2017/06/30, 2017 보안 기초 세미나

Network Security Essential

- 1장 개요 -

최창준 (changjun@pel.smuc.ac.kr)

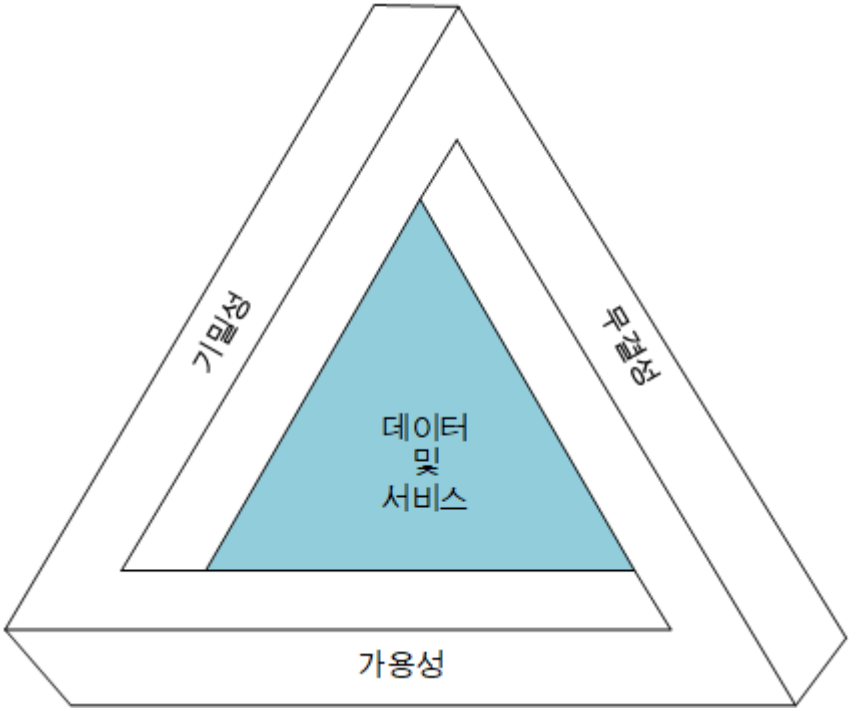
상명대학교 프로토콜공학연구실

목 차

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

컴퓨터 보안 개념

- 컴퓨터 보안 정의
  - 자동화된 정보 시스템 내 자원들의 기밀성, 무결성, 가용성을 보존하기 위해 제공되는 보호



< CIA 트라이어드 >

컴퓨터 보안 개념

- 3대 보안 목적 (1/3)
  - 기밀성 (Confidentiality)
    - 허가 받지 않은 사용자가 정보를 볼 수 없도록 하는 것
      - 명백하게 허가된 대상에게만 정보가 제공되어야 함

1. 데이터 기밀성 (Data Confidentiality)
   - 개인 정보나 기밀 정보를 부정한 사용자가 이용하거나 그들에게 노출되지 않도록 하는 것

2. 프라이버시 (Privacy)
   - 개인이 자신과 관련된 정보가 어떻게 수집되고 저장되는지, 누구에게 공개되는지, 누가 공개하는지 등을 통제하거나 영향을 미칠 수 있도록 하는 것

컴퓨터 보안 개념

- 3대 보안 목적 (2/3)
  - 무결성 (Integrity)
    - 허가 받지 않은 사용자가 데이터를 변형하지 못하도록 원본 데이터를 보호하는 것
      - 정보의 정확성과 안정성을 보장함

1. 데이터 무결성 (Data Integrity)
   - 허가된 상태에서만 정보나 프로그램을 변경할 수 있도록 하는 것

2. 시스템 무결성 (System Integrity)
   - 시스템이 의도했던 기능을 조작되지 않은 상태로 수행하도록 하는 것

컴퓨터 보안 개념

- 3대 보안 목적 (3/3)
  - 가용성 (Availability)
    - 허가 받은 사용자가 데이터를 필요로 할 때 원하는 데이터를 언제든지 제공하도록 보장하는 것
    - 시스템이 지체 없이 동작하도록 하고, 합법적인 사용자에게 서비스를 거절하지 않도록 하는 것

컴퓨터 보안 개념

- 3대 보안 목적 이외에 추가된 개념
  - 인증 (Authentication)
    - 진짜라는 성질을 확인할 수 있고 신뢰할 수 있다는 것
      - 사용자라고 하는 사람이 정말로 그 사용자인지, 시스템에 도착한 자료가 정말로 신뢰할 수 있는 출처에서 온 것인지를 확인하는 것을 의미
  - 책임 (Accountability)
    - 한 개체의 행동을 추적해서 찾아낼 수 있어야만 하는 것
      - 시스템에서 보안 침해 문제가 발생했을 때, 그 문제가 왜 발생했고 어디서 잘못되었는지 찾아낼 수 있어야 함
      - 시스템은 이 활동상황을 기록하고 분석하여 발생한 문제를 해결할 수 있어야 함

컴퓨터 보안 개념

- 보안 침해의 수준
  - 저급 위험
    - 조직의 운영, 자산 또는 개인에게 제한된 부정적 효과가 나타남
      - 수행하고 있는 주요 기능은 유지하지만 성능 및 유효성이 줄어듦
      - 개인에게 소규모 침해를 발생시킴
  - 중급 위험
    - 조직의 운영, 자산 또는 개인에게 심각한 부정적 효과가 나타남
      - 수행하고 있는 주요 기능의 성능이 심각하게 저하됨
      - 조직의 자산에 심각한 재정적 손실을 초래
  - 고급 위험
    - 조직의 운영, 자산 또는 개인에게 극심한 부정적 효과가 나타남
      - 수행하고 있는 주요 기능 중 일부 기능을 상실하고, 성능이 극심하게 저하됨
      - 개인에게 재난 수준의 손상을 끼침

OSI 보안 구조

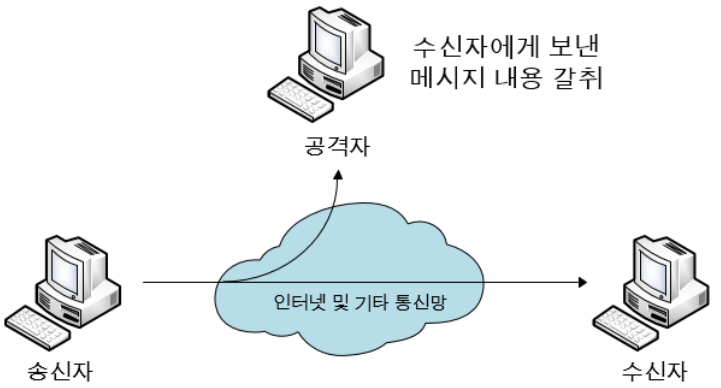
- OSI 보안 구조 정의
  - OSI (Open System Interconnection) 모델
    - 시스템 상호연결에 있어서 개방되어 있는 모델
    - 네트워크 프로토콜 통신을 7계층으로 나누어 설명한 모델
  - OSI 7계층 모델을 바탕으로 관리자가 효과적으로 보안 문제를 조직화 할 수 있게 유용한 방법을 제공하는 보안 구조

OSI 보안 구조

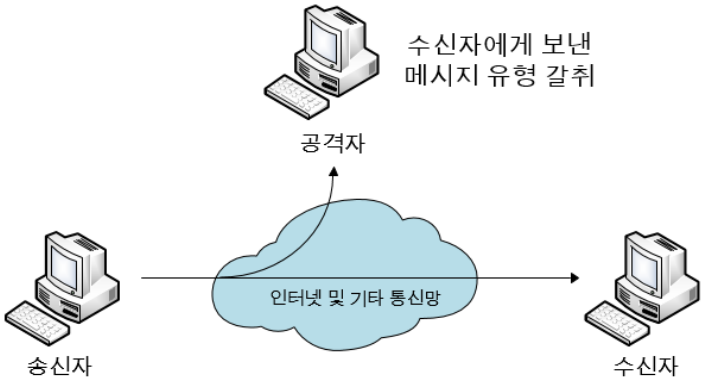
- OSI 보안 구조의 핵심 구성
  1. 보안 공격 (Security Attack)
     - 정보의 안전성을 침해하는 것과 관련된 모든 행위
  2. 보안 메커니즘 (Security Mechanism)
     - 보안 공격을 탐지, 예방하거나 공격으로 인한 침해를 복구하는 절차
  3. 보안 서비스 (Security Service)
     - 보안 공격에 대응하기 위한 처리 서비스

보안 공격

- 보안 공격의 분류 및 유형 (1/3)
  - 소극적 공격 (Passive Attack)
    - 시스템 자원에는 영향을 끼치지 않는 공격 형태
    - 메시지 내용 갈취 (Release of Message Contents)
      - 전화나 메시지를 이용한 정보 전달 내용을 갈취

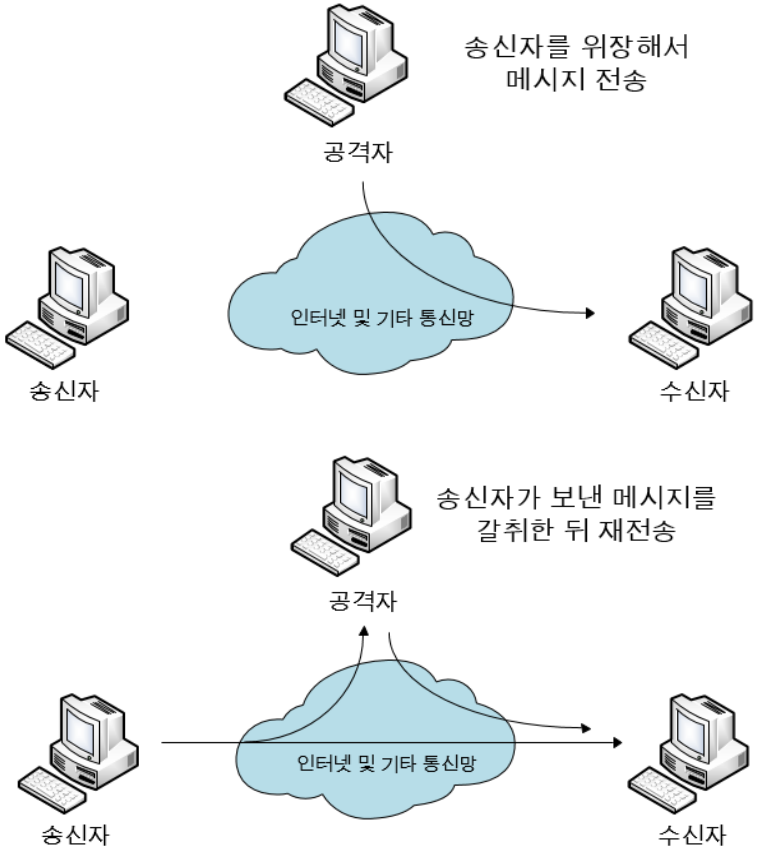


    - 트래픽 분석 (Traffic Analysis)
      - 통신자의 접속위치와 신원을 파악하거나 교환되는 메시지의 빈도와 메시지 길이 등을 관찰하여 통신자의 통신 특성 추측 가능



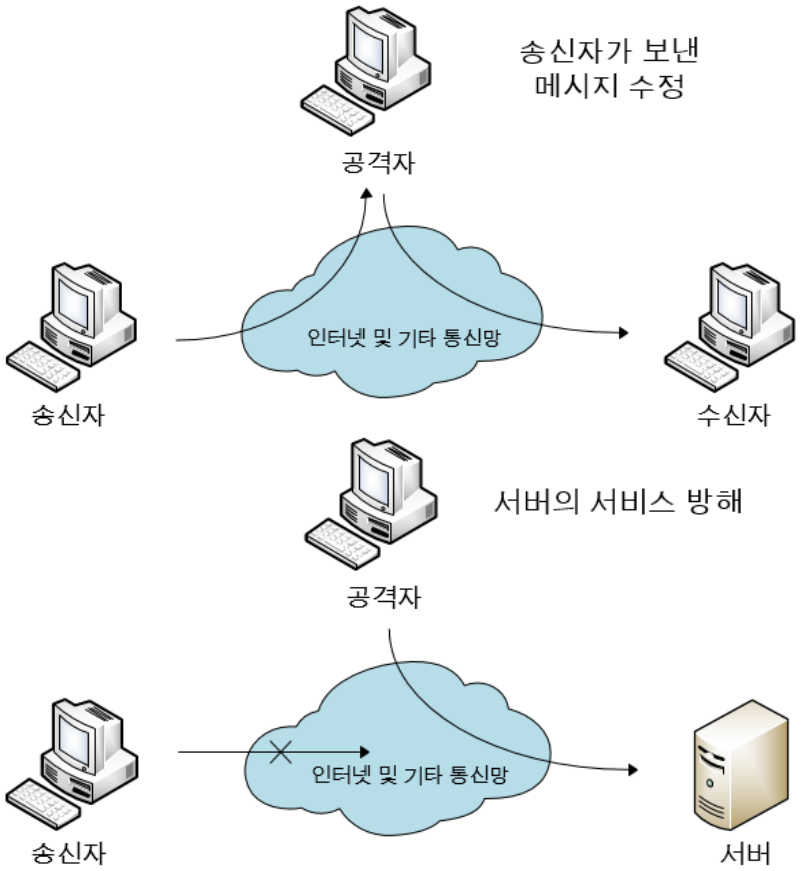
보안 공격

- 보안 공격의 분류 및 유형 (2/3)
  - 적극적 공격 (Active Attack)
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격 형태
    - 신분 위장 (Masquerade)
      - 한 개체가 다른 개체의 행세를 하는 수법
    - 재전송 (Replay)
      - 획득한 데이터를 보관하고 있다가 시간이 경과한 후 재전송하는 수법



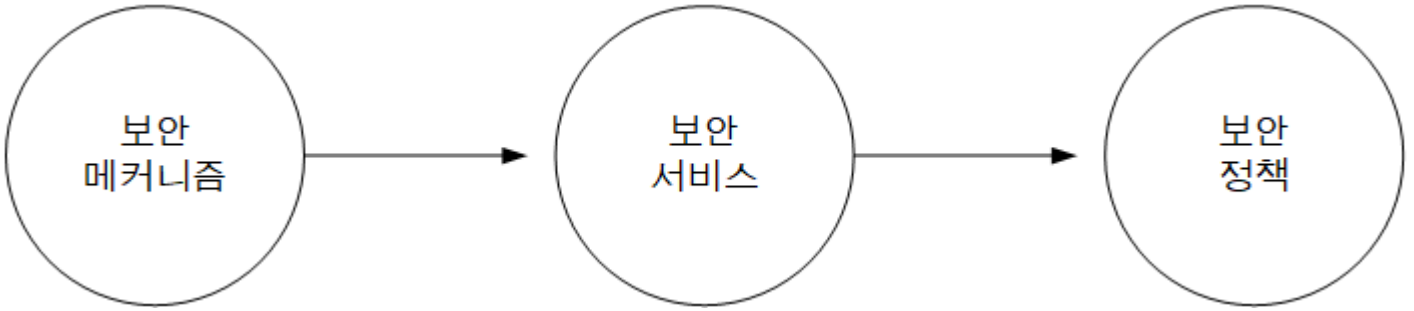
보안 공격

- 보안 공격의 분류 및 유형 (3/3)
  - 적극적 공격 (Active Attack)
    - 메시지 수정 (Modification of Message)
      - 메시지 전송을 지연시키거나 순서를 뒤바꾸어서 불법적으로 내용을 수정하는 수법
    - 서비스 거부 (Denial of Service)
      - 특정 서버에 대량의 접속을 유발하여 과부하를 일으켜 네트워크를 마비시키는 수법



보안 서비스

- 보안 서비스의 정의
  - 시스템 자원 보호를 위해 시스템이 제공하는 처리 서비스
  - 데이터 전송의 보안을 위해 프로토콜 계층에서 제공하는 서비스
  - 보안 서비스는 여러 개의 보안 메커니즘에 의해 구현되고, 보안 정책을 구현함



보안 서비스

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

    1. 대등 개체 인증 (Peer Entity Authentication)
       - 연결하고 있는 개체의 신원을 확인하기 위해 사용하는 인증

    2. 데이터 출처 인증 (Data Origin Authentication)
       - 데이터의 출처를 확인시켜주는 인증

보안 서비스

- 보안 서비스의 분류 (2/4)
  - 접근 제어 (Access Control)
    - 자원을 불법적으로 사용하지 못하도록 방지하는 서비스
  - 부인 봉쇄 (Nonrepudiation)
    - 송신자나 수신자 양측이 메시지를 전송한 사실 자체를 부인하지 못하도록 막는 서비스
  - 기밀성 서비스(Confidentiality Service)
    - 소극적 공격으로부터 데이터의 불법적 노출을 방지하는 서비스
    - 분석 공격으로부터 트래픽 흐름을 보호

보안 서비스

- 보안 서비스의 분류 (3/4)
  - 무결성 서비스 (Integrity Service)
    - 적극적 공격으로부터 데이터를 보호하는 서비스
    - 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신을 줌

    1. 연결형 무결성 서비스 (Connection Integrity Service)
       - 전송된 메시지가 중간에서 변경(복제, 추가, 수정, 순서 바뀜, 재전송 등)되지 않도록 보장하는 서비스

    2. 비연결형 무결성 서비스 (Connectionless Integrity Service)
       - 데이터의 크기가 작은 메시지만 다루고, 일반적으로 메시지 수정에 대해서만 보호를 제공하는 서비스

보안 서비스

- 보안 서비스의 분류 (4/4)
  - 가용성 서비스 (Availability Service)
    - 시스템의 가용성을 보장하기 위해 시스템을 보호하는 서비스
    - 시스템이 자원에 접근할 필요가 있거나 사용하고자 할 때, 시스템의 성능에 따라 시스템 자원에 접근할 수 있도록 하는 서비스

보안 메커니즘

- 보안 메커니즘의 분류
  - 일반 보안 메커니즘 (Pervasive Security Mechanism)
    - OSI 보안 서비스나 프로토콜 계층에 구애 받지 않는 메커니즘
  - 특정 보안 메커니즘 (Specific Security Mechanism)
    - 통신 개체가 주장하는 것처럼 정말로 그 당사자인지를 확인해주는 메커니즘

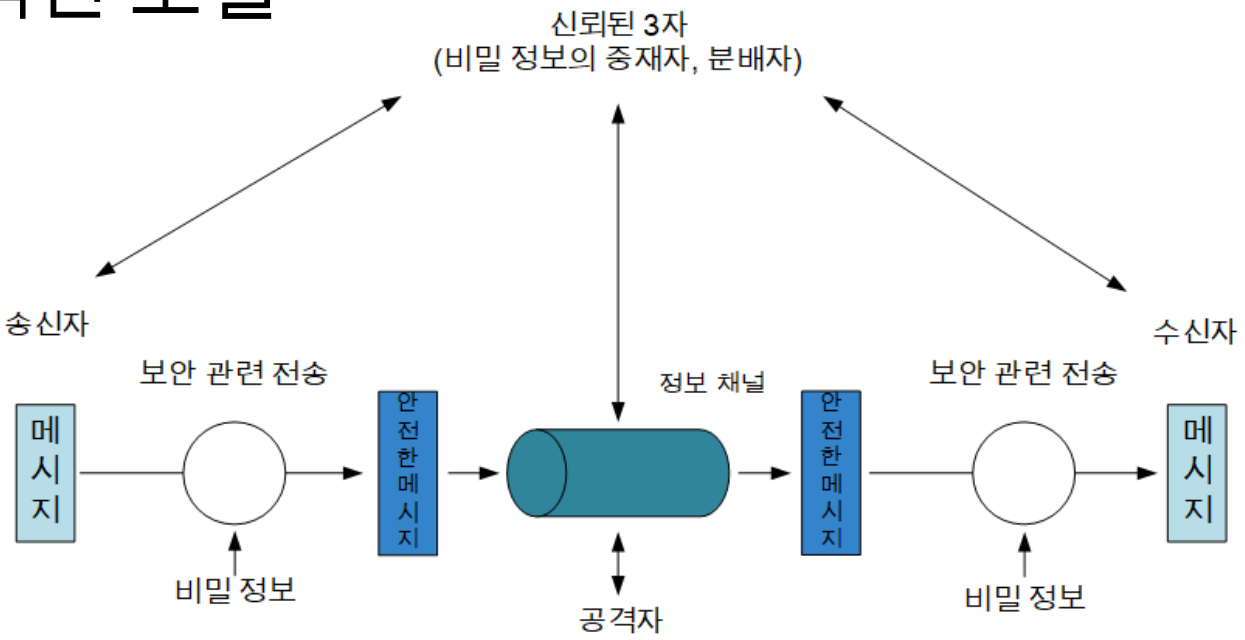
보안 메커니즘

- 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



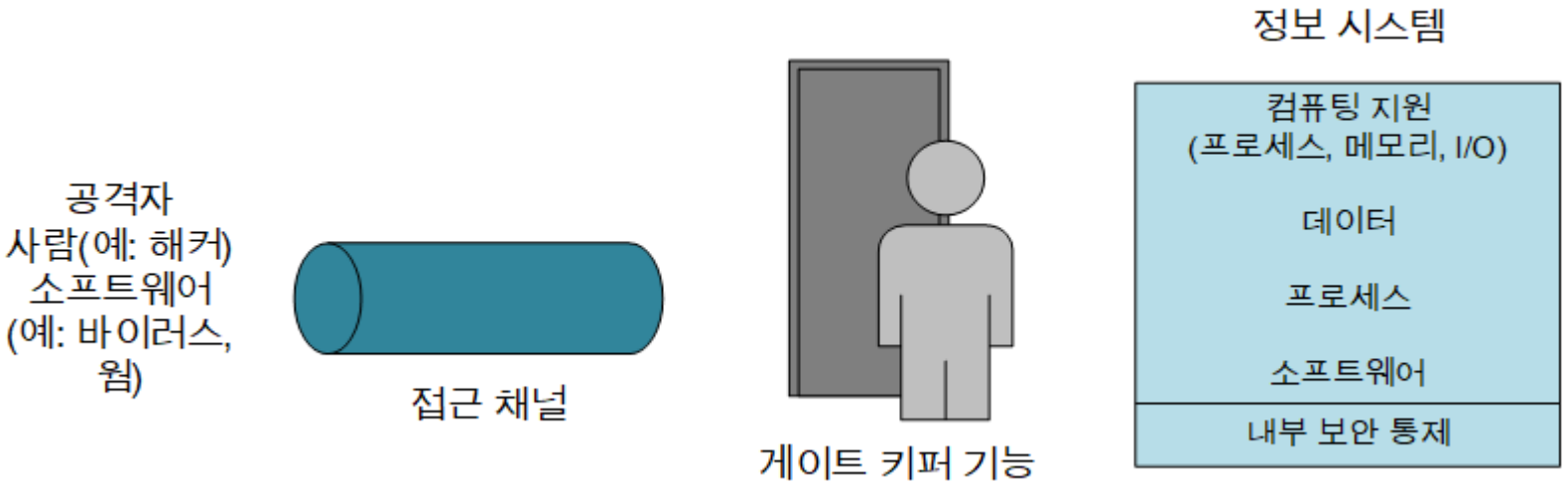
  - 특징
    - 보안을 위한 메시지 암호화
    - 메시지의 신원 확인을 위한 코드 첨부
    - 비밀 정보 공유
      - key

네트워크 보안 모델

- 네트워크 보안 위협 유형
  - 정보 접근 위협 (Information Access Threat)
    - 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정하여 자신에게 유리하도록 만드는 위협
  - 서비스 위협 (Service Threat)
    - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협
  - 대표적인 사례
    - 바이러스 (Virus), 웜 (Worm)

네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 게이트 키퍼 (Gatekeeper)
    - 로그인 과정을 이용하여 사용자를 가려내고, 바이러스나 웜 같은 공격을 탐지하여 제거하는 역할



감사합니다!