dongguk UNIVERSITY

정보보호 개론 “1주차 강의”

윤홍수

2025. 03. 06

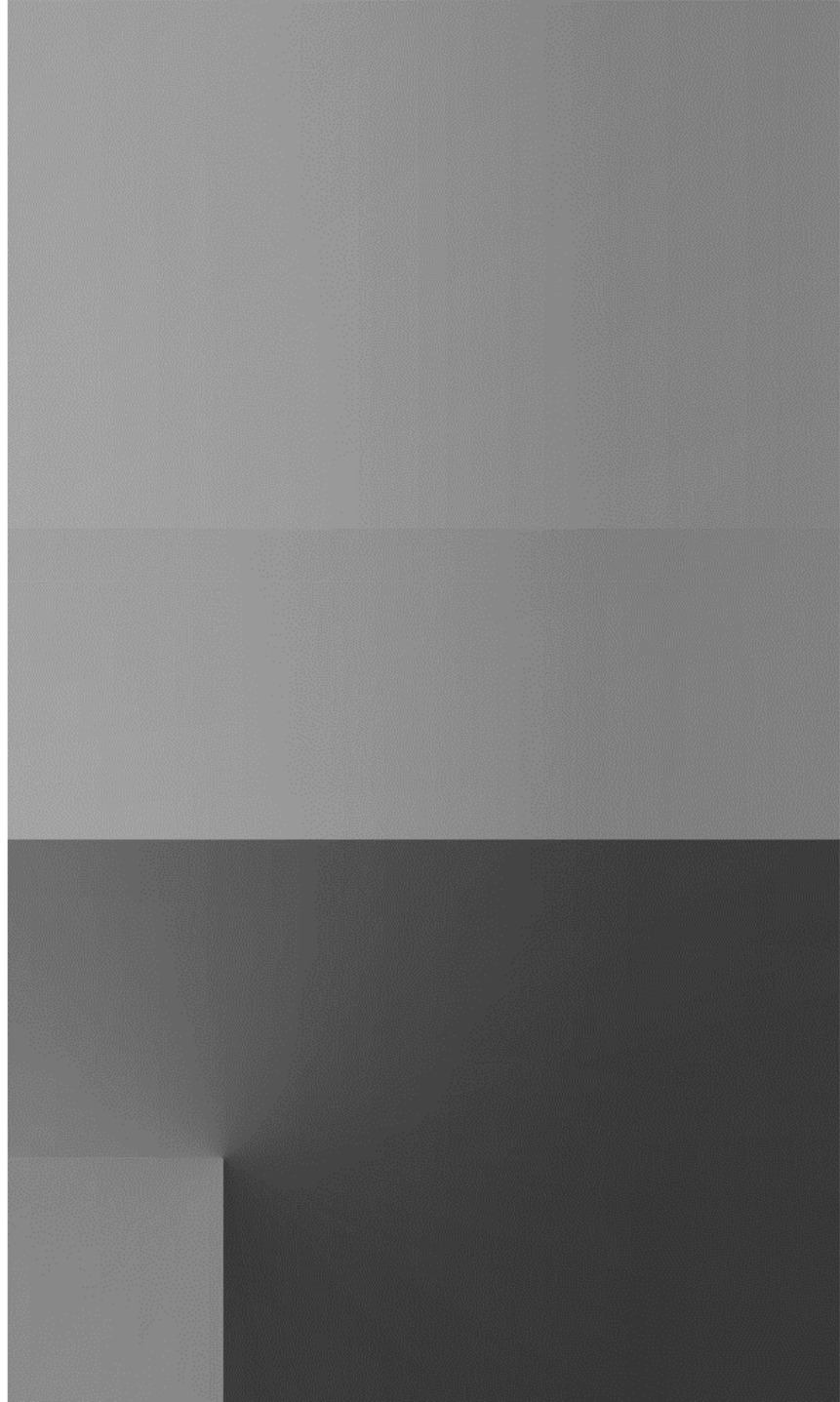
Table of Contents

I. **2025년 1학기 1주차 강의 계획**

- 소개
- 강의 평가 항목
- 강의 교재, 유의 사항
- 주별 강의 계획
- 1주차 강의 진행

  - 정보 보안의 역사

  - 정보 보안의 이해



강의 평가 항목

출석 10%, 과제 20%, 중간 30%, 기말 40%

출석평가(10%) : 학칙에 의함

평가(90%) : 중간평가, 기말평가 및 과제물평가를 합산하여 평가

- 중간/기말 평가 (70%) : 강의 학습 내용 및 교재 내용을 바탕으로 평가 진행

- 과제평가 (20%) : 수업 참여도에 따른 과제 수행 (중간고사 이후)

강의 평가 항목

출석평가(10%) : 학칙에 의함

hsyoon5809@dongguk.edu

결석 관련
- 사전 문자 필요

지각, 결석, 기타 관련된 서류 => 메일주소로 전달 (인정)

문자, 카톡 (인정 X)

하드카피 (인정 X)

강의 교재, 유의 사항

- 주 교재 : 정보 보안 개론(4판)
- 수강생 유의 사항:
  - ✓ 강의를 듣기 위해 수강생들은 교재 또는 자료를 준비하여 수업시간에 참여
  - ✓ 출석 체크는 정해진 시간표에 등록되어진 정시에 진행
  - ✓ 꼭 수업 시간 전 각 자리에 착석
  - ✓ 제공되는 강의자료(PDF) 및 보충자료는 e-Class 게시판에 업로드해서 제공, 수업전에 수강생이 다운로드 준비
  - ✓ 주차 별 학습 계획 및 진도는 강의 진행 상황에 따라 변동될 수 있음

주차별 강의 계획(1/3) – 강의 계획서는 변경 될 수 있음

주차	일정	Contents
1	3/06 목	오리엔테이션 - 교수자 소개, 평가 및 배점, 주의사항 안내 등 정보 보안의 세계 - 정보 보안의 역사, 이해
2	3/13 목	시스템 보안 - 시스템 보안의 이해 - 계정 관리, 세션 관리, 접근 제어, 권한 관리, 등
3	3/20 목	네트워크 보안 - 네트워크, 인터넷 - 암호 기술, 해시 알고리즘
4	3/27 목	웹 보안 - 웹과 HTTP의 이해 - 웹 서비스의 이해, 웹 해킹, 등
5	4/03 목	코드 보안 - 시스템 구성과 프로그램 동작 - 버퍼 오버플로 공격, 포맷 스트링 공격, 메모리 해킹

주차별 강의 계획(2/3)

주차	일정	Contents
6	4/10 목	악성 코드 - 악성 코드의 역사, 분류 - 바이러스, 웜, 트로이 목마, 악성 코드 탐지 및 대응책
7	4/17 목	암호의 이해 - 암호의 개념과 원리, 대칭 암호화 방식 - 비대칭 암호화 방식
8	4/24 목	중간고사
9	5/08 목	전자상거래 보안 - 전자 상거래의 이해 - 전자 서명과 전자 봉투, 전자 결제와 가상 화폐
10	5/15 목	보안 시스템 - 인증 시스템 - 방호벽, 침입 탐지 시스템, 침입 방지 시스템, 통제 및 감시 장비

주차별 강의 계획(3/3)

주차	일정	Contents
11	5/22 목	IOT 보안과 AI 보안 - IOT 보안, AI에 대한 이해 - AI 취약점 유형과 대안, AI를 이용한 보안
12	5/29 목	사회공학 - 사회 공학의 이해 - 사회공학 기법, 등
13	6/05 목	침해 대응과 디지털 포렌식 - 침해 대응, 포렌식 개념과 절차 - 디지털 포렌식의 증거 수집
14	6/12 목	5/01 휴무 건 ➔ 보강 ?? (확인 중) 보안 관리 - 보안 거버넌스, 보안 프레임워크, 보안 조직 - 보안 정책과 절차, 내부 통제, 보안 인증, 개인 정보 보호
15	6/19 목	기말고사

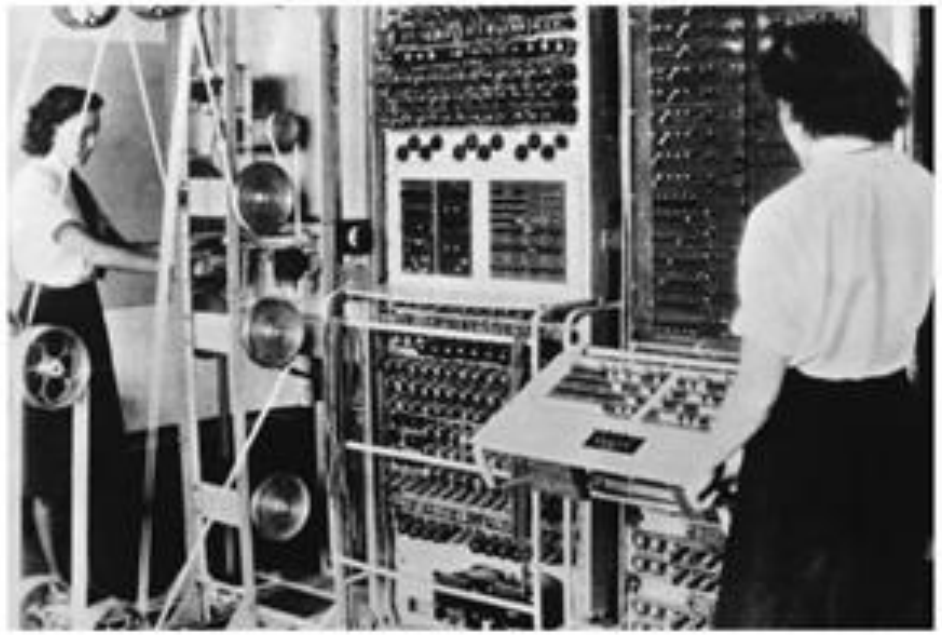
정보보안의 역사

➢ 1950년대 이전

[에니그마(Enigma)와 콜로서스(Colossus)]

- **제2차 세계대전 동안 암호와 암호 해독 기술이 어떻게 발전했는지를 보여주며, 오늘날의 정보보안 기술이 발전하는 데 큰 영향을 미침**

Enigma



Colossus

정보보안의 역사

1950년대 이전

[에니그마(Enigma) / 독일], 암호학의 시작

- 독일군이 사용한 암호화 기계로, 메시지를 강력하게 암호화하여 적이 해독하지 못하도록 만듬
- 일반적인 암호처럼 단순한 글자 치환 방식이 아니라, 매번 다른 암호 패턴을 만들어 해독이 거의 불가능
- 특징
  - 로터(rotor) 시스템을 사용하여 문자를 계속 바꿨기 때문에 같은 글자를 입력해도 매번 다른 암호문이 생성
  - 매일 또는 특정 주기에 맞춰 암호 설정(로터 위치, 플러그 연결 등)을 변경하여 보안성을 높임
- 문제점
  - 독일군은 에니그마가 절대 해독될 수 없다고 믿었지만, 암호 설정이 반복되는 패턴이 발견됨
  - 독일군의 실수(일부 암호 메시지를 반복해서 보내는 행위)가 해독의 실마리가 됨

정보보안의 역사

- 1950년대 이전

[콜로서스(Colossus) / 영국], 암호 해독의 시작

- 에니그마를 해독하기 위해 만들어진 컴퓨터
- 세계 최초의 전자식 프로그래머블 컴퓨터로, 영국의 암호 해독 기관인 블레츨리 파크(Bletchley Park)에서 개발
- 앨런 튜링(Alan Turing)과 맥스 뉴먼(Max Newman) 등의 수학자들이 개발에 기여
- 역할
  - 기존 수작업 암호 해독보다 수백 배 빠르게 암호를 분석할 수 있었음
  - 이를 통해 독일군의 전략을 사전에 파악하여 전쟁 승리에 큰 기여를 함

정보보안의 역사

- 1950년대 이전

[에니그마(Enigma)와 콜로서스(Colossus)]

- Enigma
- Colossus

Quiz

정보보안의 역사


독일 암호 해독가능해?

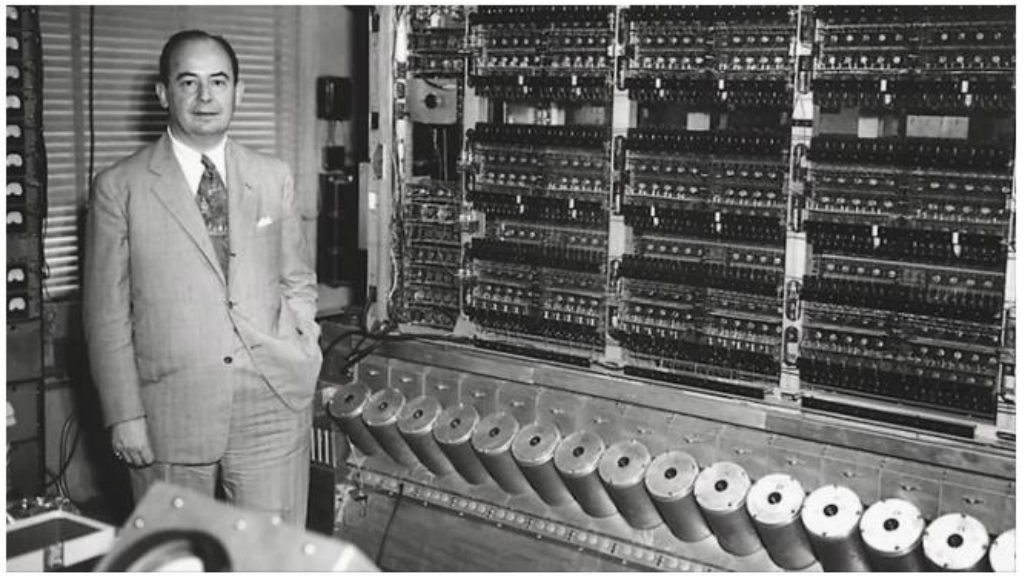

연합군 애들...
어디서 정보를 얻었지?
헐...
어떻게 해독했지?!
독일


앨런 튜링(1912~1954)
잉글랜드의 수학자, 암호학자, 논리학자이자
컴퓨터 과학의 선구적 인물이다.
똑똑한 사람
사회지식연구소
연구


튜링이라면...
해독할 수 있을거야
암...
너무 복잡해!
우리 연합군은..
튜링을 믿어!
영국

정보보안의 역사


최초의 연산능력이 가능한
컴퓨터의 개발!
헷갈리는 궁금했던 이야기
사회지식연구소
제작자




최초의 컴퓨터!(라고...)
홍보하고, 판매하자~
미국

정보보안의 역사

[콜로서스(Colossus), 에니악(ENIAC)]

- Colossus
- ENIAC

정보보안의 역사

- 1960~1970년대
  - 최초의 컴퓨터 연동망 아파넷(ARPAnet)은 미국 국방부의 고등 연구 계획국(Advanced Research Project Agency)
    - 1967년 미국 국방부는 관련 기관 사이의 정보 공유를 지원하는 ARPA 프로젝트를 통해 컴퓨터 연결망을 개발
    - IMPS(Interface Message Processors) 네트워크라고 불린 이 연동망은 오늘날 인터넷의 뿌리

  - 유닉스 운영체제의 개발
    - 1969년 켄 톰프슨과 데니스는 운영체제인 유닉스(UNIX)를 개발
    - 개발자 툴 및 컴파일러에 접근하기가 쉽고 여러 사용자가 동시에 사용할 수 있다는 특성 (해커 친화적)

정보보안의 역사

- 1960~1970년대
  - 마이크로소프트 설립
    - 1974년 MITS라는 회사가 세계 최초로 조립식 개인용 컴퓨터 앨테어 8800를 만들어 판매
    - 앨테어 8800은 조립식이며 소프트웨어도 따로 없었고 토글 스위치의 불빛을 보고 결과를 해독하는 형식
    - 같은 해 4월 하버드 대학 자퇴 후 마이크로소프트를 설립
  - 애플 컴퓨터의 탄생
    - 1979년 애플 컴퓨터가 스티브 워즈니악과 스티브 잡스의 손에 탄생
    - 오늘날의 PC와 비슷한 모습의 애플 컴퓨터는 그 당시에 666달러 66센트라는 가격에 판매

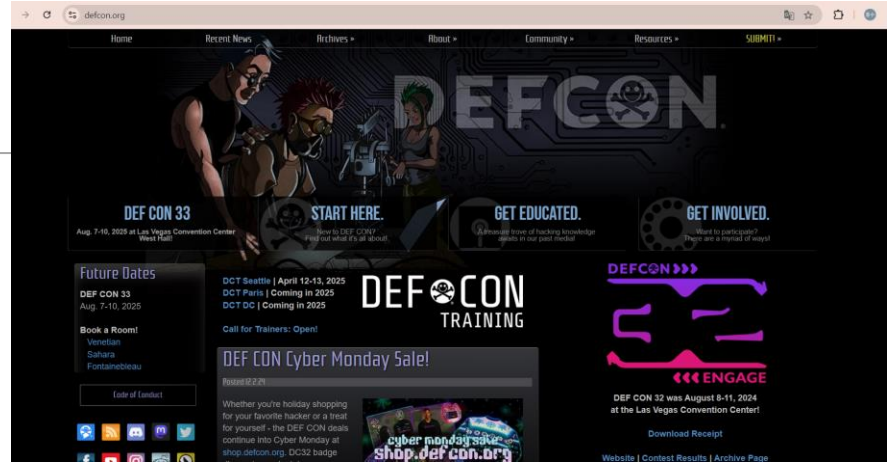
정보보안의 역사

- 1980~1990년대
  - 네트워크 해킹의 시작
    - 1980년대 초 네트워크 해커라는 개념이 처음 탄생
    - '414 Gang'은 대표적인 네트워크 해킹 사건
      - 414 Gang은 1980년대 초반 미국에서 활동한 청소년 해커 그룹
      - 학교 컴퓨터를 사용해 여러 기업과 연구소 시스템을 해킹하며 큰 논란을 일으킴
      - NASA, 국립연구소, 주요 기업 등 60여 곳의 컴퓨터 시스템을 해킹
      - 대부분 단순한 호기심으로 시스템에 침입했으나, 보안이 허술했던 점이 문제로 떠오름
      - **결국 FBI에 적발되었고, 이 사건은 해킹과 사이버 보안의 중요성을 알리는 계기가 됨**
      - **전 세계적으로 사이버 보안이 중요해지기 시작**

정보보안의 역사

- 1980~1990년대
  - 해커의 등장
    - **1980년대에 해킹이 발전하면서 역사적으로 유명한 해커들이 본격적으로 등장**
    - 1986년 구소련 **KGB로부터 자금을 지원받는 서독 해커들이 300여 기관에 불법적인 접근을** 시도하고 군사 기밀 정보를 탈취
    - 1988년 11월 22일 **코넬대학 대학원생이었던 로버트 모리스는 웜 바이러스를 구동하여 미국 전역에 피해를 끼침**
    - 전자프런티어재단은 국제 사회에서 표현의 자유, 저작물의 자유로운 이용, 개인 정보 보호, 정보 투명성을 위한 활동 수행

정보보안의 역사



- 1980~1990년대
  - 데프콘 해킹 대회
    - **최초의 해킹 대회인 '데프콘'이 1990년 라스베이거스에서 개최**
    - 데프콘 해킹 대회는 지금도 매년 열리는데, 팀 단위로 예선을 거쳐 여덟 팀이 라스베이거스에서 본선 진행
    - **자신의 팀을 보호하면서 상대 팀을 공격하여 상대 시스템을 많이 해킹한 팀이 승리**
  - 해킹 도구의 개발
    - 1994년 인터넷 브라우저인 넷스케이프가 개발되어 웹 정보에 대한 접근이 가능해짐
    - 일부 사용자들은 해킹 툴을 사용하여 개인 정보를 캐기도 하고 은행 컴퓨터의 계좌 정보를 변조
    - 언론은 이들을 해커라 부르기 시작
    - **이때부터 해커라는 용어가 순수한 목적으로 시스템 내부를 연구하는 컴퓨터광을 지칭하지 않게 됨**

정보보안의 역사

- 2000년대 이후
  - 분산 서비스 거부 공격 (DDoS)
    - 특정 서버나 네트워크에 과부하를 주어 정상적인 서비스 운영을 방해하는 공격
  - 웜과 바이러스
    - (W) 스스로 복제하여 네트워크를 통해 확산되며, 시스템 자원을 과부하시키거나 취약점을 악용하는 악성코드
    - (B)다른 프로그램이나 파일에 자신을 숨겨 감염시키며, 실행될 때마다 시스템을 손상시키거나 추가 감염을 유발하는 악성코드
  - 개인 정보 유출과 도용

정보보안의 역사

- 2000년대 이후
  - 전자 상거래 교란
    - 2006년 7월에는 안심클릭의 허점을 이용한 해킹 사기 사건이 발생
    - 범인들은 해킹으로 타인의 신용카드 번호를 입수한 후, 인터넷에서 이루어지는 신용카드 결제 방식의 제도적· 기술적 취약점을 이용하여 물품을 대신 결제하고 현금을 돌려받아 수억 원을 인출
    - 대부분의 신용카드 사용자들이 일반 사이트,쇼핑몰, 카드사 사이트의 접속 아이디와 비밀 번호를 동일한 점에 착안한 범죄
    - 2006년 3월에는 국내 대형 포털 사이트의 정보 검색 순위를 조작한 인터넷 광고 대행 업체의 대표가 입건
    - 국내 4개 대형 포털 사이트의 검색 순위에 업체의 홈페이지 주소를 상위에 노출시켜 주는 조건으로 광고주를 모집
    - 자체 개발한 프로그램을 이용하여 750개 회사의 홈페이지 주소를 자동으로 클릭하게 만들어 정보 검색 순위를 조작

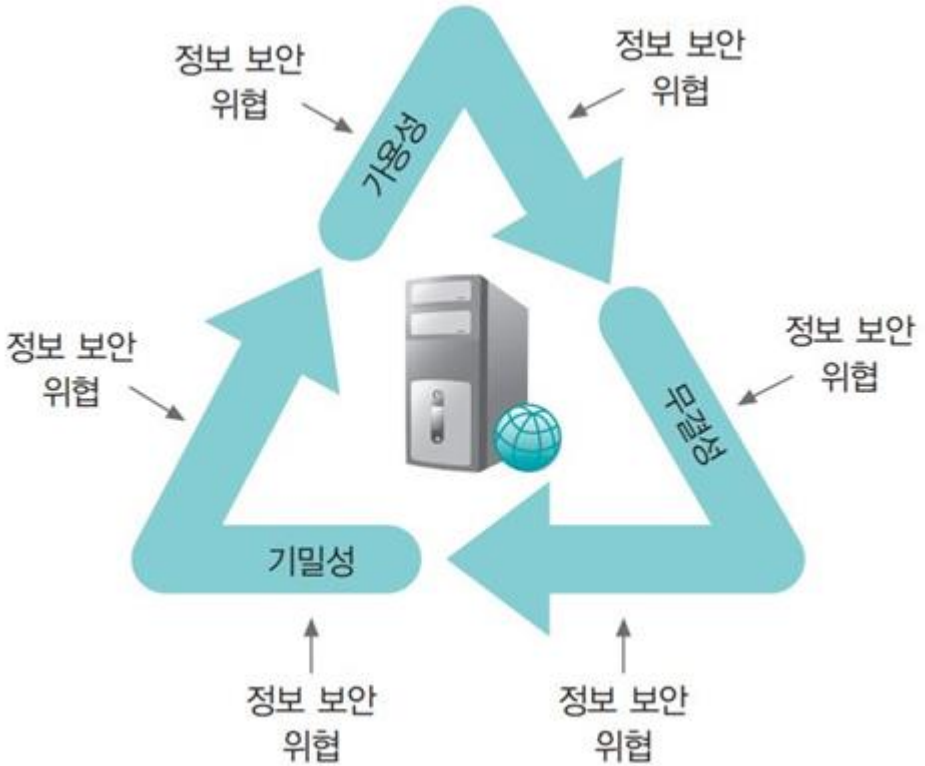
정보보안의 역사

- 2000년대 이후
  - 농협 사이버 테러
    - 2011년 4월 대규모 데이터 삭제로 농협의 전산 시스템이 멈추는 사건이 발생
    - 정부는 이를 북한의 사이버 테러라고 발표
    - 이 사건은 국내 기업의 보안 인식 자체를 바꿔 놓는 계기가 됨
  - 가상 화폐 해킹
    - 현재 가상 화폐는 큰 돈이 되고 있기 때문에 관련 해킹 사건도 증가

발생 시기	거래소 명	피해 원인	피해 규모
2019년 11월	업비트	핫월렛 해킹	580억 원
2018년 6월	빗썸	이메일 악성 코드 추정	350억 원
2018년 6월	코인레일	이메일 악성 코드 추정	400억 원
2017년 12월	유빗(구 야피존)	핫월렛해킹	172억 원

정보보안의 이해

- 보안의 3대 요소
  - 보안은 기밀성, 무결성, 가용성이라는 세 가지 속성으로 집약



정보보안의 이해

- 보안의 3대 요소
  - 기밀성 (Confidentiality)
    - 허가된 사람만 **정보에 접근할 수 있도록 보호하는 것**
    - 비밀번호가 걸린 문서나 자물쇠로 잠긴 금고처럼, 중요한 정보를 외부로부터 안전하게 지키는 것
    - 패스워드 보호 : 컴퓨터 로그인 시 비밀번호를 입력해야 함
    - 암호화 : 메시지를 암호화하여 다른 사람이 내용을 알아볼 수 없게 함
    - 방화벽(Firewall) : 외부 공격자가 내부 네트워크에 접근하지 못하도록 보호

정보보안의 이해

- 보안의 3대 요소
  - 무결성 (Integrity)
    - 정보가 **허가된 사람에 의해, 올바른 방법으로만 변경될 수 있도록 보호하는 것**
    - 허락 받지 않은 사람이 정보를 몰래 수정하거나 변조하지 못하도록 하는 것
      - 적절한 권한을 가진 사용자만 정보 변경 가능
      - 허가되지 않은 변경(해킹, 데이터 조작 등)은 무결성을 해치는 행위
      - 은행 시스템 : 계좌 잔액이 마음대로 조작되면 안 됨
      - 의료 기록 : 환자의 진료 기록이 변조되면 생명이 위험할 수도 있음
      - 소프트웨어 업데이트 : 악성코드가 포함되지 않도록 원본이 유지되어야 함

정보보안의 이해

- 보안의 3대 요소
  - 가용성 (Availability)
    - **필요할 때 언제든지 정보나 시스템에 접근할 수 있도록 보장하는 것**
    - 정보가 아무리 안전하게 보호되어 있어도, 정작 필요할 때 사용할 수 없다면 의미가 없다
    - 정보나 시스템이 항상 사용 가능해야 함
    - 서비스 중단(다운타임)이 최소화되어야 함
    - 예상치 못한 장애(해킹, 서버 고장 등)에도 대비해야 함
      - 온라인 뱅킹: 24시간 접속할 수 있어야 함
      - 응급 서비스 시스템: 병원 시스템이 다운되면 생명에 위협이 될 수 있음
      - 클라우드 서버: 기업 데이터가 언제든 접근 가능해야 함

Thank you for Listening

새로운 세상과 변화에 도전하는 동국대인이 되기를 바랍니다.