정보보호론 0311

보호 : 기술 관련, 보안 : 정책 관련

1950년 이전

에니그마(Enigma, 수수께끼)

2차 세계대전 때 독일군이 군사 통신 보안용으로 사용한 암호기계

회전판, 전선 세팅에 따라 입출력이 달라지며, 회전자 세팅을 8시간마다 변경

봄브(Bombe)

에니그마를 해독한 계산기

폴란드 암호 해독국의 수학자 개발, 힌트(글의 형식)로 이용하여 회전자의 조합을 찾아냄

콜로서스(Colossus)

최초 컴퓨터(=애니악)

에니그마 암호기계를 보완한 장치

‘hack’탄생

1948년 MIT 기차제작 동아리에서 처음 사용

정해진 것을 조작한다는 의미

MIT hack이라는 학생들의 능력과 메시지를 장난 형식으로 보여주는 이벤트가 있다.

1960 - 1970년대

최초의 컴퓨터 연결망 ARPA

오늘날 인터넷의 원조

유닉스 운영체제의 개발

오픈 소스 시작

해커 친화적 운영체제

최초의 이메일 전송

@ = at(~에게)

마이크로 소프트 설립

소프트웨어(Altair basic) 개발

저장 장치 발전(Tape > 플로피 디스크 > CD > SSD/HDD)

애플 컴퓨터 탄생

스티븐 잡스 차고에서 시작

첫 해 애플-1PC는 당시 $666.66 가격 판매

1980-1990년대

정보 권리 논쟁 시작

CCC의 설립 목표(자유주의 시절) = 정보 교류에서 국경이 사라져야 한다.

해커 탄생

인터넷 브라우저인 넷스케이프 접근 가능

White Hacker – 기업 보안 높이기 위함

Black Hacker – 개인의 이익을 위함

Gray Hacker - ??

데프콘 해킹 대회 개최

해킹 대회 데프콘(Def con) 매년 라스베이거스에서 개최 중

2000-2010년대

분산 서비스 거부 공격 등장

DDos(Distributed Denial of Service DDos) 분산 서비스 거부 공격

APT(Advanced Persistent Threat) 지능형 지속 위협

고급기술을 자유롭게 이용, 인간의 행동으로 발생시키는 위협

개인정보 유출 및 전자 상거래 교란

주민등록번호 수십만 개 유출 사건

2010-현재

스마트폰 해킹

오픈 소스의 장점 : White 해커로 인해 보안 기능 강화

오픈 소스의 단점 : Black 해커로 인해 공격 받기 쉬움

편의성과 보안성은 반비례한다.

자동차 해킹

스마트폰과 연결되어 엔진 정지, 스티어링 조작, 브레이크 제어가 가능함

블록체인 등장

2008년 사토시 나카모토가 블록체인 기술을 활용한 비트코인을 제안

블록체인

블록(거래내역)을 바꾸지 못하게 암호화하는 기술(DB 저장소)

바꿀 수 없지만, 투명하게 공개 가능한 기술

비트코인은 탈중앙화(기관 X)된 분산 원장(거래 내역 분산)기술이며, 과거에 블록 체인 검증 인센티브 비용으로 받았다고 한다.

이더리움은 블록체인에 프로그래밍하는 기술 => 스마트 컨트렉트

가상 화폐 거래소 해킹

비트코인 기술적 해킹 당하지 않았다. 주로 거래소가 해킹 당한다.

생성형 AI 등장

ChatGPT 출시 이후, AI 활용이 중요해졌다.

생성형 AI의 오남용 방지를 위한 보안 기술 연구에 집중된다. (보안 수요는 높다)

NIST(미국 국립표준기술연구소) CIA 3대 요소

기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)

기밀성

정보는 허가 받은 사용자에게만 공개(숨긴다)

대표 기술 : 암호

무결성

허가 받은 사용자만 정보를 수정할 수 있음(수정 방지), 계약서, 투표, 거래, 채팅

대표 기술 : 암호학적 해시함수, 메시지 인증 코드, 전자 서명

가용성

필요한 시점에 정보에 접근 가능할 수 있음(사용가능해야한다), 편의점

대표 기술 : 데이터 백업, 서버 증설 등(구조적 설계)

그 외 성질

인증(암호화)

개체인증 : 본인인지?

메시지인증 : 출처 확인

(송신) 부인방지(전자서명)

여기서 부인이란 내가 하지 않았다고 하는 것을 의미함

책임성

원인 파악, 추적할 수 있음