2021/07/07, 2021 보안 기초 세미나

Network Security Essentials

- Chapter_1 개요 -

발표자 : 이 태 양(taeyang2.lee@gmail.com)

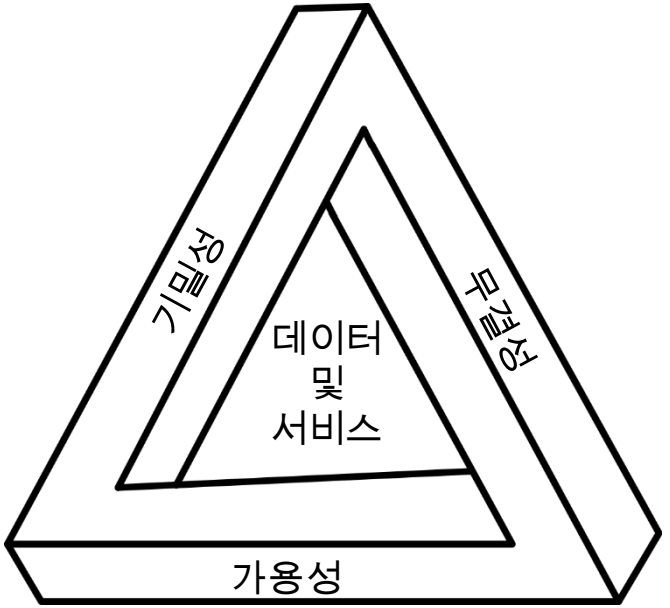
세종대학교 프로토콜공학연구실

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 무결성, 가용성, 기밀성을 보전을 위해 제공된 보호
    - 정보시스템 자원
      - 하드웨어
      - 소프트웨어
      - 펌웨어
      - 정보/데이터
      - 통신
    - CIA 트라이어드
      - 기밀성(Confidentiality)
      - 무결성(Integrity)
      - 가용성(Availability)



<CIA 트라이어드>

컴퓨터 보안 개념

- 컴퓨터 보안의 3가지 주요 목표 (1/3)
  - 기밀성 (Confidentiality)
    - 인가된 사람, 프로세스, 시스템만이 시스템에 접근해야 한다는 성질
      - 데이터 기밀성 (Data Confidentiality)
        - 인가되지 않은 사람이 개인정보나 기밀정보를 이용하거나 그들에게 노출되지 않도록 하는 것
      - 프라이버시 (Privacy)
        - 개인이 자신과 관련된 어떤 정보가 수집, 저장되는지, 누구에게 누가 공개하는지 등을 통제하거나 권한을 갖는 것
    - 특성
      - 정보 접근과 공개에 대해 합법적 제한조건을 지키는 것
      - 기밀성을 상실하게 되면 정보가 부정하게 공개됨

컴퓨터 보안 개념

- 컴퓨터 보안의 3가지 주요 목표 (2/3)
  - 무결성 (Integrity)
    - 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성실
      - 데이터 무결성 (Data integrity)
        - 허가된 상태에서만 정보나 프로그램을 변경할 수 있도록 하는 것
      - 시스템 무결성 (System integrity)
        - 시스템이 기능을 손상되지 않은 채로 수행하도록 하는 것
    - 특성
      - 부적절한 정보 수정이나 파괴를 막을 수 있도록 함
      - 무결성을 상실하게 되면 정보가 무단으로 수정되거나 파괴됨

컴퓨터 보안 개념

- 컴퓨터 보안의 3가지 주요 목표 (3/3)
  - 가용성 (Availability)
    - 시스템이 지체 없이 동작하도록 하고, 합법적 사용자에게 서비스를 거절하지 않도록 하는 것
    - 특성
      - 정보사용에 있어서 시간성과 신뢰성 있는 접근을 할 수 있도록 함
      - 가용성을 상실하게 되면 정보나 정보 시스템을 사용하거나 접근이 불가능함

컴퓨터 보안 개념

- 보안 실무 필드에서 필요한 개념
  - 인증 (Authentication)
    - 진짜라는 성질을 확인할 수 있고 신뢰할 수 있다는 것
      - 전송, 메시지, 메시지 출처 유효성에 대한 확신
      - 사용자라고 하는 사람이 정말 그 사용자인지, 시스템에 도착한 자료가 정말로 신뢰할 수 있는 출처에서부터 온 것인지를 확인하는 것
  - 책임 (Accountability)
    - 보안이 미치는 범위에서는 보안 침해에 대한 정보를 기록, 분석, 추적하고 관련된 분쟁을 해결할 수 있다는 것
      - e.g., 부인봉쇄, 억제, 결함 분리, 침입 탐지 및 예방, 사후 복구, 법적 조치

컴퓨터 보안 개념

- 보안 침해의 3가지 수준
  - 저급 위험
    - 개인이나 조직에게 제한된 부정적 효과가 발생
    - 조직의 주요 기능을 그대로 유지할 수 있지만 어느 기간 동안 성능이 떨어지고 개인이나 조직에게 소규모 침해가 발생
  - 중급 위험
    - 개인이나 조직에게 심각한 부정적 효과가 발생
    - 조직의 주요 기능에 대하여 특정 기간 동안 성능이 심각하게 저하되고 개인이나 조직에게 심각한 손상을 끼침
  - 고급 위험
    - 개인이나 조직에게 극심하고 재난수준의 부정적 효과를 줌
    - 조직의 주요 기능 중 한두 가지를 상실하여 성능이 극심하게 저하됨 개인이나 조직에게 극심한 재난수준의 손상을 끼침

OSI 보안 구조

- OSI 보안 구조
  - OSI (Open System Interconnection)
    - 서로 다른 종류의 정보처리시스템 사이를 접속하여 정보교환과 데이터처리를 할 수 있도록 표준화한 컴퓨터 네트워크 구조
    - 물리, 데이터 링크, 네트워크, 전송, 세션, 표현, 응용의 순으로 7계층

OSI 보안 구조

- OSI 보안 구조의 정의
  - 관리자가 효과적으로 보안 문제를 조직화 할 수 있는 유용한 방법
  - OSI 보안 구조의 핵심
    - 보안 공격 (Security attack)
      - 기관이 소유한 정보의 안정성을 침해하는 것과 관련된 모든 행위
    - 보안 메커니즘 (Security mechanism)
      - 보안 공격을 탐지, 예방하거나 공격으로 인한 침해를 복구하는 절차
    - 보안 서비스 (Security service)
      - 정보 전송과 데이터 처리 시스템의 보안을 강화하기 위한 처리 서비스 또는 통신 서비스
      - 보안 공격에 대응하기 위한 것
      - 하나 이상의 보안 메커니즘을 사용하여 서비스를 제공

보안 공격

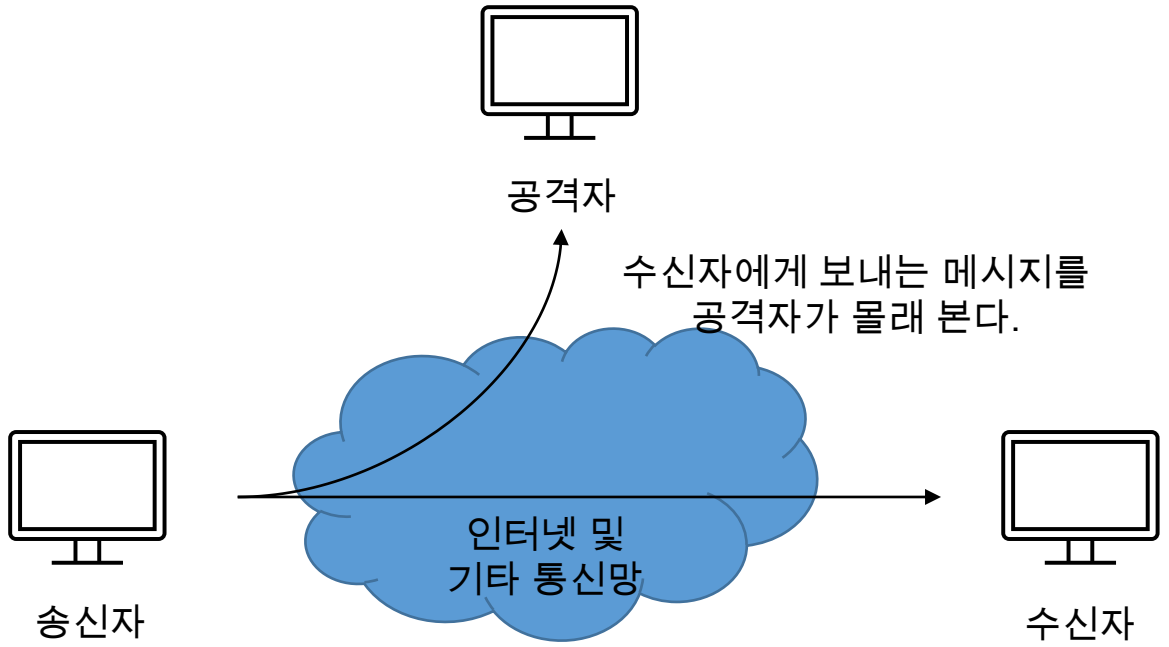
- 위협과 공격
  - 위협 (Threat)
    - 보안 취약점을 이용하려는 잠재적인 위험
      - 보안 침해와 위해를 가할 수 있는 환경, 능력, 행동 사건
  - 공격 (Attack)
    - 지적인 위협을 수반하는 시스템 보안에 대한 침범
      - 지적인 위협이란 보안 서비스를 교묘히 피하거나 시스템 보안 정책을 위반하는 정교한 시도

보안 공격

- 보안 공격의 분류 (1/2)
  - 소극적 공격 (Passive attack)
    - 시스템으로부터 정보를 획득하거나 사용하려는 시도
    - 시스템 자원에 영향을 끼치지 않는 공격 형태
    - 전송 정보에 대한 도청이나 감시
    - 전송 중인 정보를 취득하는 것이 목표
    - 유형으로 메시지 내용 갈취, 트래픽 분석이 있음
    - 공격을 탐지하기 어려워 예방에 더 신경을 써야 함

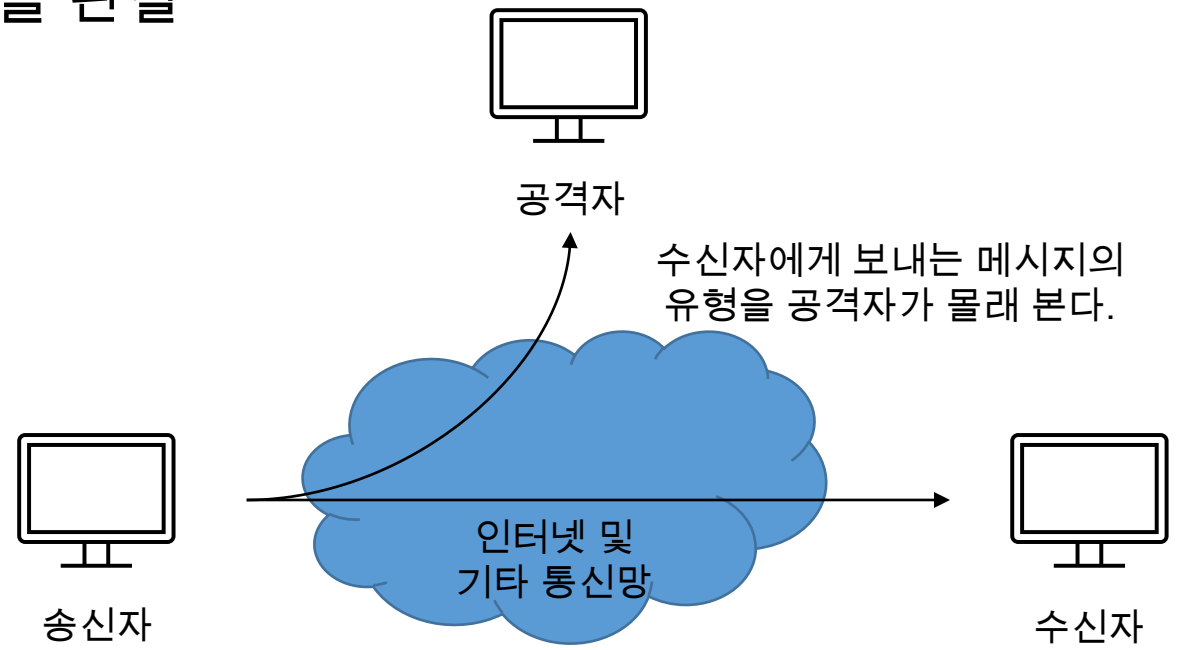
보안 공격

- 보안 공격의 분류 (1/2)
  - 소극적 공격 (Passive attack) (1/2)
    - 메시지 내용 갈취 (Release of message contents)
      - 공격자가 전달되는 정보와 내용을 몰래 취득하거나 보는 것



보안 공격

- 보안 공격의 분류 (1/2)
  - 소극적 공격 (Passive attack) (2/2)
    - 트래픽 분석 (Traffic analysis)
      - 메시지의 유형을 관찰하여 통신자의 통신 특성을 추측하는 것
      - 통신자의 접속위치, 신원파악, 교환되는 메시지의 빈도, 메시지 길이 등을 관찰

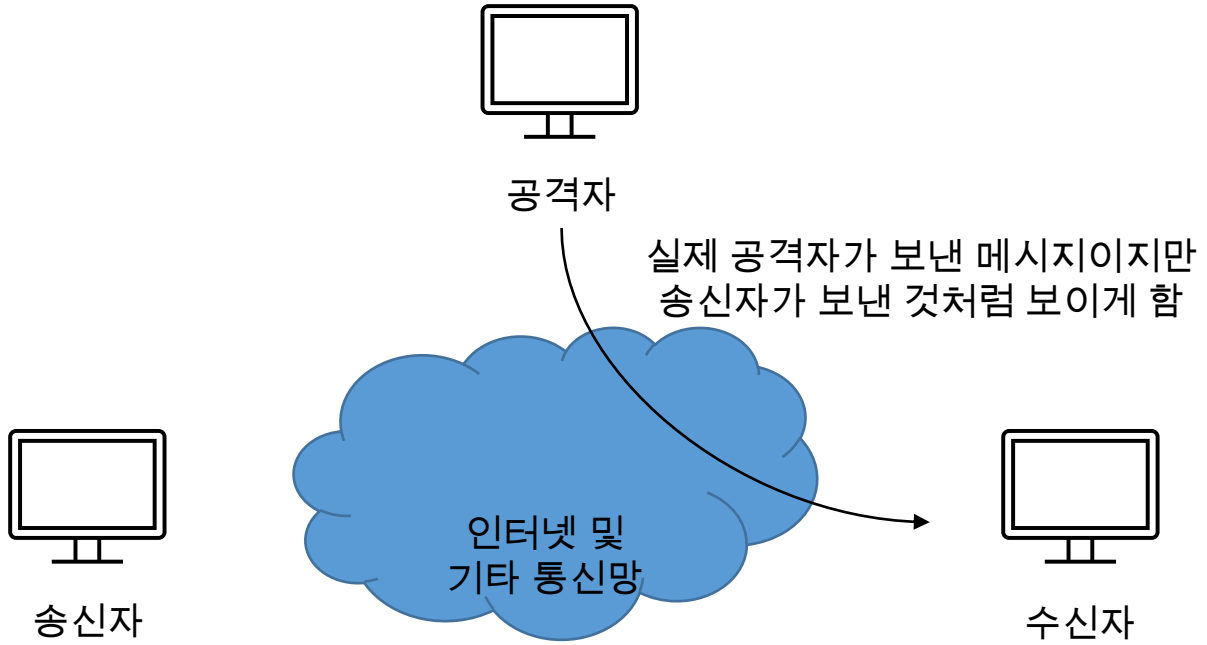


보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack)
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격 형태
    - 신분위장, 재전송, 메시지 수정, 서비스 거부의 형태가 있음
    - 적극적 공격을 완벽하게 차단하는 것은 불가능함
    - 공격으로 인한 피해를 복구하는 것이 목표

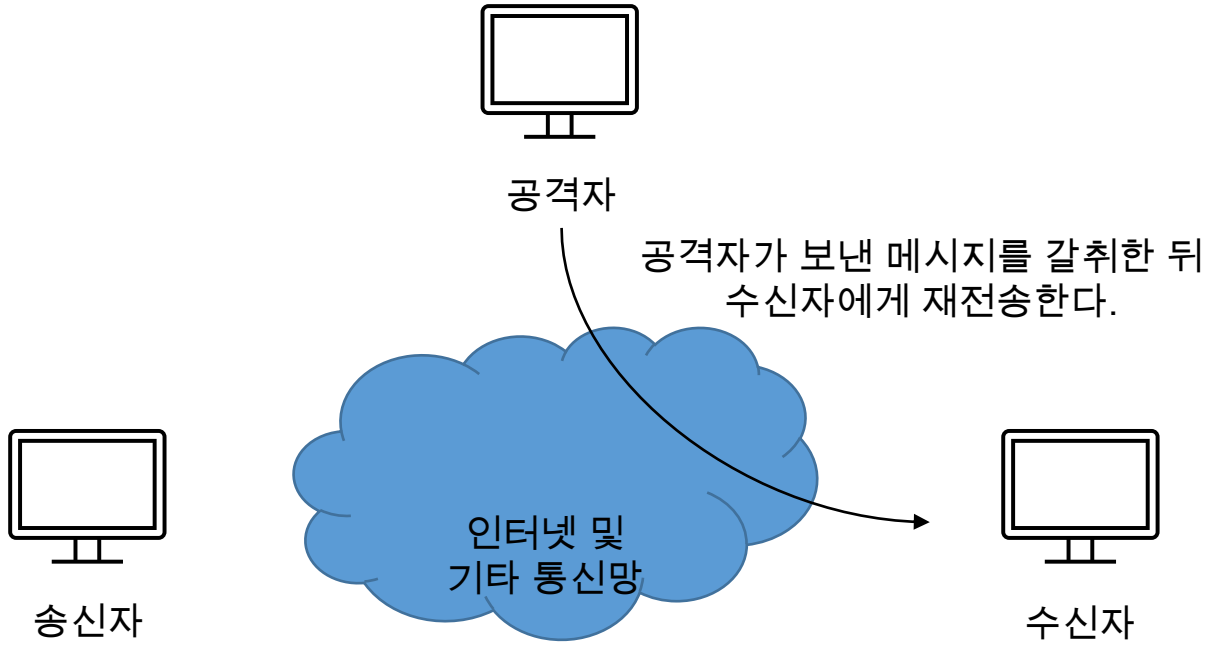
보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (1/4)
    - 신분 위장 (Masquerade)
      - 한 개체가 다른 개체의 행세를 하는 것
      - 다른 형태의 적극적 공격과 병행해서 수행됨
        - e.g., 메시지를 갈취한 다음 메시지 재전송을 시도



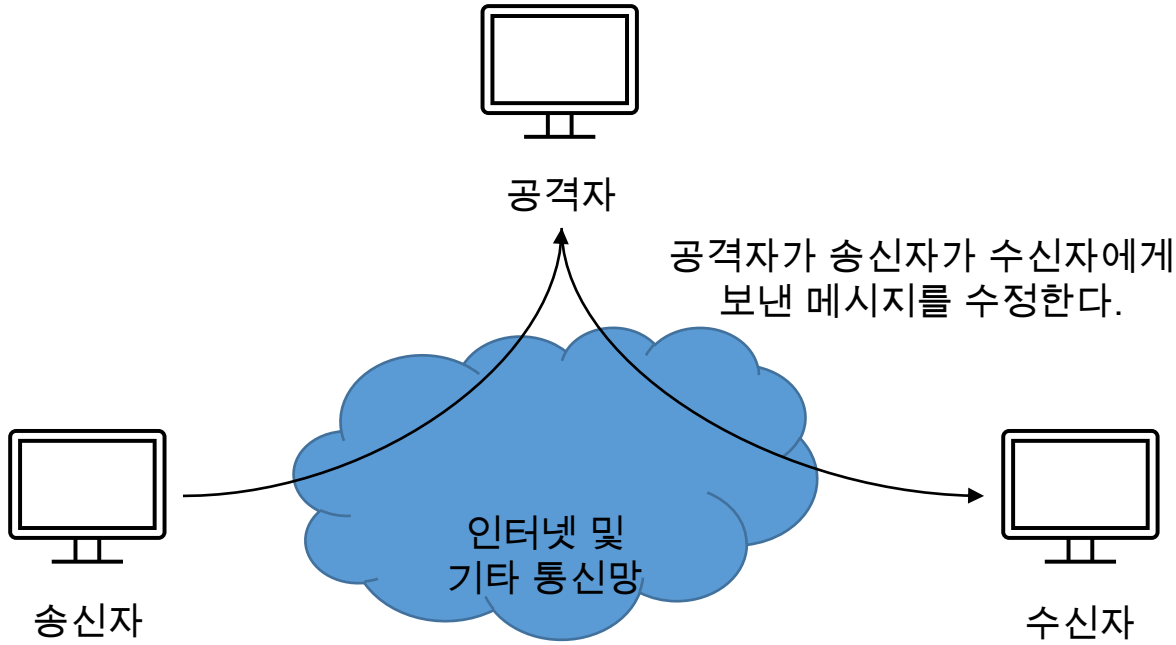
보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (2/4)
    - 재전송 (Replay)
      - 획득한 데이터 단위를 보관하고 있다가 시간이 경과한 후 재전송하여 인가되지 않은 사항에 접근하는 공격 형태



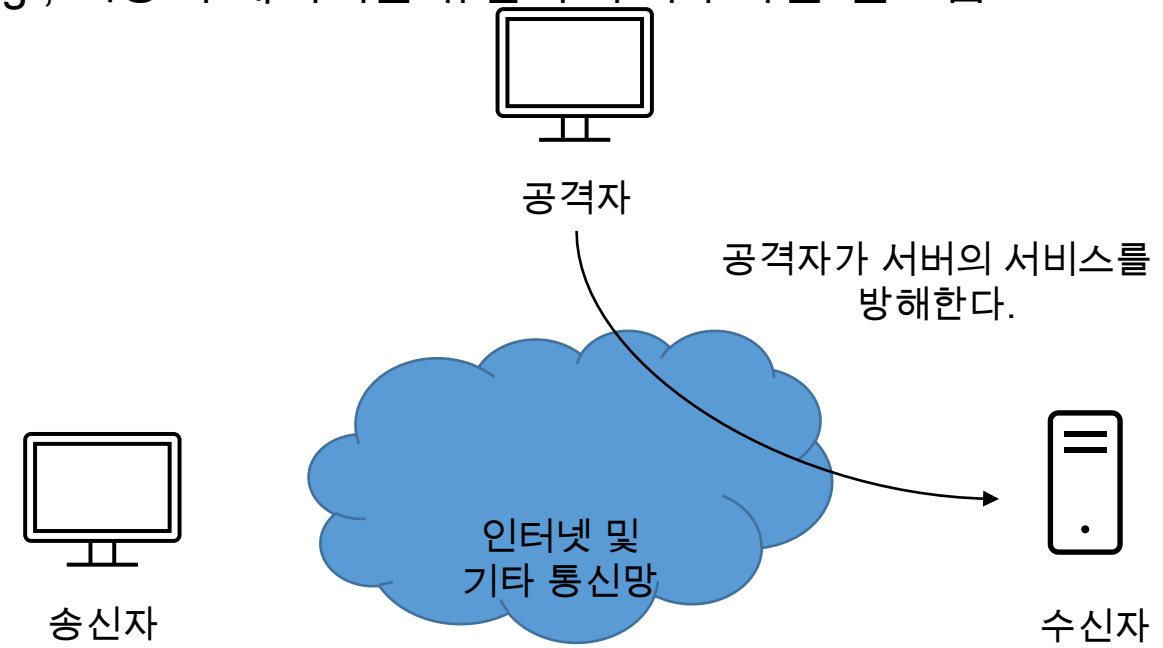
보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (3/4)
    - 메시지 수정 (Modification of Message)
      - 메시지의 일부를 불법으로 수정하거나 메시지 전송을 지연시키거나 순서를 뒤바꾸어 인가되지 않은 효과를 노리는 공격 행태



보안 공격

- 보안 공격의 분류 (2/2)
  - 적극적 공격 (Active attack) (4/4)
    - 서비스 거부 (Denial of service)
      - 통신설비가 정상적으로 운용되거나 관리되지 못하도록 방해하는 공격 형태
      - 특정 목표물을 대상을 할 수 있음
        - e.g., 대량의 메시지를 유발하여 과부하를 일으킴



보안 서비스

- 보안 서비스의 정의
  - 시스템의 적절한 보안이나 데이터 전송의 보안을 보장하기 위해 제공되는 서비스
  - 보안서비스는 보안 정책을 구현하고, 보안 메커니즘에 의해 구현됨

보안 서비스

- 보안 서비스의 분류 (1/6)
  - 인증 서비스 (Authentication service)
    - 통신이 검증되었다는 것을 확인해주는 것
    - 대등 개체 인증 (Peer Entity Authentication)
      - 연결하고 있는 개체의 신분을 확신 시켜 줌
    - 데이터-출처 인증 (Data-Origin Authentication)
      - 비연결 전송에서 수신된 데이터의 출처를 확인해 줌

보안 서비스

- 보안 서비스의 분류 (2/6)
  - 접근 제어 (Access Control)
    - 통신 링크를 통한 호스트 시스템과 응용 간의 접근을 제한하고 통제할 수 있는 것
      - 서비스를 누가, 어떤 조건하에, 어떤 자원을 사용하도록 하는지를 말하는 자원에 접근할 수 있는 제한을 말함
    - 신원 확인에 따라 해당 개체에 적합한 접근 권한을 부여

보안 서비스

- 보안 서비스의 분류 (3/6)
  - 데이터 기밀성 (Data Confidentiality)
    - 소극적 공격으로부터 데이터를 보호하는 것
    - 분석공격으로부터 트래픽 흐름을 보호하는 것

- 보안 서비스의 분류 (4/6)
  - 데이터 무결성 (Data Integrity)
    - 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신
    - 연결형 무결성 서비스
      - 보낸 메시지가 변경 없이 송신되는 것을 보장함
    - 비연결형 무결성 서비스
      - 작은 단위 메시지 수정에 대해서만 보호 서비스를 제공

보안 서비스

- 보안 서비스의 분류 (5/6)
  - 부인봉쇄 (Nonrepudiation)
    - 통신의 주체가 통신에 참여했던 사실을 부인하는 것을 방지
      - 수신자가 송신자로부터 온 메시지라는 것을 확신함
      - 송신자에게는 메시지를 받은 주체가 수신자라는 것을 확신함

- 보안 서비스의 분류 (6/6)
  - 가용성 서비스 (Availability Service)
    - 가용성은 사용자가 요구할 때 시스템 성능에 따라 서비스를 제공하는 것
    - 가용성 서비스는 시스템의 가용성을 보장하기 위해 시스템을 보호하는 서비스

보안 메커니즘

- 보안 메커니즘의 분류
  - 특정 보안 메커니즘, 일반 보안 메커니즘으로 분류
  - 특정 보안 메커니즘 (Specific Security Mechanism)
    - 통신 개체가 주장하는 것처럼 정말로 그 당사자인지를 확인해주는 것
  - 일반 보안 메커니즘 (Pervasive Security Mechanism)
    - 임의의 특정 OSI 보안 서비스나 프로토콜 계층에 구애받지 않는 메커니즘

보안 메커니즘

- 특정 보안 메커니즘 (Specific Security Mechanism)
  - 종류
    - 암호화 (Encipherment)
      - 데이터를 읽을 수 없는 형태로 변환하는 데 수학적 알고리즘을 사용하는 것
      - 데이터의 변환과 복구는 알고리즘과 사용되는 키에 따라 달라짐
    - 디지털 서명 (Digital Signature)
      - 데이터 수신자가 데이터의 발신자와 무결성을 입증하기 위한 기술
      - 위조를 막도록 데이터에 붙이는 데이터 또는 데이터 단위의 암호적 변경
    - 접근 제어 (Access Control)
      - 자원에 접근할 권한을 제한하는 다양한 메커니즘
    - 데이터 무결성 (Data Integrity)
      - 데이터 단위나 데이터 단위의 스트림의 무결성을 확신하는데 사용되는 메커니즘

보안 메커니즘

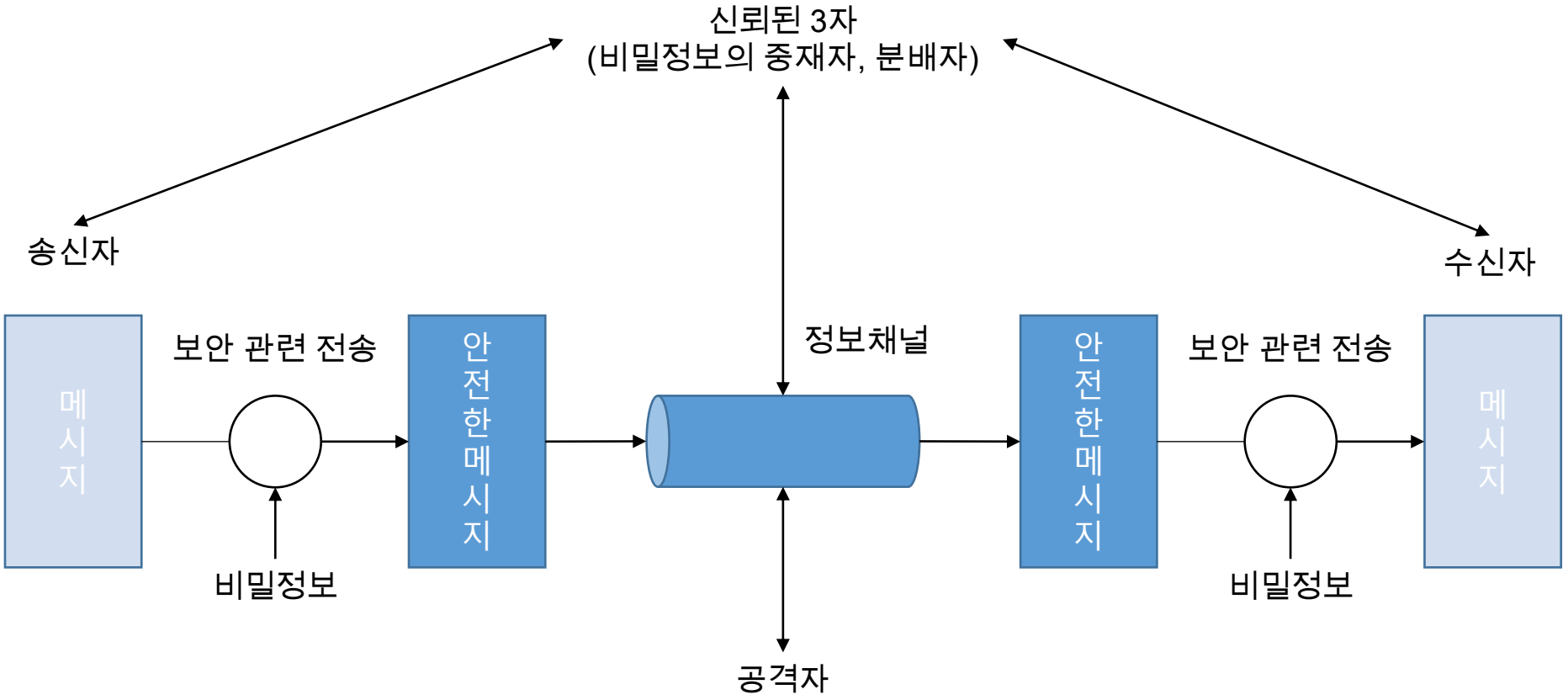
- 특정 보안 메커니즘 (Specific Security Mechanism)
  - 종류
    - 인증교환 (Authentication Exchange)
      - 정보교환을 통해 개체의 신원을 확인하는 데 사용하는 메커니즘
    - 트래픽 패딩 (Traffic Padding)
      - 트래픽 분석 시도를 방해하기 위해 데이터 스트림 안의 빈 곳에 비트를 채워 넣는 것
    - 경로 제어 (Routing Control)
      - 특정 데이터에 대해 물리적으로 안전한 경로를 선택할 수 있도록 하는 것
      - 보안침해가 의심스런 경우 경로를 변경할 수 있게 함
    - 공증 (Notarization)
      - 데이터 교화의 어떤 성질을 확신하기 위해 신뢰받는 제3자를 이용하는 것

보안 메커니즘

- 일반 보안 메커니즘 (Pervasive Security Mechanism)
  - 종류
    - 신뢰받는 기능 (Trusted Functionality)
      - 보안정책과 같은 기준으로 볼 때 올바른 것으로 여겨지는 것
    - 보안 레이블 (Security Label)
      - 자원의 보안속성에 이름을 붙이거나 자원의 보안속성을 지정하는 그 자원에 대한 표시
    - 사건 탐지 (Event Detection)
      - 보안 관련 사건을 탐지하는 것
    - 보안 감사 추적 (Security Audit Trail)
      - 보안 감사를 하기 위해 수집하거나 이용되는 데이터로서 시스템 기록과 동작을 독립적으로 조사하고 검토하는 것
    - 보안 복구 (Security Recovery)
      - 사건처리와 관리기능 같은 메커니즘의 요구사항을 다루고 복구 동작을 수행

네트워크 보안 모델

- 네트워크 보안 모델 (Network Security Model)
  - 일반적인 모델



네트워크 보안 모델

- 네트워크 보안 모델 (Network Security Model)
  - 인터넷을 통한 메시지 송신과정에서 통신주체(Principals)의 양쪽은 교환을 위한 협조가 필요
  - 송신자로부터 수신자까지 인터넷을 통과하는 경로를 정의
  - 양 통신주체는 통신 프로토콜(TCP/IP)을 사용하기로 협의하여 논리적 정보 채널을 구성해야 함

  - 모든 보안기술의 성질
    - 보안을 위해 전송될 정보를 변환하여 암호화, 신원 확인을 위한 코드를 메시지에 첨부
    - 양 통신주체는 비밀정보를 공유함

네트워크 보안 모델

- 네트워크 보안 모델 (Network Security Model)
  - 안전한 전송을 위해 신뢰할 수 있는 제 3자가 필요한 경우
    - 제3자는 공격자가 모르는 비밀정보를 두 송신 주체에게 책임지고 전달하는 임무를 가짐
    - 메시지 전송의 인증에 있어서 양쪽 통신 주체 간 분쟁이 발생할 경우 조정자 역할을 함
  - 특정 보안 서비스를 설계의 4가지 기초적인 임무
    - 보안을 위한 변환을 수행할 알고리즘 설계
    - 이 알고리즘에서 사용될 비밀 정보를 생성해야 함
    - 비밀 정보를 공유하고 배분할 수 있는 방법을 개발해야 함
    - 특정 보안 서비스를 위해 보안 알고리즘 및 비밀정보를 사용할 양쪽 통신 주체가 사용할 프로토콜을 구체화해야 함

네트워크 보안 모델

- 침입 보호 목적의 보안 모델

공격자

- 사람(예: 해커)
- 소프트웨어
  (예 : 바이러스, 웜)

접근 채널

게이트 키퍼
기능

정보 시스템

컴퓨팅 지원 (프로세스, 메모리, I/O) 데이터 프로세스 소프트웨어
내부 보안 통제

네트워크 보안 모델

- 침입 보호 목적의 보안 모델
  - 해커 (Hacker)
    - 시스템을 깰 수 있다는 자기만족을 위해 침입하는 공격자
  - 침입자 (Intruder)
    - 손해를 끼칠 의도가 있는 공격자
  - 침입 유형
    - 정보 접근 위협 (Information Access Threats)
      - 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정해서 그 사용자 자신에게 유리하도록 만드는 위협
    - 서비스 위협 (Service Threats)
      - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협

네트워크 보안 모델

- 침입 보호 목적의 보안 모델
  - 소프트웨어 공격의 대표적인 사례
    - 악성 로직이 잠복된 시스템 공격, 네트워크를 통해 전염 될 수 있음
    - 바이러스 (Virus)
      - 악의적 목적을 가진 스스로를 복제하는 악성 소프트웨어, 프로그램에 기생함
    - 웜 (Worm)
      - 악의적 목적을 가진 스스로를 복제하는 악성 소프트웨어, 독자적으로 실행 됨, 복사본을 네트워크로 전송

네트워크 보안 모델

- 침입 보호 목적의 보안 모델
  - 불법 침입 문제의 보안 방법
    - 케이트키퍼 (Gate Keeper)
      - 패스워드 로그인 과정을 이용해서 인가받지 않은 사용자를 가려내고 악성 소프트웨어를 탐지하고 제거하는 것
    - 모니터링 (Monitoring)
      - 1차적으로 인가받지 못한 사용자, 악성 소프트웨어 차단
      - 2차적으로 침입자 탐지를 위해 컴퓨터 동작 모니터링, 저장된 정보 분석 등의 내부적 제어를 수행

Thanks!

이 태 양 (taeyang2.lee@gmail.com)