1주차

정보 보안

- 정보 및 정보 시스템의 무단 접근, 사용, 공개, 방해, 변경 또는 파괴로부터의 보호를 위한 활동으로, 기밀성, 무결성 및 가용성을 제공하기 위함입니다.

컴퓨터 보안

- 컴퓨터가 처리하고 저장하는 정보의 기밀성, 무결성 및 가용성을 보장하기 위한 조치 및 제어입니다.

주요 보안 개념(key security concepts)

Confidentiality(기밀성)

- 정보 접근 및 공개에 대한 권한 제한을 보존하는 것을 포함하여 개인 정보 및 자산 정보를 보호하기 위한 수단

Integrity(무결성)

- 정보 변경이나 파괴를 방지하기 위한 것으로, 정보의 부인 불가능성 및 신뢰성을 보장하는 것을 포함합니다.

Availability(가용성)

- 정보에 대한 적시성과 신뢰성 있는 접근 및 사용을 보장하는 것

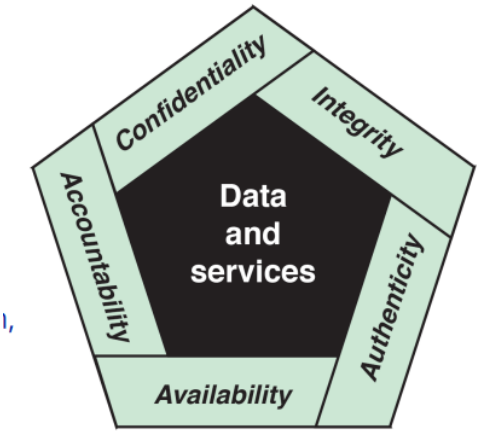


Fig 1.1 Essential Network and Computer Security Requirement

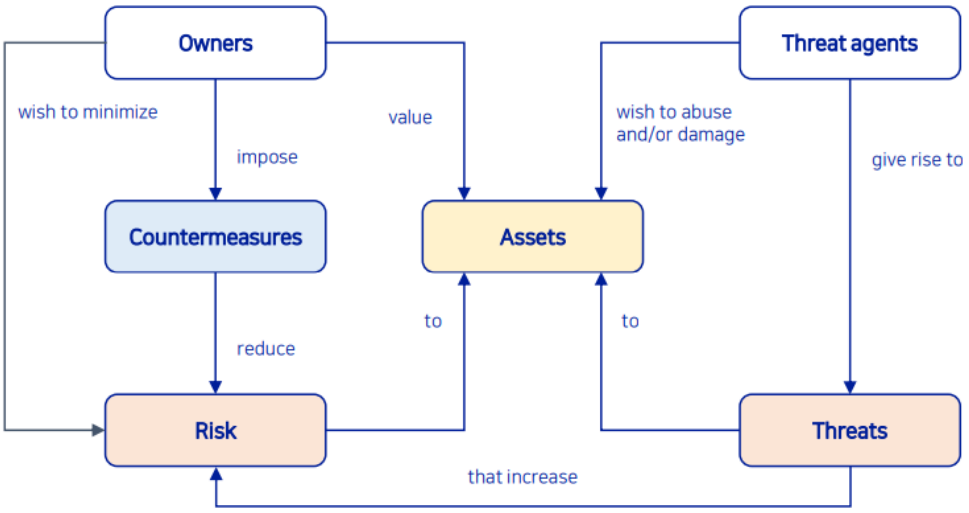
영향수준(Levels of impact)

Impact

- 정보의 무단 공개, 정보의 무단 수정, 정보의 무단 파괴 또는 정보나 정보 시스템의 가용성 손실로 인한 결과로 예상되는 피해의 크기

	주요기능	조직자산	재정손실	생명 또는 부상
Low	뚜렷하게 감소	소량의 피해	소량의 손실	경미한 피해
Moderate	상당히 감소	상당한 피해	상당한 손실	중대한 피해
High	사용 불가	대규모 피해	주요 손실	생명을 위협하는 심각한 부상

보안 개념과 관계(Security concepts and relationships)



컴퓨터 시스템의 자산(Assets of a computer system)

Hardware

- 컴퓨터 시스템 및 데이터 처리, 데이터 저장 및 데이터 통신 장치

Software

- 운영 체제, 시스템 유틸리티 및 응용 프로그램

Data

- 파일 및 데이터베이스, 그리고 비밀번호 파일과 같은 보안 관련 데이터

Communication facilities and network

- 지역 및 광대역 네트워크 통신 링크, 브리지, 라우터 등

취약점, 위협 및 공격(vulnerabilities, Threats and Attacks)

Categories of vulnerabilities

- 손상된, 누수된, 사용 불가능하거나 매우 느린

Threats

- 취약점을 이용할 수 있는
- 자산에 대한 잠재적 보안 위협을 대표

Attacks(threats carried out)

- 수동 공격 및 능동 공격
- 내부자로부터의 공격 및 외부자로부터의 공격

대응책(Countermeasures)

Goal

- 자신에 대한 잔여 위험 수준을 최소화 하는 것

Means

- 공격을 방지
- 공격을 감지한 다음 공격의 효과로부터 회복

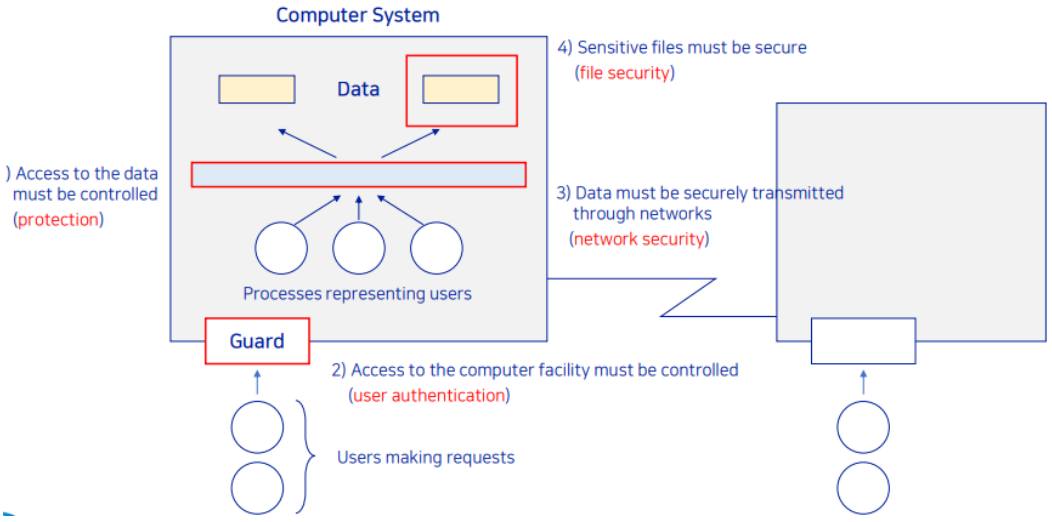
Dealing with vulnerabilities

- 잔여 취약점
- 새로운 취약점

위협과 공격

위협 결과	위협 행동 (공격)

미인가된 공개(Unauthorized Disclosure): 주체가 승인되지 않은 데이터에 접근하는 상황 또는 사건.	노출(Exposure): 민감한 데이터가 직접 승인되지 않은 주체에게 공개됨. 가로채기(Interception): 민감한 데이터를 승인된 소스와 목적지 간에 이동하는 동안 승인되지 않은 주체가 직접 액세스함. 추론(Inference): 승인되지 않은 주체가 통신의 특성이나 부산물로부터 추론을 통해 간접적으로 민감한 데이터에 액세스합니다 (그러나 반드시 통신에 포함된 데이터는 아님). 침입(Intrusion): 승인되지 않은 주체가 시스템의 보안 보호를 우회하여 민감한 데이터에 액세스합니다.
속임수(Deception): 승인된 주체가 거짓 데이터를 받고 그것이 진실로 여기는 상황 또는 사건.	위장(Masquerade): 미승인된 주체가 승인된 주체로 위장하여 시스템에 액세스하거나 악의적인 행위를 수행. 위조(Falsification): 거짓된 데이터가 승인된 주체를 속임. 부인(Repudiation): 주체가 행위에 대한 책임을 거짓으로 부인하여 다른 사람을 속임.
방해(Disruption): 시스템 서비스와 기능의 올바른 작동을 방해하거나 방해하는 상황 또는 사건.	무력화(Incapacition): 시스템 구성 요소를 비활성화하여 시스템 작동을 방해하거나 중단. 훼손(Corruption): 시스템 기능이나 데이터를 악의적으로 수정하여 시스템 작동을 원치 않게 변경. 방해(Obstruction): 시스템 작동을 방해하여 시스템 서비스의 전달을 중단하는 위협 행동.
도용(Usurpation): 무단 엔티티가 시스템 서비스나 기능을 제어하게 되는 상황이나 사건.	부정 사용: 주체가 시스템 자원을 무단으로 논리적 또는 물리적으로 제어합니다. 남용: 시스템 구성 요소가 시스템 보안에 해로운 기능이나 서비스를 수행하도록 합니다.



위협 사례가 포함된 자산(Assets with examples of threats)

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted USB drive is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Comm. lines and networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Attacks

Passive Attacks(수동공격)

- 시스템에서 정보를 배우거나 활용하려고 하지만 시스템 자원에 영향을 주지 않는 것
  - 전송의 도청 또는 모니터
  - 공격자의 목표는 전달되고 있는 정보를 획득하는 것.
- 두 가지 유형:
  - 메시지 내용의 공개
  - 트래픽 분석

Active Attacks(능동공격)

- 시스템 자원을 변경하거나 그 작동에 영향을 주려는 시도
- 데이터 스트림의 일부 수정이나 가짜 스트림의 생성을 포함
- 네 가지 범주:
  - 재생
  - 위장
  - 메시지 수정

    - 서비스 거부

Attack surface

- 시스템 내에서 접근 가능하고 악용 가능한 취약점으로 구성.
- 예시:
    - 외부로 향하는 웹 및 기타 서버의 개방된 포트 및 해당 포트에서 수신 대기 중인 코드
    - 방화벽 내부에서 제공되는 서비스
    - 수신되는 데이터, 이메일, XML, 사무 문서 및 산업별 사용자 정의 데이터 교환 형식을 처리하는 코드
    - 인터페이스, SQL 및 웹 양식
    - 사회 공학 공격에 취약한 민감한 정보에 접근 권한이 있는 직원

Attack surface categories

Network Attack Surface

- 기업 네트워크, 광대역 네트워크 또는 인터넷에서의 취약점
- 이 범주에는 서비스 거부 공격, 통신 링크의 중단 및 다양한 형태의 침입자 공격에 사용되는 네트워크 프로토콜 취약점이 포함

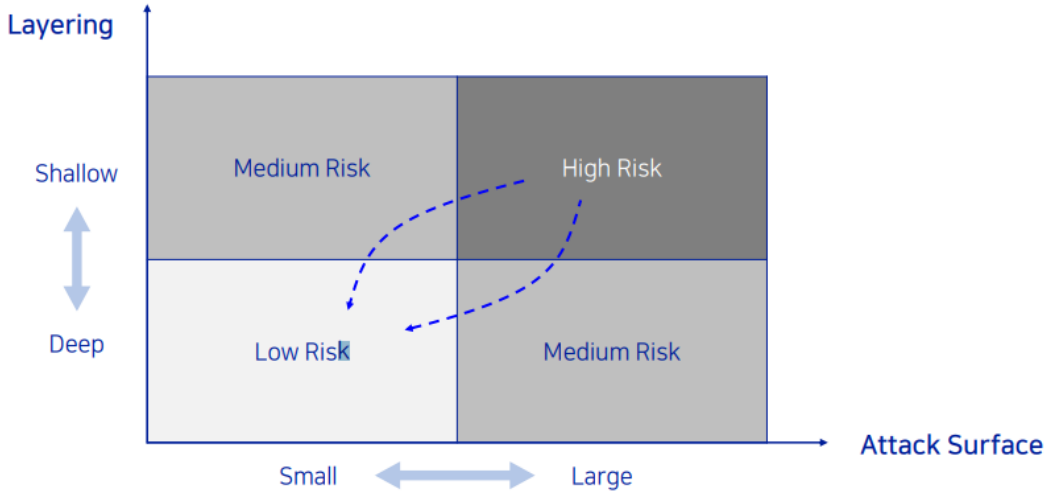
Software Attack Surface

- 응용 프로그램, 유틸리티 또는 운영 체제 코드의 취약점
- 특히 웹 서버 소프트웨어에 중점을 둡니다.

Human Attack Surface

- 사회 공학, 인간의 실수 및 신뢰할 수 있는 내부자와 같은 인적 요인이나 외부자에 의해 생성된 취약점

Defense in depth and Attack surface



Computer security strategy

Security Policy

- 시스템 또는 조직이 민감하고 중요한 시스템 자원을 보호하기 위해 보안 서비스를 제공하는 방법을 지정하거나 규제하는 규칙과 실천 방법의 공식적인 진술

Security Implementation

- 네 가지 보완적인 조치를 포함합니다: 예방 > 탐지 > 대응 > 복구

Assurance(확증)

- 시스템 설계 및 시스템 구현 모두를 포함하며, 확증은 정보 시스템의 속성으로, 시스템이 보안 정책이 시행되도록 작동하여 시스템이 안정적으로 운영됨을 확신할 수 있는 근거를 제공.

Evaluation(평가)

- 특정 기준을 기준으로 컴퓨터 제품이나 시스템을 조사하는 과정
- 테스트를 포함하며 형식적인 분석 또는 수학적인 기법을 사용할 수도 있음