네트워크 보안 에센셜

- 1장 개요 -

임연주(yeonjoo@pel.smuc.ac.kr)

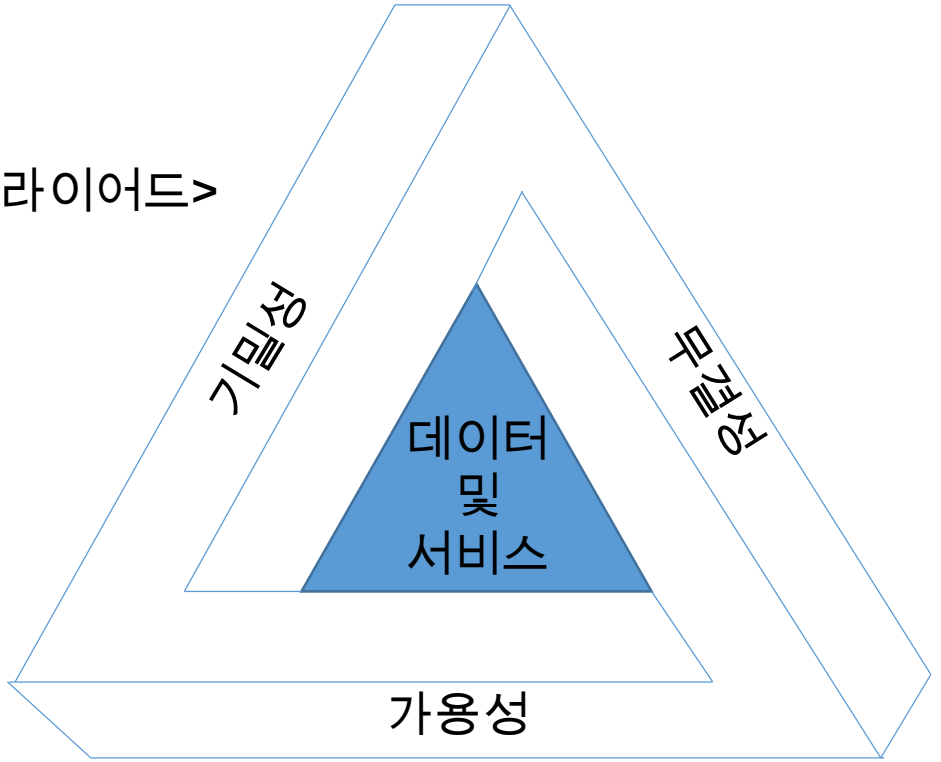
상명대학교 프로토콜공학연구실

목 차

컴퓨터 보안 개념

- 컴퓨터 보안 정의
  - **무결성, 가용성, 기밀성**을 보전하고자 하는 목표

<CIA 트라이어드>



컴퓨터 보안 개념

- 컴퓨터 보안 목적
  - 기밀성 (Confidentiality): 허가 받지 않은 자에게 정보노출이 되지 않도록 하는 것
    - 데이터 기밀성: 실제 데이터를 기밀화
    - 프라이버시: 자신의 데이터의 기밀화를 통제함
  - 무결성 (Integrity): 허가 받지 않은 자가 정보를 변조하지 못하게 하는 것
    - 데이터 무결성: 실제 데이터를 무결화
    - 시스템 무결성: 시스템의 조작이 이루어져도 조작되지 않게 기능하는 것

컴퓨터 보안 개념

- 컴퓨터 보안 목적
  - 가용성 (Availability) : 시스템이 지체 없이 동작하면서, 허가 받은 자에게만 서비스를 제공 하는 것
  - 인증 (Authentication) : 진짜라는 성질을 확인할 수 있고 신뢰할 수 있다는 것
  - 책임 (Accountability) : 한 개체의 행동을 추적하고 찾아내는 것 (보안 침해에 대한 문제를 해결 할 수 있어야 함)

컴퓨터 보안 개념

- 보안 침해로 미치는 위험
  - 저급 위험
    - 주요 기능은 유지할 수 있지만 일정 기간 동안 기능의 유효성이 떨어짐
  - 중급 위험
    - 특정 기간 동안 성능이 심각하게 저하되고, 개인이나 조직에게 재정이나 생명의 위협이 됨
  - 고급위험
    - 재난 수준의 부정적 효과를 줌

OSI 보안 구조

- 관리자가 효과적으로 보안 문제를 조직화할 수 있는 유용한 방법을 제공함

- 크게 3가지 나눌 수 있음

1. 보안 공격
   - 정보의 안전성을 침해하는 것
2. 보안 메커니즘
   - 보안 공격을 탐지,예방 그리고 공격으로 인한 침해 복구
3. 보안 서비스
   - 보안 공격을 대응 하기 위한 처리 서비스

OSI 보안 구조

- 참고) 위협과 공격
  - 위협 : 침해의 가능성, 잠재적 위험
  - 공격 : 실제적인 침해 시도

보안 공격

- 보안공격의 종류

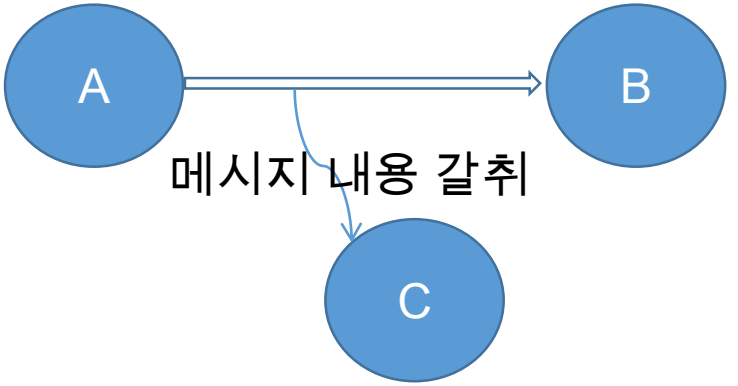
1. 소극적 공격
   - 실제로 데이터 변경 하지 않고 데이터를 획득하거나 사용
   - 시스템 자원에 영향을 주지 않음

2. 적극적 공격
   - 시스템자원을 변경 가능
   - 작동에 영향을 끼침

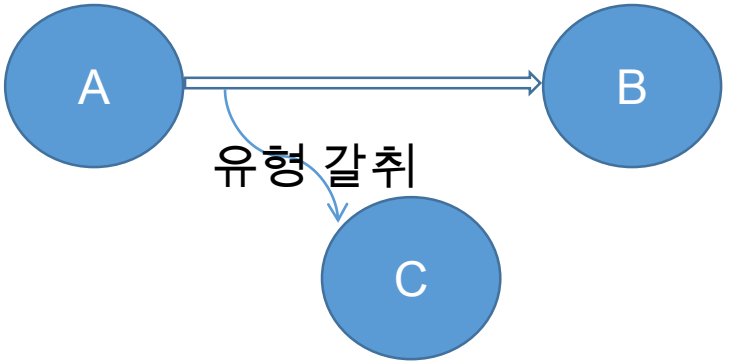
보안 공격

1. 소극적 공격 (Passive attack)

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



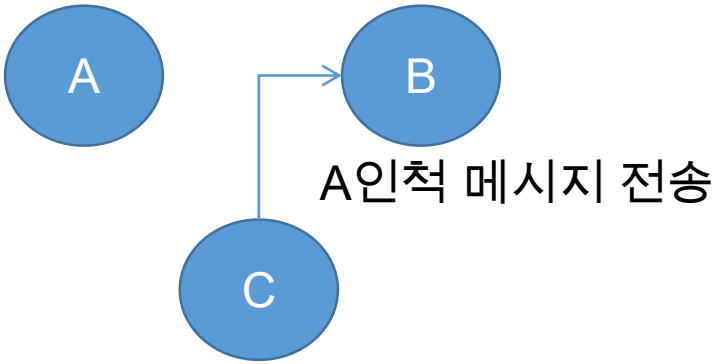
2. 트래픽 분석 (Traffic analysis) : 암호화된 메시지를 통신자의 위치, 신원 등을 파악해 내용유추



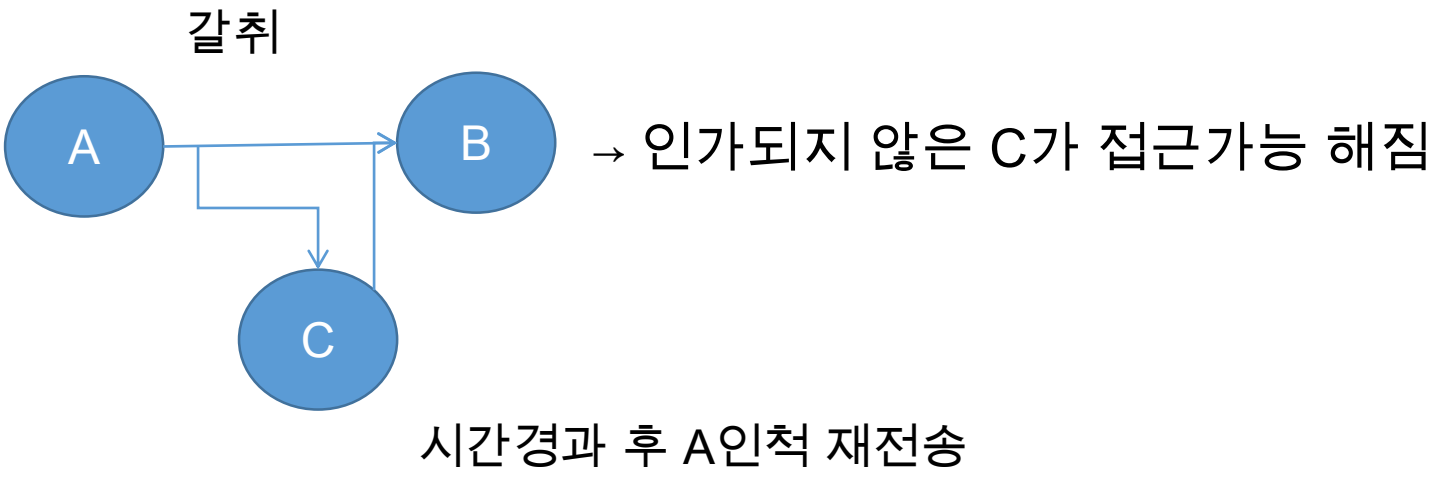
보안 공격

- 적극적 공격 (Active attack)

1. 신분위장



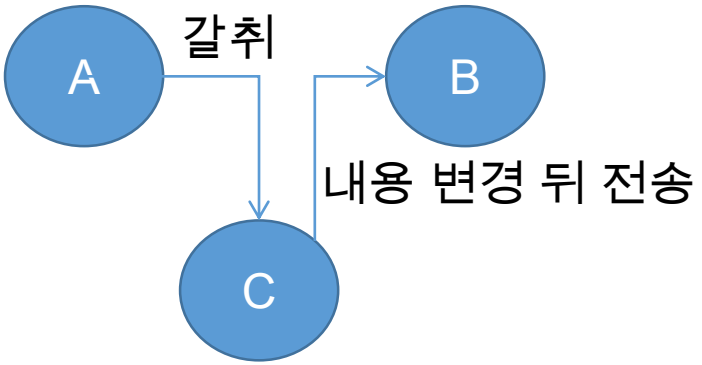
2. 재전송



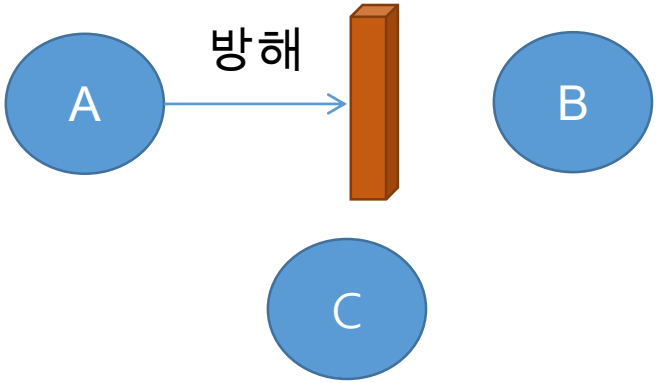
보안 공격

- 적극적 공격 (Active attack)

3. 메시지 수정



4. 서비스 거부



보안 서비스

- 보안 서비스란?
  - RFC 2828에 의하면, 시스템 자원보호를 위해 시스템이 제공하는 처리 서비스나 통신서비스 (즉, 실제 보안 공격에 대응하기 위한 것)
  - 특정 보안 메커니즘과 관계가 깊음
- 가용성 서비스란?
  - 허가된 사용자에게만 서비스를 제공하는 것
  - 서비스가 제공되지 않을 시에, 이를 방해하는 공격인 서비스 거부 공격상황과 비슷하여 중요한 보안 문제로 여겨지고 있음

보안 서비스

- 인증 서비스 (Authentication)
  - 통신 개체가 주장하는 것처럼 정말로 그 당사자인지 확인해 주는 서비스

- 두 가지 구체적인 인증 서비스
  1. 대등 개체 인증: 초기연결에 사용됨, 양 측 모두 적합한 개체인지 확신 시켜주는 인증
  2. 데이터-출처 인증: 비연결 전송에서 중간에 제 3자의 공격이 없었는지, 출처가 정말 주장하고 있는 곳에서 온 것인지 확신시켜주는 인증

보안 서비스

- 접근제어 (Access Control)
  - 신원을 확인해 해당 개체가 적합하면 접근권한을 부여하는 서비스
- 데이터 기밀성(Data Confidentiality)
  - 소극적 공격으로부터 데이터를 보호하는 서비스
  - 분석 공격으로부터 트래픽 흐름 (날짜, 위치, 빈도 등)을 보호

보안 서비스

- 데이터 무결성 (Data Integrity)
  - 적극적 공격으로부터 보호
  - 보낸 메시지가 중간에서 변경이 되지 않았음을 보장하는 서비스 (즉, 수정, 추가, 제거 혹은 재전송이 없음을 확인)
  - 소프트웨어나 사람이 직접 복구하는 경우 말고 자동화된 복구 메커니즘이 가장 많이 쓰임

- 부인봉쇄 (Nonrepudiation)
  - 송신자나 수신자 양측이 메시지 전송한 사실 자체를 부인하지 못하도록 무결성을 제공 (증명 가능)

보안 메커니즘

- 특정 보안 메커니즘과 일반 보안 메커니즘으로 나뉨
  - 특정 보안 메커니즘 (Specific Security Mechanisms)
    - 특정 보안 서비스를 메커니즘으로 제공하는 것, 크게 8가지 정도 있음
  - 일반 보안 메커니즘 (Pervasive Security Mechanisms)
    - 임의의 특정 OSI 보안 서비스나 프로토콜 계층에 구애 받지 않는 메커니즘

보안 메커니즘

- 보안 서비스와 메커니즘의 관계 표

서비스	메커니즘							
	암호화	디지털 서명	접근 제어	데이터 무결성	인증 교환	트래픽 패딩	경로 제어	공증
대등 개체인증	Y	Y			Y			
데이터 출처인증	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			

보안 메커니즘

- 특정 보안 메커니즘
  - 암호화
    - 데이터를 읽을 수 없는 형태로 변환(수학적 알고리즘)
  - 디지털 서명
    - 송수신자간의 무결성을 입증하고 위조를 막기 위해서 데이터나 데이터 단위의 암호적 변경을 함
  - 접근제어
    - 자원에 접근할 권한을 제한함
  - 데이터 무결성
    - 데이터 단위나 데이터 단위의 스트림의 무결성을 확신

보안 메커니즘

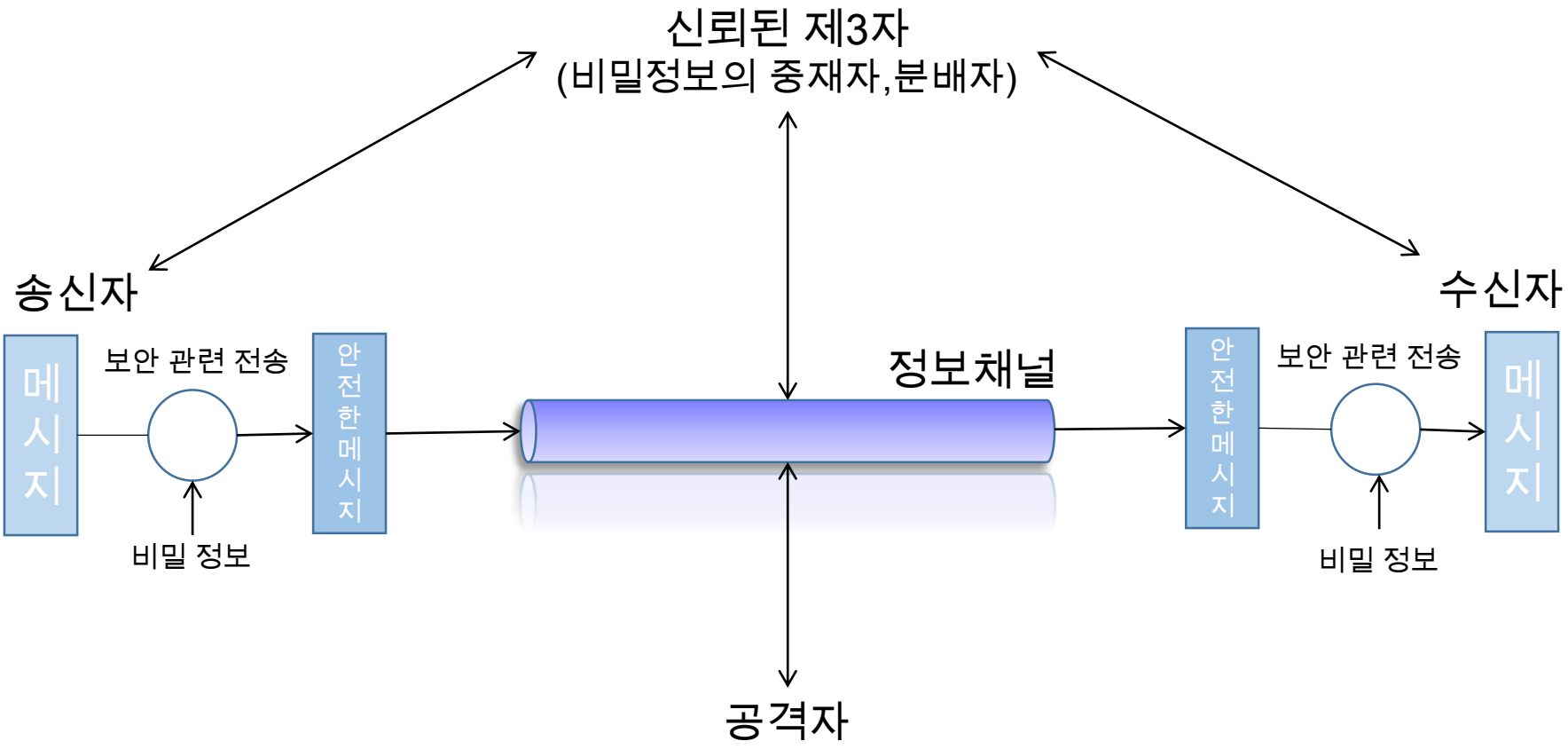
- 특정 보안 메커니즘
  - 인증 교환
    - 정보교환을 통해 개체의 신원을 확인
  - 트래픽 패딩
    - 트래픽 분석 시도를 방해하기 위해서 데이터 스트림의 빈 곳에 비트를 채워 넣는 것
  - 경로 제어
    - 보안침해가 의심스런 경우 경로를 바꿀 수 있게 제어하는 것
  - 공증
    - 신뢰 받는 제 3자를 이용하여 데이터 교환

네트워크 보안 모델

- 일반 보안 모델
  - 4가지 기초적인 과정
    1. 보안을 위한 변환을 수행할 알고리즘을 설계
    2. 알고리즘에 사용될 비밀 정보를 생성
    3. 비밀 정보를 공유하고 배분할 수 있는 방법을 개발함
    4. 특정 보안 서비스를 위한 보안 알고리즘 및 비밀정보를 사용할 양쪽 통신 주체가 사용할 프로토콜을 구체화 해야 함

네트워크 보안 모델

- 안전한 전송을 위해 신뢰할 수 있는 제 3자를 필요로 하는 경우

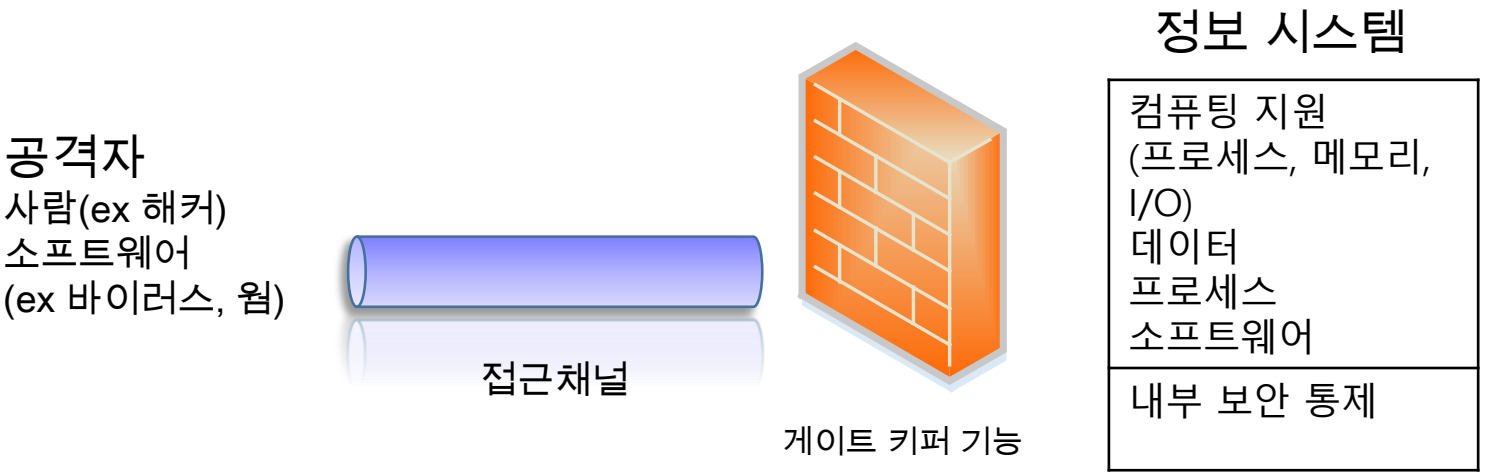


네트워크 보안 모델

- 네트워크 접근 보안 모델
  - 접근 보안 용어
    - 해커: 컴퓨터 시스템을 깰 수 있다는 자기만족을 위해서 침입을 시도라는 사람
    - 침입자: 피해를 입히기 위한 목적으로 침입하는 사람 (범죄에 해당)
    - 정보 접근 위협: 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정해서 자신에게 유리하게 만드는 위협
    - 서비스 위협: 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터의 서비스 결함을 악용하는 위협

네트워크 보안 모델

- 네트워크 접근 보안 모델 그림



감사합니다!