디지털보안학

[2주차. 디지털보안에 대한 이해]

Digital Security

디지털 보안 개념 변화

정보 보안 < 디지털 보안

컴퓨터보안

사이버보안
융합 보안
디지털 위험 관리

정보보안(Information security) 개념

- 정보를 여러가지 위협으로부터 보호하는 것
- 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미

정보보안 핵심 원칙 : CIA

기밀성(Confidentiality)

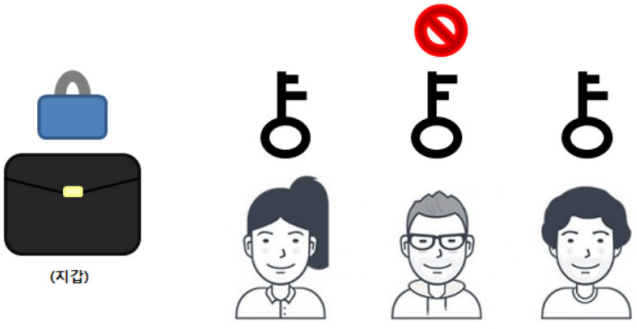
- 데이터의 보관이나 데이터의 송수신 과정에서 원래 메시지의 어떠한 정보도 노출되지 않도록 해야 함
  - 쉽게 말하면 인가되지 않은 사람에게는 절대 그 정보를 공개해서는 안되는 것
- 사용을 승인받은 사람만 해당 정보에 접근할 수 있는 성질

2015 매출 1위
9900원 피자 맛집!

2016 매출 1위
8900원 피자 맛집!

기밀성
Confidentiality

허가를 받은 사람만 이용할 수 있다.

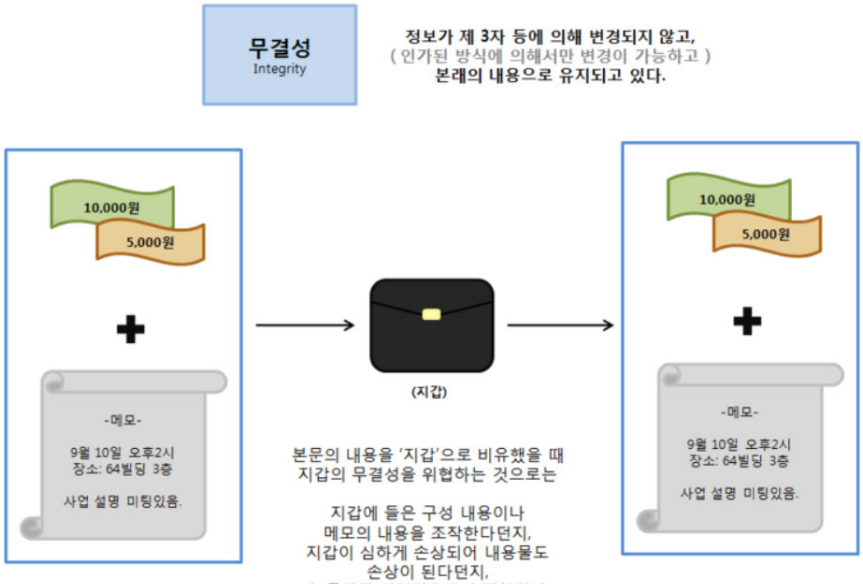


(지갑)

본문의 내용을 '지갑'으로 비유했을 때
지갑의 기밀성을 위협하는 것으로는
지갑에 들어가는 돈이나 메모지, 명함등을 훔쳐본다던지
그것들을 가로채기, 열쇠 도난, 허가된 열쇠를 이용하는 부정 접근 등이 있다.

무결성(Integrity)

- 정보를 정확하고 완벽한 상태로 보존해야 함
  - 쉽게 말하면 정보를 티끌 하나 건드리지 않고 원상태 그대로 보존하는 것
- 기밀성의 장치인 접근 권한이 적절한 것인지 완전성과 정확성을 보장하는 성질



가용성(Availability)

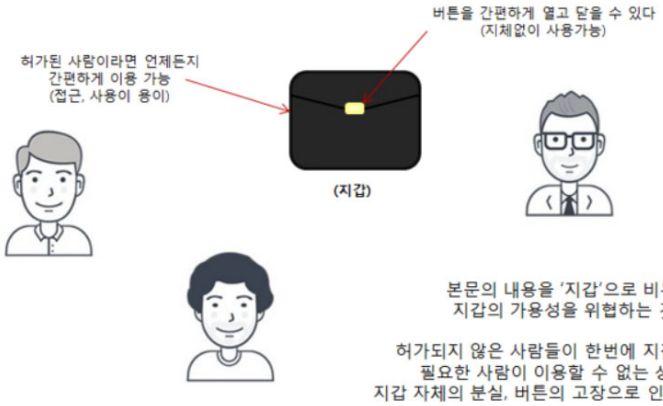
- 사용자가 필요로 할 때 항상 정보를 이용할 수 있도록 유지해야 함
  - 쉽게 말하면 사용자가 찾으면 언제 어디서든 짠하고 눈앞에 나타나줘야 하는 5분 대기조인 것
- 이중삼중으로 얽히고설킨 보안장치가 있음에도 언제든 적절한 때에 정보에 접근할 수 있는 성질

어제까지만 해도
신나게 갖고 놀던 mp3

정작 필요한 날에
사라져 버린 mp3

가용성
Availability

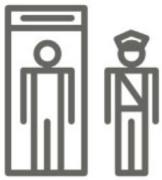
필요로 할 때에 적절하게 사용할 수 있는 상태다.



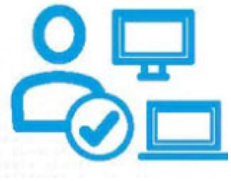
본문의 내용을 '지갑'으로 비유했을 때
지갑의 가용성을 위협하는 것으로는

허가되지 않은 사람들이 한번에 지갑에 몰려들어서
필요한 사람이 이용할 수 없는 상황이라던지,
지갑 자체의 분실, 버튼의 고장으로 인한 지체 등이 있다.

정보보안 부가 원칙 : AAN



Access Control

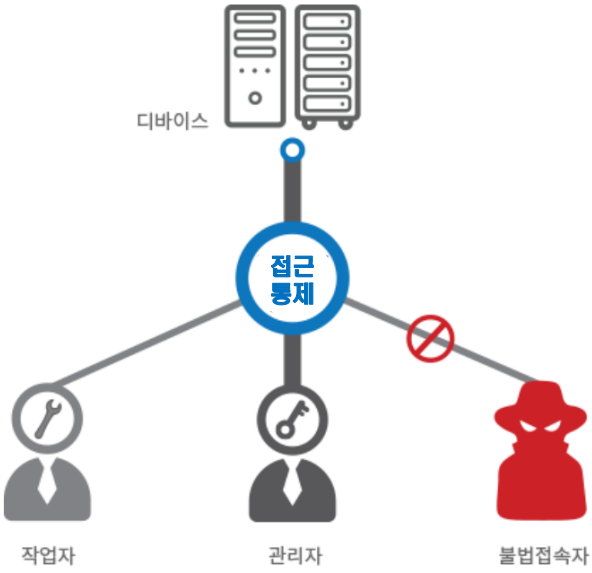


Authentication

Non-Repudiation

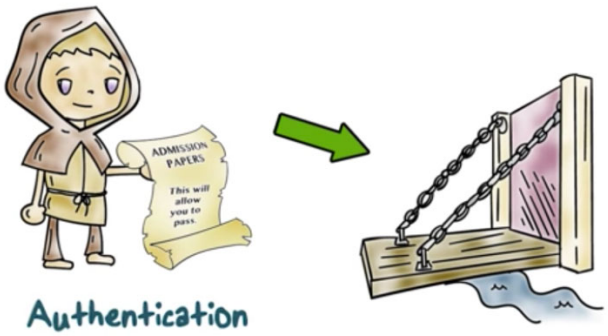
접근 제어(Access Control)

- 사용자 및 기기의 특성에 따라 서비스 접근 가능성을 차등 부여하여 접근 통제 하는 것



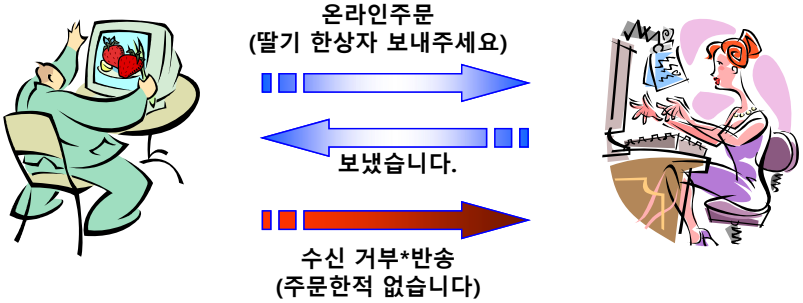
인증(Authentication)

- 정당한 사용자임을 확인하는 것
  - 내가 누구인지 그 증거를 보이고 확인시키는 것



부인 방지 (Non-Repudiation)

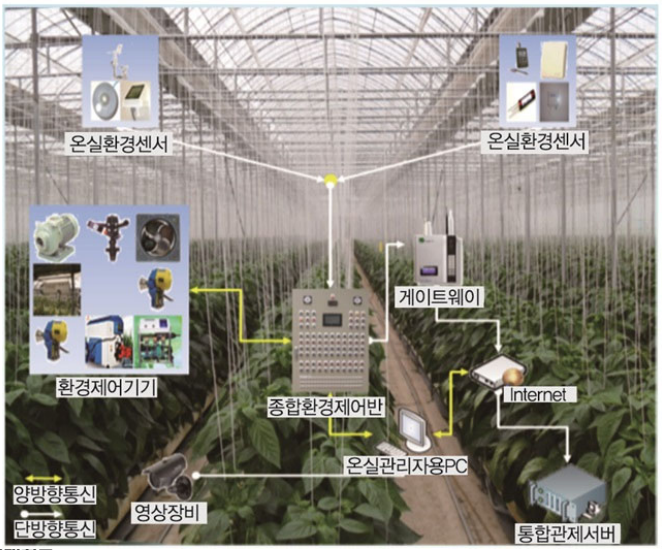
- 송수신 사실을 부인할 수 없도록 하는 것
  - 쌍방간의 행위에 기술적인 증거를 제공하는 것



최근의 보안 위협 양상

- 정보만을 노리는 것이 아니라, 해당 시스템이 작동되는 방식에 오류나 장애를 일으키는 방향으로 전개됨

스마트팜 위협 : DDoS(Distributed Denial of Service)

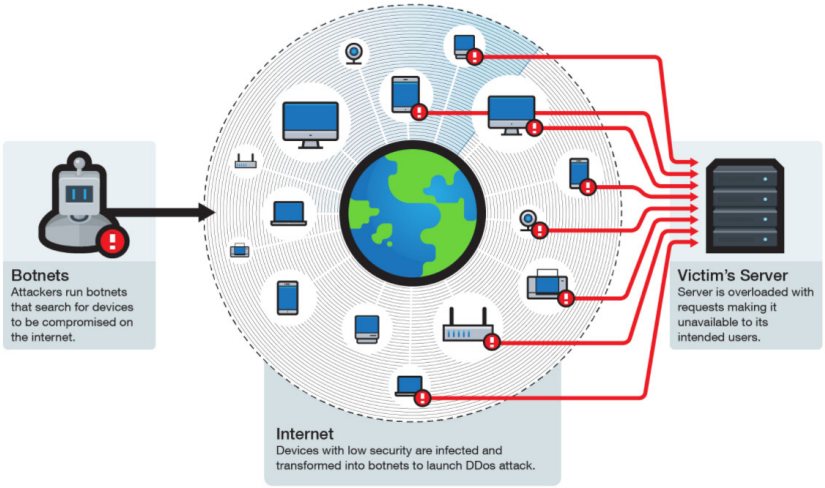


스턱스넷(Stuxnet)

- 발전소, 공항, 철도 등 기간시설을 파괴할 목적으로 제작된 컴퓨터 바이러스
- 스턱스넷에 감염이 되면 스카다 시스템이 무력화되어 산업시설등이 컨트롤이 되지 않는 등 큰 피해가 있을 수 있으며, 그렇기 때문에 '사이버 미사일'이라고 불리기도 함

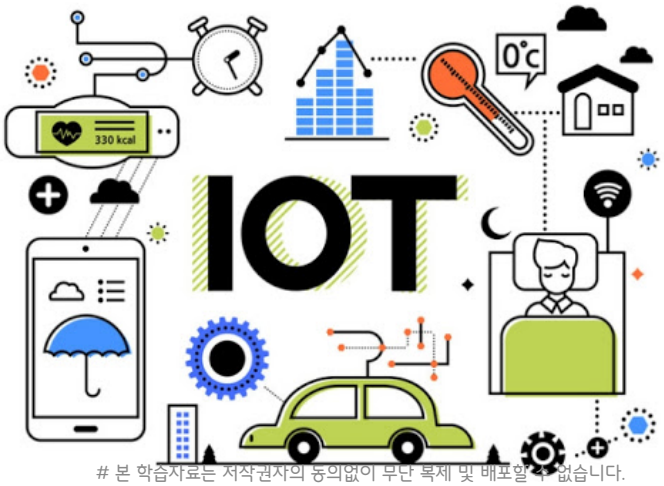
미라이봇넷(Mirai Botnet)

- 보안이 취약한 IOT 장치를 대상으로 구성한 좀비 네트워크 집단



디지털 보안 (Digital Security)

- 디지털 환경에서 안전하고 신뢰할 수 있는 활동 및 서비스가 이루어지도록 보호하고 관리하는 행위



디지털 보안 위협 핵심 트렌드

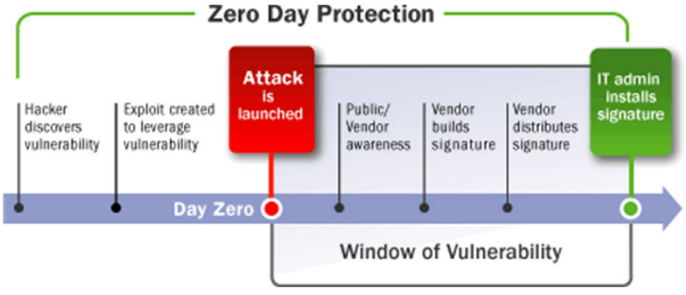
- APT(Advanced Persistent Threat)
  - 표적으로 정한 뒤 장기간에 걸쳐 다양한 수단을 총동원하는 지능적 공격 방식

- Zero-day Attack
  - 공격의 신속성을 의미하는 것으로, 보안 취약점이 발견된 뒤에 취약점 패치가 발표되기 전에 취약점을 이용한 공격

APT (Advanced Persistent Threat, 지능적 지속 위협)

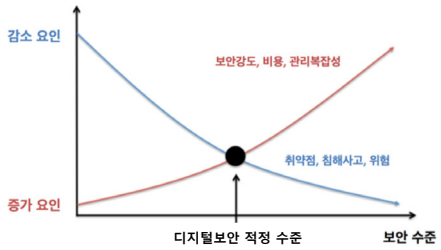
Zero-day Attack

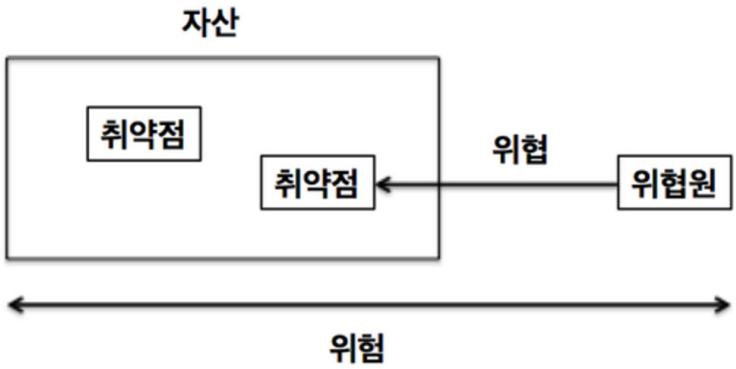
- 취약성 완화에 관심이 있는 사람들(대상 소프트웨어의 공급 업체 포함)에게 알려지지 않은 컴퓨터 소프트웨어 취약점
  - 예: Sony Pictures Entertainment(2014, Guardian of Peace), Microsoft(2016, BuggiCorp)



디지털 보안 관리 < 디지털 위험 관리

- 위험 = 자산의 가치 X 취약점 X 위협





- 자산(Asset) - 데이터 혹은 자산의 소유자가 가치를 부여한 개체 (개인정보, 영업비밀, 기자재)
- 위협원(Threat agents) - 정보자산에 해를 끼치는 행동을 할 수 있는 주체 (해커, 임직원, 단체, 자연재해)
- 위협(Threat) - 자산에 대한 위협원의 공격 행동 (해킹, 위/변조, 삭제, 파손, 유출)
  - 정보시스템이나 통신망에 피해를 입힐 수 있는 잠재적 가능성을 갖고 있는 이벤트나 활동
  - 자연적 또는 물리적: 화재, 홍수, 지진, 정전
  - 부주의: 사전 지식이 없는 사용자에 의한 사고
  - 고의: 공격자, 테러리스트, 산업스파이, 악성코드

- 취약점(Vulnerability) - 위협이 발생하기 위한 사전 조건/상황 (평문전송, 입력값 미검증, 비밀번호 공유)
  - 안전 장치의 부재 또는 미비
  - 물리적, 자연적: 잠그지 않은 문, 고장 난 시스템
  - 하드웨어/소프트웨어: 업데이트 되지 않은 바이러스 백신소프트웨어
  - 통신: 암호화 되지 않는 프로토콜
- 위험(Risk) - 위협원이 취약점을 이용하여 위협이라는 행동을 통해 자산에 악영향을 미치는 결과를 가져올 가능성