Information and Network Security

컴퓨터개론

(Introduction to Computer Systems)

GEN1030

정보보안이란?

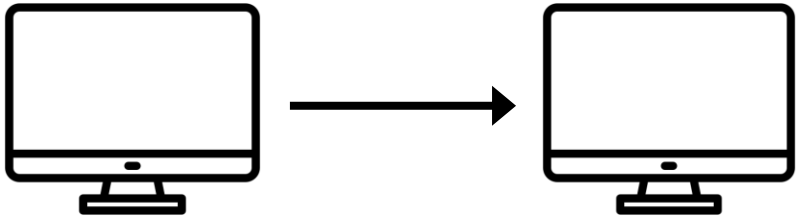
정보보안 개요

- 정보의 생성, 가공, 유통, 배포, 사용 과정에서 발생할 수 있는 위협에 대응하는 활동

- 정보기술의 발전으로 정보보안의 중요성이 증대
  - 과거: 개인이나 특정 조직이 정보를 독점적으로 소유 및 유통
  - 현대: 정보가 사회 전반과 전 세계로 *빠르게* 공유 됨

정보보안 개요

- 문제가 발생하는 위치에 따른 구분



컴퓨터 자체

컴퓨터 보안

Computer Security

컴퓨터 자체와 그 안에 저장된 정보를 보호하기 위한 기술

네트워크

네트워크 보안

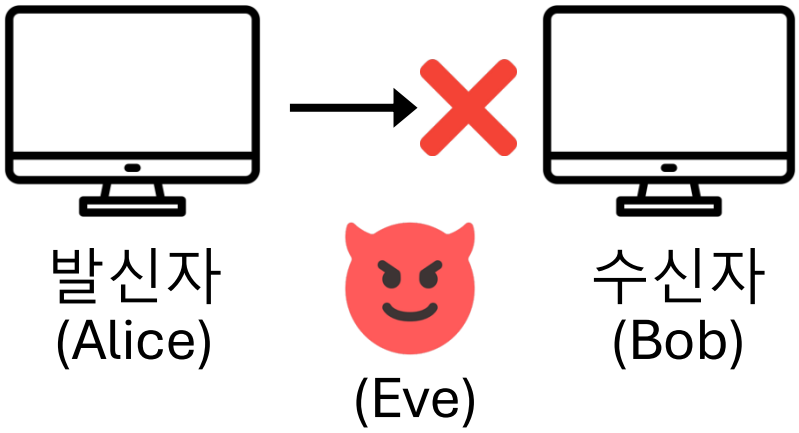
Network Security

컴퓨터 사이에서 오가는 정보를 보호하기 위한 기술

정보보안 개요

- 네트워크 보안 위협 예시

정보 전송 방해/차단 (interruption)

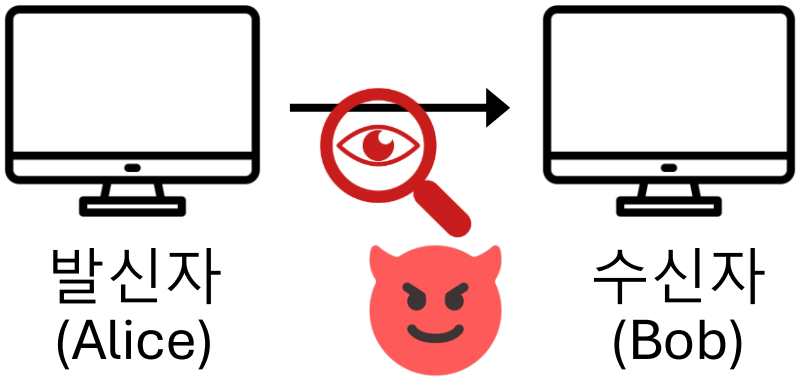


Alice가 Bob에게 전송하는
정보를 공격자(Eve)가 차단

정보보안 개요

- 네트워크 보안 위협 예시

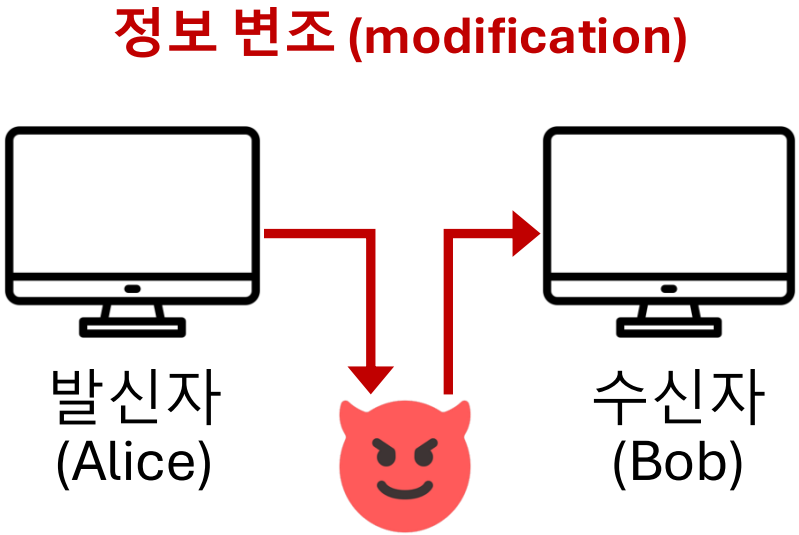
정보 가로채기 (interception)



Alice가 Bob에게 전송하는
정보를 공격자 중간에서
몰래 확인
→ 정보 유출

정보보안 개요

- 네트워크 보안 위협 예시

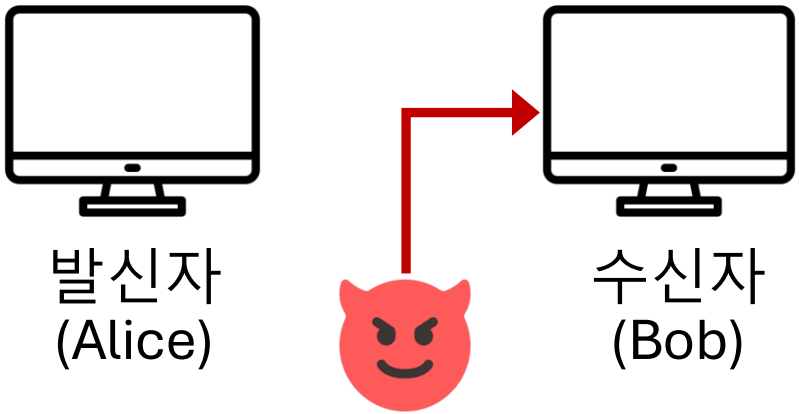


Alice가 Bob에게 보내는 정보의
일부 혹은 전부를 공격자가
변경하여 Bob에게 전송

정보보안 개요

- 네트워크 보안 위협 예시

정보 위조 (fabrication)



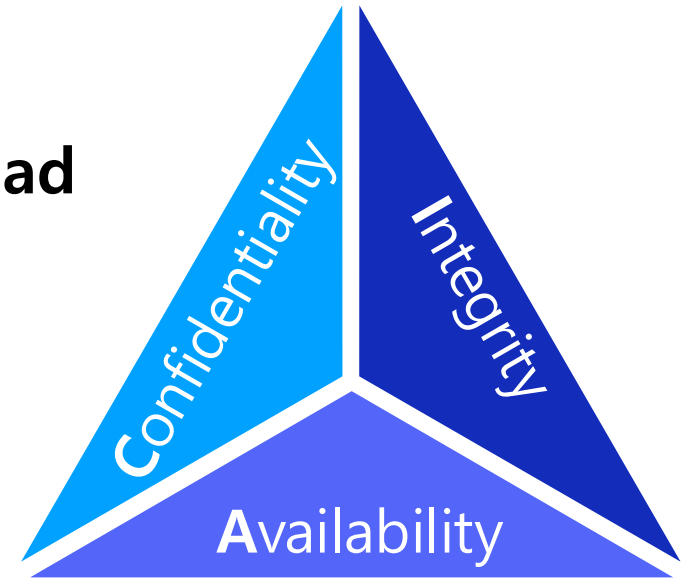
공격자가 Alice가 보낸 것처럼
가짜 정보를 만들어
Bob에게 전송
(Alice는 이를 알지 못함)

정보보안 목표

- 기본적인 목표
  - 내부 또는 외부의 공격자에 의한 정보의 파괴/변조/유출 등으로부터 중요한 정보를 보호

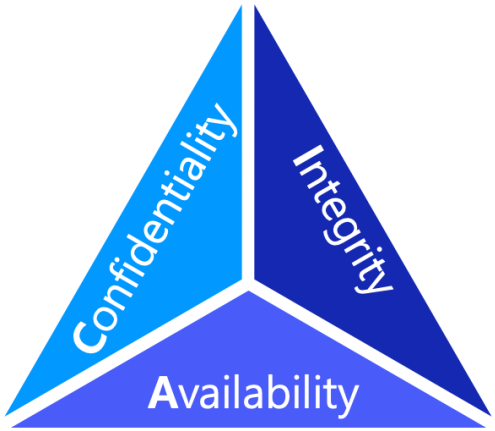
- 3대 목표

CIA Triad



정보보안 목표

- 기본적인 목표
  - 내부 또는 외부의 공격자에 의한 정보의 파괴/변조/유출 등으로부터 중요한 정보를 보호

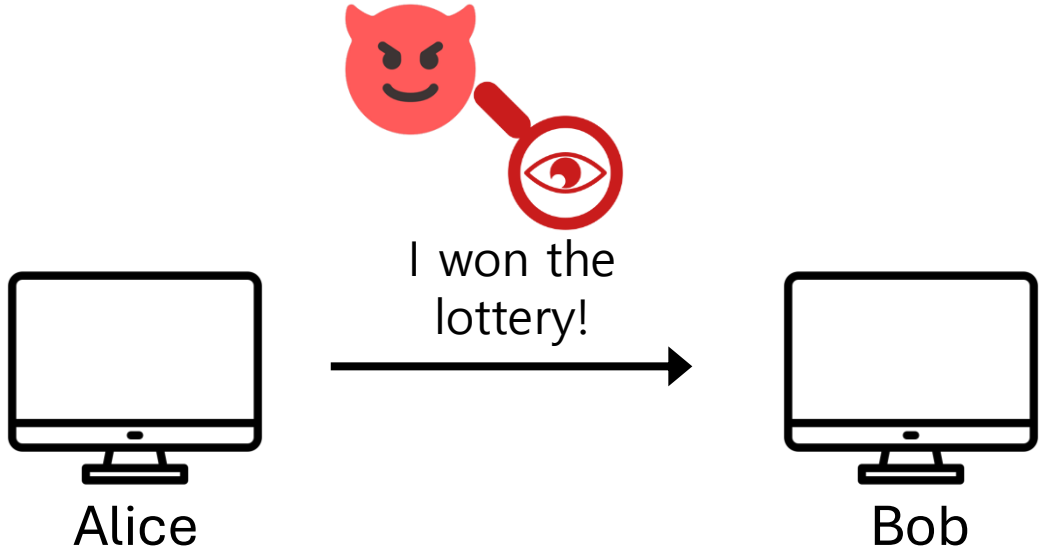


- 3대 목표
  - 비밀성(Confidentiality)
    - 허가된 사용자만 정보에 접근할 수 있도록 보호함
  - 무결성(Integrity)
    - 비인가된 변경, 삭제 생성 등으로부터 정보를 보호하여 정보의 정확성과 완전성을 보장
  - 가용성(Availability)
    - 정당한 권한을 가진 사용자가 필요할 때 정보와 서비스를 사용할 수 있도록 보장하는 원칙

비밀성(Confidentiality)

- 허가된 사용자만 정보에 접근할 수 있도록 보호함
  - 정보는 소유자 또는 관리자의 인가를 받은 사용자만 접근 가능
  - 인가되지 않은 사용자에게 정보 공개 방지

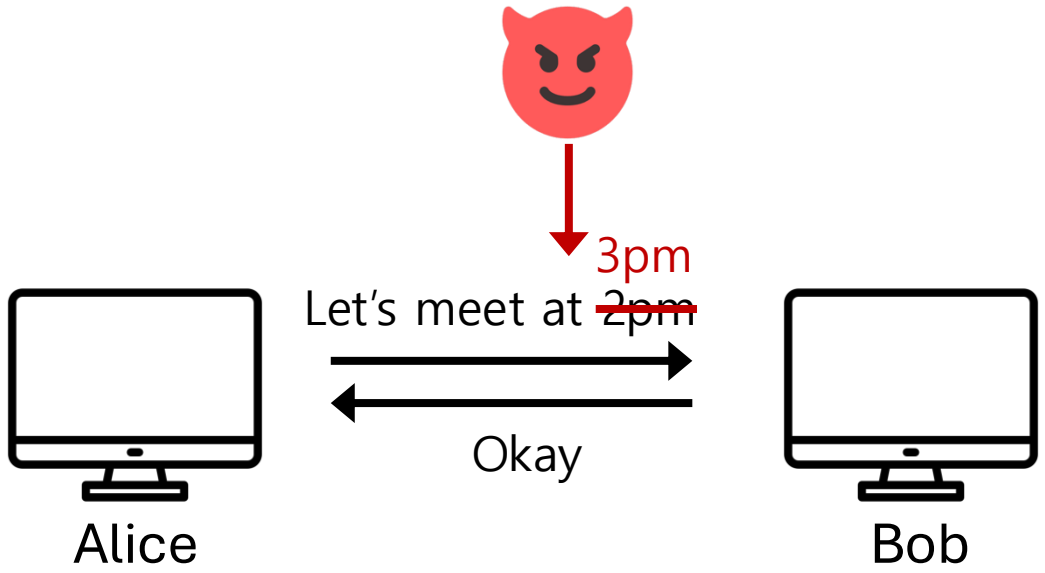
- 메커니즘
  - 접근 통제
  - 암호화
  - …



무결성(Integrity)

- 비인가된 변경, 삭제 생성 등으로부터 정보를 보호하여 정보의 **정확성**과 **완전성**을 보장
  - 공격자가 데이터를 중간에서 바꾸거나, 잘못된 데이터를 추가하면 무결성이 깨짐

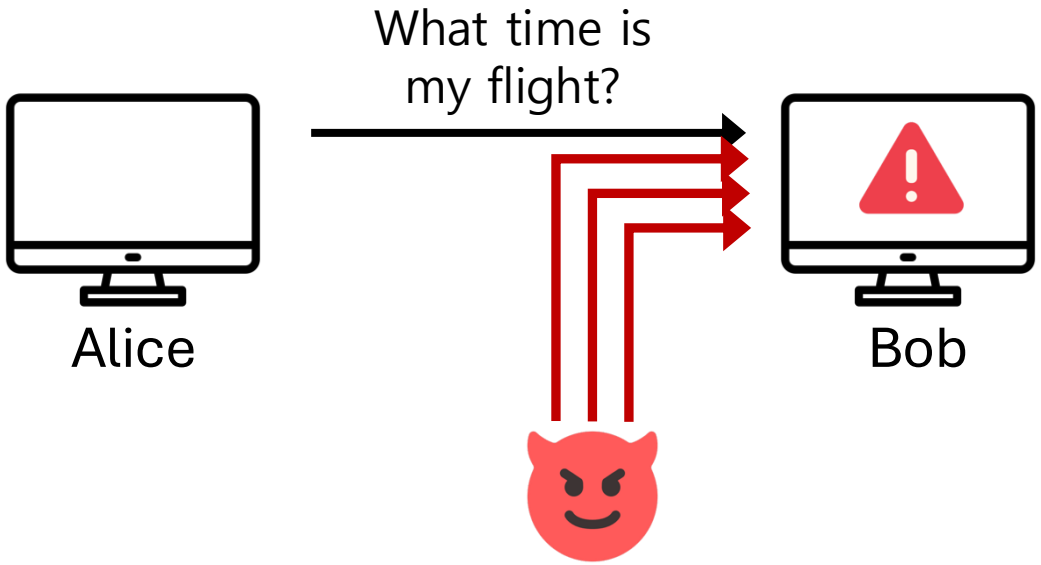
- 메커니즘
  - 디지털 서명
  - 접근 제어
  - …



가용성(Availability)

- 정당한 권한을 가진 사용자가 필요할 때 정보와 서비스를 사용할 수 있도록 보장하는 원칙
  - 시스템이 정상적으로 동작하고, 서비스가 거부되지 않아야 함
  - Ex) DDoS 공격으로 인한 웹사이트 접속 불가

- 메커니즘
  - 백업(Backup)
  - 중복성 유지
  - DDoS 방어
  - …



민감한 정보의 종류

- 다양한 개인정보
  - 과거: 개인을 식별하기 위한 기본 정보 중심
  - 현재: 전자상거래, 금융거래, SNS, 위치기반 서비스 등 다양한 활동에서 생성되는 정보로 확대

일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 국적, 성별 등
가족정보	가족구성원들의 이름, 생년월일, 직업, 전화번호 등
부동산정보	소유주택, 토지, 소유차량 등
소득정보	급여내역, 경력, 이자소득, 사업소득 등
신용정보	신용카드 정보, 거래내역, 대출기록 등
의료정보	병력, 진료기록, 혈액형, 약물 테스트 결과 등
위치정보	GPS 등에 의한 개인의 위치 정보
통신정보	E-mail, 전화통화내용, 메신저 기록, 인터넷 사용 기록 등

악성 프로그램과 사이버 공격

악성 프로그램

- 제작자가 의도적으로 사용자나 시스템에 피해를 주기 위해 만든 프로그램
  - 컴퓨터 시스템을 파괴하거나
  - 작업을 지연 또는 방해하거나
  - 정보를 훔치거나 유출할 수 있음

- 다양한 종류 존재
  - 바이러스(Virus)
  - 웜(Worm)
  - 트로이목마(Trojan)
  - 스파이웨어(Spyware)
  - 랜섬웨어(Ransomware)
  - …

악성 프로그램

- **컴퓨터 바이러스(Virus)**
  - 컴퓨터의 운영을 방해하는 악성 프로그램
  - 사용자 몰래 컴퓨터에 들어와 자기 자신 또는 변형된 형태를 복사
  - 프로그램이나 실행 가능한 부분을 변형
  - 감염 대상을 가지고 있지만 자체 전파/번식 능력은 보통 없음
  - 보조 저장장치, 전자메일, 파일 다운로드, 메신저 등을 통해 감염 가능

  - 대표적인 감염 증상
    - PC 사용 중 비정상적인 그림, 메시지, 소리 등이 나타날 경우
    - 사용자가 실행하지 않은 프로그램이 실행됨
    - 이유 없이 프로그램 실행속도가 저하되고 시스템이 자주 멈출 경우

악성 프로그램

- **컴퓨터 웜(Worm)**
  - 자기 자신을 복제하고 전파할 수 있는 악성 프로그램
  - 감염 대상(파일)이 없어도 독립적으로 실행 가능
  - 자체 전파 능력으로 빠르게 확산 될 수 있음
    - 주로 네트워크, 이메일 등을 통해

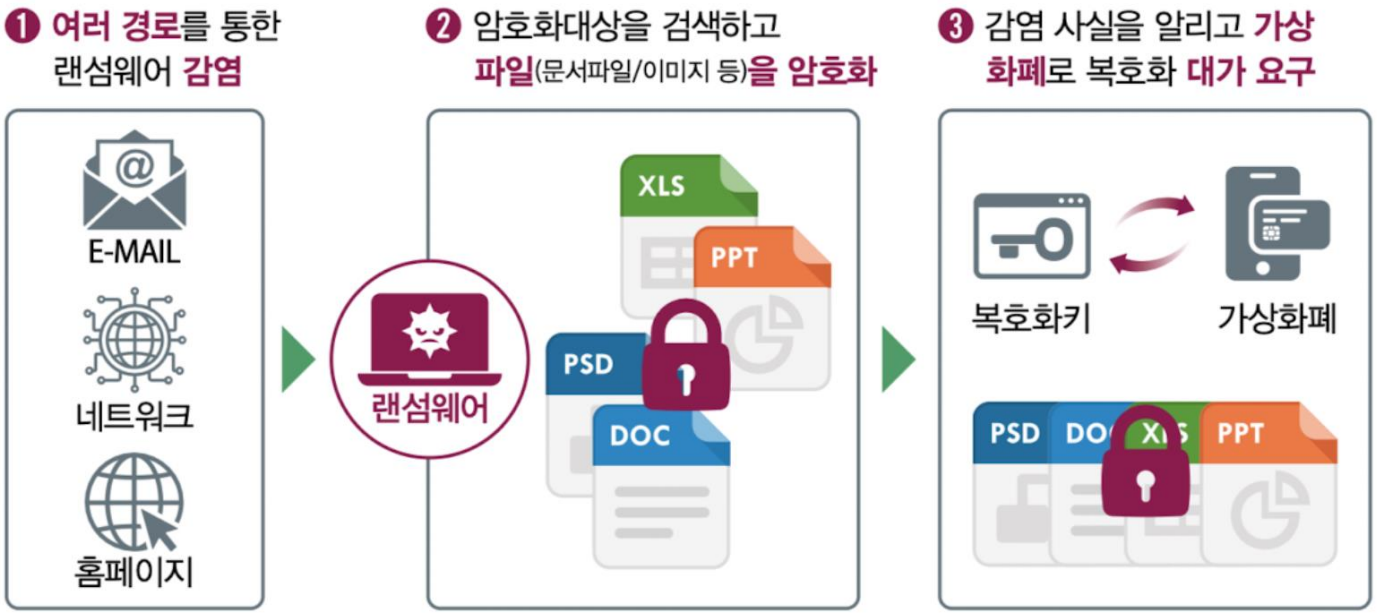
- **트로이목마(Trojan)**
  - 정상 프로그램처럼 위장하여 사용자 컴퓨터에 설치 되는 악성 프로그램
    - 겉으로는 정상적인 문서, 설치 파일처럼 보일 수 있음
  - 감염된 컴퓨터의 정보를 외부로 유출하거나 원격 제어 기능을 제공할 수 있음
  - 일반적으로 자기 복제 능력은 없음

악성 프로그램

- **스파이웨어(Spyware)**
  - 사용자 몰래 정보를 수집하거나 감시하는 악성 프로그램
    - 사용자 동의 없이 설치되는 경우가 많음
  - 웹 사용 기록, 계정 정보, 키보드 입력 등을 수집 가능
    - ex) 수집 된 정보는 외부 공격자 혹은 광고 업체로 전송

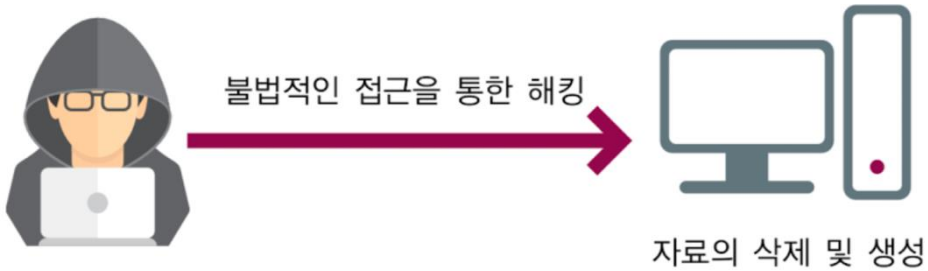
악성 프로그램

- 랜섬웨어(Ransomware)
  - Ransome + Software
  - 사용자의 파일이나 시스템을 사용할 수 없게 만든 뒤 금전을 요구하는 악성 프로그램
  - 파일을 암호화하거나 시스템을 잠가 사용자가 접근하지 못하게 함
  - 복구를 조건으로 금전 또는 가상화폐 요구



해킹과 사이버 공격

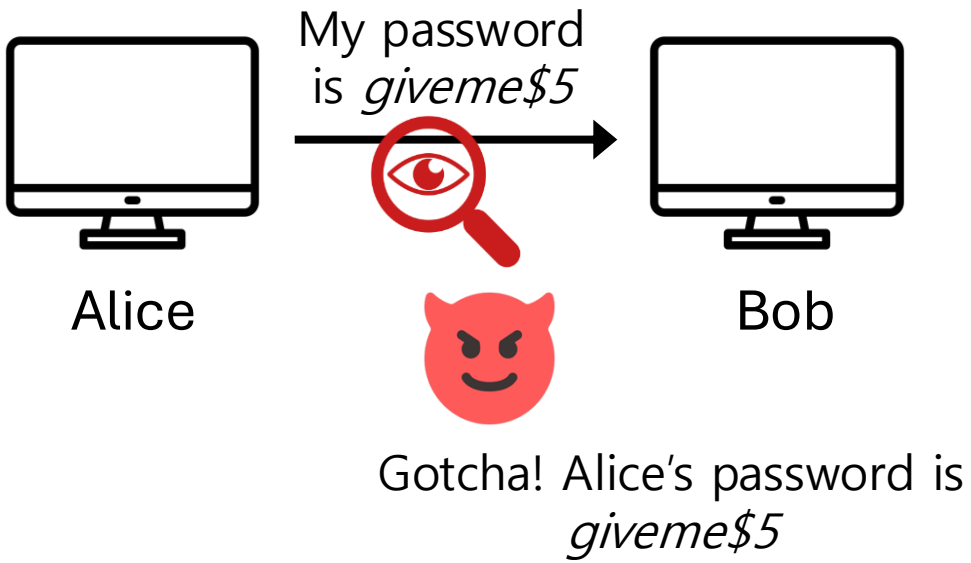
- 해킹(Hacking)
  - 컴퓨터 통신망을 통해 허가되지 않은 시스템에 접근하여 정보를 빼내거나, 파일을 삭제하거나, 시스템 또는 프로그램을 손상시키는 행위



  - 해커(Hacker)
    - 넓은 의미로는 컴퓨터 시스템의 구조와 동작을 깊이 이해하고 탐구하는 사람
    - 다른 사람의 컴퓨터에 불법으로 침입하여 악의적 행위를 하는 사람

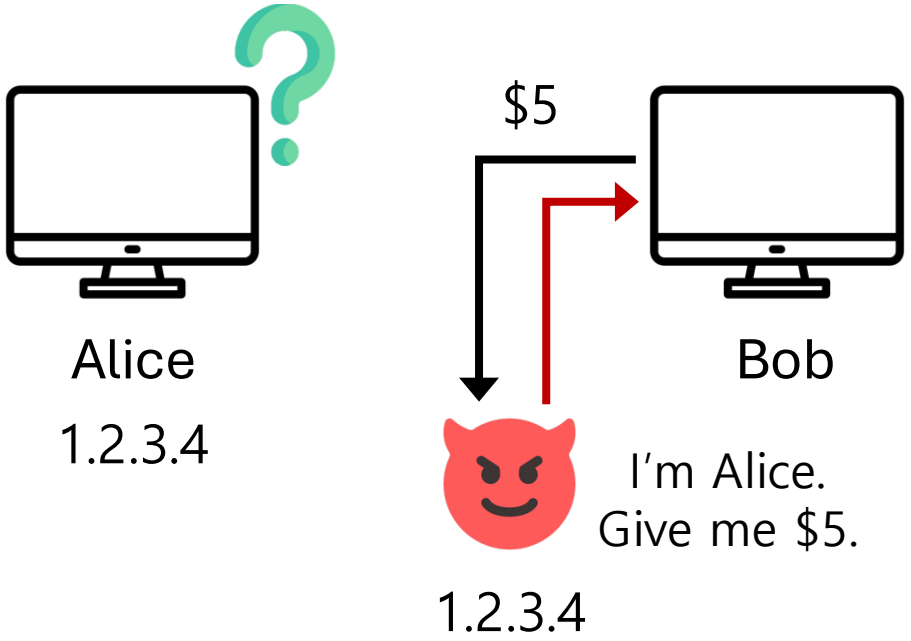
사이버 공격

- 스니핑(Sniffing)
  - 네트워크를 지나가는 트래픽(traffic), 패킷(packet)을 몰래 캡쳐하여 내용을 확인하는 기법
  - 민감한 정보(ex. 패스워드, 메시지 내용 등)가 유출 될 수 있음



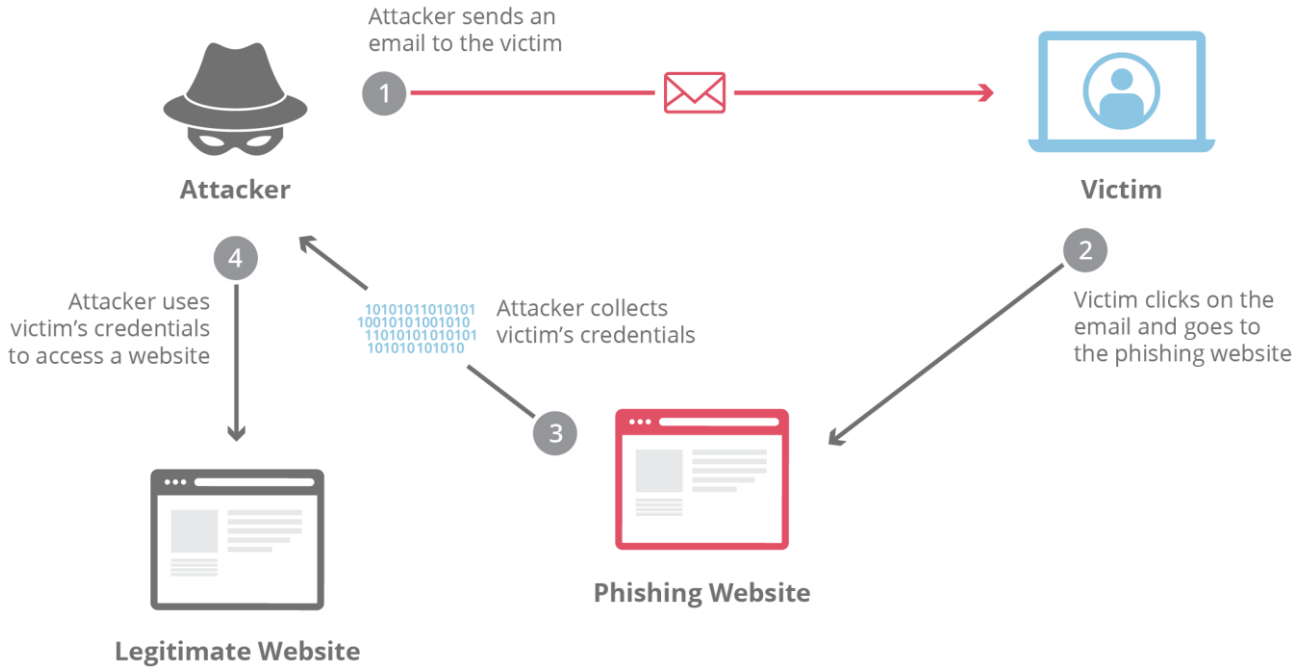
사이버 공격

- 스푸핑(Spoofing)
  - 자신의 신원이나 주소를 다른 사람 또는 정상 시스템처럼 위장하는 기법
  - 공격자는 정상 사용자나 정상 서버인 것처럼 보임
  - IP address, MAC address, DNS 정보, 이메일 sender 등을 위조할 수 있음



사이버 공격

- 피싱(Phishing)
  - 개인정보(Private data) + 낚시(Fishing)
  - 신뢰할 수 있는 기관이나 사람인 것처럼 속여 개인정보를 탈취하는 공격 기법
    - 은행, 카드사, 쇼핑몰, 학교, 회사 등을 사칭
  - 이메일, 문자, 가짜 웹사이트 등을 이용해 사용자가 직접 ID, password, 카드/계좌 비밀번호 등을 입력하도록 유도

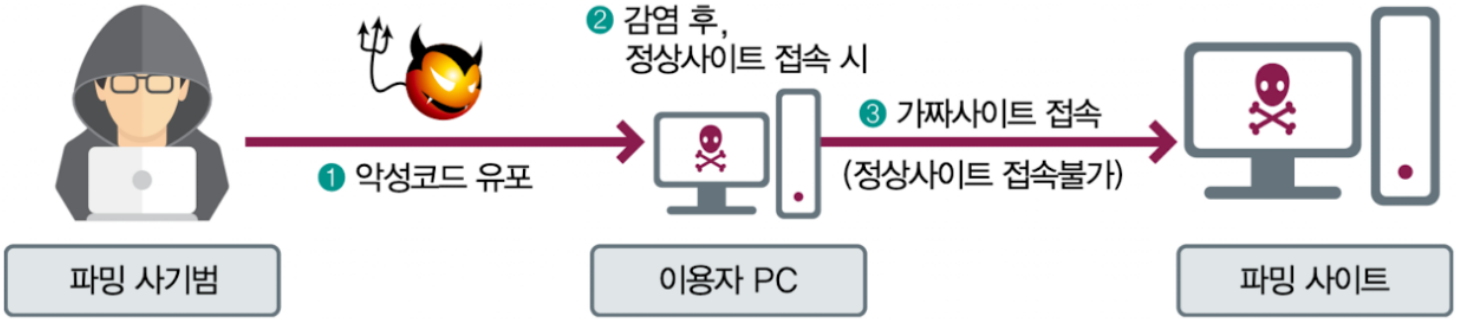


사이버 공격

- 스미싱(Smishing)
  - 문자메시지(SMS) + 피싱(Phishing)
  - 문자메시지를 이용한 피싱 공격
  - 문자 안의 링크를 클릭하도록 유도
    - Ex) 택배, 쿠폰, 공공기관 안내 등을 사칭
  - 링크 접속 시 악성 앱 설치, 가짜 사이트로 연결

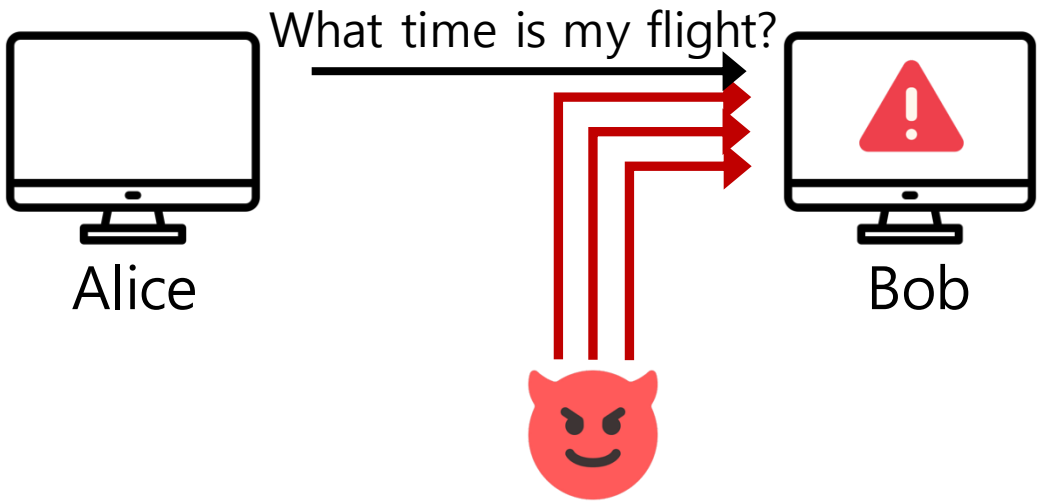
사이버 공격

- 파밍(Pharming)
  - 정상 웹사이트에 접속한 것처럼 보이지만, 실제로는 가짜 사이트로 유도하는 공격
  - 사용자가 정상 주소를 입력해도 가짜 사이트로 연결 될 수 있음
  - 악성코드, DNS 변조 등을 사용



DoS

- DoS (Denial of Service)
  - 서비스 거부 공격
  - 공격자가 서버에 과도한 요청을 보내 정상 서비스를 방해
  - Confidentiality나 integrity 보다는 availability를 깨뜨리는 공격
  - 서버의 CPU, memory, network bandwidth 등을 고갈시킬 수 있음
    - 서버는 요청을 처리하기 위해 위 자원을 사용
    - 공격자가 너무 많은 요청을 보내면 서버의 자원이 고갈되어 정상 사용자의 요청을 처리하지 못함



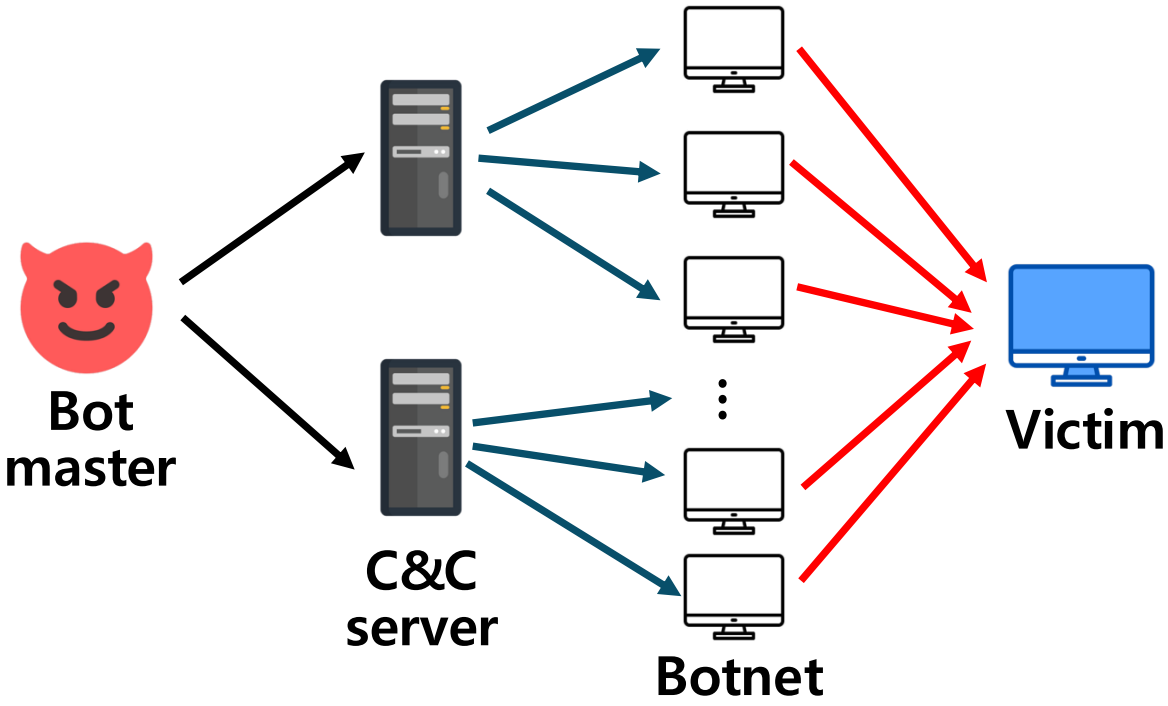
DDoS

- Distributed Denial of Service (DDoS)
  - 분산 서비스 거부 공격
  - 여러 대의 감염된 컴퓨터가 동시에 타겟 서버 공격
    - Botnet 사용
  - 공격 규모가 크고 여러 위치에서 발생하므로 방어가 어려움

- Botnet
  - Bot + Network
  - 악성코드에 감염되어 공격자가 원격으로 조종할 수 있는 컴퓨터의 집합
    - 감염된 컴퓨터를 bot이라고 부름
  - 사용자는 자신의 컴퓨터가 공격에 이용되고 있다는 사실을 모를 수 있음
  - 공격자는 여러 bot에게 동시에 명령 내려 대규모 공격 수행

DDoS

- 공격 방식
  - Bot master: Botnet을 제어하는 공격자(ex. 공격 명령 내림)
  - Command & Control (C&C) server: 감염된 PC들에게 명령을 전달
  - Botnet: 여러 Bot으로 구성된 공격 네트워크



DoS and DDoS

- 공격의 목표는 동일
  - 정상 사용자가 서비스를 이용하지 못하게 해서 availability를 깨뜨리는 것

- 공격에 참여하는 시스템의 수
  - DoS
    - 하나의 공격 시스템이 목표에 과도한 요청을 보냄
    - 공격 출처가 주로 하나
  - DDoS
    - 여러 대의 감염된 컴퓨터로 동시에 목표를 공격
    - 공격 출처가 여러 곳으로 분산