Chapter 2-1 : Computer Security Overview

Objectives

1. 보안의 주요 필수 요소 : **CAI** (기밀성 - Confidentiality, 무결성 - Integrity, 가용성 - Availability)
2. 보안 공격 및 위협의 유형?
3. 기본 보안 설계의 원리
4. 공격의 발생 경로와 가능성
5. 전반적인 보안 전략

Computer Security의 정의

1. Wikipedia;

H/W, S/W 또는 정보의 도난, 손상으로부터 Computer System을 보호하며, 서비스 중단으로부터 보호하는 것

2. NIST 1955;

정보 위주의 보안이며 범위가 넓음. 정보 시스템 자원(H/W, S/W, firmware, 정보/데이터통신 등)의 C.I.A를 유지하기 위한 자동화된 정보 시스템에 제공되는 보호

⭐CIA : Three Key Objectives⭐

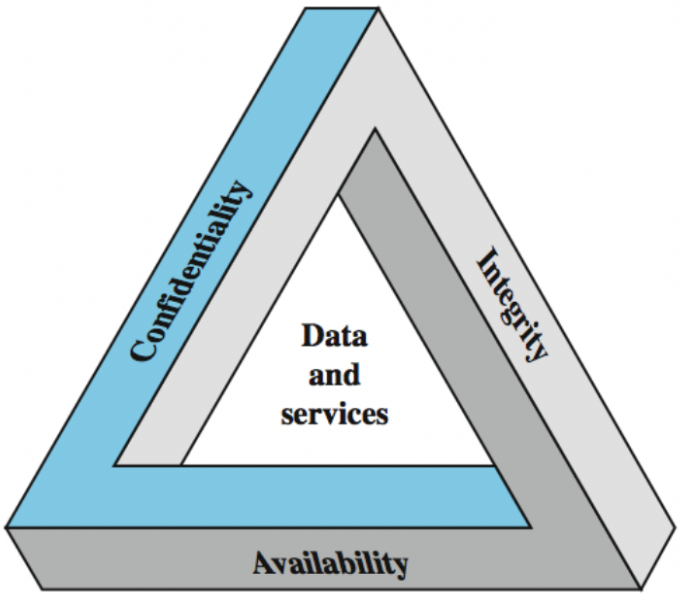


Figure 1.1 The Security Requirements Triad

Confidentiality : 기밀성

- 사용을 승인 받은 사람만 해당 정보에 접근이 가능함

1. Data Confidentiality : 허가되지 않은 개인에게 노출하지 않는다. (unauthorized individuals)
2. Privacy : 민감 정보는 안됨. (정보에 초점) 어떤 정보를 모으고 저장해야 하는지 (sensitive information)

Integrity : 무결성

- 적절한 권한을 가진 사용자에 의해 인가된 방식으로만 정보를 변경할 수 있음

1. Data integrity : 정보와 프로그램이 **지정된 방법**과 **인가된 방식**으로만 변경되도록 허용
2. System Integrity : 시스템이 정해진대로 동작해야 함 (의도한대로 작동)

Availability : 가용성

- 정보 자산에 대해 적절한 시간에 접근이 가능해야 한다
  - Ex) 24시간 편의점

1. 시스템이 합법적인 사용자에게 사용되어야 함
    a. 돈 냈는데 써야 함. ex) 카카오톡의 서비스 장애 등

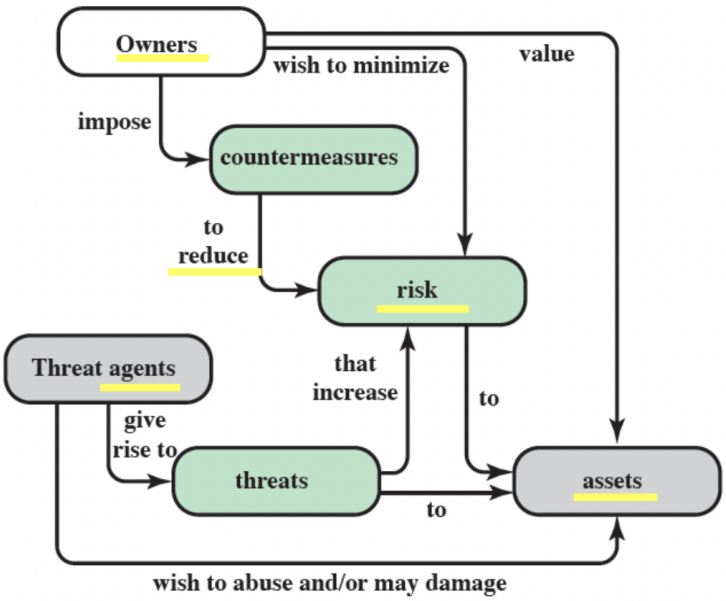
CIA Examples

- **Confidentiality : 기밀성**
    - Severe | 학생 학점 정보 (학생에게만 이용가능해야 함, 법률적으로 보장)
    - Serious | 디렉토리 정보, 학생 등록 정보 (법률적 보장은 아님)
    - Limited | 보도자료, course 정보, 연구발행물
- **Integrity : 무결성**
    - Severe | 병원 환자의 알러지 정보
    - Serious | 온라인 뉴스 그룹 등록 데이터
    - Limited | 익명의 온라인 설문조사
- **Availability : 가용성**
    - Severe | 인증을 제공하는 시스템
    - Serious | 대학교의 공개 웹사이트
    - Limited | 온라인 전화번호 검색

추가적인 보안 개념

- **Authenticity : 확실성, 진정성**
    - 검증 가능하고 신뢰성 있는 특성
    - 전송물, 메시지 또는 발신자의 유효성에 대해 확신하는 특성
- **Accountability : 책임 추적성 (공격이 일어난다면 추적 가능해야 함)**
    - 개체의 행동을 독특하게 추적하여 그 개인을 지원하는 부인방지, 존경 등의 요구 사항을 생성하는 속성

⭐Security 개념과 관계⭐



Adversary (threat agent)

- 공격하는 주체
- Asset에 피해를 입히거나 악용할 목적을 갖는다.

Attack

- 실제 공격 (피해 발생)

Countermeasure

- 보안 매커니즘

Risk (위험)

- 취약점이 공격으로 발생할 손실의 기대값
- 예상되는 위협에 의해 자산에 발생할 가능성이 있는 손실의 기대치 **(제어 O)**

Security Policy

- 보안을 어떻게 막을지에 대한 정책

System Resource (Asset)

- 보안할 자산

Threat (위협)

- 위협, 보안이 위반될 수 있는 잠재적 가능성

- 자산의 손실을 발생시키는 위험이나 행위 **(제어 X)**

Vulnerability

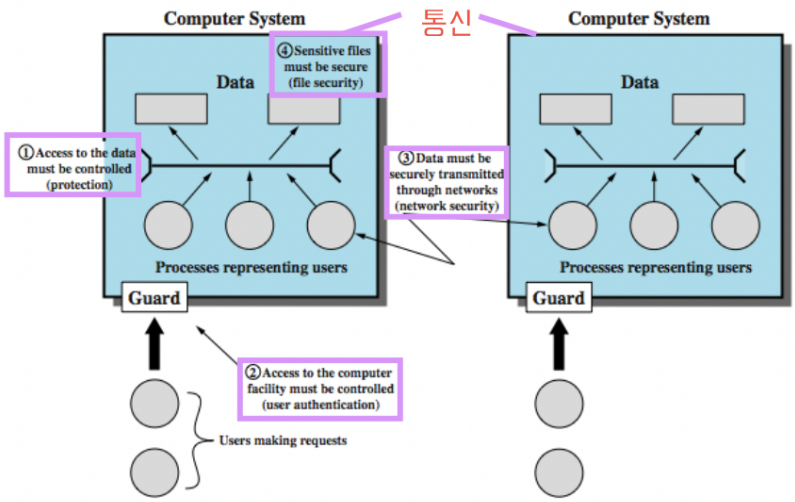
- 정보시스템이 지니게 되는 보안 취약점

Threat Consequences (위협의 결과)

- **Unauthorized disclosure**
  - **무단 공개 : 기밀성 위협**
  - 데이터 노출(exposure), 가로채기(interception), 추론(inference), 침입(intrusion)
  - interception - 통신 상황에서 민감 정보를 낚아챔. (중간자공격)
  - inference - 정보에 직접적 접근은 하지 않음.
  - intrusion - 허가되지 않은 일반사용자가 접근
- **Deception**
  - **속임수, 기만(위/변조) : 무결성 위협**
  - 위장(masquerade), 변조(데이터 변경: falsification), 부인(repudiation)
- **Disruption**
  - **중단 : 무결성, 가용성 위협**
  - 기능 장애(파괴: incapacitation), 손상(백도어 로직: corruption), 방해(통신 방해, 회선 과부하: obstruction)
- **Usurpation**
  - **차지 : 무결성 위협 (강탈)**
  - 무단 도용(서비스 도용: misappropriation), 오용(해커가 불법적으로 접근: misuse)

컴퓨터 보안과 위협의 범위

컴퓨터 보안 과정



< Scope of Computer Security >

1. 데이터 접근
2. 인증 (접근자 등)
3. 데이터 전송 상황에서 안전히 보호 (네트워크 프로토콜에 대한 보안 포함)
4. 파일에 대한 보호

위협의 예시

< Examples of Threats >

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service. 도난당한 경우	An unencrypted CD-ROM or DVD is stolen.	
Software	프로그램이 삭제된 경우, 바뀐 경우 등 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	파일이 삭제된 경우 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.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable. 메세지 파괴	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

기본 보안 설계 4원칙

Separation of Privilege

- 권한을 계층까지 나눠야 한다

Least Privilege

- 최소한의 권한을 가져야 한다 (주어진 업무만 할 수 있도록)

Least Common Mechanism

- 다른 사용자에게 공유되는 것을 최소화해야한다.

Psychological Acceptability

- 심리적인 수용성 (허용가능성)
- 사용자가 불편하게 느껴질 만하게 하면 안됨! 지나치게 보안 한답시고 간섭 X

Attack Surfaces

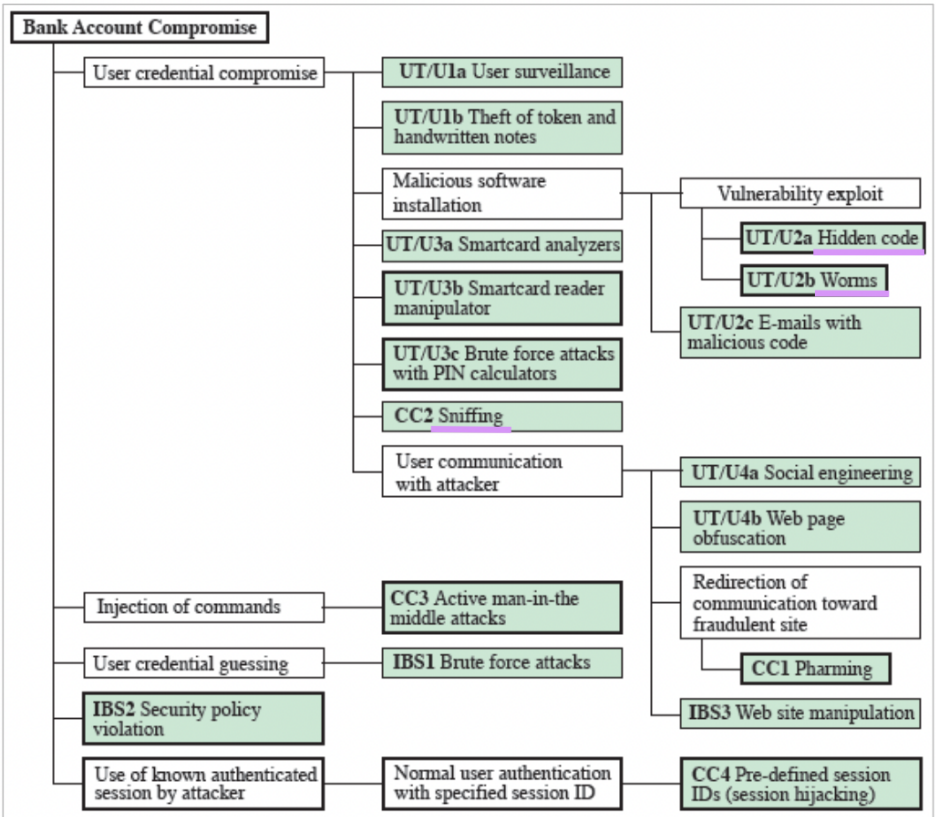
Attack Surfaces

- 공격자 관점에서 공격이 가능한 (도달 가능한) 취약점(Valnerabilities)

3개의 분야 존재

- **Network attack surface (i.e., network vulnerability)**
  - open ports를 이용한 방법.
  - 알려진 취약점에 대한 정보수집을 통해 시간/돈을 절약
- **Software attack surface (i.e., software vulnerability)**
  - Memory safety violations(주소에 대한 접근이 가능) - 버퍼 오버플로우, 포인터 dangling
- **Human attack surface (e.g., social engineering - 사회공학적 관점에서)**
  - 사용자 인증을 통해 접근
  - ex) sensitive information 정보를 SNS를 통해 쉽게 접근 가능

Attack Trees



정의

- Wikipedia; how an asset, target, might be attacked

목적

- 알려진 공격 패턴을 잘 활용함

Security Taxonomy (보안 분류)

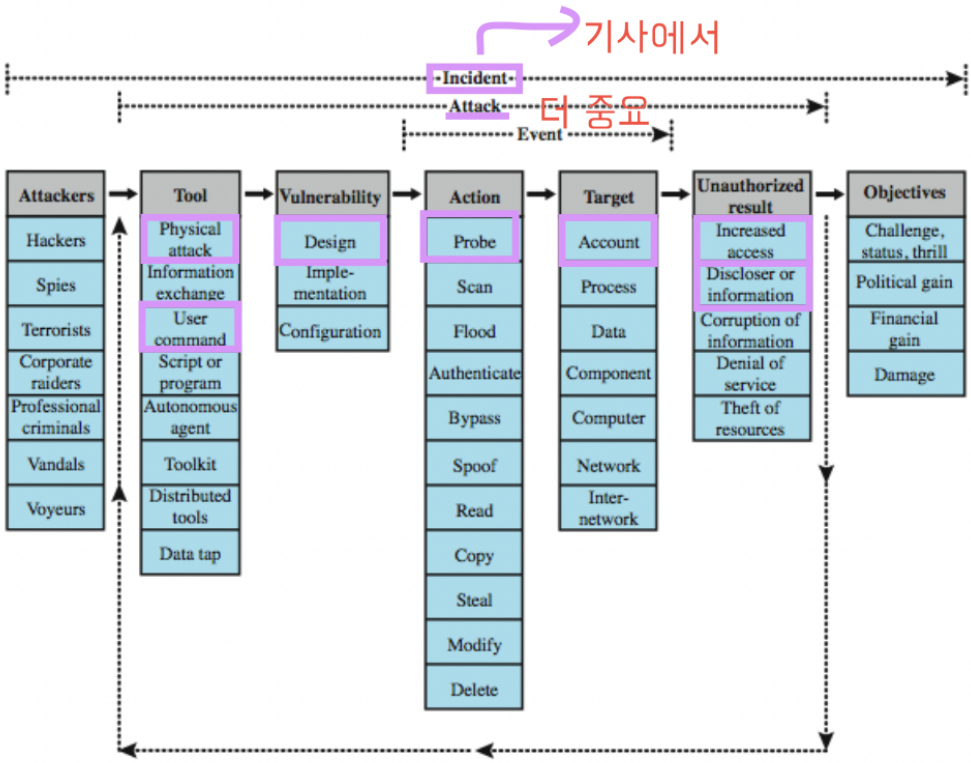
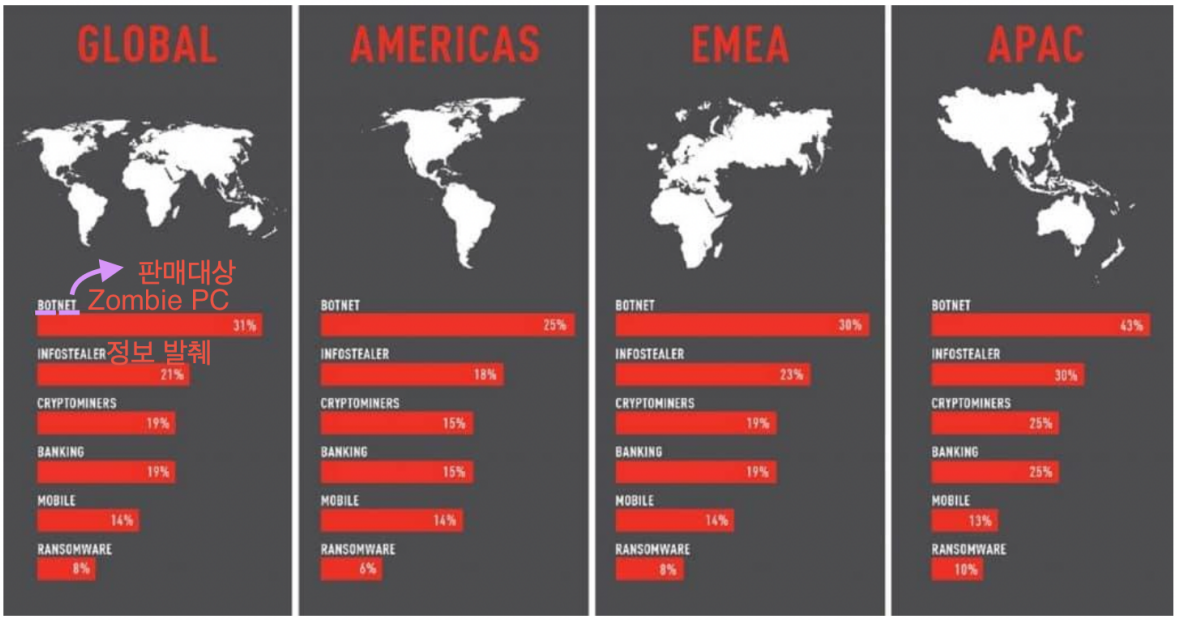


Figure 1.4 Computer and Network Security Incident Taxonomy

- 2022 Cyber Attack Trends



Network Infrastructure Security