부	O	O
숙주 여부	O	X
주요 감염 경로	e.g., 이동식 저장장치, 컴퓨터 프로그램	e.g., 인터넷, 네트워크

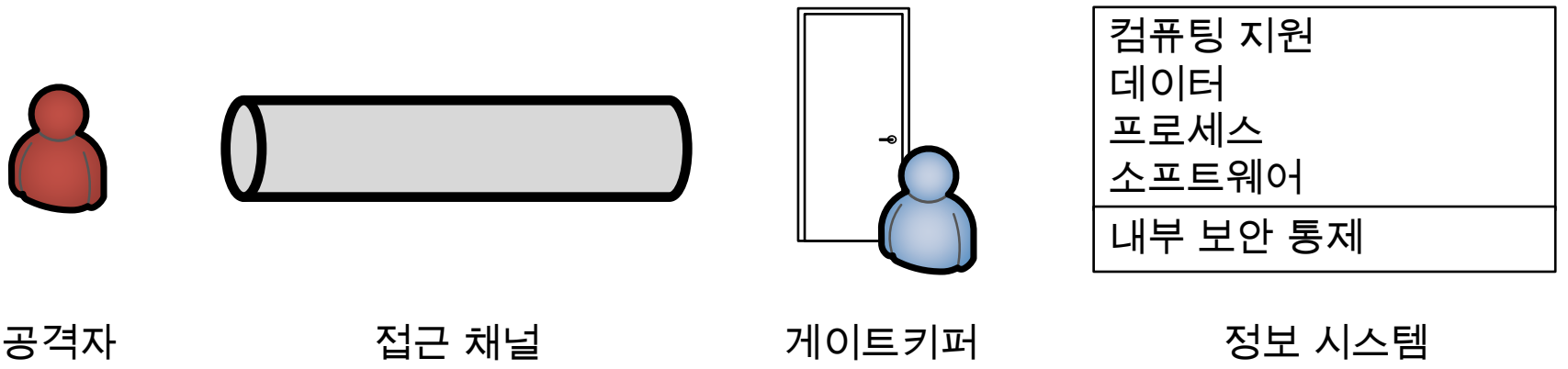
네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 프로그램 위협 형태
    - 정보 접근 위협(Information Access Threat)
      - 특정 사용자로부터 접근 권한이 부여되지 않은 데이터를 가로채거나 수정하여, 사용자 자신에게 유리하도록 만드는 위협
    - 서비스 위협(Service Threat)
      - 인가된 사용자의 시스템 접근 및 사용을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협



네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 불법 침입에 대한 보안 메커니즘
    - 게이트키퍼(Gate Keeper)
      - 비인가 사용자 및 악성 소프트웨어 탐지 및 제거
    - 모니터링(Monitoring)
      - 침입자 탐지를 위한 컴퓨터 동작 모니터링 및 저장된 데이터 분석 등의 내부적 제어 수행



Thanks!

김 지 혜 (jihye@pel.sejong.ac.kr)