2018/01/02, 2018 보안 기초 세미나

Network Security Essentials

- Chapter_1 개요 -

김경선 (kyeongseon@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

컴퓨터 보안 개념

- 정보 시스템 3대 보안 목적(1/3)
  - 기밀성(Confidentiality)
    - 인가된 사용자에게만 정보접근과 공개 가능
      - 개인 프라이버시와 소유권에 대한 정보를 보호하는 수단을 포함
        - e.g., 학생 성적, 고객정보 유출

1. 데이터 기밀성(Data Confidentiality)
   - 데이터를 허락 받지 않은 사용자에게 이용하거나 노출되지 않도록 하는 것
2. 프라이버시(Privacy)
   - 정보를 공개하고 사용하는 대상을 통제할 수 있도록 하는 것

컴퓨터 보안 개념

- 정보 시스템 3대 보안 목적(2/3)
  - 무결성(Integrity)
    - 인증되지 않은 데이터 변경으로부터 보호하는 것
      - 무결성에 실패한 데이터는 손상 되었다고 말함
        - e.g., DB에 저장된 환자 진료 정보, 온라인 설문 조사

1. 데이터 무결성(Data Integrity)
   - 인증된 데이터만 정보나 프로그램을 변경할 수 있음

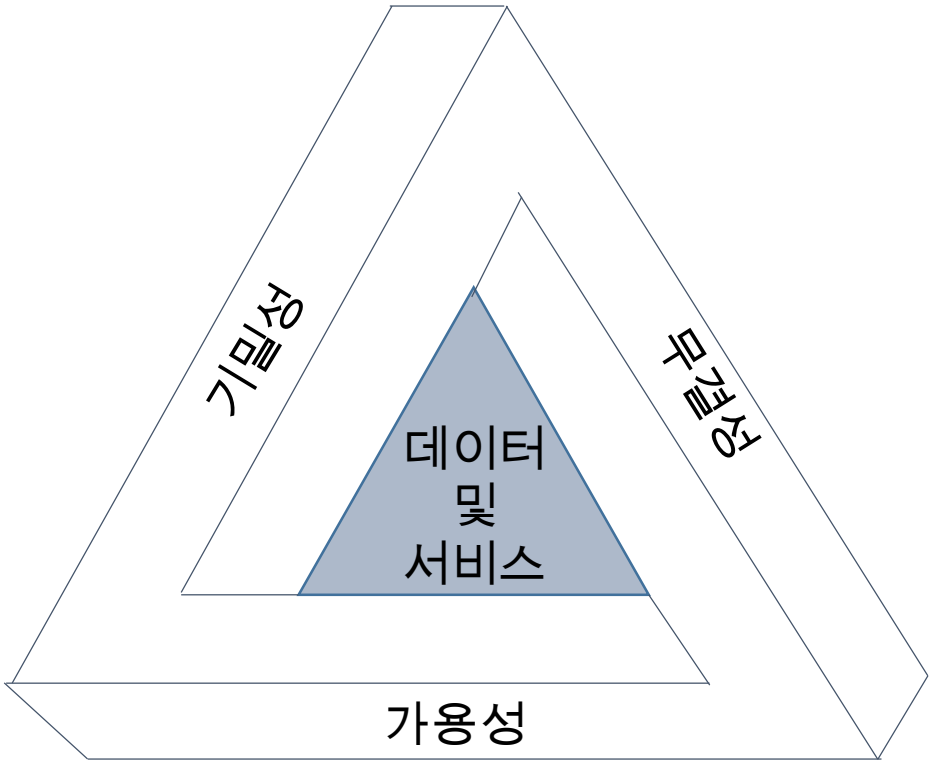
2. 시스템 무결성(System Integrity)
   - 시스템이 손상되지 않은 상태로 수행 하도록 하는 것

컴퓨터 보안 개념

- 정보 시스템 3대 보안 목적(3/3)
  - 가용성(Availability)
    - 인가된 사용자가 적절한 시간 안에 데이터나 서비스를 사용할 수 있도록 하는 것
      - e.g., 학교 홈페이지, 온라인 전화번호부 접근
    - 정보 사용에 있어서 시간성과 신뢰성있는 접근을 의미
      - 가용성을 상실하게되면 정보나 정보시스템 사용과 접근이 불가

컴퓨터 보안 개념

- CIA 트라이어드(CIA Triad) 그림



<CIA 트라이어드>

컴퓨터 보안 개념

- 보안 실무 필드에 필요한 개념 추가
  - 인증(Authentication)
    - 통신 개체가 그 당사자인지를 확인하는 것
      - 전송, 메시지, 메시지 출처 유효성에 대한 확인
        - e.g., 사용자 이름, 패스워드, 생체측정 스캐닝
  - 책임(Accountability)
    - 개체의 행동을 추적해서 찾기 위해 증거와 기록을 남기는 것
      - e.g., 부인봉쇄, 억제, 결함 분리, 침입 탐지 및 예방, 사후 복구

컴퓨터 보안 개념

- 보안 침해 세가지 수준
  - 저급 위험
    - 조직의 운영, 조직의 자산, 또는 개인에게 미칠 제한된 부정적 효과가 나타남
      - 조직이나 개인에게 소규모 손상과 침해가 발생함
  - 중급 위험
    - 조직의 운영, 조직의 자산, 또는 개인에게 심각한 부정적 효과를 줌
      - 조직이나 개인에게 심각한 손실과 손상을 끼침
  - 고급 위험
    - 조직의 운영, 조직의 자산, 또는 개인에게 극심하고 재난수준의 부정적 효과를 줌
      - 조직이나 개인에게 엄청난 손실과 손상을 끼침

OSI 보안 구조

- OSI(Open System Interconnection)
  - 정의
    - 개방형 시스템간 상호접속으로 ISO(국제표준화기구)가 작성하고 있는 컴퓨터 통신절차에 관한 국제표준규격
    - 프로토콜을 표준화, 컴퓨터 네트워크 간의 상호통신을 가능하게 함
  - OSI 보안구조 핵심
    - 보안 공격(Security Attack)
      - 정보의 안정성을 침해하는 모든 행위
        - e.g., 스누핑(Snooping), 트래픽분석(Traffic Analsis), 변경(Modification), 가장(Masquerading), 재전송(Replay), 부인(Repudiation), 서비스거부(Denial of Service)등

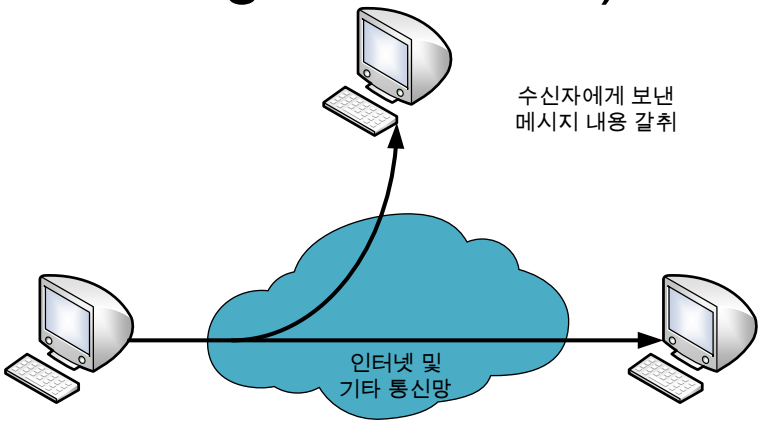
OSI 보안 구조

- OSI 보안구조 핵심
  - 보안 메커니즘(Security Mechanism)
    - 보안 공격을 탐지, 예방하거나 공격으로 인한 침해를 복구하는 절차 또는 장치
    - 일반적으로 한 가지 이상의 알고리즘이나 프로토콜로 구성됨
  - 보안 서비스(Security Service)
    - 조직의 정보 전송과 데이터 처리 시스템의 보안을 강화하기 위한 처리 서비스 또는 통신 서비스
    - 보안 서비스는 보안 정책(Security Mechanism)을 구현하는 반면, 보안 메커니즘에 의해서 구현됨

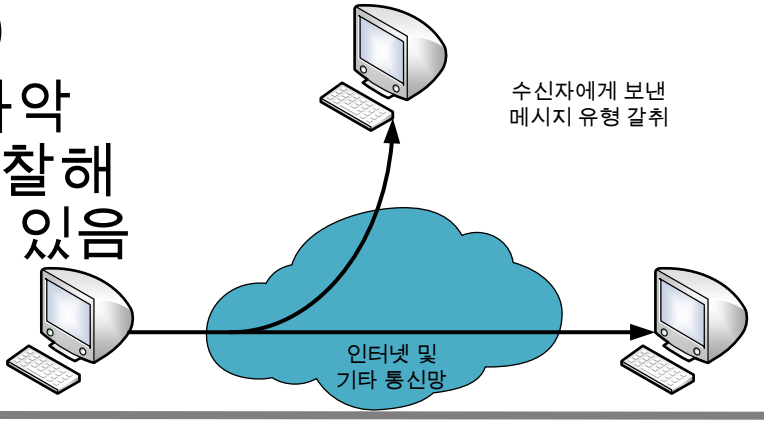
보안 공격

- 보안 공격 분류(1/3)
  - 소극적 공격
    - 시스템으로부터 정보를 획득하거나 사용하려는 시도

1. 메시지 내용 갈취(Release of Message Contents)
   - 전화나 메세지를 이용한 정보 전달 내용을 갈취
     - e.g., 통장 비밀번호를 가로챔



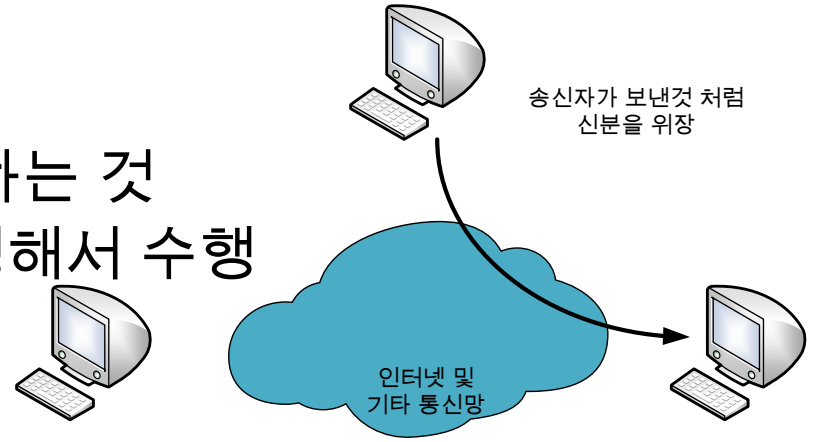
2. 트래픽 분석(Traffic Analysis)
   - 통신자의 접속 위치와 신원을 파악하고 메시지의 빈도와 길이를 관찰해 통신자의 통신 특성을 추측할 수 있음
     - e.g., 국가 간의 연락



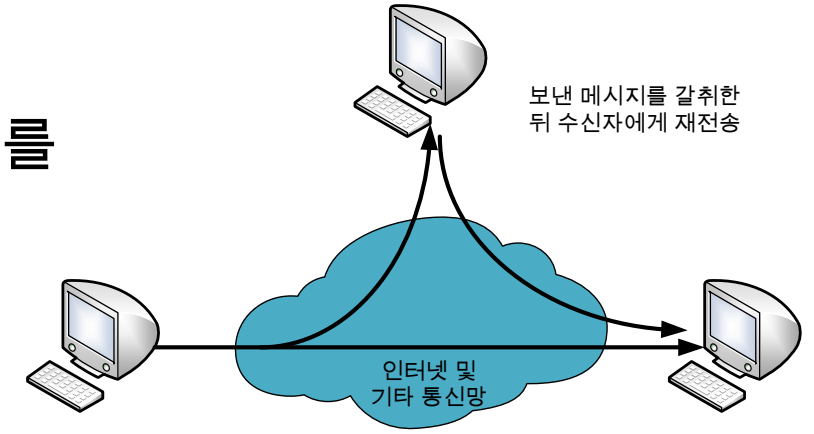
보안 공격

- 보안 공격 분류(2/3)
  - 적극적 공격
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격 형태

1. 신분위장(Masquerade)
   - 한 개체가 다른 개체의 행세를 하는 것
   - 다른 형태의 적극적 공격과 병행해서 수행
     - e.g., 은행인 척 위장하고 개인정보 요구

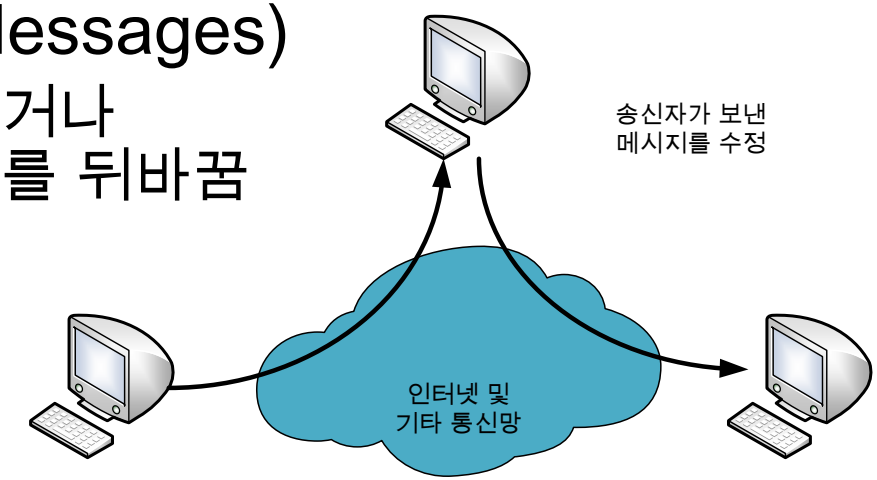


2. 재전송(Replay)
   - 소극적 공격으로 획득한 데이터를 보관하다가 시간이 경과한 후에 재전송
     - e.g., 메시지 내용 갈취로 얻은 번호를 재전송으로 사용

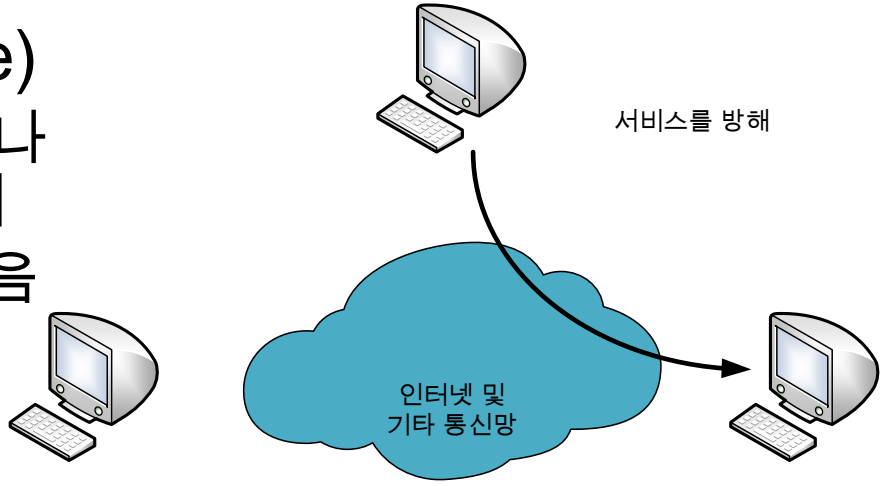


보안 공격

- 보안 공격 분류(3/3)
  - 적극적 공격
    3. 메시지 수정(Modification of Messages)
       - 메시지의 일부를 불법으로 수정하거나 메시지 전송을 지연시키거나 순서를 뒤바꿈

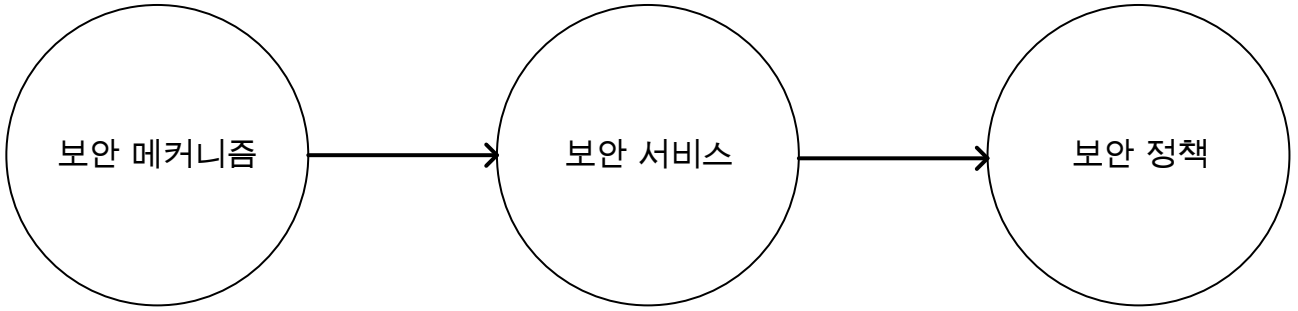


    4. 서비스 거부(Denial of Service)
       - 통신설비가 정상적으로 운용되거나 관리되지 못하도록 방해하는 행위
       - 특정 목표물을 대상으로 할 수 있음
         - e.g., 홈페이지가 마비되어 서비스가 거부 됨



보안 서비스

- 보안 서비스의 정의
  - 시스템 자원 보호를 위해 시스템이 제공하는 처리 서비스나 통신 서비스
  - 보안 정책(Security Policy)을 구현하고, 보안 메커니즘 (Security Mechanism)에 의해서 구현 됨



보안 서비스

- 보안 서비스의 분류(1/4)
  - 인증 서비스(Authentication Service)
    - 통신이 검증되었다는 것을 확인해주는 서비스

1. 대등 개체 인증(Peer Entity Authentication)
   - 통신하는 상대방의 신원을 확인시켜 줌
   - 상대방이 신분위장을 하거나 재전송을 하지 않는다는 확신을 갖게 함

2. 데이터-출처 인증(Data Origin Authentication)
   - 데이터 단위의 출처에 대한 확인
   - 비연결 전송에서 수신된 데이터의 출처가 정말 주장하고 있는 곳에서 온 것인지를 확신시켜주는 인증

보안 서비스

- 보안 서비스의 분류(2/4)
  - 접근제어(Access Control)
    - 누군가가 무언가를 사용하는 것을 허가하거나 거부하는 기능
      - e.g., DB 접근제어, 앱의 접근제어
  - 데이터 기밀성(Data confidentiality)
    - 소극적 공격으로부터 데이터를 보호하는 것
    - 분석공격으로부터 트래픽 흐름을 보호하는 것

보안 서비스

- 보안 서비스의 분류(3/4)
  - 데이터 무결성(Data Integrity)
    - 데이터가 변경되거나 파괴되지 않고 보존되는 특성

1. 연결형 무결성 서비스
   - 메시지가 중간에서 복제, 추가, 수정, 순서가 바뀌거나 재전송됨이 없이 그대로 송신되는 것을 보장

2. 비연결형 무결성 서비스
   - 데이터가 작은 메시지만 다룸
   - 일반적으로 메시지 수정에 대해서만 보호 서비스를 제공

보안 서비스

- 보안 서비스의 분류(4/4)
  - 부인봉쇄(Nonrepudiation)
    - 송신자나 수신자 양측이 메시지를 전송한 사실 자체를 부인하지 못하도록 막는 것
      - 특정 개체가 메시지를 수신했음을 보장
  - 가용성 서비스(Availability Service)
    - 시스템의 가용성을 보장하기 위해 시스템을 보호하는 서비스

보안 메커니즘

- 보안 메커니즘의 정의
  - 보안 기능을 소프트웨어나 하드웨어상에 구현하기 위한 논리 또는 알고리즘
- 보안 메커니즘의 분류
  1. 일반 보안 메커니즘
  2. 특정 보안 메커니즘

보안 메커니즘

- 보안 메커니즘의 분류
  - 일반 보안 메커니즘(Pervasive Security Mechanisms)
    - OSI 보안 서비스나 프로토콜 계층에 구애 받지 않는 메커니즘
    - 종류
      - 신뢰받는 기능(Trusted Functionality)
        - 어떤 기준으로 볼 때 올바른 것으로 여겨지는 것
      - 보안 레이블(Security Label)
        - 데이터 단위의 보안속성에 붙인 이름이나 표시
      - 사건 탐지(Event Detection)
      - 보안 감사 추적(Security Audit Trail)
        - 보안 감사를 하기위해 수집하거나 이용되는 데이터
      - 보안 복구(Security Recovery)
        - 사건처리와 관리기능 같은 메커니즘의 요구사항을 다루고 복구 동작을 수행

보안 메커니즘

- 보안 메커니즘의 분류
  - 특정 보안 메커니즘(Specific Security Mechanisms)
    - 통신 개체가 주장하는 것처럼 정말로 그 당사자인지를 확인해주는 메커니즘
    - 종류
      - 암호화(Encryption)
      - 디지털 서명(Digital Signature)
        - 데이터 수신자가 데이터의 발신자와 무결성을 입증하고 위조를 막도록 함
      - 접근제어(Access Control)
      - 데이터 무결성(Data Integrity)
      - 인증 교환(Authentication Exchange)
      - 트래픽 패딩(Traffic Padding)
        - 트래픽 분석 시도를 방어하기 위해서 데이터 스트림 안의 빈 곳에 비트를 채워 넣는 것

보안 메커니즘

- 보안 메커니즘의 분류
  - 특정 보안 메커니즘
    - 종류
      - 경로 제어(Routing Control)
      - 공증(Notarization)
        - 내용, 시작 시간, 전송 등과 같은 특성을 정확성에 대한 차후 보증을 위해 믿을 수 있는 제3자와 등록을 하는 것

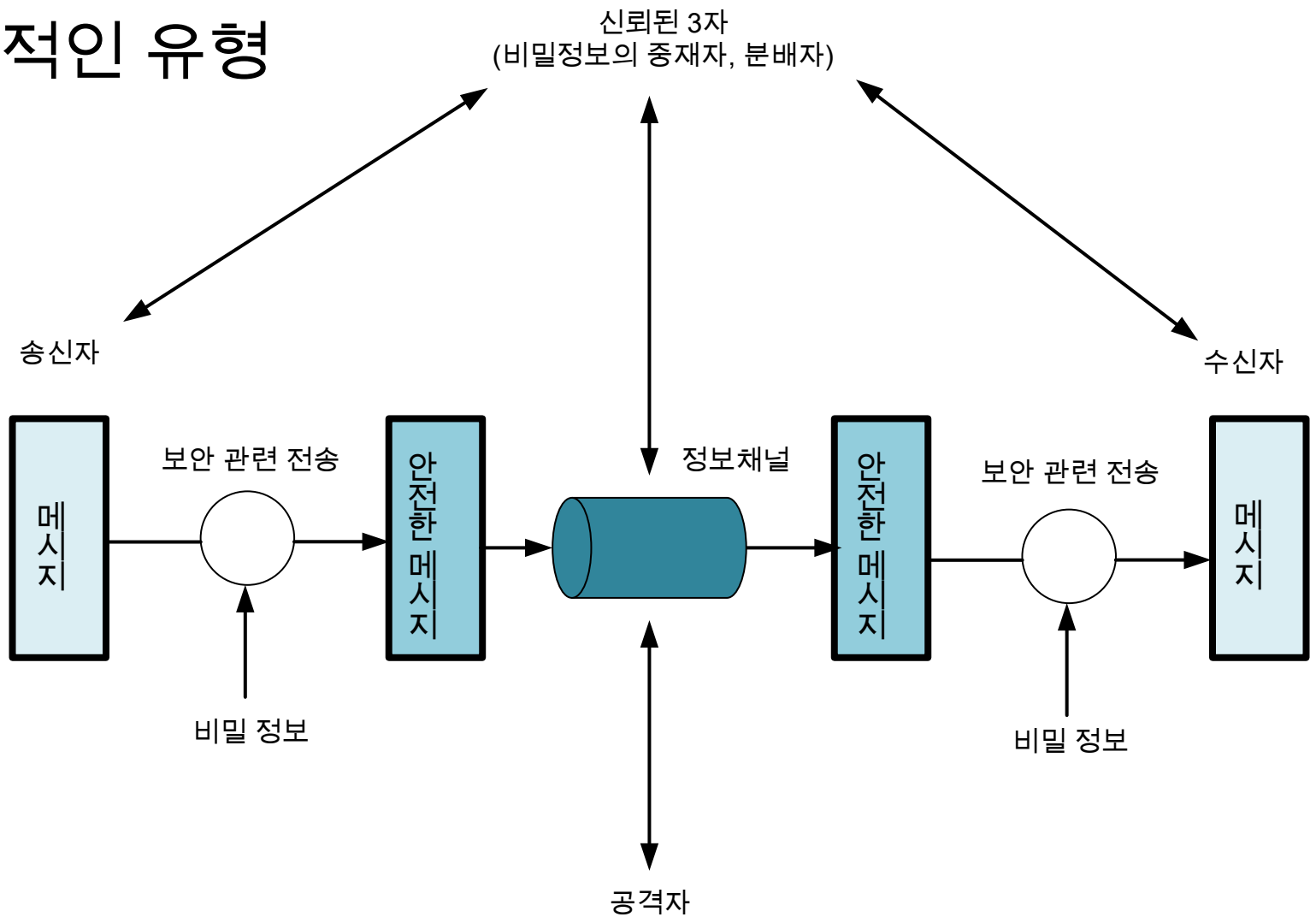
보안 메커니즘

- 보안 서비스와 보안 메커니즘의 관계

서비스	메커니즘							
	암호화	디지털 서명	접근제어	데이터 무결성	인증교환	트래픽 패딩	라우팅 제어	공증
대등 개체 인증	Y	Y			Y			
데이터 출처인증	Y	Y						
접근제어			Y					
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y	Y	
데이터 무결성	Y	Y		Y				
부인봉쇄		Y		Y				Y
가용성				Y	Y			

네트워크 보안 모델

- 네트워크 보안 모델
  - 일반적인 유형

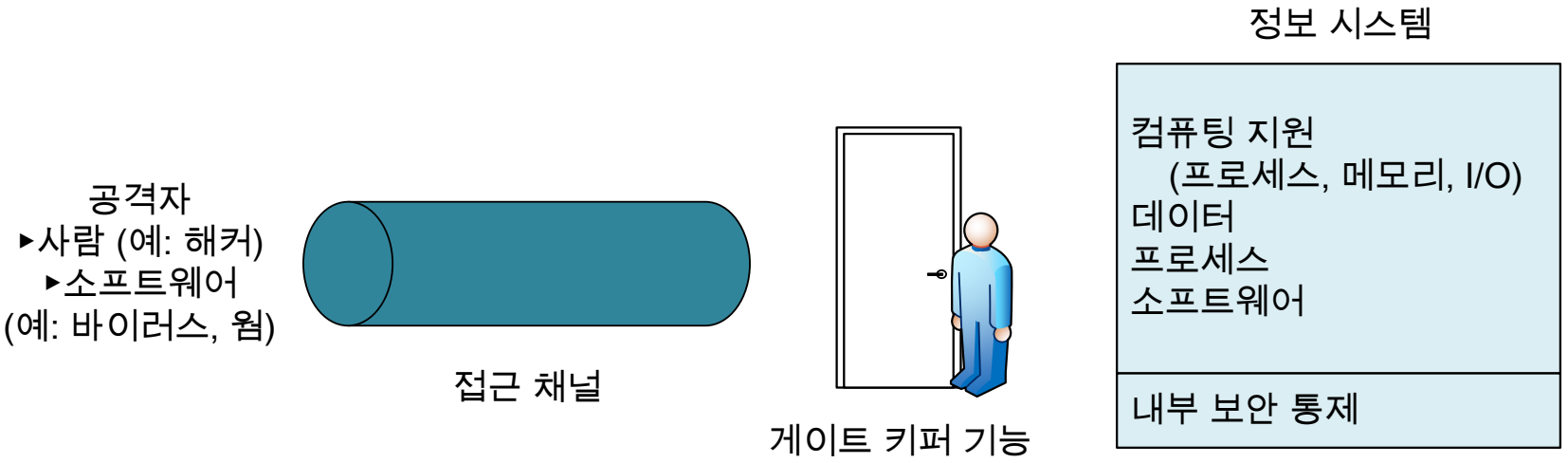


네트워크 보안 모델

- 네트워크 보안 위협 형태
  - 정보 접근 위협(Information access threats)
    - 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정해서 그 사용자 자신에게 유리하도록 만드는 위협
      - e.g., 어느 사이트를 해킹해 얻은 회원 정보를 돈 받고 팜
  - 서비스 위협(Service threats)
    - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협
      - e.g., 바이러스(Virus), 웜(Worm)

네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 게이트키퍼(Gatekeeper)
    - 패스워드 로그인 과정을 이용해서 인가받지 않은 사용자를 가려내고 웜이나 바이러스 같은 공격을 탐지하여 제거하는 것



감사합니다!