2018/01/02, 2018 보안 기초 세미나

Network Security Essentials

- Chapter_1 개요 -

최서윤 (seoyun@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

목 차

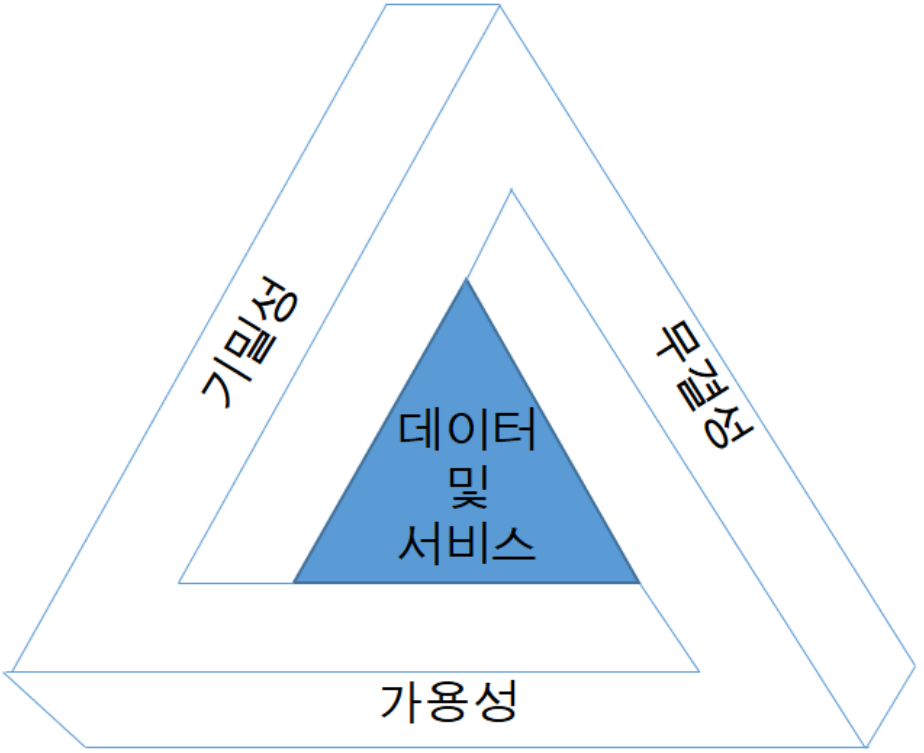
컴퓨터와 보안

- 최근 보안 동향
  - Symantec 2018 Cyber Security Predictions
    - 블록체인 기술 자체보다 코인 교환 및 지갑에 공격 집중될 것
    - 파일리스(Fileless)공격 증가
      - 파일을 이용하지 않고 컴퓨터의 RAM에 직접 기록하는 감염
    - 공급망(Supply Chain) 공격이 사이버 공격의 주류가 될 것
      - 계약자, 시스템, 공급 업체 침해
    - 기관은 SaaS(Security-as-a-Service)와 IaaS(Infrastructure-as-a-Service) 보안에 유의해야 할 것
    - IoT 기기가 공격에 노출됨과 동시에 공격에 이용될 것

목 차

컴퓨터 보안 개념

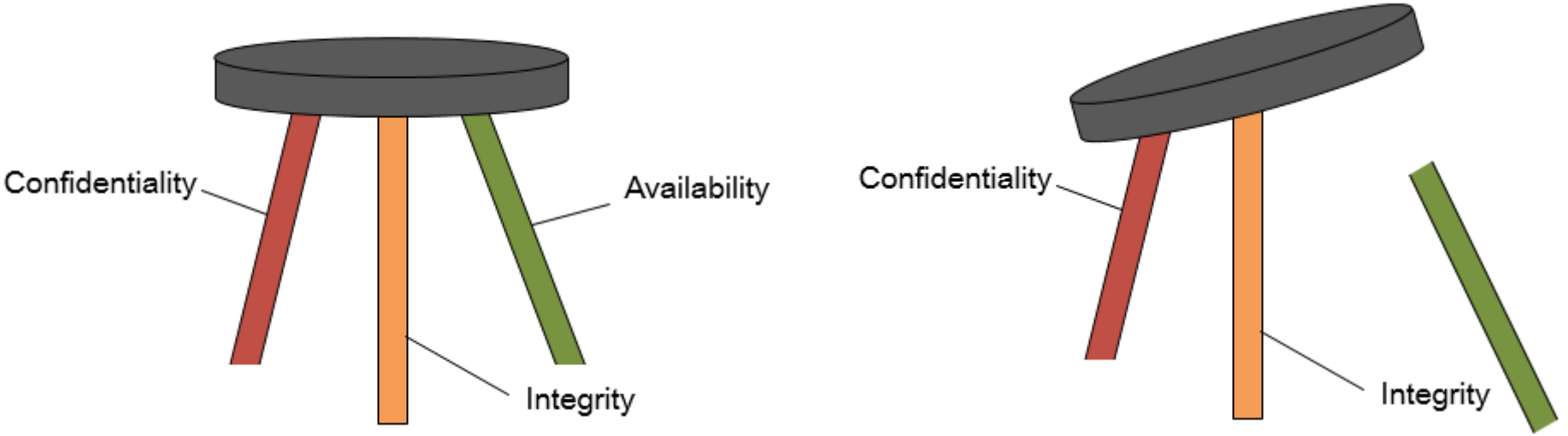
- 컴퓨터 보안 정의
  - 정보 시스템의 자원을 보호하기 위해 자동화 된 시스템에 제공되는 보호



<CIA 트라이어드>

컴퓨터 보안 개념

- CIA 트라이어드(Triad)
  - 컴퓨터 보안에 있어서 가장 핵심이 되는 3가지 주요 목표
    - 기밀성(Confidentiality)
    - 무결성(Integrity)
    - 가용성(Availability)



<CIA 트라이어드 설명 이미지>

컴퓨터 보안 개념

- CIA 트라이어드(CIA Triad)
  - 기밀성
    - 인가된(Authorized) 사용자만 정보에 접근할 수 있도록 하는 것
      - 데이터 기밀성(Data Confidentiality)
        - 인가된 사용자만 데이터 자체에 접근 할 수 있는 것
      - 프라이버시(Privacy)
        - 정보의 범위나 정보 공개 범위를 통제하는 것
          - e.g., 공개할 정보의 범위, 정보를 공개할 대상의 범위
    - 특성
      - 정보 접근과 공개에 대해 합법적 제한 조건이 지켜져야 함
      - 기밀성을 상실하게 되면 정보가 부정하게 공개

컴퓨터 보안 개념

- CIA 트라이어드(CIA Triad)
  - 무결성
    - 인가되지 않은(Unauthorized) 사용자 및 방법을 통한 정보의 변경, 삭제, 생성을 막는 것
      - 데이터 무결성(Data Integrity)
        - 인가되지 않은 사용자가 데이터 자체를 변경, 삭제, 생성하지 않도록 막는 것
      - 시스템 무결성(System Integrity)
        - 인가되지 않은 사용자가 시스템을 변경, 삭제, 생성하지 않도록 막는 것
    - 특성
      - 부적절한 정보 수정 및 파괴를 막아야 함
      - 무결성을 상실하게 되면 정보가 무단으로 수정되거나 파괴

컴퓨터 보안 개념

- CIA 트라이어드(CIA Triad)
  - 가용성
    - 인가된 사용자가 적시에 신뢰된 정보 및 서비스에 접근 할 수 있도록 보장하는 것
    - 특성
      - 정보 사용에 있어 시간성과 신뢰성 있는 접근
      - 가용성을 상실하게 되면 정보 시스템 사용 및 접근 불가

컴퓨터 보안 개념

- CIA 트라이어드(CIA Triad) 외의 추가적 보안 개념
  - 인증(Authentication)
    - 데이터 및 사용자의 신뢰성 및 신원을 검증해주는 절차
      - 데이터 인증, 메시지 출처 유효성에 대한 확신 제공
        - e.g., 접근하려는 자가 진짜 사용자가 맞는가, 데이터가 정말로 신뢰할 수 있는 출처에서 온 것인가
  - AAA
    - 계정에 대한 인증과 권한을 부여해주는 서버
      - Authentication(인증)
        - e.g., 아이디와 패스워드를 입력하는 것 (정상이면 인증 완료)
      - Authorization(인가)
        - 신원이 인증된 사람에게 권한이 허락되는 것
          - e.g., 로그인 이후 데이터 접근 허가
      - Accounting(계정 관리)
        - 시스템에 로그인한 후 시스템이 이에 대한 기록을 남기는 활동

컴퓨터 보안 개념

- CIA 트라이어드(CIA Triad) 외의 추가적 보안 개념
  - 책임(Accountability)
    - 정의
      - 개체의 행동을 추적하여 찾아낼 수 있도록 하기 위해 증거 및 기록을 남기는 것
      - 발생된 보안 사고에 대해 법적 조치를 취하는 것
    - 예시
      - 부인봉쇄(Non-repudiation)
      - 억제(Deterrence)
      - 결함분리(Fault Isolation)
      - 침입 탐지 및 예방(Prevention)
      - 사후 복구와 법적인 조치(After-action Recovery and Legal Action)
    - 시스템은 반드시 활동 상황(로그)을 기록해야 함
      - 포렌식 분석을 통해 추적 및 전송 관련 분쟁 해결을 위함

컴퓨터 보안 개념

- 보안 침해 사고 수준
  - 저급위험
    - 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

목 차

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

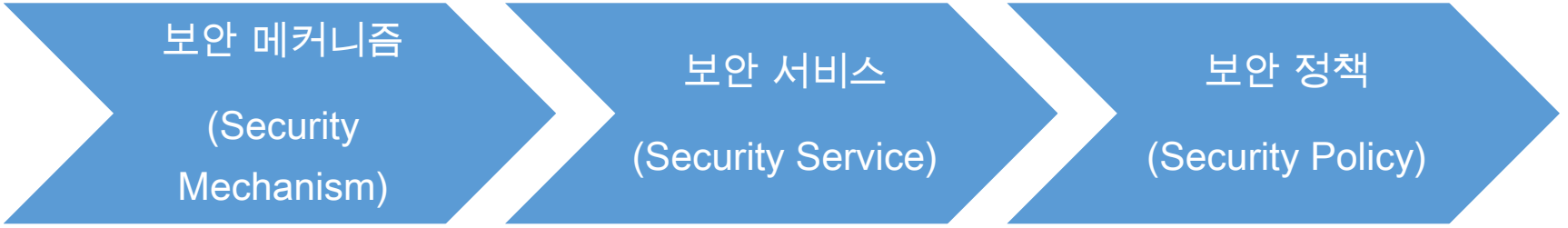
OSI 보안구조

- Security Architecture for OSI
  - OSI 모형을 위한 보안구조
    - OSI(Open Systems Interconnection) 모형
      - 컴퓨터 네트워크 프로토콜 디자인과 통신을 7개의 계층으로 나누어 설명한 것
      - 국제 표준화 기구에서 개발
  - 기능
    - 보안 문제에 대해 유용한 방법 제공
    - 제품 및 서비스에 표준화 된 규정을 적용하여 발전시킬 수 있음

<OSI 모형>

OSI 보안구조

- 핵심
  - 보안 공격(Security Attack)
    - 정보의 안전성을 침해하는 것에 관련된 모든 행위
  - 보안 서비스(Security Service)
    - 정보 전송 및 데이터 처리 시스템의 보안을 강화하기 위해 이루어지는 기능
  - 보안 메커니즘(Security Mechanism)
    - 보안 공격을 탐지, 예방하거나 공격으로 인한 침해를 복구하는 절차 및 장치



목 차

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

보안 공격

- 위협과 공격
  - 위협(Threat)
    - 보안 취약점을 이용하려는 잠재적 위험
      - 아직 공격을 당한 것은 아니지만 공격이 가해질 수 있는 환경, 능력, 행동, 사건
  - 공격(Attack)
    - 위협을 수반하는 시스템 보안에 대한 모든 침범 행위

보안 공격

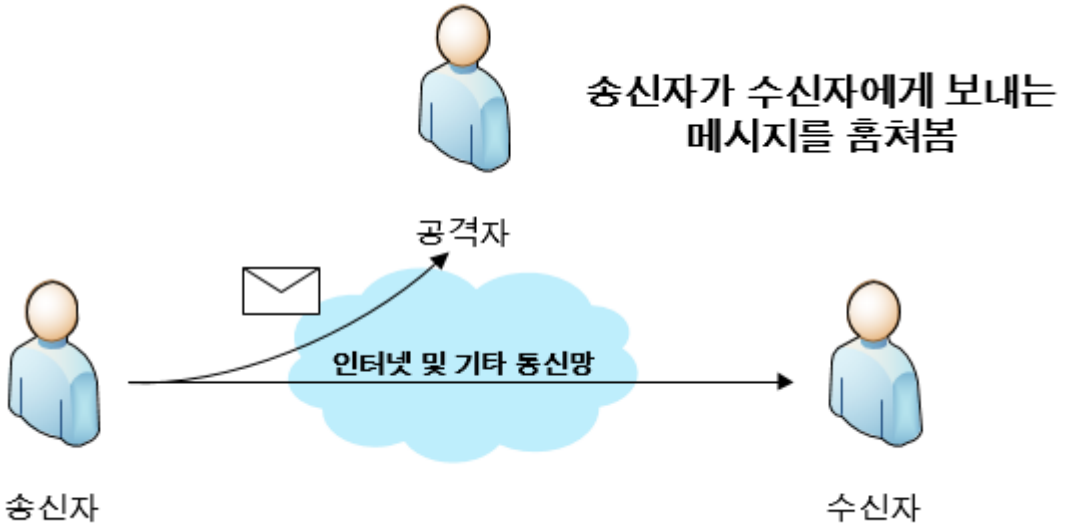
- 분류
  - 소극적 공격(Passive Attack)
    - 시스템으로부터 정보를 획득하거나 사용하려는 시도
    - 시스템 자원에는 영향을 끼치지 않는 공격 형태
      - e.g., 전송 정보에 대한 도청이나 감시
  - 적극적 공격(Active Attack)
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격 형태

보안 공격

- 소극적 공격
  - 공격자의 목표
    - 전송중인 정보 취득
  - 방어 목표
    - 실제로 데이터가 변경되지 않았으므로 공격을 탐지하기가 어려움
      - 탐지보다 예방에 더욱 신경 써야 함
  - 공격 유형 분류
    - 메시지 내용 갈취(Release of Message Content)
    - 트래픽 분석(Traffic Analysis)

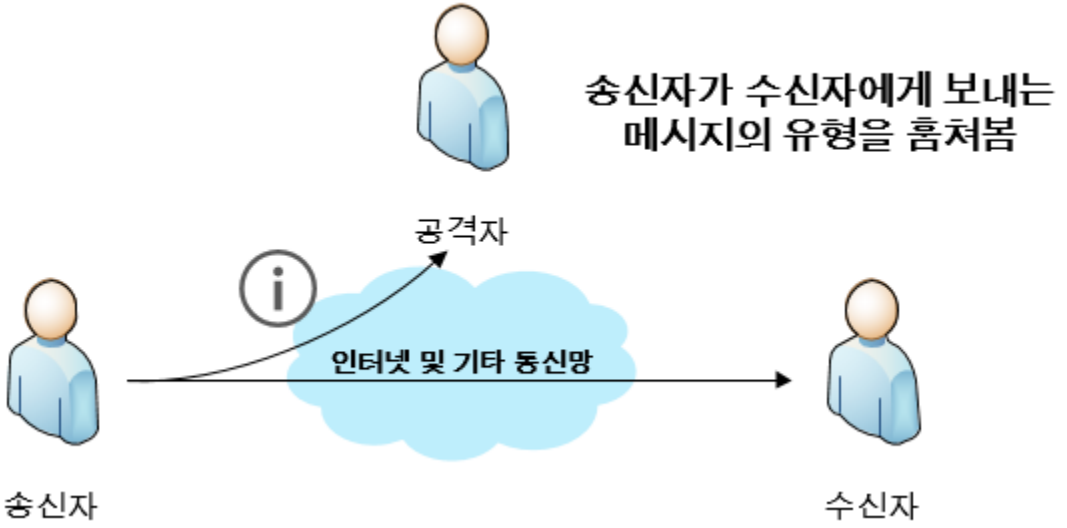
보안 공격

- 소극적 공격
  - 메시지 내용 갈취(Release of Message Contents)
    - 공격자가 전달되는 정보를 취득하거나 보는 것
      - e.g., 공격자가 내 공인인증서 패스워드를 갈취해 계좌의 돈을 모두 자신의 계좌로 송금



보안 공격

- 소극적 공격
  - 트래픽 분석(Traffic Analysis)
    - 메시지의 내용이 아닌 유형을 관찰하는 것
      - 통신자의 접속 위치, 신원, 메시지의 빈도 및 길이 등
      - e.g., 와이어샤크를 통한 패킷 분석

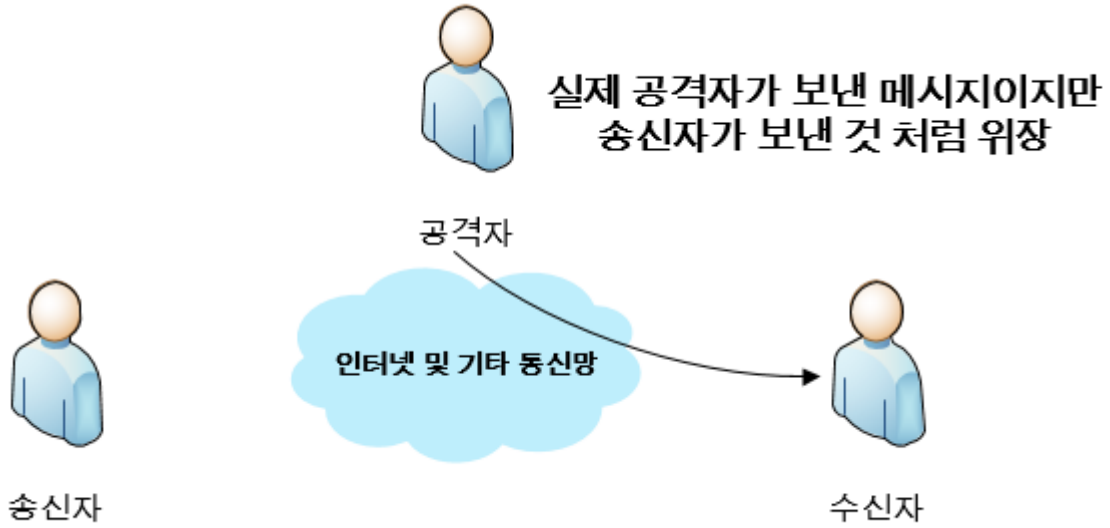


보안 공격

- 적극적 공격
  - 의미
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격 형태
  - 방어 목표
    - 최소 시간 내 탐지
    - 공격으로 인한 피해 복구
  - 공격 유형 분류
    - 신분위장(Masquerade)
    - 재전송(Replay)
    - 메시지 수정(Modification of Messages)
    - 서비스 거부(Denial of Service)

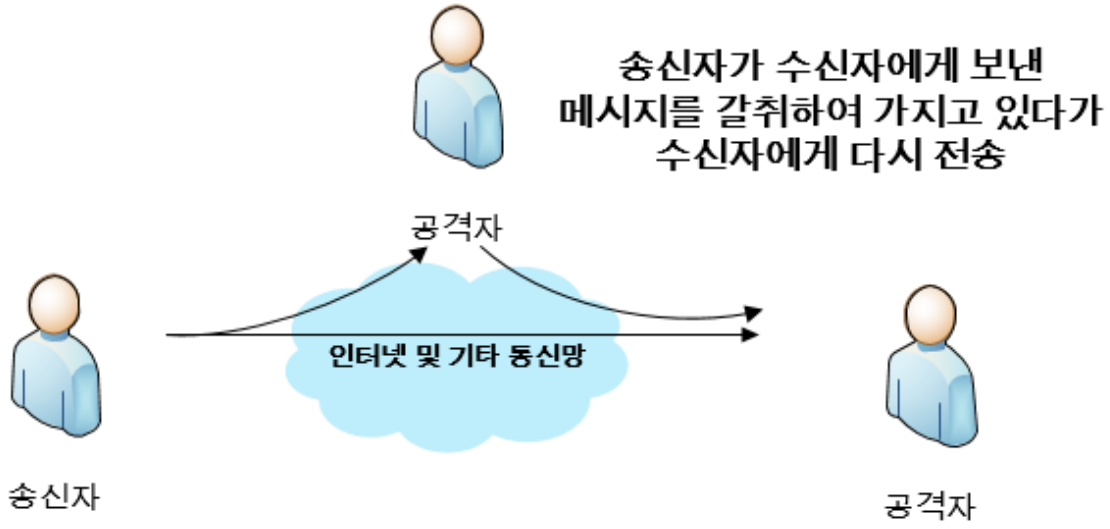
보안 공격

- 적극적 공격
  - 신분위장(Masquerade)
    - 한 개체가 다른 개체의 행세를 하는 공격
      - e.g., 서버 관리자인 것 처럼 위장하여 권한을 상승시키라는 메시지를 전송하는 경우



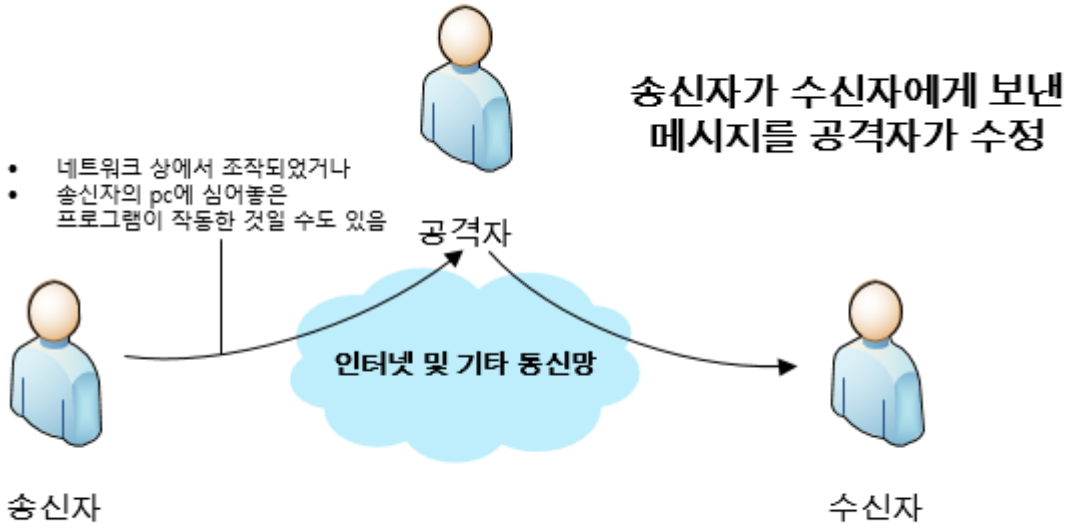
보안 공격

- 적극적 공격
  - 재전송(Replay)
    - 갈취한 데이터를 보관하고 있다가 시간이 경과한 후 재전송하는 공격
      - e.g., 공격자가 공인인증서 비밀번호를 갈취해두었다가 직접 로그인하는 경우



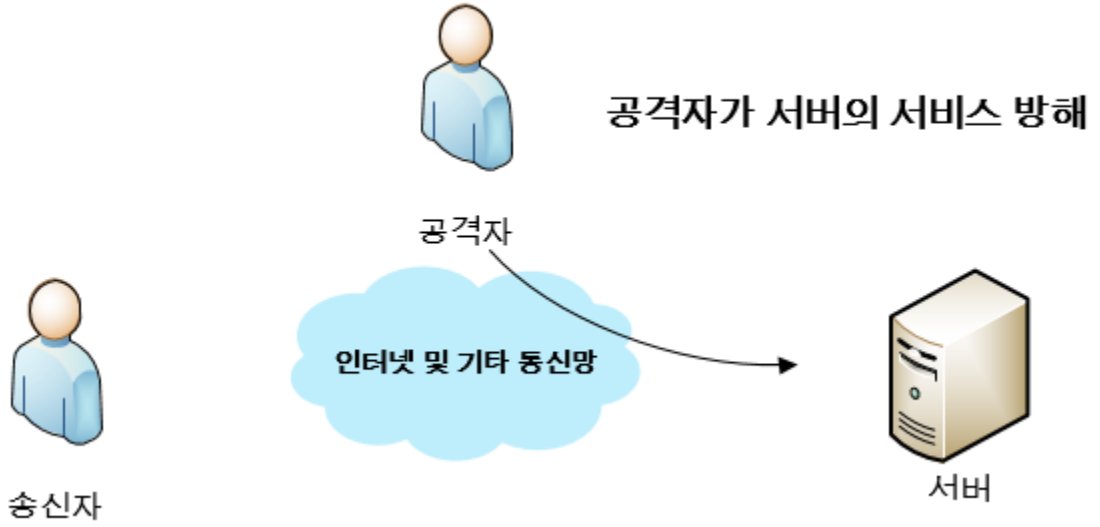
보안 공격

- 적극적 공격
  - 메시지 수정(Modification of Messages)
    - 메시지의 일부를 수정하거나 전송을 지연시키는 공격
      - e.g., 아무리 비밀번호를 입력해도 로그인 되지 않는 경우
      - e.g., 신용카드 사용 내역을 변조하여 카드 회사에 전송하는 경우



보안 공격

- 적극적 공격
  - 공격 유형 분류
    - 서비스 거부(Denial of Service)
      - 시스템의 자원을 부족하게 하여 정상적으로 사용될 수 없도록 하는 공격
        - e.g., 대량의 메시지를 유발하여 과부하
        - e.g., 미라이 봇넷, BlackNurse 공격



보안 공격

- 네트워크 보안 위배 사례 예시
  - 공격자가 통신 중 파일의 복사본을 몰래 가로챈 경우
  - 메시지를 가로채서 임의로 사용자를 수정한 뒤 전달한 경우
  - 새로 작성한 메시지를 관리자로부터 작성된 것처럼 꾸며 수신자에게 전송한 경우
  - 해고된 직원이 자신의 계정말소 메시지가 서버에 전송되기 전 중요한 정보를 탈취한 경우
  - 송신자가 자신이 보낸 메시지가 아니라고 발뺌하는 경우

목 차

보안 서비스

- 정의
  - 정보 전송 및 데이터 처리 시스템의 보안을 강화하기 위해 이루어지는 기능

- 서비스 분류
  - 인증(Authentication)
  - 접근제어(Access Control)
  - 데이터 기밀성(Data Confidentiality)
  - 데이터 무결성(Data Integrity)
  - 부인봉쇄(Nonrepudiation)
  - 가용성 서비스(Availability Service)

보안 서비스

- 서비스 분류
  - 인증(Authentication)
    - 의의
      - 통신 개체가 주장하는 것처럼 정말 당사자인지를 확인해주는 것
    - 기능
      - 양측이 모두 검증된 개체인지 확인
      - 권한이 없거나 수신을 시도하는 제 3자에 의해 통신을 방해 받지는 않았는지 여부 확인

보안 서비스

- 서비스 분류
  - 인증(Authentication)
    - 구체적 서비스 표준
      - 대등 개체 인증(Peer Entity Authentication)
        - 내 신원 확인 (컴퓨터 정보)
        - 통신하는 상대방 신원 확인
        - 연결을 설정할 때와 데이터를 전송하는 과정 중 해당 인증서비스 사용
      - 데이터 출처 인증(Data Origin Authentication)
        - 데이터가 전송 중에 변조되지 않았는지 확인
        - 예상된 송신자로부터 온 것이 맞는지 확인

보안 서비스

- 서비스 분류
  - 접근제어(Access Control)
    - 자원을 불법적으로 사용하지 못하도록 방지하는 것
      - 누가, 어떤 조건 하에, 어떤 자원을 사용하도록 하는지를 말하는 자원에 접근할 수 있는 제한
      - 접근시도를 하는 각 개체에 대해 신원을 확인하거나 인증한 뒤 적합한 접근 권한을 부여
        - e.g., 어플리케이션 접근 허용, 서버 권한 관리

보안 서비스

- 서비스 분류
  - 데이터 기밀성(Data Confidentiality)
    - 인가되지 않은 사용자로부터의 데이터 접근을 막는 것
      - 트래픽 흐름을 보호하는 것도 포함
  - 데이터 무결성(Data Integrity)
    - 인증된 개체가 보낸 데이터와 수신된 데이터가 일치하는지에 대한 확신
    - 연결형 무결성 서비스
      - 메시지가 중간에서 복제, 추가, 수정, 순서 변환, 재전송 되지 않고 송신되었음을 보장
    - 비연결형 무결성 서비스
      - 일반적으로 작은 단위의 메시지 수정에 대해 보호 서비스 제공

보안 서비스

- 서비스 분류
  - 부인봉쇄(Nonrepudiation)
    - 송신자나 수신자 양측이 메시지를 전송한 사실 자체를 부인하지 못하도록 막는 것
      - 수신자에게는 송신자로부터 온 것이 맞음을 보장
      - 송신자에게는 수신자로부터 온 것이 맞음을 보장
  - 가용성 서비스(Availability Service)
    - 인가된 사용자가 적시에 정보에 접근할 수 있도록 보장해주는 서비스

목 차

보안 메커니즘

- 분류
  - 일반 보안 메커니즘(Pervasive Security Mechanism)
    - 특정 OSI 보안 서비스나 프로토콜 계층에 구애 받지 않는 메커니즘
    - 메커니즘 종류
      - 신뢰받는 기능(Trusted Functionality)
        - 보안정책과 같은 규정된 기준에서 볼 때 올바른 것으로 여겨지는 것
      - 보안 레이블(Security Label)
        - 자원의 보안 속성에 이름 설정
      - 사건 탐지(Event Detection)
      - 보안 감사 추적(Security Audit Trail)
        - 보안 감사를 하기 위해 수집하거나 이용되는 데이터 조사
      - 보안 복구(Security Recovery)
        - 사건처리 및 관리기능 등의 메커니즘 요구사항들을 다루며 복구 동작 수행

보안 메커니즘

- 분류
  - 특정 보안 메커니즘(Specific Security Mechanism)
    - 통신 개체가 주장하는 당사자가 맞는지를 확인해주는 것
  - 메커니즘의 종류
    - 암호화(Encipherment)
      - 알고리즘을 사용하여 데이터를 읽을 수 없는 형태로 변환하는 것
    - 디지털서명(Digital Signature)
      - 수신자에게 발신자 및 내용의 무결성을 인증하기 위해 공개키와 개인키로 암호화하는 것
    - 접근제어(Access Control)
    - 데이터 무결성(Data Integrity)
    - 인증 교환(Authentication Exchange)
      - 정보 교환을 통해 개체의 신원을 확인하는 것

보안 메커니즘

- 분류
  - 특정 보안 메커니즘(Specific Security Mechanism)
    - 통신 개체가 주장하는 당사자가 맞는지를 확인해주는 것
  - 메커니즘의 종류
    - 트래픽 패딩(Traffic Padding)
      - 트래픽 분석을 방해하기 위해 데이터 스트림 안의 빈 곳에 비트를 삽입하는 것
    - 경로 제어(Routing Control)
      - 특정 데이터에 대해 물리적으로 안전한 경로를 설정하는 것
    - 공증 (Notarization)
      - 데이터 교환의 어떤 성질을 확신하기 위해 신뢰받는 제 3자를 이용하는 것

보안 메커니즘

- 보안 서비스와 메커니즘의 관계

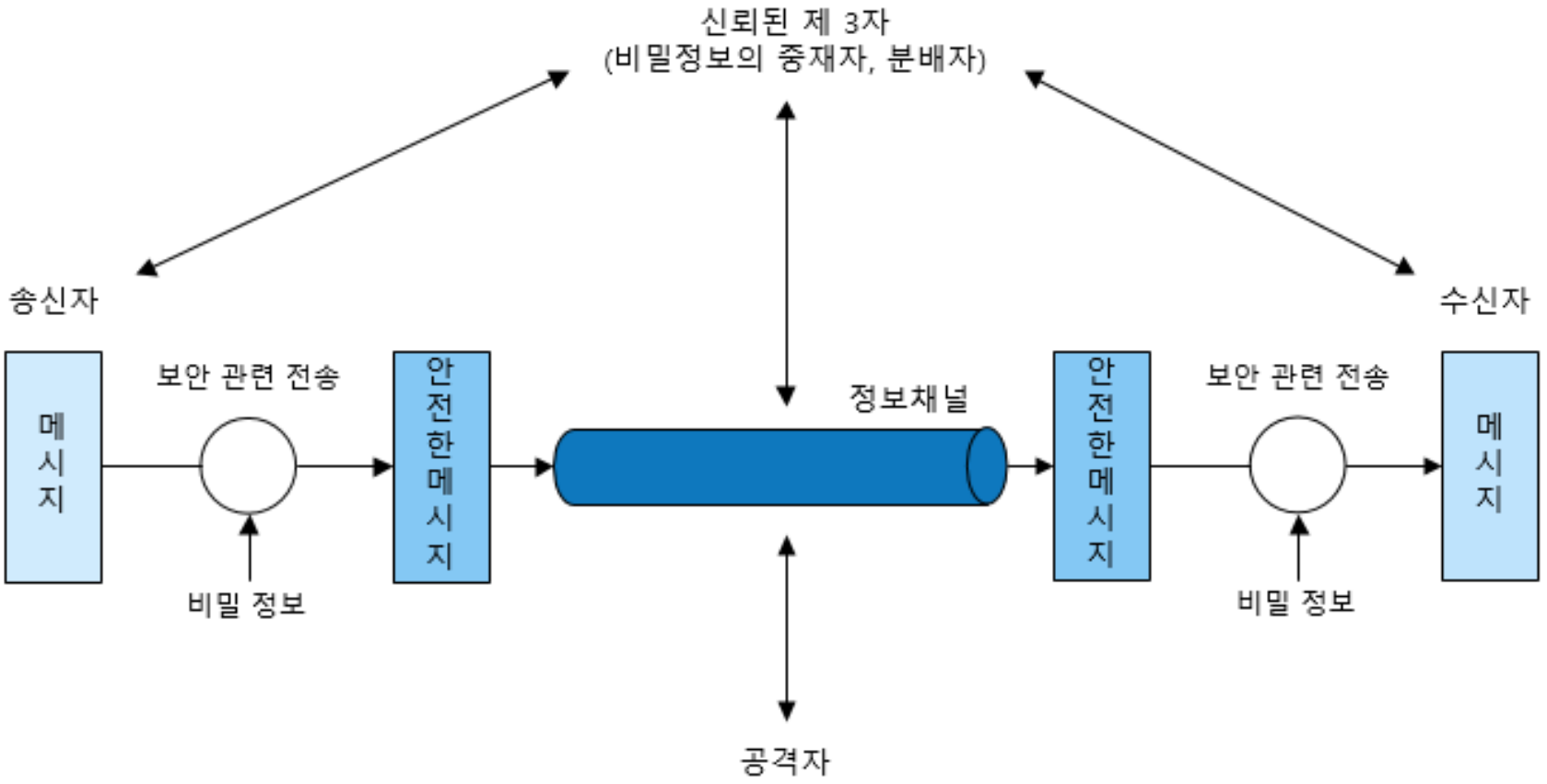
서비스	메커니즘							
	암호화	디지털 서명	접근 제어	데이터 무결성	인증 교환	트래픽 패딩	경로 제어	공증
대등 개체 인증	Y	Y			Y			
데이터 출처 인증	Y	Y						
접근 제어			Y					
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y	Y	
데이터 무결성	Y	Y		Y				
부인 봉쇄		Y		Y				Y
가용성				Y	Y			

목 차

- 컴퓨터와 보안
  - 최근 보안 동향
- 컴퓨터 보안 개념
- OSI 보안 구조
  - 보안 공격
  - 보안 서비스
  - 보안 메커니즘
- 네트워크 보안 모델

네트워크 보안 모델

- 일반적인 네트워크 보안 모델



네트워크 보안 모델

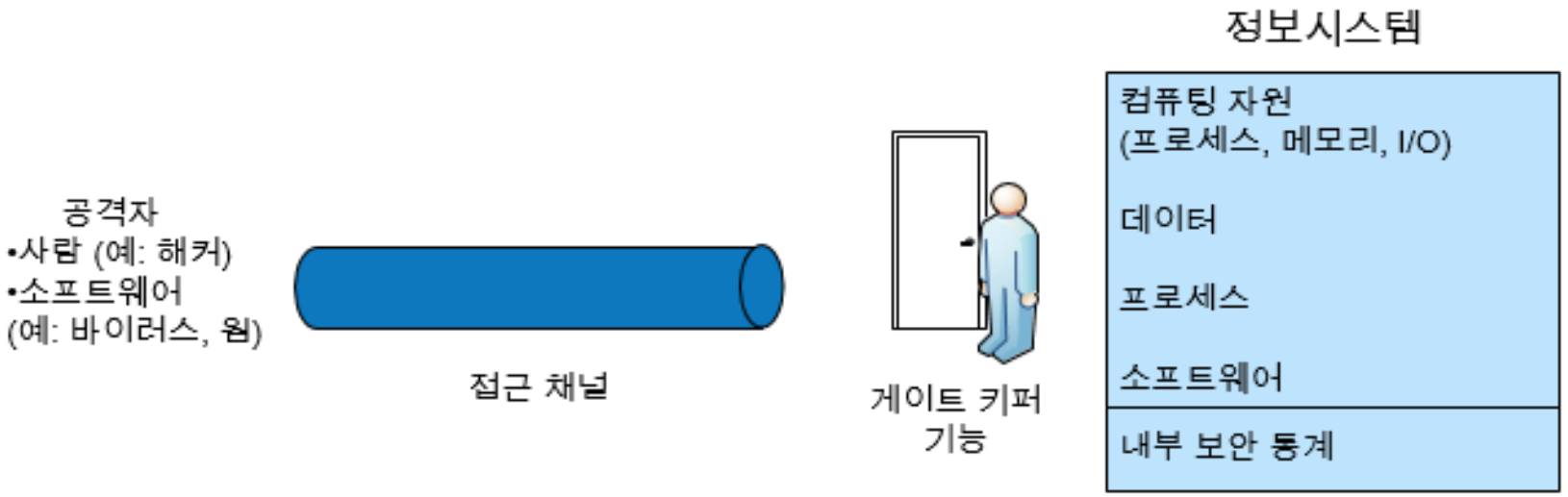
- 일반적인 네트워크 보안 모델
  - 조건
    - 통신주체(Principals)로서의 양쪽은 교환이 이루어지도록 서로 협조해야 함
    - 통신 프로토콜(TCP/IP)을 사용하기로 협의하여 논리적 정보 채널을 구성하여야 함
  - 신뢰할 수 있는 제 3자(Trusted Third Party, TTP)
    - 안전한 전송을 위해 필요
      - 송신자와 수신자가 모두 신뢰하여야 함
      - 공격자가 모르는 비밀정보를 두 송신 주체에게 전달하는 책임
      - 양쪽 통신 주체 간 분쟁이 발생했을 때 조정자 역할

네트워크 보안모델

- 일반적인 네트워크 모델
  - 4가지 기초적 임무
    1. 보안을 위한 변환을 수행 할 알고리즘 설계
    2. 알고리즘에서 사용될 비밀 정보 생성
    3. 비밀 정보를 공유하고 배분할 수 있는 방법 개발
    4. 보안 알고리즘 및 비밀정보를 사용할 양쪽 통신 주체가 사용할 프로토콜 구체화

네트워크 보안 모델

- 침입 보호 목적의 보안 모델



네트워크 보안 모델

- 침입 보호 목적의 보안 모델
  - 침입 유형
    - 단순히 자기만족을 위해 침입을 시도하는 해커에 의한 침입
    - 시스템의 취약점을 이용하기 위해 시스템 내부에 설치된 악성 프로그램에 의한 침입
      - 정보 접근 위협(Information Access Threats)
        - 접근 권한이 없는 데이터를 가로채거나 수정해 자신에게 유리하도록 만드는 위협
      - 서비스 위협(Service Threats)
        - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협

네트워크 보안 모델

- 대표적 악성 프로그램(Malware)
  - 바이러스(Virus)
    - 감염대상을 통해 복제되어 전파되며 주로 시스템 및 파일을 손상시킴
  - 웜(Worm)
    - 독자적으로 복제되어 전파되며 네트워크를 손상시킴
  - 백도어(Backdoor)
    - 공격자의 비인가 접근에 이용됨
  - 트로이목마(Trojan Horse)
    - 정상적인 기능을 하는 것처럼 보이나 실제로는 다른 기능을 수행하는 프로그램
  - 봇넷(Botnet)
    - 악성 프로그램에 감염된 다수의 좀비 PC로 구성된 네트워크

네트워크 보안 모델

- 불법침입 문제에 대한 메커니즘
  - 게이트 키퍼(Gatekeeper) 기능
    - 패스워드 로그인 과정을 이용해 인가 받지 않은 사용자를 가려 냄
    - 웜이나 바이러스와 같은 공격 탐지 및 제거
  - 내부적 제어 수행 기능
    - 1차적으로 인가 받지 않은 사용자 및 악성소프트웨어 접근 차단
    - 2차 방어선에서 컴퓨터 동작 모니터링 및 저장된 정보 분석을 통해 침입 탐지

감사합니다!