Network Security Essentials

- 1장 개요 -

전 상 기(jsg2861@gmail.com)

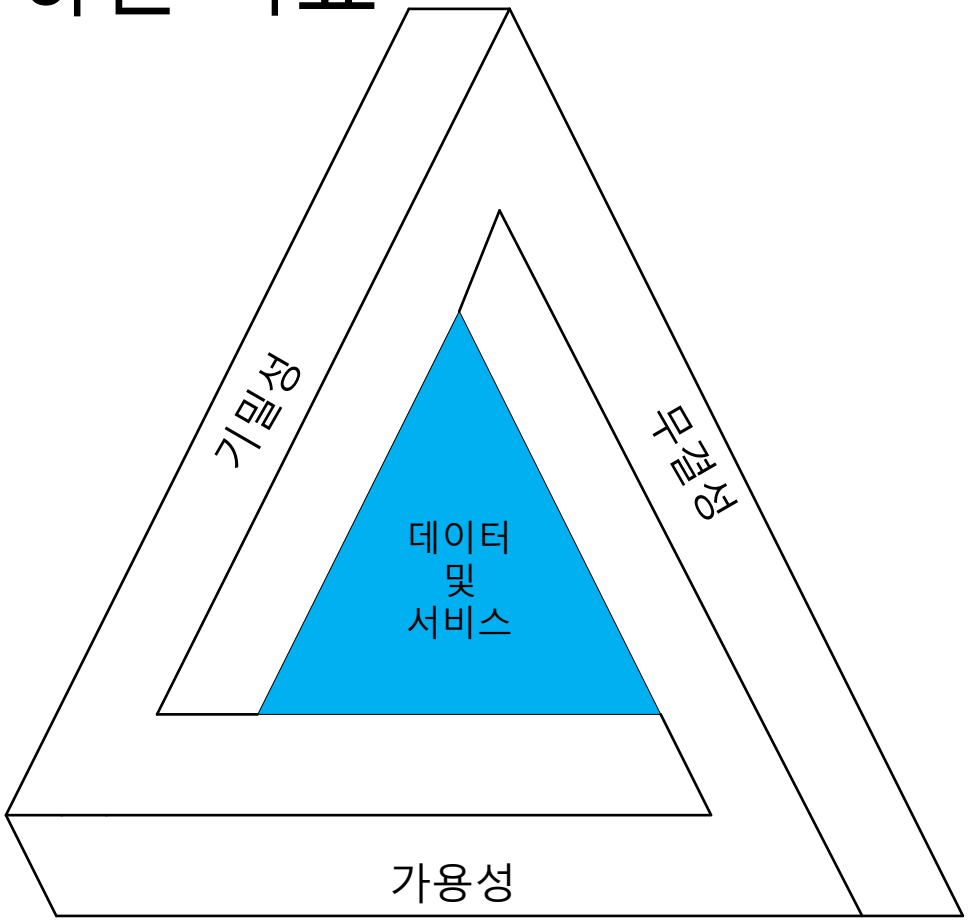
상명대학교 프로토콜공학연구실

목 차

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

컴퓨터 보안 개념

- 정보시스템 자원의 **무결성, 가용성, 기밀성**을 보전하고자 하는 목표



<CIA 트라이어드>

컴퓨터 보안 개념

- 컴퓨터 보안 3가지 주요 목표

1. 기밀성(Confidentiality) : 정보 접근과 공개에 대해 합법적 제한 조건을 지키는 것
   ① 데이터 기밀성 : 개인 정보나 기밀정보를 노출되지 않도록 하는 것
   ② 프라이버시 : 개인이 자신과 관련된 어떤 정보를 통제하거나 영향을 미칠 수 있도록 하는 것
2. 무결성(Integrity) : 부적절한 정보 수정이나 파괴를 막는 것
   ① 데이터 무결성 : 규정에 따라서 또는 허가된 상태에서만 정보나 프로그램을 변경할 수 있도록 하는 것
   ② 시스템 무결성 : 시스템이 의도했던 기능을 손상되지 않은 채 부정하게 시스템이 조작되지 않은 상태로 수행하도록 하는 것

컴퓨터 보안 개념

- 컴퓨터 보안 3가지 주요 목표

  3. 가용성(Availability) : 정보 사용에 있어서 시간성과 신뢰성 있는 접근을 제공하는 것

- 보안 실무 필드에서 추가된 두 가지 개념

  1. 인증(Authentication) : 진짜라는 성질을 확인할 수 있고 신뢰 할 수 있다는 것
  2. 책임(Accountability) : 한 개체의 행동을 추적해서 찾아 낼 수 있어야만 하는 것

컴퓨터 보안 개념

- 보안 침해 세 가지 수준
  - 저급 위험 : 주요 기능은 유지하지만 성능 및 유효성이 줄어듬
  - 중급 위험 : 주요 기능의 성능이 심각하게 저하되며 개인에게 심각한 손상을 끼침
  - 고급 위험 : 주요 기능 중에서 일부 기능을 상실하며 재난 수준의 개인적 손상을 끼침

OSI 보안 구조

- 정의
  - 관리자가 효과적으로 보안 문제를 조직화할 수 있는 유용한 방법을 제공
- OSI 보안 구조 핵심

1. 보안공격 : 정보의 안전성을 침해하는 제반 행위
2. 보안 메커니즘 : 보안 공격을 탐지, 예방 하거나 공격으로 인한 침해를 복구하는 절차
3. 보안 서비스 : 보안 공격을 대응 하기 위한 처리 서비스

*참고 : 보안 서비스는 보안 정책을 구현하고 보안 메커니즘에 의해서 구현된다.

보안 공격

- 보안 공격의 종류

  1. 소극적 공격(Passive attack) : 시스템으로 부터 정보를 획득하거나 사용하려는 시도

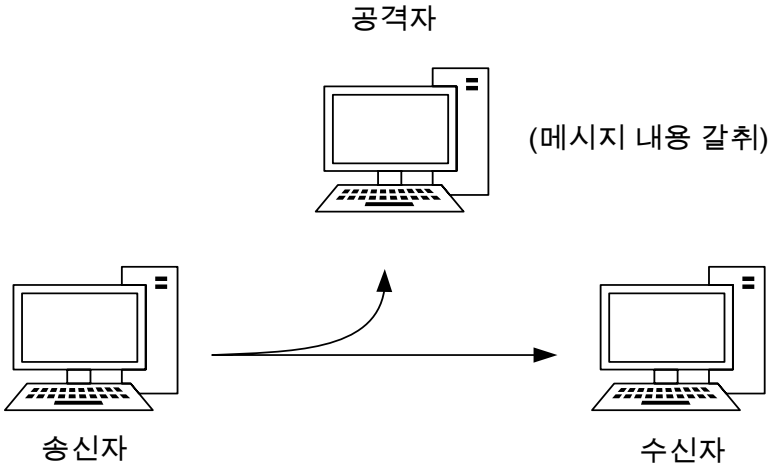
  2. 적극적 공격(Active attack) : 데이터 스트림을 수정하거나 가짜 데이터 스트림을 만드는 행위

- 보안 공격의 차이점
  - 소극적 공격 : 시스템 자원에 영향을 끼치지 않음
  - 적극적 공격 : 시스템 자원 및 시스템 작동에 영향을 끼침

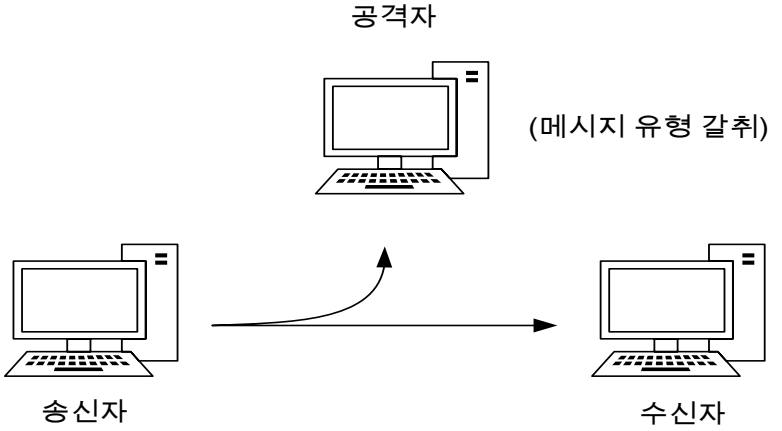
보안 공격

- 소극적 공격 유형

1. 메시지 내용 갈취(Release of message contents)
   : 전달 내용 갈취



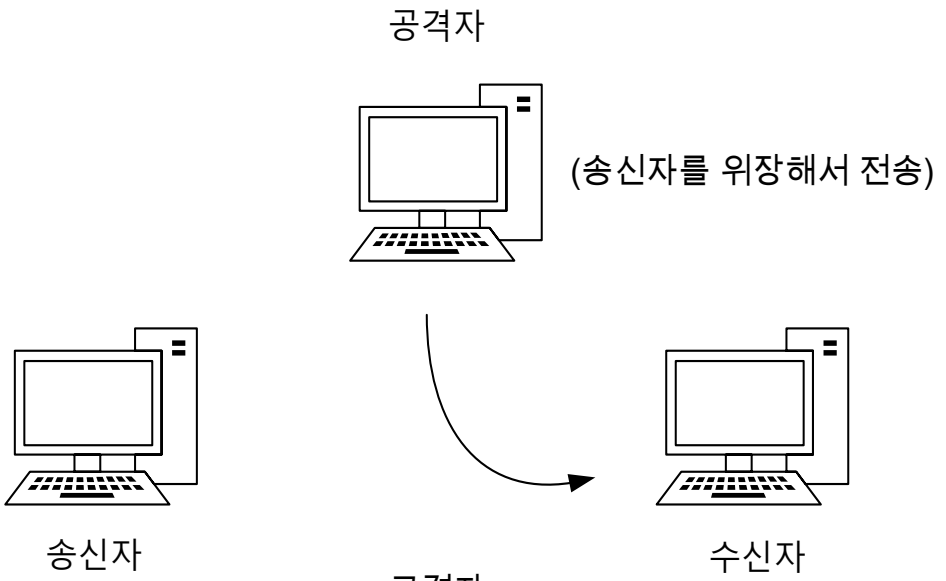
2. 트래픽 분석(Traffic analysis)
   : 통신자의 접속 위치,신원을 파악하거나 메시지의 정보를 관찰



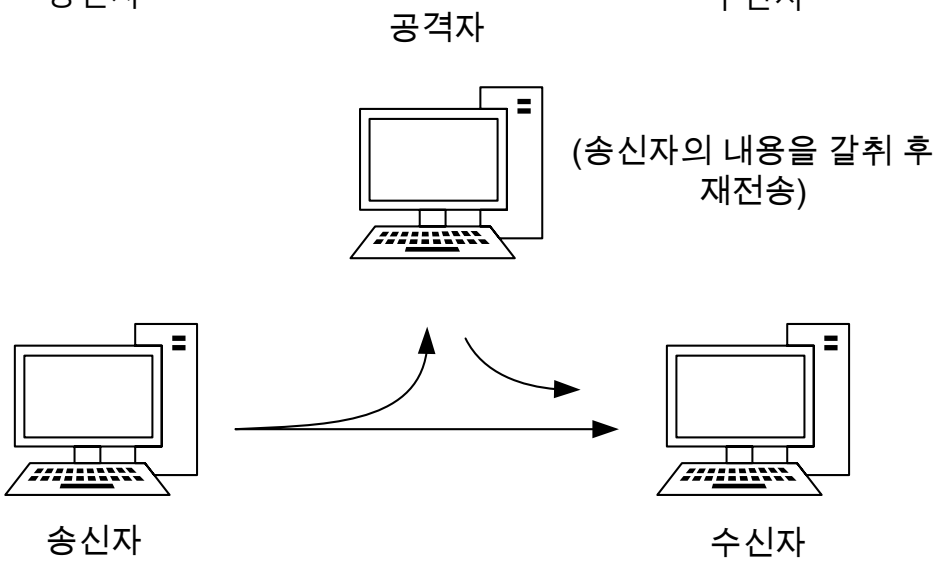
보안 공격

- 적극적 공격 유형

1. 신분위장(Masquerade) : 한 개체가 다른 개체의 행세를 하는 것



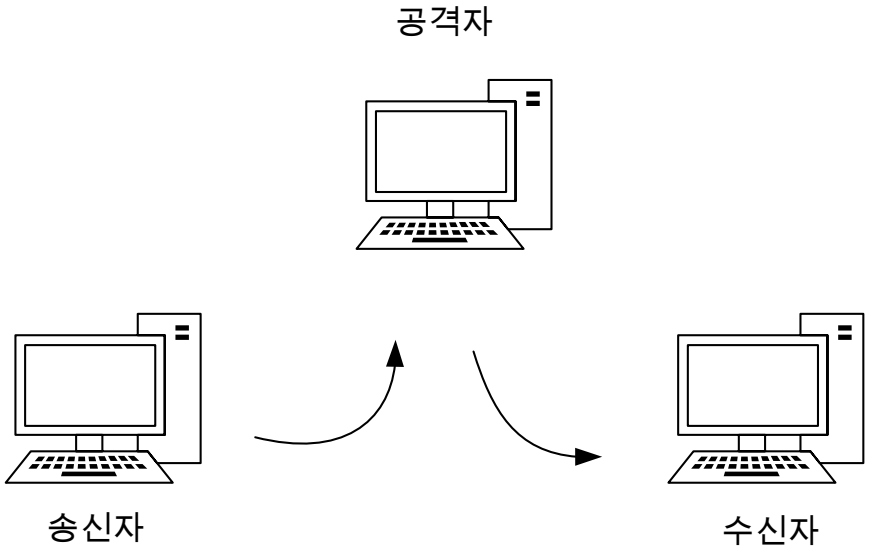
2. 재전송(Replay): 획득한 데이터 단위를 보관하고 있다가 시간이 경과한 후 재전송하는 것



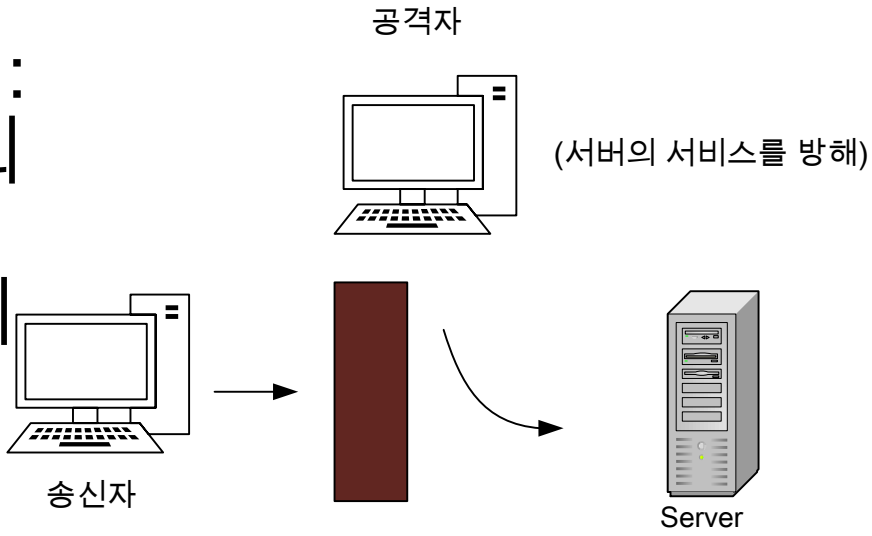
보안 공격

- 적극적 공격 유형

3. 메시지 수정(Modification of messages) : 메시지를 수정, 전송 지연, 순서를 바꾸는 행위



4. 서비스 거부(Denial of service) : 통신 설비가 정상적으로 운용되거나 관리 되지 못하도록 방해하는 행위(어느 개체를 역류, 네트워크를 마비 하는 방법)



보안 서비스

- 정의
  - 시스템, 데이터 전송의 적절한 보안을 보장하는 통신 개방 시스템의 프로토콜 계층에 의해서 제공되는 서비스
    - 가용성 서비스 : 시스템이 자원에 접근할 필요가 있거나 사용하고자 할 때 시스템의 성능에 따라 시스템 자원에 접근할 수 있도록 하는 것

보안 서비스

- 보안 서비스의 분류

1. 인증 서비스(Authentication service) : 통신이 검증 되었다는 것을 확인 해주는 것
   ① 대등 개체 인증(Peer entity authentication) : 통신하는 상대방의 신원을 확인 시킴(연결을 설정할 때와 데이터를 전송하는 과정 중에 사용함)
   ② 데이터 출처 인증(Data origin authentication) : 데이터 단위의 출처에 대한 확인을 함(데이터 단위가 수정 되거나 복제되는 것을 방어하지 못함)
2. 접근 제어(Access control) : 통신 링크를 통한 호스트 시스템과 응용 간의 접근을 제한하고 통제할 수 있는 능력
3. 데이터 기밀성(Data confidentiality) : 공격으로 부터 데이터와 트래픽 흐름을 보호하는 것

보안 서비스

- 보안 서비스의 분류

4. 데이터 무결성(Data integrity)
   - 수신된 데이터와 인증된 개체가 보낸 것이 정확히 일치하는지에 대한 확신을 줌
   - 적극적인 공격과 연관됨
   - 자동화된 복구 메커니즘을 많이 사용

   ① 연결형 무결성 서비스 : 복제, 추가, 수정, 순서 바뀜, 재전송 됨이 없이 그대로 전송되는 것을 보장

   ② 비연결형 무결성 서비스 : 작은 단위에 메시지만 다루는데 일반적으로 메시지 수정에 대해서만 보호

5. 부인 봉쇄(Nonrepudiation) : 송신자나 수신자 양측이 메시지를 전송한 사실 자체를 부인하지 못하도록 막는 것

보안 메커니즘

- 일반 보안 메커니즘과 특정 보안 메커니즘으로 나뉨
  - 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 것 처럼 그 당사자 인지 확인 해주며 8가지로 나뉨

보안 메커니즘

- 보안 서비스와 메커니즘의 관계

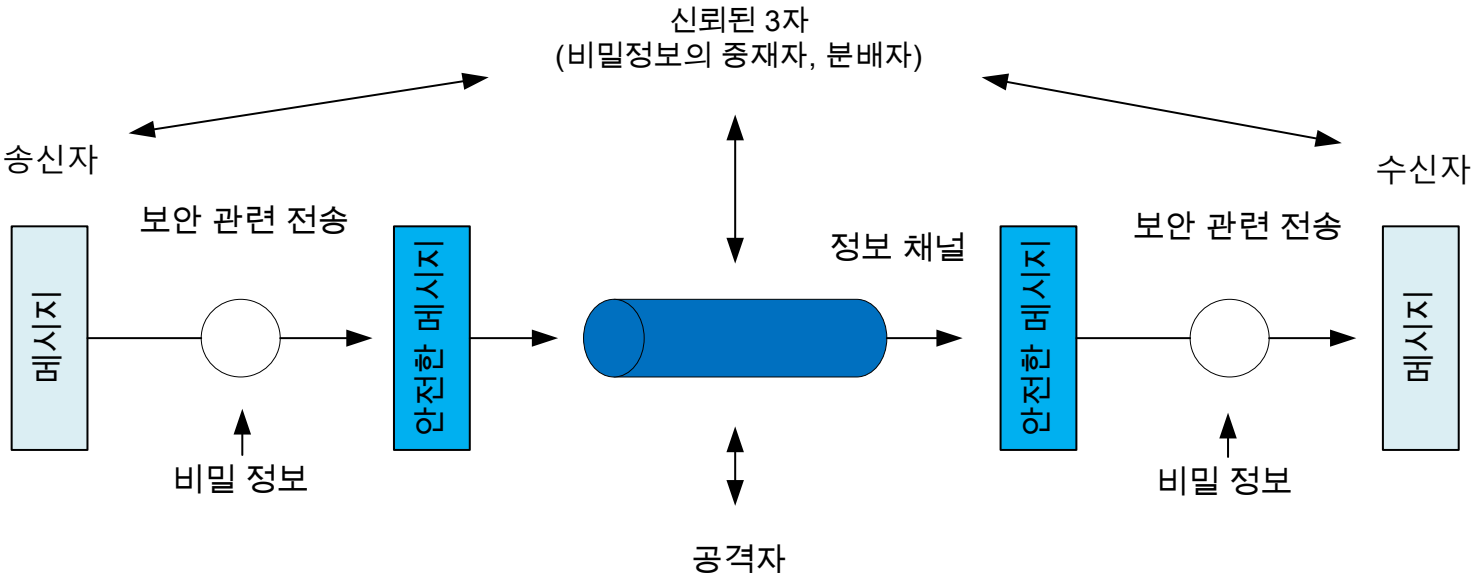
서비스	메커니즘							
	암호화	디지털 서명	접근 제어	데이터 무결성	인증 교환	트래픽 패딩	라우팅 제어	공증
대등 개체인증	Y	Y			Y			
데이터 출처인증	Y	Y						
접근제어			Y					
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y	Y	
데이터 무결성	Y	Y		Y				
부인봉쇄		Y		Y				Y
가용성				Y	Y			

네트워크 보안 모델

- 네트워크 보안 모델 조건
  - 통신주체로서의 양쪽은 교환을 위한 협조가 필요
  - 송신자에서 수신자까지 통과하는 인터넷의 경로를 정의
  - 통신 프로토콜(TCP/IP)을 사용하기로 협의하여 논리적 정보 채널을 구성해야 함
- 모든 보안 기술의 성질
  - 보안을 위한 암호화, 신원 확인을 위한 코드를 메시지에 첨부
  - 각 주체는 비밀정보를 공유

네트워크 보안 모델

- 안전성을 위해 제 3자를 필요로 하는 경우
  - 4가지 기초적인 임무
    1. 보안을 위한 변화를 수행할 알고리즘을 설계
    2. 이 알고리즘에서 사용될 비밀 정보를 생성
    3. 비밀 정보를 공유하고 배분할 수 있는 방법을 개발
    4. 보안 알고리즘 및 비밀정보를 사용하는 양쪽 통신 주체가 사용할 프로토콜을 구체화



네트워크 보안 모델

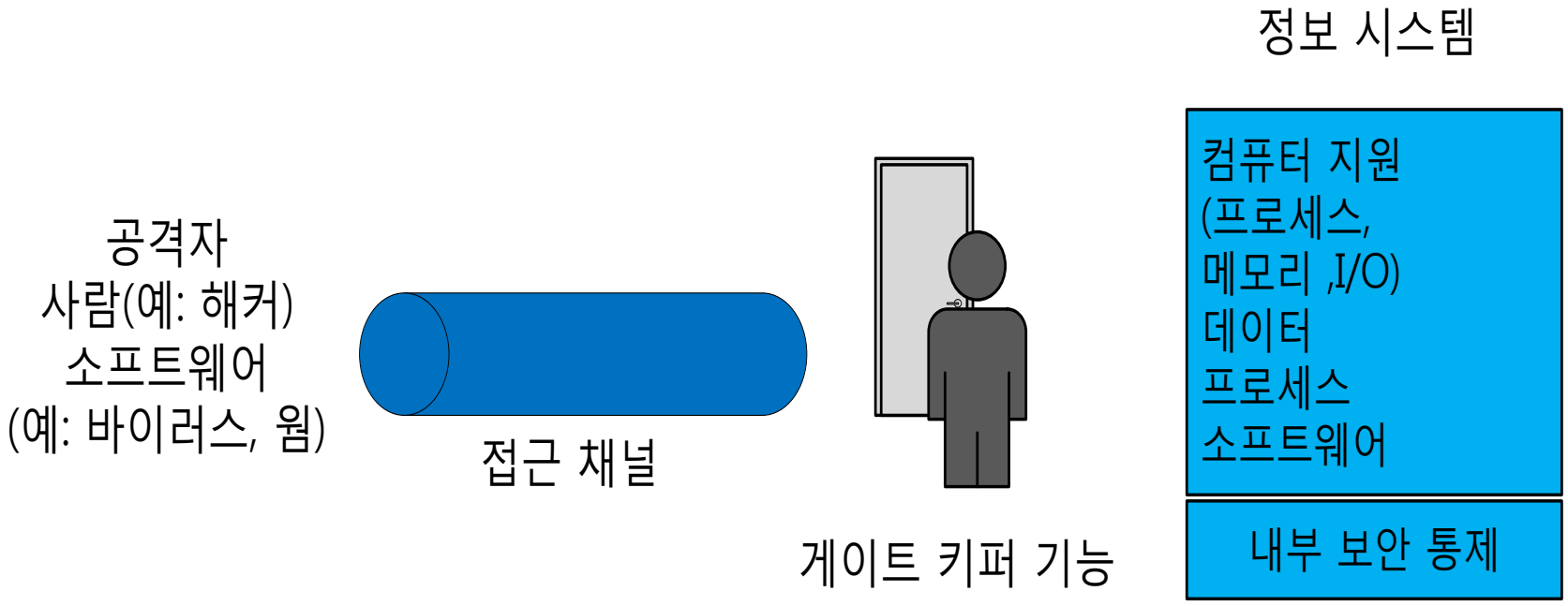
- 논리(Logic)을 심어놓은 프로그램의 위협 형태

1. 정보 접근 위협(Information access threats) : 접근 불허된 데이터를 가로채거나 수정해서 자신에게 유리하도록 만드는 위협
2. 서비스 위협(Service threats) : 합법적인 사용자가 이용하는 것을 방해하기 위해 서비스 결함을 악용하는 위협

- 대표적인 사례 : 바이러스(Virus), 웜(Worm)이 있음

네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 게이트 키퍼(Gatekeeper) : 로그인 과정을 이용해서 사용자를 가려내고 바이러스나 웜 같은 공격을 탐지하여 제거



감사합니다!