기업 데이터보호를 위한 실전 보안 마스터 과정

한국생산성본부

Contact liz0904@teiren.io

010-6539-2122

Orientation

해당 강의자료는 외부 반출을 금합니다.

목차

시간	세션	주요 내용 및 활동
09:30 ~ 10:00 (30분)	오리엔테이션	· 강사 소개 및 교육 커리큘럼 설명
10:00 ~ 11:10 (1시간)	보안의 기본 개념 이해	· 보안 3대 요소 및 그와 관련한 보안 개념 단어 익히기
11:00 ~ 12:00 (1시간)	보안 취약점 진단 이해	· 기술적 보안 취약점의 이해
12:00 ~ 14:00 (2시간)	네트워크 보안 취약점	· 네트워크 보안 위협 개념 및 보안 대책 분석 · 방화벽 구성 실습
14:00 ~ 16:00 (2시간)	웹 취약점 (1)	· 기초 해킹 실습 (XSS, 파라미터 변조, 쿠키 변조)
16:00 ~ 17:30 (1시간 30분)	웹 취약점 (2)	· BurpSuite를 사용한 웹 취약점 분석

목차

시간	세션	주요 내용 및 활동
09:30 ~ 10:00 (30분)	1일차 복습	· 1일차 복습
10:00 ~ 11:00 (1시간)	개인정보보호의 이해	· 인터넷 윤리 기초 및 사회적 책임 · 개인정보보호의 이해
11:00 ~ 12:00 (1시간)	개인정보 침해 사례 분석 (1)	· ISMS-P, GDPR 등 보안 법률 및 인증의 이해 · 가상 기업 개인정보 침해 사례 개요
12:00 ~ 14:00 (2시간)	개인정보 침해 사례 분석 (2)	· 가상 기업 컴플라이언스 제정 및 관리 서류 작성하기
14:00 ~ 15:00 (1시간)	기업 보안 솔루션 (1)	· 기업 보안 솔루션의 역할과 주요 기능 · 실무 솔루션 적용 사례 및 활용 방안
15:00 ~ 16:00 (1시간)	기업 보안 솔루션 (2)	· 기업 보안 솔루션 사용 실습
16:00 ~ 17:30 (1시간)	마무리	· 추가 학습 로드맵 제시 및 질의 응답 · 설문조사 및 수료증 발급

강사 소개

김성연
(주) 테이렌 대표이사
E-mail: liz0904@teiren.io
Phone: 010-6539-2122
LinkedIn: linkedin.com/in/liz0904-teiren

[이력]

- 한국은행, 신한은행, 인천공항공사 보안 취약점 점검 업무 이력
- KITRI ‘Youth-Cyber Guardiauns’ 강사
- 아시아재단 ‘아시아재단-마이크로소프트 Skills2Work-Seoul’ 멘토
- 중소벤처기업부 예비창업패키지, 초기창업패키지, TIPS R&D 선정
- 미국 Rabbit Ventures, 한국 더벤처스, 더이노베이터스 등 투자 유치
- 여성창업경진대회 ‘입상’, ‘Girls Unicorn Contest’ 대상, 성균관대 대학원 ‘기업가정신상’ 수상
- 한국정보기술연구원 ‘표창장-연구원장상’, 벤처기업협회 ‘창업활성화 부문 올해의벤처상’ 협회장상 수상
- ‘Graph DB 보안위협탐지 모델링’ 국내 특허 등록 및 해외 PCT 출원
- ‘볼라틸리티를 기반으로 한 인스턴트 메신저 툴’ SW 저작권 등록, ‘Teiren Cloud SIEM’ SW 저작권 등록

https://web-hacking.kro.kr

강의에 꼭 필요한 웹페이지인, 꼭 들어가야 합니다!

보안의 기본 개념 이해

해킹(Hacking)이란?

- 자신의 실력을 자랑하기 위해서, 또는 돈을 벌기 위해서 남의 시스템에 **허가 없이 침입**하는 행위
- 컴퓨터 네트워크의 **보안 취약점**을 찾아내 **그 문제를 해결**하고, 악의적으로 이용되는 것을 **방지하는** 것

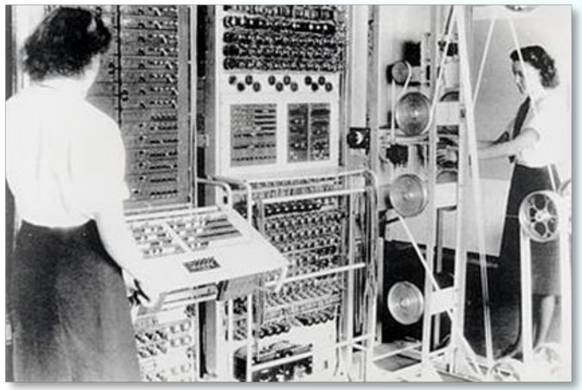
크래킹(Cracking)이란?

- **나쁜 목적**을 가지고 시스템에 침입하여, 남의 정보를 훔치거나 시스템을 파괴하는 행위

해킹 != 크래킹

대중매체에서는
해킹을 단순히 피해를 끼치는 부정적인 의미로만 사용하고 있는 실태이지만,
해킹과 크래킹은 다른 의미입니다.

해킹의 역사



1950년대

- 암호화 기계 애니그마
- 애니그마를 해독한 콜로서스

해킹의 역사

1960년대

- 전화망 침입을 통한 무료 전화 해킹
- 2,600Hz의 휘파람을 불면, 장거리 전화를 무료로 쓸 수 있다는 사실을 발견
- 시리얼에 들어있던 장난감 호루라기를 불면 2,600Hz가 발생해, 무료 통화가 가능해짐

네트워크 해킹의 시작, 1980년대

414 Gang 사건

주체	미국 위스콘신주 밀워키의 고등학생 7명
이름 유래	지역 전화 지역번호가 414라서 이름이 붙음
행위	모뎀을 통해 여러 기관의 컴퓨터에 무단 침입 국립 실험실(로스앨러모스), 미 국방부 컴퓨터,여러 기업 및 연구기관 등
목적	금전적 이득보다 “호기심”과 “재미” 위주였음.
결과	· 연방수사국(FBI)에 의해 검거 · 청소년 신분이라 비교적 가벼운 처벌을 받았지만, 미국 내에서 최초로 대중적 주목을 받은 청소년 해킹 사건이 되었음.

해커와 해킹문화의 등장

•해커를 소재로 한 최초의 영화 <War Games>, 해킹 잡지 <Phrack> 등

해킹의 활성화, 1990년대

해킹 대회 DEFCON의 설립

- 세계적인 해킹 대회인 DEFCON이 설립됨
- 데프콘에서 트로이목마 프로그램인 '백 오피리스'가 발표됨

리눅스 운영체제의 공개

- 리누스 토발즈가 리눅스 운영체제를 만들어 공개함

인터넷 브라우저의 등장

- 인터넷 브라우저가 등장하며, 웹 해킹이 새롭게 시작되기 시작함.

해킹의 역사

2000년대

- 분산 서비스 거부 공격(DDoS), 웜(Worm), 바이러스
- 개인정보유출과 도용

2010년대

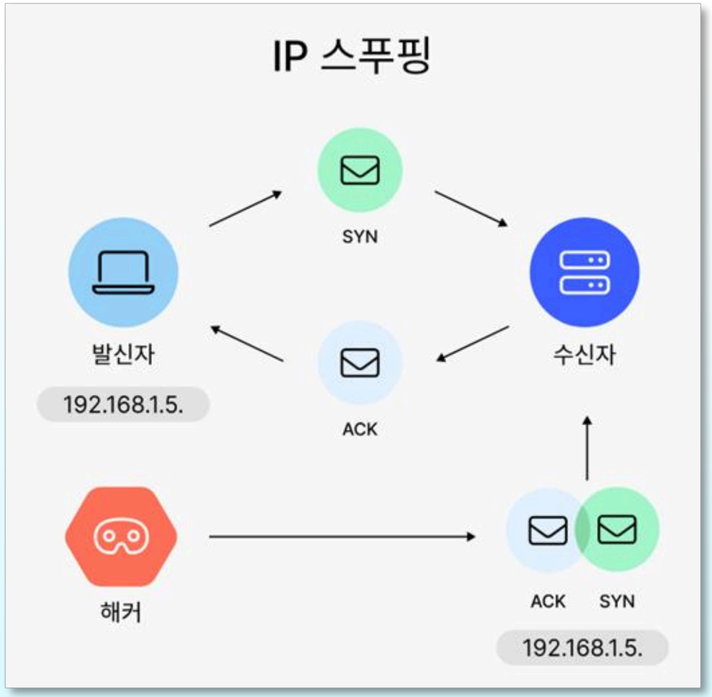
- 농협 사이버테러 사건 발생
- 스마트폰 해킹 증가

보안의 3대 요소

CIA Triangle

기밀성(Confidentiality)이란?

- 적절한 권한을 가진 사용자가 **인가한 방법으로만 정보를 변경**할 수 있도록 하는 것
  - 정보가 변질되지 않아야 함(무단 수정 방지, 일관성 보장, 데이터 손상 방지)



무결성을 해치는 공격

- 위조, 부인(Repudiation), 스푸핑(Spoofing)

무결성을 보안하는 방법

- 접근제어, 메시지 인증 등

BN 바이라인네트워크

스타벅스 와이파이, 해커가 만든 가짜라면?

기자들은 스타벅스를 좋아한다. 무선 인터넷과 전원 플러그를 제공하기 때문이다. 근무 시간의 대부분을 사무실 외부에서 일하는 기자들에겐 스타벅스...

1. 해커의 와이파이 설치 →
2. 무료 와이파이 접근
3. 은행 어플 로그인
4. 은행 비밀번호 입력
5. ← 은행 정보 탈취

무결성(Integrity)이란?

- **인가된 사용자만 정보 자산에 접근**할 수 있는 것
- 특정 데이터가 인증되지 않은/또는 허가받지 않은 사용자에게 노출되지 않게 해야 함

기밀성을 해치는 공격

- 도청(*Sniffing, 스니핑), 사회공학

기밀성을 보안하는 방법

- 식별, 인증, 권한 부여, 암호화

연합뉴스
https://www.yna.co.kr › 최신기사

'두개의 전쟁'에 불안한 민항사 조종사들…전자전에 운항 …

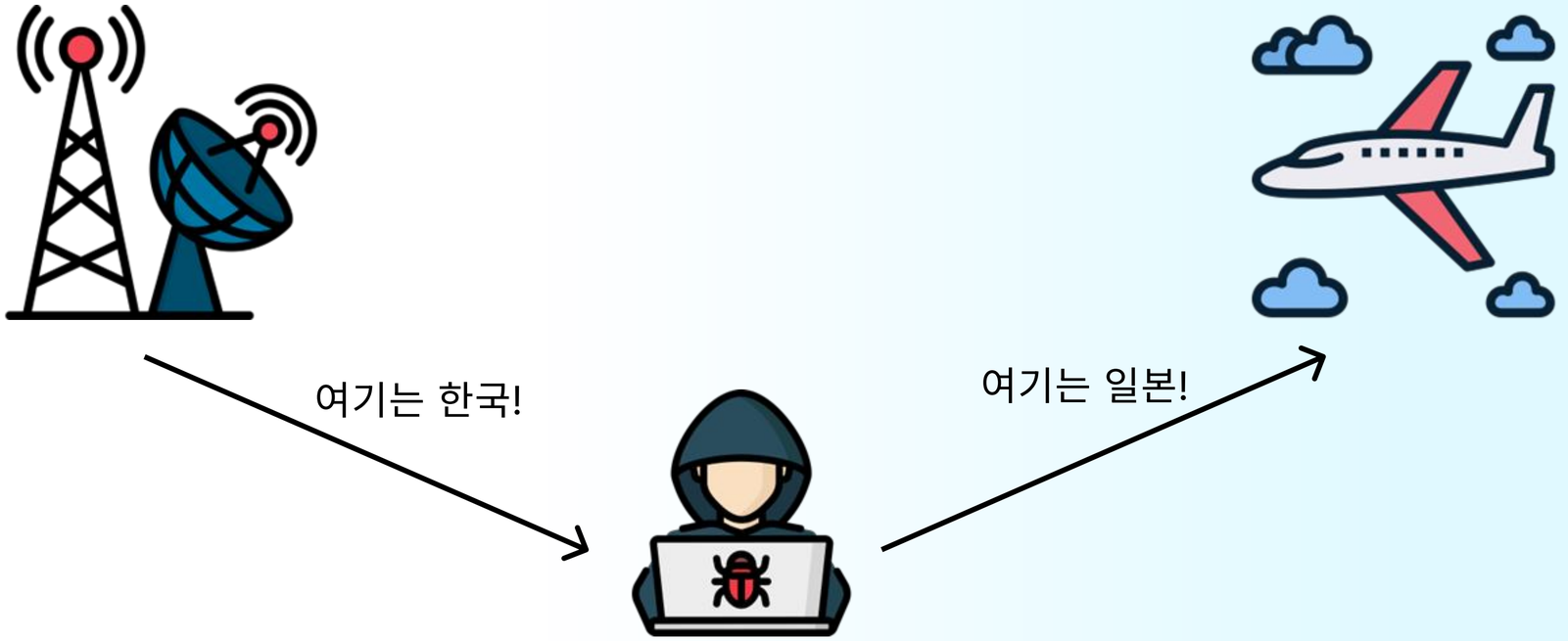
2023. 11. 22. — 유럽연합(EU) 규제당국과 항공사 내부 문건에 따르면 전파 방해나 가짜 신호를 보내는 '스푸핑'으로 항공기들이 위성 신호 수신을 방해받고 잘못된 …

여기는 한국!

연합뉴스
https://www.yna.co.kr › 최신기사

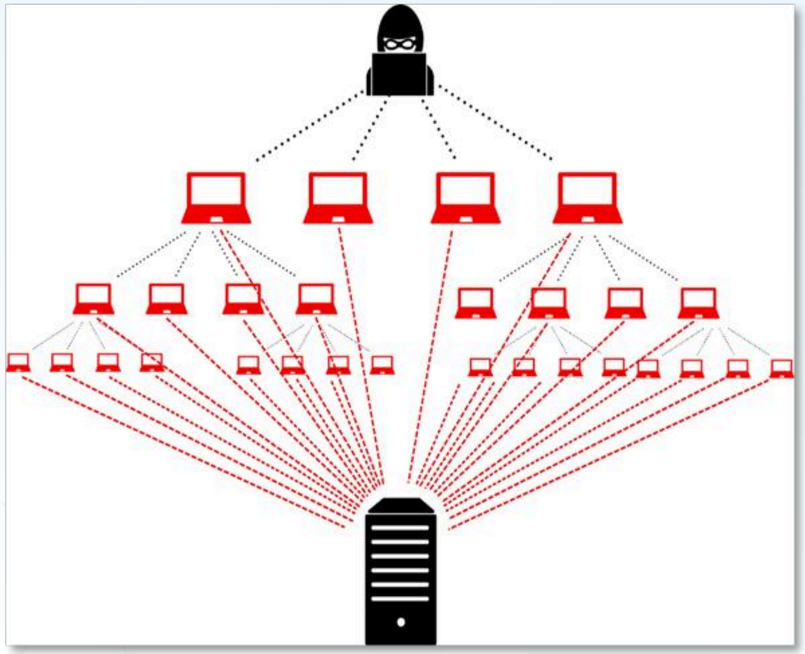
'두개의 전쟁'에 불안한 민항사 조종사들…전자전에 운항 …

2023. 11. 22. — 유럽연합(EU) 규제당국과 항공사 내부 문건에 따르면 전파 방해나 가짜 신호를 보내는 '스푸핑'으로 항공기들이 위성 신호 수신을 방해받고 잘못된 …



가용성(Availability)이란?

- **필요한 시점**에 정보 자산에 대한 **접근이** 가능하도록 하는 것

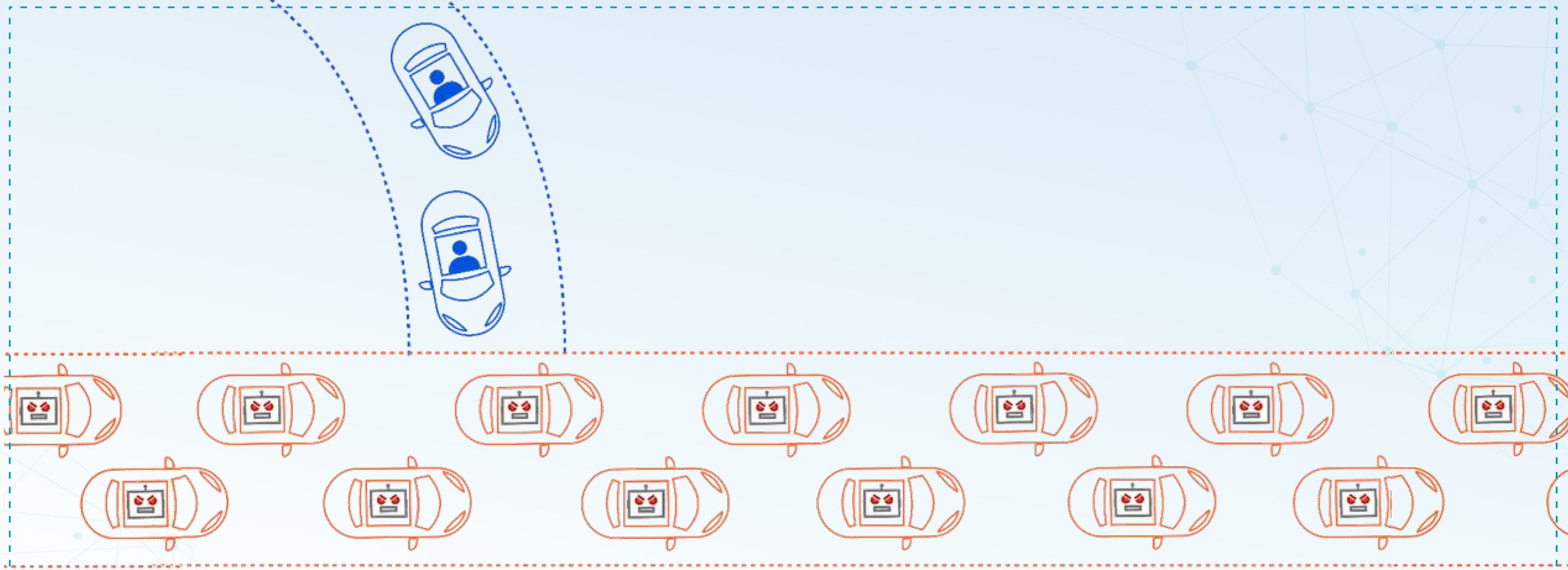


가용성을 해치는 공격

- *DoS, *DDoS, 재해, 재난

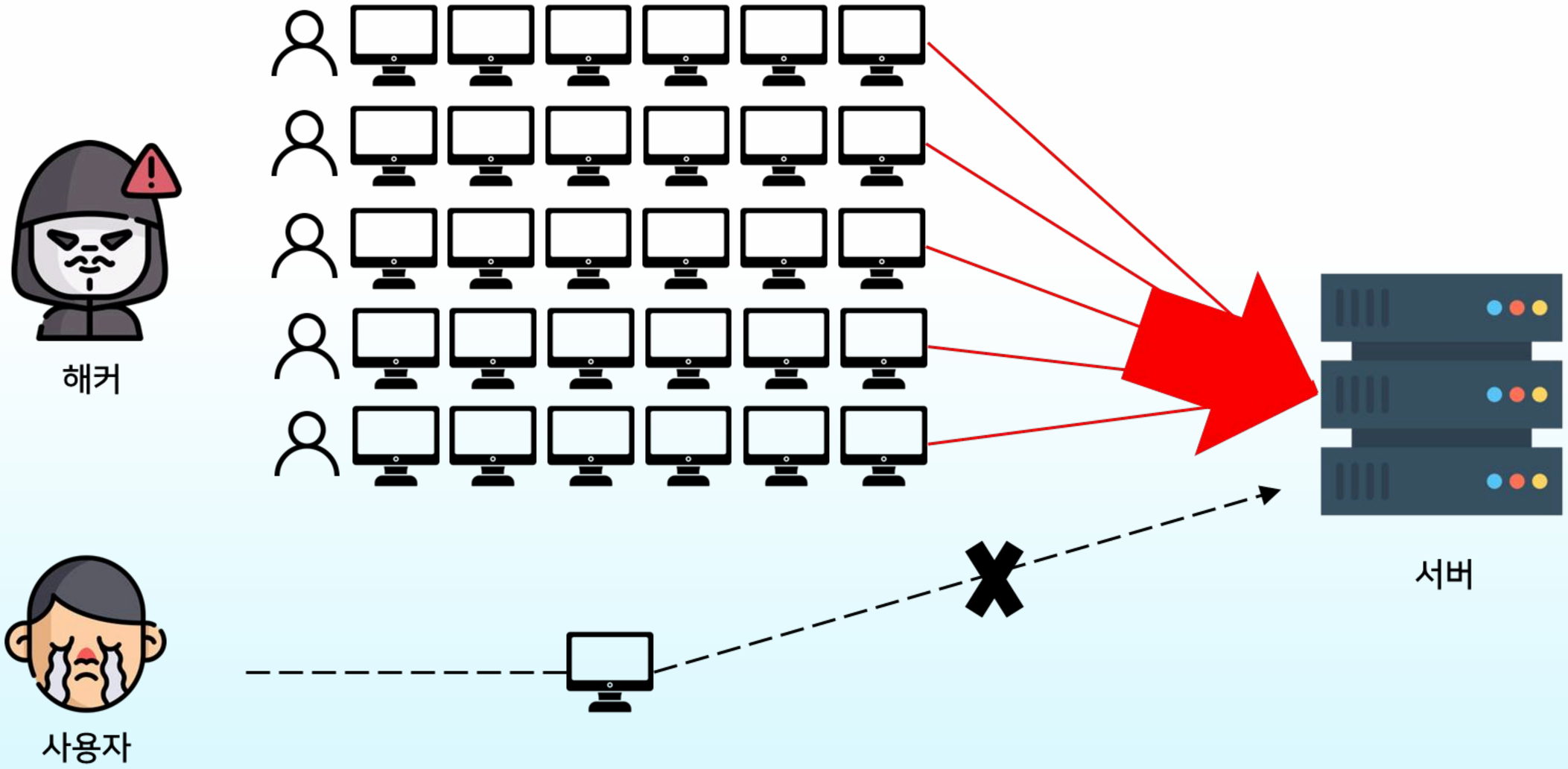
가용성을 보안하는 방법

- 백업, 결함허용시스템, 클러스터링



- 네트워크 상에는 허용할 수 있는 데이터의 양이 정해져 있음.
- 허용된 양 이상의 데이터가 서버에 들어오게 되면 통신 속도가 느려지거나, 아예 통신이 되지 않고 서버가 죽어버림
- 해커의 문제 뿐만 아니라, 재해·재난으로 인해 서버가 고장 났을 때에도 가용성이 파손됨.

DDoS 공격으로 인한 가용성 침해



블랙햇 해커와 화이트햇 해커

고전적인 서부 영화에서 악당들이 검은 모자를 쓰고,
영웅들이 흰색 모자를 쓰는 이미지에서 유래