

Network Security Essentials

- Chapter_1 개요 -

발표자: 박 재 형(qkrwogud1224@gmail.com)

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

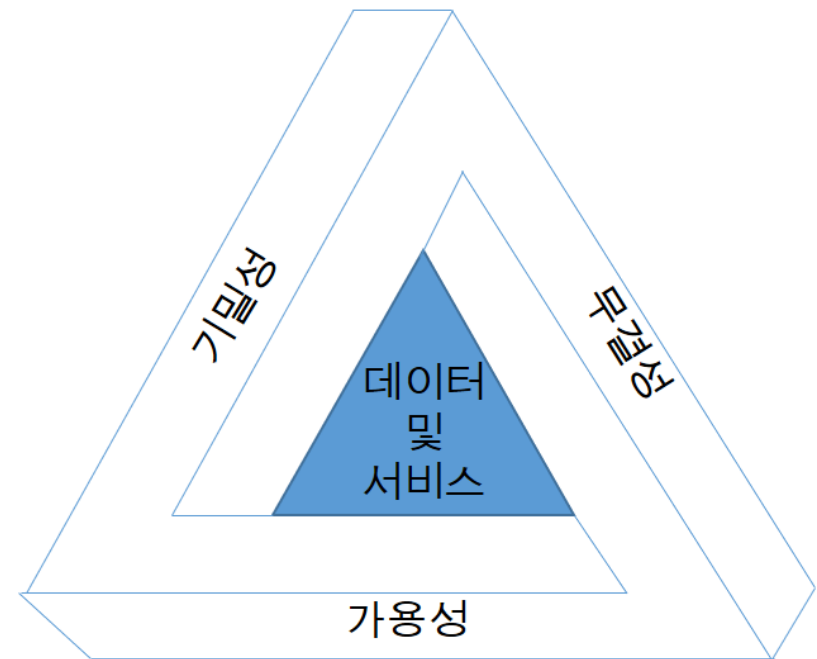
• 정보시스템 자원의 기밀성, 무결성, 가용성을 보호하는 것

• 정보 시스템 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)

- 허가 되지 않은 사용자에게 정보 노출을

- 1. 데이터 기밀성 (Data confidentiality)

- 인증되지 않은 사용자가 정보를 이용하거나 그에게 노출되지 않게 하는 것

- 2. 프라이버시 (Privacy)

- 자신과 관련된 정보가 어디에 수집, 저장되는지, 누구에게 누가 공개하는지 통제하거나 영향을 미칠 수 있도록 하는 것

- 특성

- 정보 접근과 공개에 대해 합법적 제한 조건을 지킬 수 있도록 함
 - 기밀성을 상실하게 되면 정보가 부정하게 공개됨

컴퓨터 보안 개념

- 컴퓨터 보안의 3가지 주요 목표(2/3)

- 무결성 (Integrity)

- 인증된 사용자만이 정보나 프로그램을 변형 할 수 있도록 하는 것

1. 데이터 무결성 (Data integrity)

- 허가된 상태에서만 정보나 프로그램을 변형 할 수 있도록 하는 것

2. 시스템 무결성 (System integrity)

- 시스템이 기능을 손상되지 않은 채 수행하거나 부정하게 시스템이 조작되지 않은 상태로 수행하도록하는 것

- 특성

- 부적절한 정보 수정이나 정보 파괴를 막을 수 있도록 함
- 무결성을 상실하게 되면 정보가 무단으로 수정되거나 파괴 됨

컴퓨터 보안 개념

- 컴퓨터 보안의 3가지 주요 목표(3/3)
 - 가용성 (Availability)
 - 정보 사용에 있어서 원하는 때와 정확한 정보를 사용 할 수 있는 것
 - 특성
 - 정보 사용에 있어서 시간성과 신뢰성 있는 접근을 할 수 있도록 함
 - 가용성을 상실하게 되면 정보나 정보 시스템을 사용하거나 접근이 불가능 함

컴퓨터 보안 개념

- 보안 실무 필드에서 필요한 추가 개념
 - 인증 (Authentication)
 - 진짜라는 성질을 확인할 수 있고 신뢰할 수 있다는 것
 - 사용자라는 사람이 정말 그 사용자인지, 시스템에 도착한 정보가 정말 신뢰할 수 있는 출처에서부터 온 것인지를 확인 하는 것
 - 책임 (Accountability)
 - 보안 침해가 발생하였을 때 보안 침해를 추적 하거나 분쟁을 해결 할 수 있는 것
 - 한 개체의 행동을 유일하게 추적해서 찾아 내야 함
 - 시스템은 반드시 이들의 활동상황을 기록하고 포렌식 분석을 할 수 있어야 함

컴퓨터 보안 개념

- 보안 침해의 수준

- 저급 위험

- 조직 또는 개인에게 미칠 제한된 부정적 효과가 나타나는 것
 - 주요기능은 원래대로 유지 할 수 있지만 어느 기간 동안 성능이 떨어짐

- 중급 위험

- 조직 또는 개인에게 심각한 부정적 효과를 줌
 - 특정 기간 동안 성능이 심각하게 저하됨
 - 조직이나 개인에게 심각한 손상을 끼침

- 고급 위험

- 조직 또는 개인에게 극심하고 재난 수준의 부정적 효과를 주는 것
 - 주요 기능 중 한 두 가지 기능을 상실하여 특정 기간 동안 성능이 극심하게 저하됨

OSI 보안 구조

- OSI 보안 구조 정의

- 관리자가 효과적으로 보안 문제를 조직화 할 수 있는 유용한 방법

- OSI 보안 구조의 핵심

- 보안 공격 (Security attack)

- 기관이 소유한 정보의 안정성을 침해하는 제반 행위
 - 지적인 위협을 수반하는 시스템 보안에 대한 침해

- 보안 메커니즘 (Security mechanism)

- 보안 공격을 탐지, 예방, 침해에 대한 복구하는 절차 또는 절차를 처리하는 장치

- 보안 서비스 (Security service)

- 정보 전송과 데이터 처리 시스템의 보안을 강화하기 위한 처리 또는 통신 서비스
 - 보안 공격에 대처하기 위한 서비스

보안 공격

- 위협과 공격

- 위협 (Threat)

- 보안 취약점을 이용하려는 잠재적인 위협
 - 보안 침해와 위협을 가할 수 있는 환경, 능력, 행동, 사건

- 공격 (Attack)

- 지적인 위협을 수반하는 시스템 보안에 대한 침범
 - 지적인 위협이란 보안 서비스를 교묘히 피하거나 시스템 정책을 위반하는 정교한 시도

보안 공격

- 보안 공격의 분류

- 소극적 공격 (Passive attack)

- 시스템으로 부터 정보를 획득하거나 사용하려는 시도
- 시스템 자원에 영향을 끼치지 않는 공격 형태
- 소극적 공격에 대해서는 실제로 데이터를 변경하지 않기 때문에 탐지보다는 예방에 더 신경 쓸 필요가 있음
- 메시지 내용 갈취, 트래픽 분석의 2가지 유형이 있음

- 적극적 공격 (active attack)

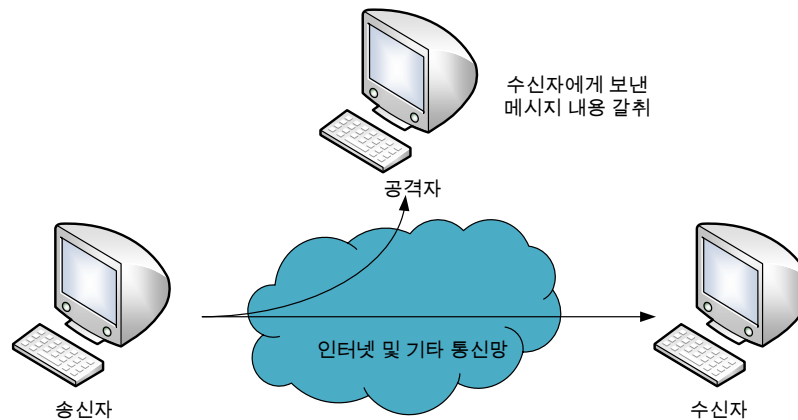
- 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격 형태
- 빠른 시간내 탐지, 공격으로 인한 피해 복구
- 신분 위장, 재전송, 메시지 수정, 서비스 거부의 4가지 유형이 있음

보안 공격

- 소극적 공격

- 메시지 내용 갈취 (Release of message contents)

- 공격자가 정보와 내용을 몰래 취득하거나 갈취하는 것
 - e.g., 공격자가 전화 내용을 도청하여 내 주민번호를 알아 내는 것

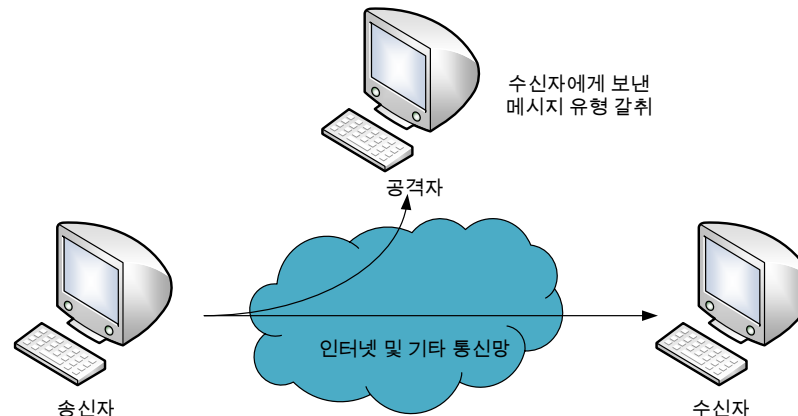


보안 공격

- 소극적 공격

- 트래픽 분석 (Traffic analysis)

- 메시지 유형을 관찰하여 통신자의 접속 위치와 신원을 파악하거나 메시지 빈도와 메시지 길이 등을 관찰
- 메시지 유형 관찰로 인한 정보를 이용하여 통신자의 특성을 추측
 - e.g., 공격자가 트래픽 분석을 통하여 나의 집주소를 알아 내는 것

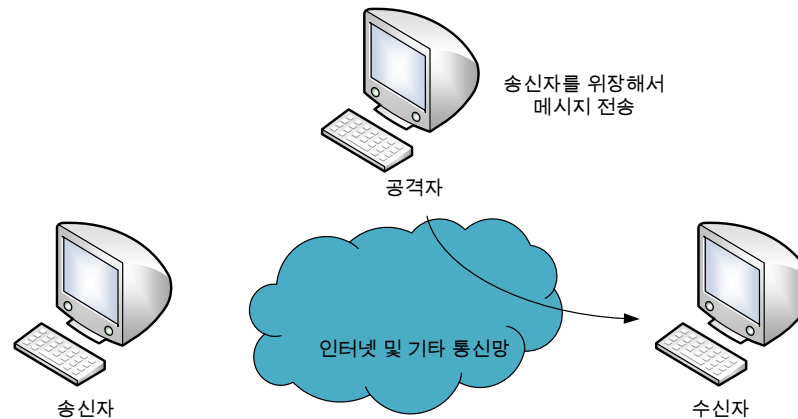


보안 공격

- 적극적 공격

- 신분 위장 (Masquerade)

- 한 개체가 다른 개체의 행세를 하는 것
- 다른 형태의 적극적 공격과 병행해서 수행됨
 - e.g., 공격자가 관리자로 신분 위장 후 관리자 행세를 하여 나의 비밀 문서 파일을 열람 함

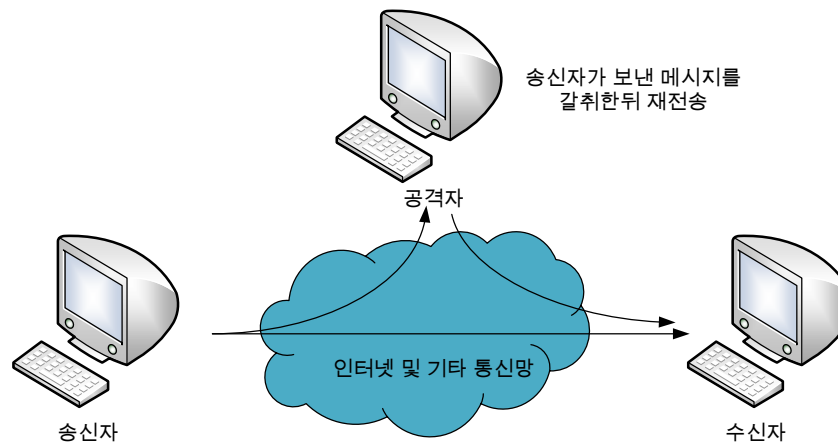


보안 공격

- 적극적 공격

- 재전송 (Replay)

- 데이터 단위를 획득하여 보관하고 있다가 시간이 경과한 후에 재전송을 함으로써 인가되지 않은 사항에 접근하는 공격 형태
 - e.g., 나의 게임 아이디 비밀번호를 갈취해 두었다가 나중에 직접 나의 게임 아이디에 로그인하는 함

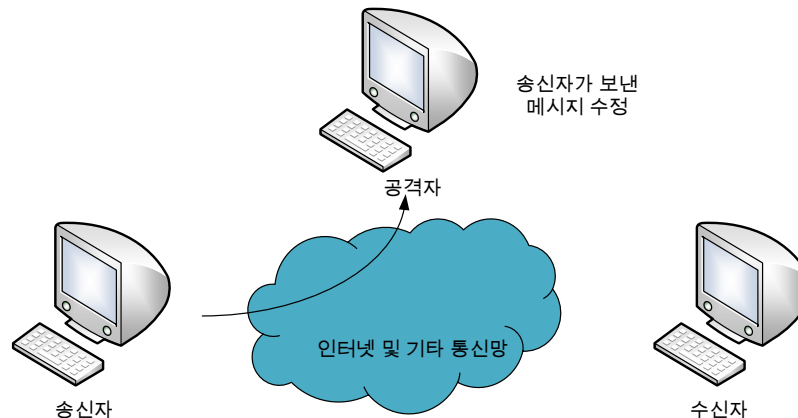


보안 공격

- 적극적 공격

- 메시지 수정 (Modification of Messages)

- 메시지의 일부를 불법으로 수정하거나 메시지 전송을 지연시키거나 순서를 뒤바꾸어 인가되지 않은 효과를 노리는 공격 형태
 - e.g., 나에게 부여된 파일 열람 권한 메시지를 공격자가 수정하여 파일을 열람함



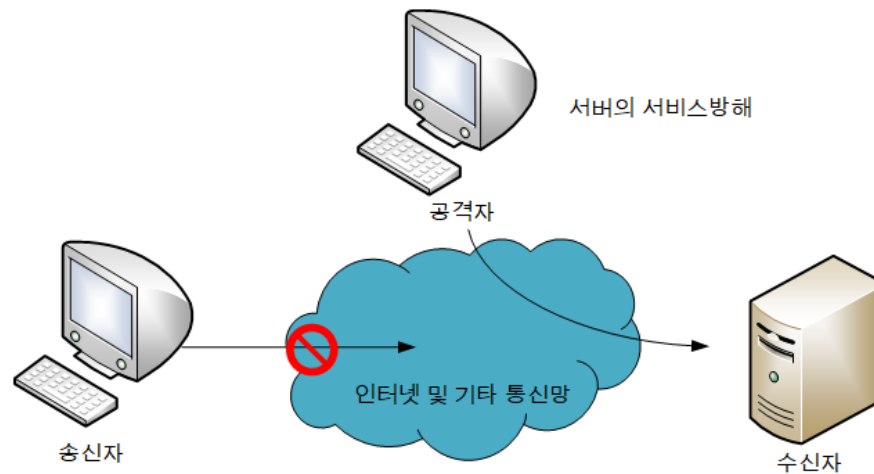
보안 공격

- 적극적 공격

- 서비스 거부 (Denial of service)

- 통신 설비가 정상적으로 운용되거나 관리되지 못하도록 방해하는 공격 형태

- e.g., 배달 음식 주문을 했는데 공격자가 많은 양의 허위 주문을 넣어 나의 배달 음식 주문 전달을 늦추거나 방해 함



보안 서비스

- 보안 서비스의 정의

- 시스템의 적절한 보안이나 데이터 전송의 보안을 보장하기 위해 제공되는 서비스
- 보안서비스는 보안 정책을 구현하고, 보안 메커니즘에 의해서 구현 됨



보안 서비스

- 보안 서비스의 분류
 - 인증 (Authentication)
 - 접근 제어 (Access control)
 - 데이터 기밀성 (Data Confidentiality)
 - 데이터 무결성 (Data Integrity)
 - 부인 봉쇄 (Nonrepudiation)
 - 가용성 서비스 (Availability Service)

보안 서비스

- 보안 서비스의 분류
 - 인증 (Authentication)
 - 통신이 검증되었다는 것을 확인해주는 것
 - 대등 개체 인증 (Peer Entity Authentication)
 - 연결하고있는 개체의 신분에 대한 확신을 주기 위해서 논리적 연결에서 사용하는 인증
 - 데이터-출처 인증 (Data Origin Authentication)
 - 비 연결 전송에서 수신된 데이터의 출처가 정말 주장하고 있는 곳에서 온 것인지 확신시켜주는 인증

보안 서비스

- 보안 서비스의 분류
 - 접근 제어 (Access Control)
 - 자원을 불법적으로 사용하지 못하도록 방지하는 것
 - 서비스를 누가, 어떤 조건하에, 어떤 자원을 사용하도록 하는지를 말하는 자원에 접근 할 수 있는 제한을 말함
 - 접근을 시도하는 사용자가 인증이 된다면 그에 맞는 권한을 부여하는 것

보안 서비스

- 보안 서비스의 분류
 - 데이터 기밀성 (Data Confidentiality)
 - 소극적 공격으로부터 데이터를 보호하는 것
 - 트래픽의 흐름을 보호하는 것
 - 데이터 무결성 (Data Integrity)
 - 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신을 주는 것
 - 무결성에 대한 침해가 탐지하게 되면 이 서비스는 단지 침해 내용만을 보고함
 - 연결형 무결성 서비스
 - 보낸 메시지가 중간에 변형 없이 송신되는 것을 보장 함
 - 비 연결형 무결성 서비스
 - 작은 단위 메시지 수정에 대해서만 보호 함

보안 서비스

- 보안 서비스의 분류
 - 부인 봉쇄 (Nonrepudiation)
 - 송신자나 수신자 양쪽이 메시지를 전송한 사실을 부인하지 못하도록 막는 것
 - 수신자에게 송신자로부터 온 메시지라는 것을 확신 함
 - 송신자에게는 메시지를 받는 주체가 수신자라는 것을 확신 함
 - 가용성 서비스 (Availability Service)
 - 사용자가 요구할 때 시스템 성능에 따라 서비스를 제공하는 것

보안 메커니즘

- 보안 메커니즘의 분류

- 일반 보안 메커니즘 (Pervasive Security Mechanism)
 - 임의의 특정 OSI서비스나 프로토콜 계층에 구애 받지 않는 메커니즘
- 일반 보안 메커니즘의 종류
 - 신뢰받는 기능 (Trusted Functionality)
 - 보안정책 같은 기준으로 볼 때 올바른 것으로 여겨지는 것
 - 보안 레이블 (Security Label)
 - 자원의 보안 속성에 이름을 붙이는 것
 - 사건 탐지 (Event Detection)
 - 보안 관련 사건을 탐지하는 것
 - 보안 감사 추적 (Security Audit Trail)
 - 보안 감사를 하기 위해 이용되는 데이터를 조사하고 검토하는 것
 - 보안 복구 (Security Recovery)
 - 사건처리와 관리기능 같은 메커니즘의 요구사항을 다루고 복구 동작을 수행 함

보안 서비스

- 보안 메커니즘의 분류

- 특정 보안 메커니즘 (Specific Security Mechanism)

- 통신 개체가 주장하는 것처럼 정말로 그 당사자 인지를 확인해주는 것

- 메커니즘의 종류

- 암호화 (Encipherment)

- 데이터를 읽을 수 없는 형태로 변환하는 데 수학적 알고리즘을 사용하는 것
- 데이터 변환과 복구는 알고리즘과 사용되는 키에 따라 달라짐

- 디지털 서명 (Digital Signature)

- 데이터 발신자가 데이터 수신자에게 데이터가 변형되지 않았음을 인증하기 위해 데이터에 붙이는 데이터 단위의 암호

- 접근 제어 (Access Control)

- 자원에 접근할 권한을 제한하는 다양한 메커니즘

- 데이터 무결성 (Data Integrity)

- 데이터 단위의 데이터 흐름의 무결성을 확신하는데 사용되는 메커니즘

보안 서비스

- 보안 메커니즘의 분류

- 특정 보안 메커니즘 (Specific Security Mechanism)

- 통신 개체가 주장하는 것처럼 정말로 그 당사자 인지를 확인해주는 것

- 메커니즘의 종류

- 인증 교환 (Authentication Exchange)

- 정보 교환을 통해 개체의 신원을 확인하는 데 사용하는 메커니즘

- 트래픽 패딩 (Traffic Padding)

- 트래픽 분석 시도를 방해하기 위해서 데이터 흐름 안의 빈 곳에 비트를 채워 넣는 것

- 경로 제어 (Routing Control)

- 특정 데이터에 대해 물리적으로 안전한 경로를 선택할 수 있게 함
- 보안 침해가 의심 시 경로를 바꿀 수 있게 한다

- 공증 (Notarization)

- 데이터 교환의 어떤 성질을 확신하기 위해 신뢰 받는 제3자를 이용함

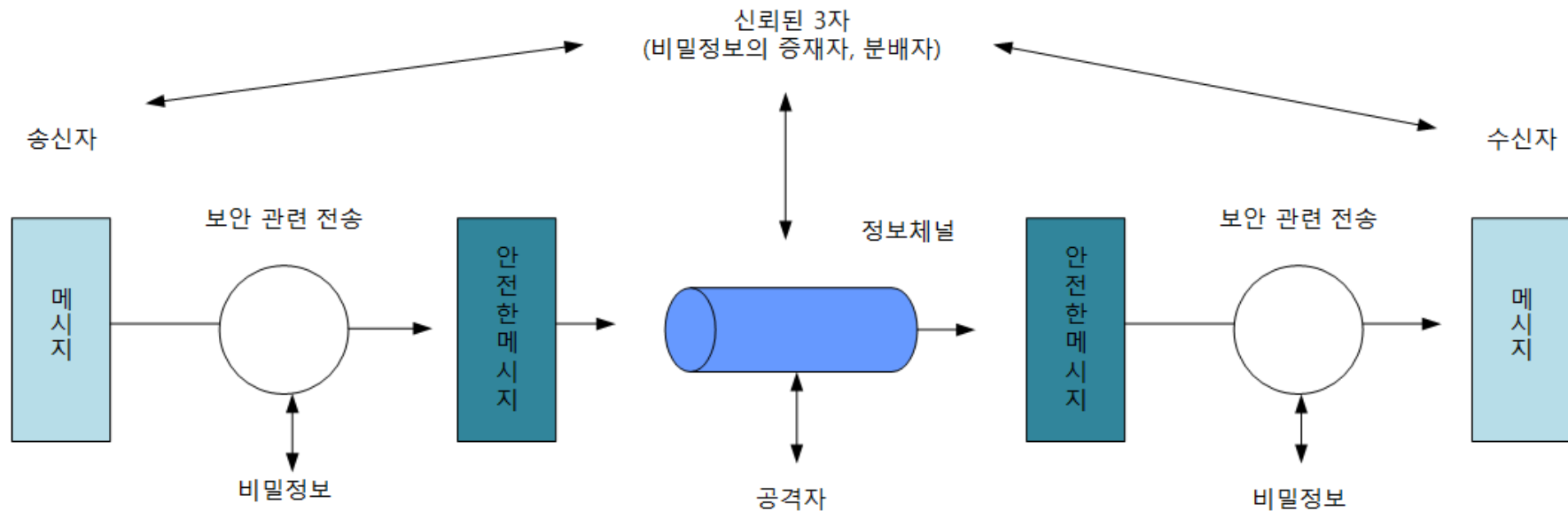
보안 서비스

• 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						
접근제어			Y				Y	
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y		
데이터 무결성	Y	Y		Y				
부인봉쇄		Y		Y				Y
가용성				Y	Y			

네트워크 보안 모델

- 네트워크 보안 모델
 - 일반적인 모델



네트워크 보안 모델

- 네트워크 보안 모델의 성질

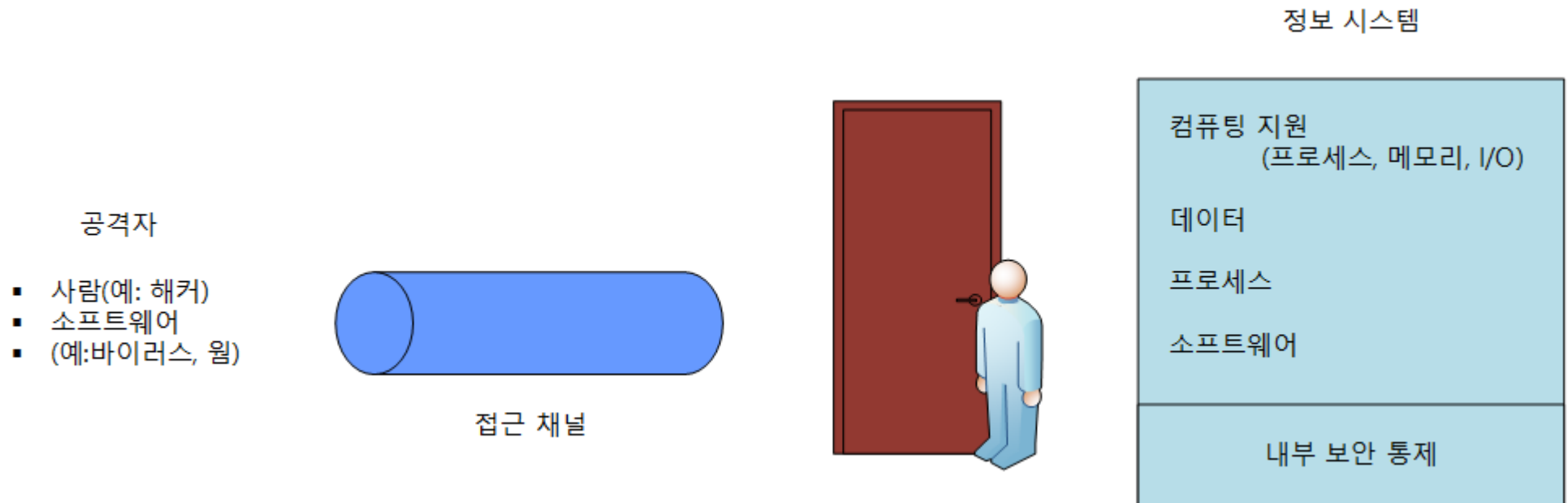
- 보안을 위해서 전송될 정보를 변환한다
 - 메시지를 암호화
- 메시지의 신원확인을 위한 코드 첨부
- 통신 주체들만 알 수 있는 비밀정보를 공유

- 네트워크 보안 모델 설계의 4가지 기초 임무

- 변환을 수행할 알고리즘을 설계한다
- 이 알고리즘에서 사용될 비밀 정보를 생성 해야 함
- 비밀 정보를 공유하고 배분 할 수 있는 방법을 개발해야 함
- 양쪽 통신 주체가 사용할 프로토콜을 구체화해야 함

네트워크 보안 모델

- 침입 보호 목적의 보안 모델
 - 게이트 키퍼(Gatekeeper)
 - 패스워드 로그인 과정을 이용해서 사용자를 가려내고 바이러스나 웜 같은 공격을 탐지하여 제거하는 역할



네트워크 보안 모델

- 침입 보호 목적의 보안 모델

- 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

- 소프트웨어 공격의 대표적인 사례
 - 바이러스(Virus)
 - 스스로 복제하여 컴퓨터를 감염시키는 프로그램
 - 시스템이나 하드웨어, 파일들을 손상시킴
 - 웜(Worm)
 - 독자적으로 실행되며 다른 실행 프로그램이 필요하지 않음
 - 네트워크 성능 저하
- 바이러스와 웜의 차이점
 - 둘은 자가복제기능의 공통점을 가짐
 - 바이러스는 파일을 통해 감염 시키며 감염시킬 대상이 없을 시 실행되지 않음
 - 웜은 감염시킬 대상이 존재하지 않아도 스스로 실행됨
 - 바이러스는 파일 손상 웜은 네트워크 성능을 저하시킴

Thanks!

박 재 형 (qkrwogud1224@gmail.com)