2018/01/02, 2018 보안 기초 세미나

Network Security Essentials

- Chapter_1 개요 -

권순홍 (soonhong@pel.smuc.ac.kr)

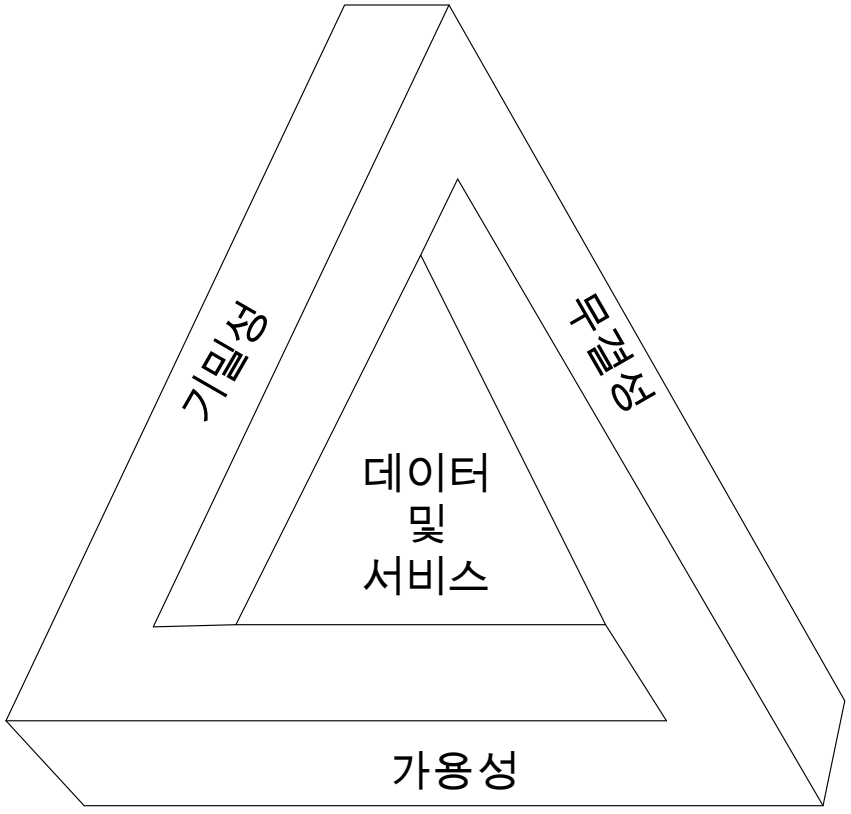
상명대학교 프로토콜공학연구실

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 기밀성,무결성,가용성을 보전하고자 하는 목표 달성을 위해 제공되어져야만 하는 보호



<CIA 트라이어드 그림>

컴퓨터 보안 개념

- 3대 보안 목적
  - 기밀성(Confidentiality)
    - 인가된 사용자만 정보에 접근할 수 있도록 하는것
      - 데이터 기밀성(Data Confidentiality)
        - 인가된 사용자만 데이터 자체에 접근 할 수 있는 것
      - 프라이버시(Privacy)
        - 개체의 정보의 범위나 정보 공개 범위를 통제하는 것
    - 특성
      - 정보 접근과 공개에 대해 합법적 제한조건을 지키는 것
      - 기밀성을 상실할 시 정보가 인가되지 않은 사용자에게 부정하게 공개됨

컴퓨터 보안 개념

- 3대 보안 목적
  - 무결성(Integrity)
    - 인가되지 않은 사용자 및 방법을 통한 정보의 변경, 삭제, 생성을 막는 것
      - 데이터 무결성(Data Integrity)
        - 인가되지 않은 사용자가 데이터를 변경,삭제,생성 하는 것을 막는 것
      - 시스템 무결성(System Integrity)
        - 인가되지 않은 사용자가 시스템을 변경,삭제,생성 하는 것을 막는 것
    - 특성
      - 부적절한 정보 수정이나 정보 파괴를 막는 것
      - 무결성이 상실될 시 정보가 무단으로 수정되거나 파괴됨

컴퓨터 보안 개념

- 3대 보안 목적
  - 가용성(Availability)
    - 인가된 사용자가 적시에 시스템 동작 및 서비스를 이용할 수 있도록 하는 것
  - 특성
    - 정보 사용에 있어서 시간성과 신뢰성 있는 접근을 의미
    - 가용성 상실 시 정보나 정보시스템을 사용하거나 적시에 접근이 불가능

컴퓨터 보안 개념

- 보안 실무 필드에서 필요한 개념
  - 인증(Authentication)
    - 데이터 및 사용자의 신뢰성 및 신원을 검증해주는 것
      - 전송,메시지,메시지 출처 유효성에 대한 확신
        - e.g., 아이디 또는 패스워드를 잃어버렸을 때의 휴대폰 인증
  - 책임(Accountability)
    - 한 개체의 행동을 추적하기 위해 기록을 남겨두는 것
      - 시스템은 반드시 이들의 활동상황(로그)를 기록해야함
        - 로그를 기반으로 포렌식 분석을 하기 위해
      - e.g., 부인봉쇄,억제,결함,분리,침입 및 탐지,사후 복구와 법적인 조치 등

컴퓨터 보안 개념

- 보안 실무 필드에서 필요한 개념
  - 예시
    - 부인봉쇄(Non-Reputation)
      - 송신자나 수신자 양측이 메시지를 전송한 사실을 부인하지 못하도록 하는 것
    - 억제
      - 자산,정보,시스템에 대한 보안위험을 피하거나 감지하고,최소화 하는 것
    - 결함 분리
      - 결함이 있는 구성 요소나 처리상의 오류 확인하여 원인 분석및 분리
    - 침입 탐지 및 예방
    - 사후 복구와 법적인 조치

컴퓨터 보안 개념

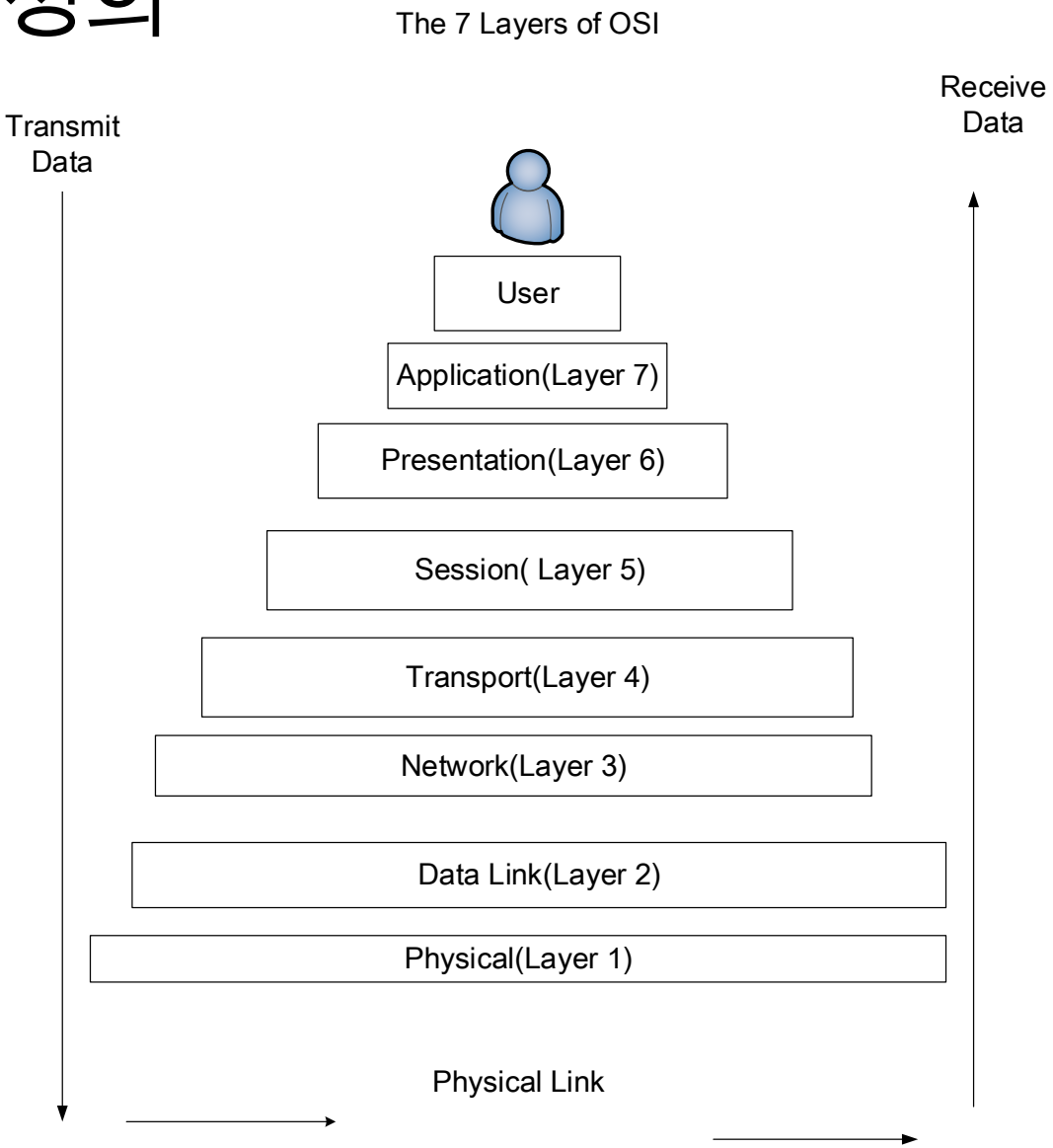
- 보안 침해의 수준
  - 저급 위험
    - 조직 또는 개인에게 미칠 제한된 부정적 효과가 나타날 것으로 예상되는 정도의 수준
  - 중급 위험
    - 조직 또는 개인에게 심각한 부정적 효과를 주는 수준
  - 고급 위험
    - 조직 또는 개인에게 극심한 재난 수준의 부정적 효과를 주는 수준

OSI 보안 구조

- OSI 모델 정의
  - OSI(Open System Interconnection)
    - 국제 표준화 기구(ISO)에서 개발한 7개의 계층으로 프로토콜을 구현하는 네트워킹 프레임 워크를 정의
  - 특성
    - 레이어 1-4는 하위 레이어로 간주되며 대부분 데이터 이동과 관련
    - 레이어 5-7에는 응용 프로그램 수준의 데이터가 포함
    - 각 레이어는 매우 구체적인 작업을 처리 한 다음 데이터를 다음 레이어로 전달

OSI 보안 구조

- OSI 보안 구조 정의



OSI 보안 구조

- OSI 보안구조
  - 관리자가 효과적으로 보안문제를 조직화 할 수 있는 유용한 방법을 제공
  - 핵심 구성
    - 보안 공격(Security Attack)
    - 보안 메커니즘(Security Mechanism)
    - 보안 서비스(Security Service)

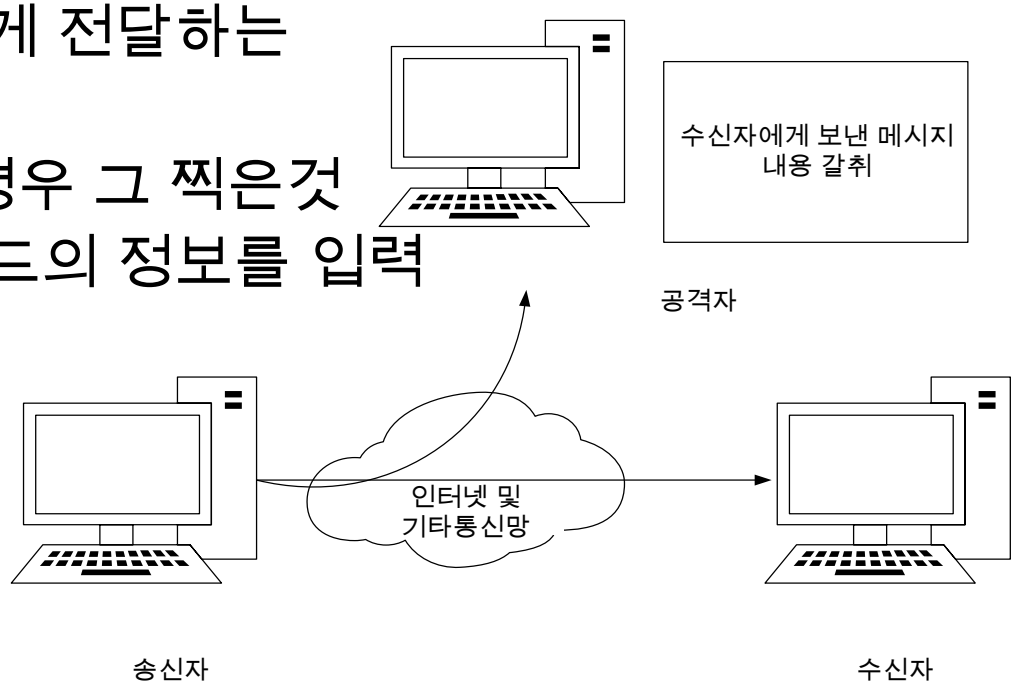
OSI 보안 구조

- OSI 보안 구조의 핵심 구성
- 보안 공격
  - 정보의 안정성을 침해하는 제반 행위
- 보안 서비스
  - 시스템의 보안을 강화하기 위해 이루어지는 기능
    - 보안 서비스가 구현되는데 보안 메커니즘 필요
- 보안 메커니즘
  - 보안 공격을 탐지,예방하거나 공격으로 인한 침해를 복구하는 절차
    - 보안 서비스를 구현하는데 필요

보안 공격

- 보안 공격 분류 및 유형
  - 소극적 공격(Passive Attack)
    - 시스템 자원에 영향을 끼치지 않는 공격 형태

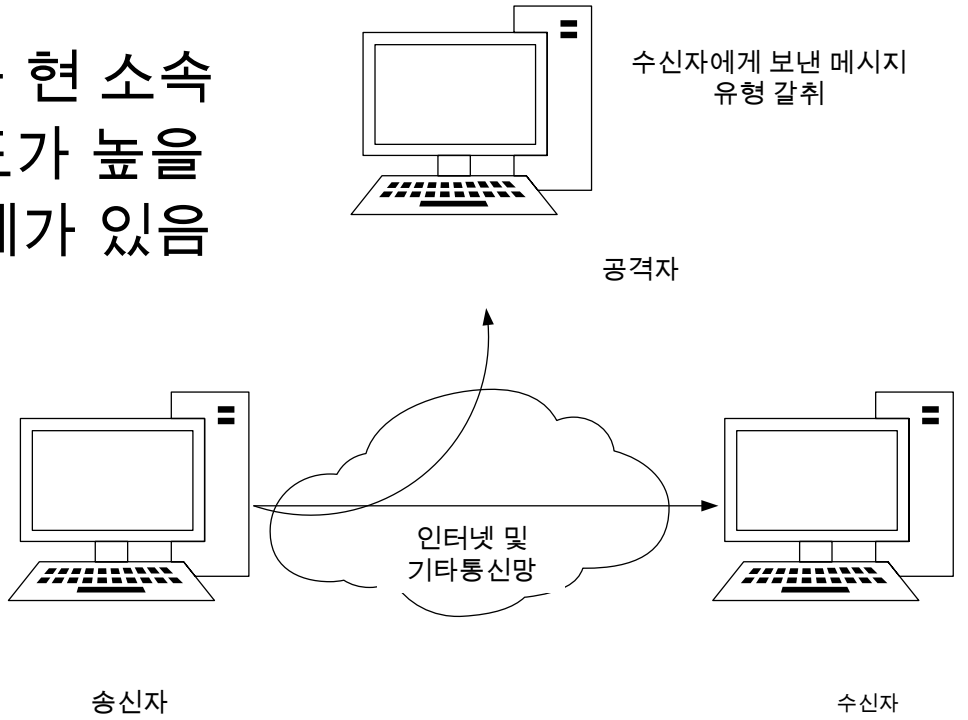
1. 메시지내용 갈취(Release of Message Contents)
   - 공격자가 송신자가 수신자에게 전달하는 정보를 갈취 하는 것
   - e.g., Secom 카드를 찍었을 경우 그 찍은것에 대한 정보를 갈취하여 그 카드의 정보를 입력하여 출입할 수 있음



보안 공격

- 보안 공격 분류 및 유형
  - 소극적 공격
    2. 트래픽 분석(Traffic Analysis)
       - 통신자의 메시지 내용이 아닌 유형을 관찰하는 것

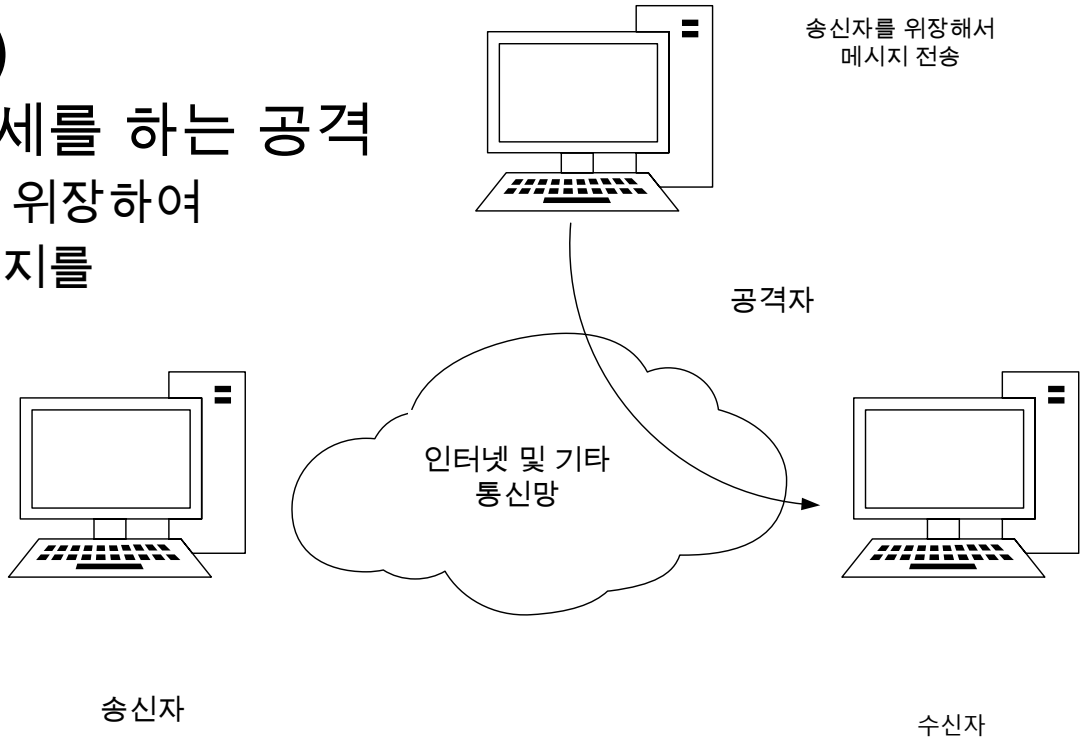
       - e.g., 축구선수 A의 에이전트가 현 소속 팀이 아닌 다른 팀과의 연락 빈도가 높을 경우 축구선수A가 다른팀과 관계가 있음을 알 수 있음



보안 공격

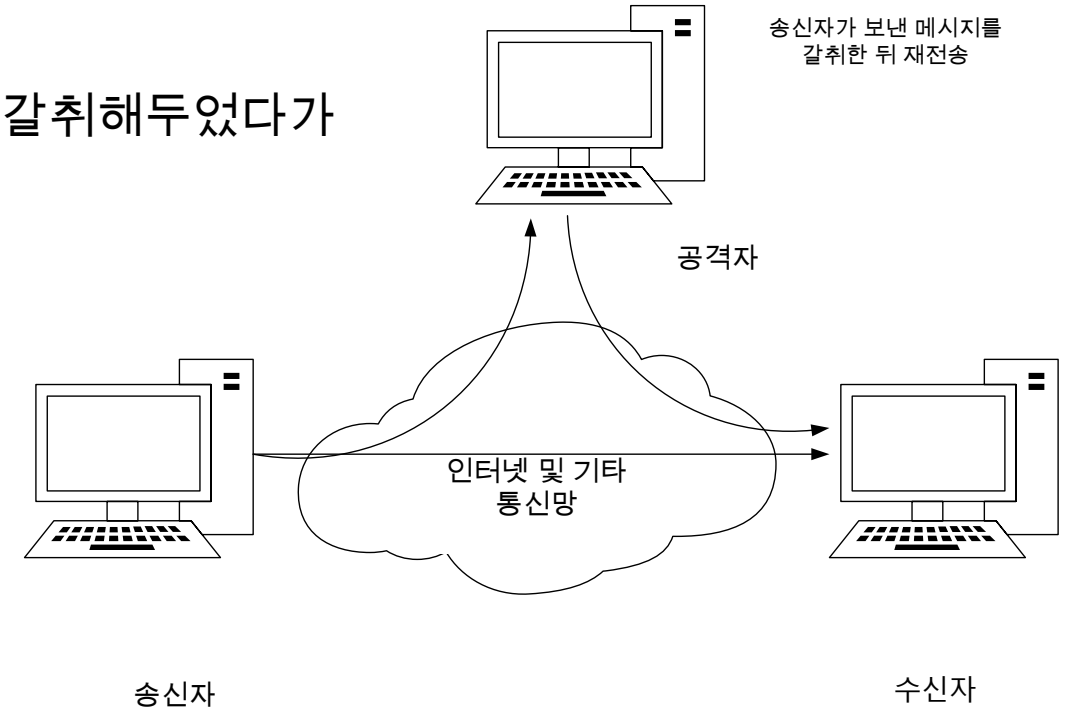
- 보안 공격 분류 및 유형
  - 적극적 공격(Active Attack)
    - 시스템 자원에 영향을 끼치는 공격형태

1. 신분위장(Masquerade)
   - 한 개체가 다른 개체의 행세를 하는 공격
     - e.g., 공장의 주인인 것처럼 위장하여 공장 생산을 중단하라는 메시지를 전송하는 경우



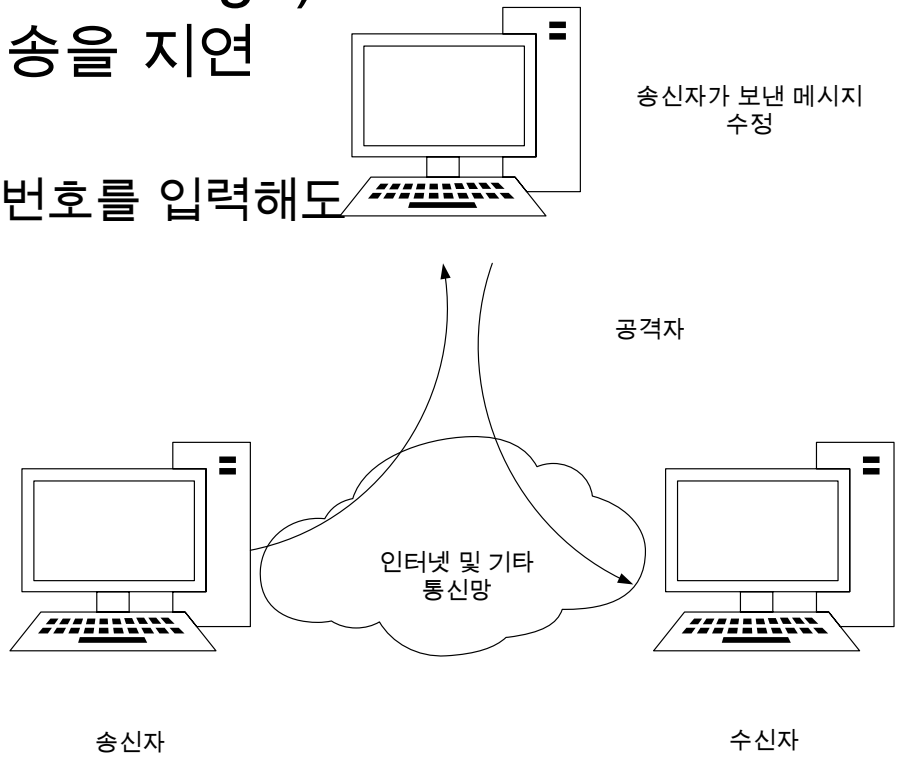
보안 공격

- 보안 공격 분류 및 유형
  - 적극적 공격
    2. 재전송(Reply)
       - 갈취한 데이터를 보관하고 있다가 시간이 지난 뒤 재전송 하는 공격
         - e.g., 공격자가 비밀번호를 갈취해두었다가 직접 로그인 하는 경우



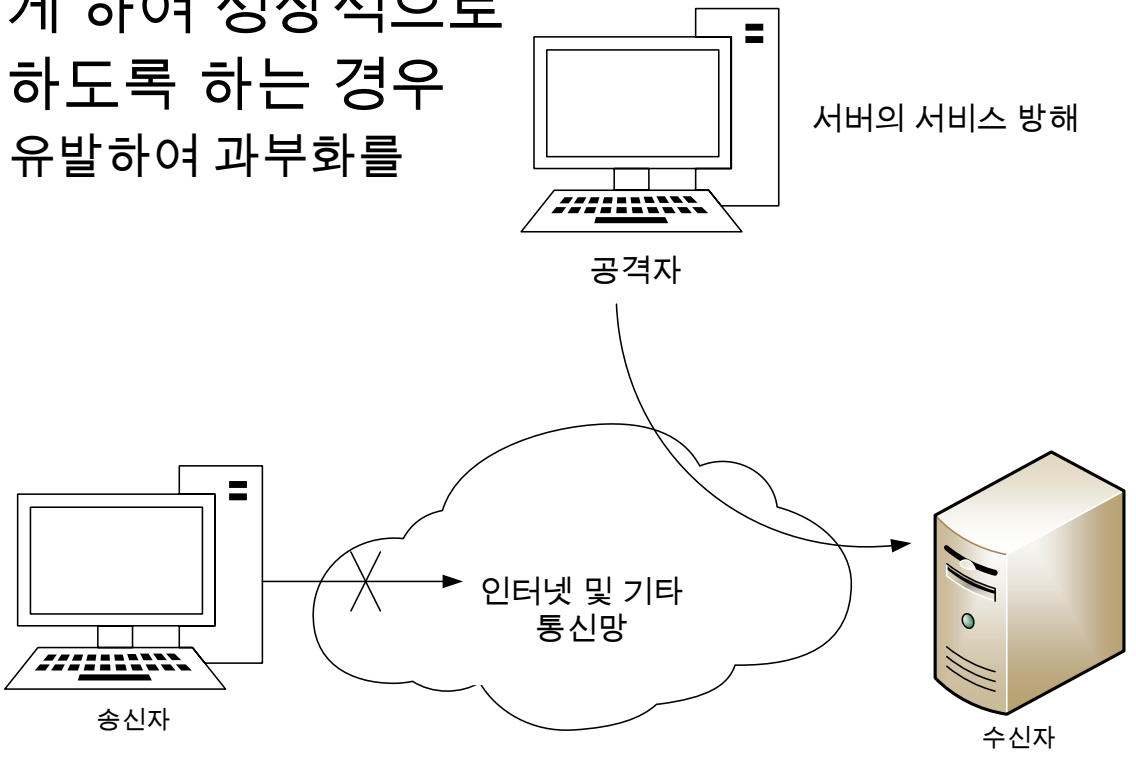
보안 공격

- 보안 공격 분류 및 유형
  - 적극적 공격
    3. 메시지 수정(Modification of Message)
       - 메시지의 일부를 수정하거나 전송을 지연 시키는 행위
         - e.g., 아이디를 로그인하려고 비밀번호를 입력해도 로그인이 안되는 경우



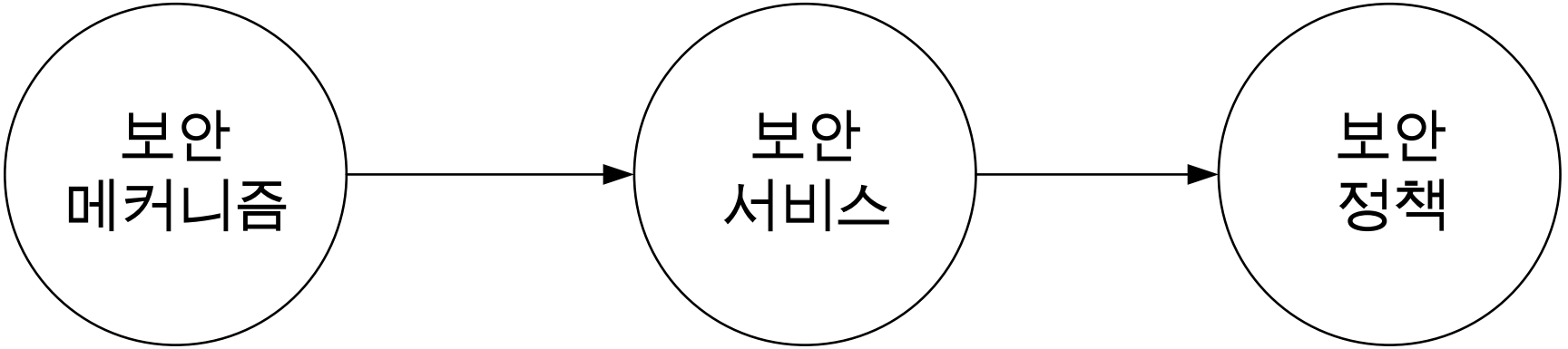
보안 공격

- 보안 공격 분류 및 유형
  - 적극적 공격
    4. 서비스 거부(Denial of Service)
       - 시스템 자원을 부족하게 하여 정상적으로 서비스를 사용하지 못하도록 하는 경우
         - e.g., 대량의 메시지를 유발하여 과부화를 일으키는 방법



보안 서비스

- 서비스 특징
  - 보안 메커니즘은 보안 서비스를 구현하고 보안 서비스는 보안 정책 구현



보안 서비스

- 서비스의 분류
  - 인증(Authentication)
    - 어느 개체가 주장하는 것처럼 정말 당사자 인지를 확인해주는 것
    - 기능
      - 양측이 모두 적법한 개체임을 확신 시켜줌
      - 상호 간의 통신이 권한이 없는 전송이나 수신을 시도하는 제3자에 의해서 방해받지 않았다는 것을 확신 시켜줌
    - 구체적 서비스
      1. 대등 개체 인증(Peer Entity Authentication)
         - 통신 하는 상대방의 신원 확인
      2. 데이터 출처 인증(Data Origin Authentication)
         - 예상된 출처로부터 온 것이 맞는지 확인

보안 서비스

- 서비스의 분류
  - 접근 제어(Access Control)
    - 인가되지 않은 사용자의 접근을 제한하는 능력
      - 이 서비스는 누가,어떤 조건하에,어떤 자원을 사용하도록 하는지를 제한
        - e.g., 서버의 권한 관리

보안 서비스

- 서비스의 분류
  - 데이터 기밀성(Data Confidentiality)
    - 인가되지않은 사용자로부터 데이터 접근을 막는 것
      - 다른측면에서는 분석공격으로부터 트래픽 흐름을 보호 하는 것
  - 데이터 무결성(Data Integrity)
    - 인증된 객체가 보낸 데이터가 수신한 데이터와 일치하는에 대한 확신
      - 수정,추가,제거,재전송이 없음을 확인

보안 서비스

- 서비스의 분류
  - 데이터 무결성
    - 연결형 무결성 서비스
      - 메시지가 중간에서 복제,추가,수정,순서 변환,재전송 되지 않고 송신되었음을 보장
    - 비연결형 무결성 서비스
      - 일반적으로 작은 단위의 메시지 수정에 대해 보호서비스 제공

보안 서비스

- 보안 서비스의 분류
  - 부인봉쇄(Nonrepudiation)
    - 송신자나 수신자 양측이 메시지를 전송한 사실 자체를 부인하지 못하도록 막는 것
      - 수신자에게는 송신자가 보낸것임을 확신
      - 송신자에게는 수신자가 수신한것을 확신
  - 가용성 서비스(Availability)
    - 인가된 사용자가 적시에 정보에 접근 할 수 있도록 보장하는 서비스

보안 메커니즘

- 메커니즘의 분류
  - 일반 보안 메커니즘(Pervasive Security Mechanisms)
    - 임의의 특정 OSI 보안 서비스나 프로토콜 계층에 구애받지 않는 메커니즘
  - 특정 보안 메커니즘(Specific Security Mechanisms)
    - 통신 개체가 주장하는 것처럼 정말로 그 개체 인지를 확인해 주는 것

보안 메커니즘

- 메커니즘의 분류
  - 특정 보안 메커니즘(Specific Security Mechanisms)
    - 종류
      - 암호화(Encipherment)
        - 데이터를 읽을 수 없는 형태로 변환하는 데 수학적 알고리즘을 사용하는 것
      - 디지털 서명(Digital Signature)
        - 데이터의 위조를 막기위하여 데이터에 붙이는 데이터나 데이터 단위
      - 접근 제어(Access Control)
        - 인가되지 않은 사용자의 접근을 제어하는 것
      - 데이터 무결성(Data Integrity)
        - 인가된 개체가 보낸 데이터와 받은 데이터가 일치하는지에 대한 확신

보안 메커니즘

- 메커니즘의 분류
  - 특정 보안 메커니즘(Specific Security Mechanisms)
    - 종류
      - 인증 교환(Authentication Exchange)
        - 정보교환을 통해 개체의 신원을 확인하는 데 사용하는 메커니즘
          - e.g., 아이디나 비밀번호를 잊어버렸을 경우 사용하는 휴대폰 인증
      - 트래픽 패딩(Traffic Padding)
        - 트래픽 분석 시도를 방해하기 위해서 데이터 스트림 안의 빈 곳에 비트를 채워 넣는것
      - 경로 제어(Routing Control)
        - 물리적으로 안정한 경로를 선택할 수 있게 하는 것
          - 보안침해가 의심스러운 경우 경로를 바꿀 수 있게 함
      - 공증(Notarization)
        - 데이터 교환의 어떤 성질을 확인하기 위해 신뢰받는 제 3자를 이용

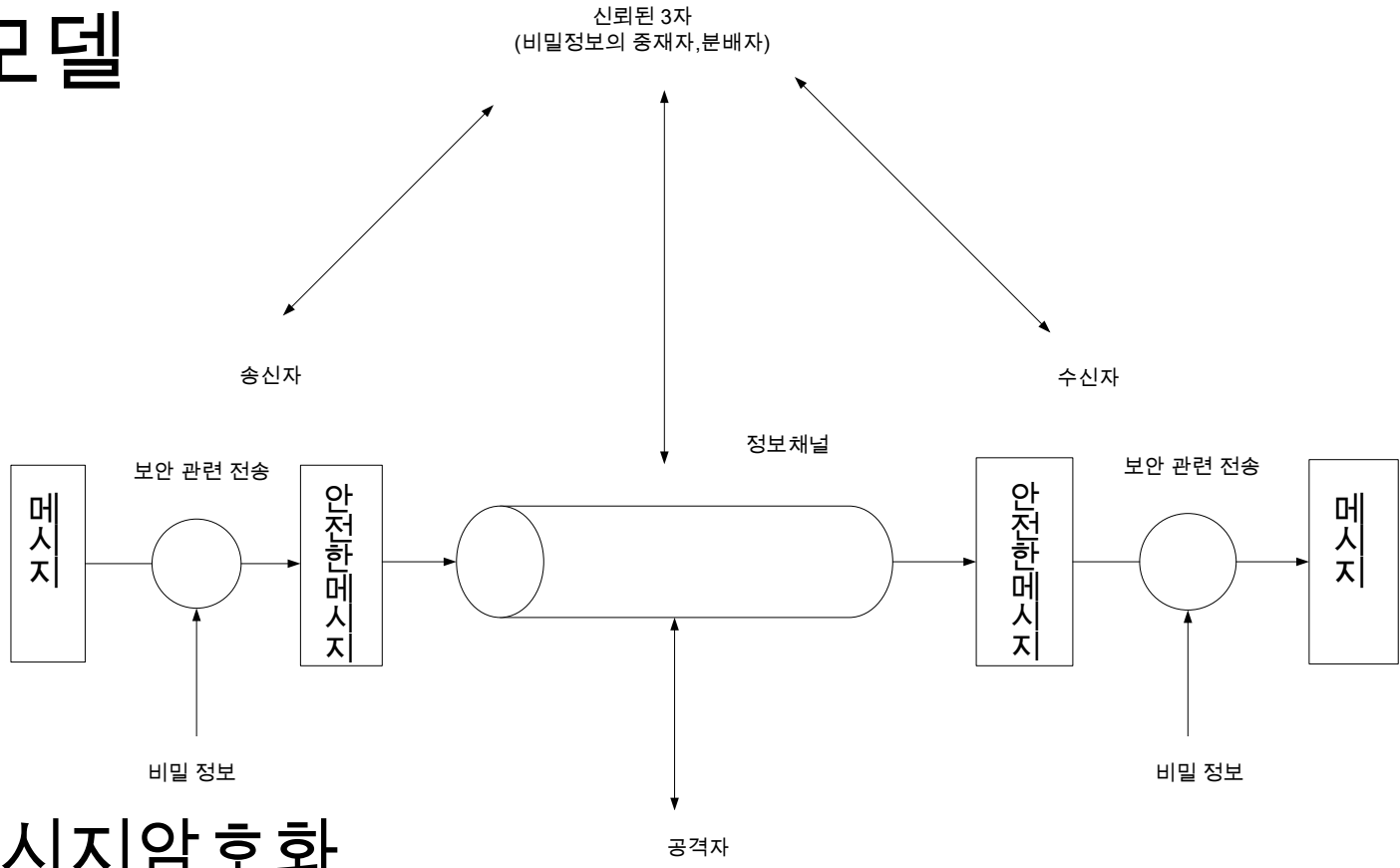
보안 메커니즘

- 보안 서비스와 메커니즘의 관계

서비스	메커니즘							
	암호화	디지털 서명	접근 제어	데이터 무결성	인증 교환	트래픽 패딩	라우팅 제어	공증
대등 개체인증	Y	Y			Y			
데이터 출처인증	Y	Y						
접근 제어			Y					
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y	Y	
데이터 무결성	Y	Y		Y				
부인 봉쇄		Y		Y				Y
가용성				Y	Y			

네트워크 보안 모델

- 네트워크 보안 모델
- 일반적인 모델



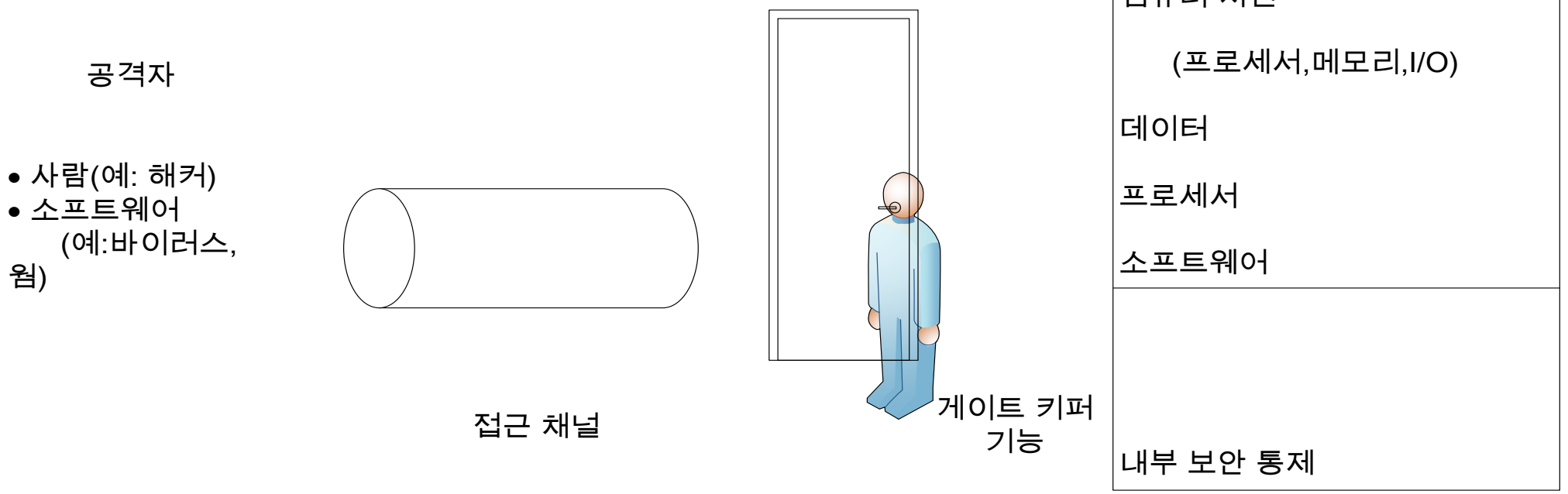
- 특징
  - 보안을 위한 메시지암호화
  - 메시지의 신원 확인을 위한 코드 첨부
  - 비밀 정보 공유

네트워크 보안 모델

- 네트워크 보안 위협 유형
  - 정보 접근 위협(Information Access Threat)
    - 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정해서 그 사용자 자신에게 유리하도록 만든 위협
  - 서비스 위협(Service Threat)
    - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협
  - 소프트웨어 공격의 대표적인 사례
    - 바이러스(Virus)
      - 프로그램을 통해 감염되는 악성 코드(악의적 목적을 가진 스스로를 복제)
    - 웜(Worm)
      - 컴퓨터의 취약점을 찾아 네트워크를 통해 스스로 감염되는 악성코드

네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 불법침입 문제에 대한 해결 방법
    - 게이트 키퍼(Gatekeeper)
      - 로그인 과정을 이용하여 사용자를 가려내고 바이러스나 웜 같은 공격을 탐지하여 제거하는 역할



네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 불법침입 문제에 대한 해결 방법
    - 모니터링(Monitoring)
      - 1차적으로 인가받지 못한 사용자,악성 소프트웨어 차단
      - 2차적으로 침입자 탐지를 위해 컴퓨터 동작 모니터링,저장된 정보 분석 등의 내부적 제어 수행

감사합니다!