2주차

**1**

**소프트웨어의 정의**

컴퓨터 프로그램 및 그와 관련된 문서

**소프트웨어의 종류**

1. 응용 소프트웨어

특정한 응용분야에 사용하기 위해 개발된 소프트웨어

1. 시스템 소프트웨어

응용 소프트웨어를 지원하는 소프트웨어

[컴퓨터 시스템의 계층적 구조]

하드웨어 <-> 시스템 소프트웨어 <-> 응용 소프트웨어 <-> 사용자

**소프트웨어의 역할**

보안을 제공하는 동시에, 보안 문제가 발생하는 주요 원인

**역대 소프트웨어 버그**

1. 소련 조기 경보 시스템 오류

미국이 미사일을 발사했다는 잘못된 경보 울렸음.

원인 : 위성이 구름위에서 반사되는 햇빛을 오인

1. 미국 전화 통신회사 AT&T 전화망 마비

교환기 한대가 기계적인 문제를 겪었는데

소프트웨어에 대한 업그레이드가 발생하면서 오류 발생

1. 아리안 5 폭발버그

발사 후 몇초만에 폭파되는 사고

오버플로가 발생해서 일어난 사고

**2**

**소프트웨어 보안**

소프트웨어가 기능을 제공할 때 위험을 파악하고 이것들을 관리하는 것

보안은 항상 보조 관심사로 묻혀진다

따라서 **보안과 기능 사이에서 충돌**이 일어난다.

또한 **보안과 관련한 성과를 확인하기 어렵다.**

**소프트웨어 보안 방법**

보안 위협

1. 정보 누출
2. 정보의 변조
3. 디도스 공격
4. 스푸핑(위장)
5. 불법적 접근

보안 기술 및 대책

1. 암호 기법
2. 접근 제어
3. 보안 기반 언어

보안대책이 새로운 보안취약점을 만드는 원인이 종종 되기도 한다.(ex 무차별 대입공격)

소프트웨어 보안 모델

대책 <-> 취약점간의 선순환을 거치면서 보안성을 증진시킨다

**3**

**악성코드란?**

악의적 목적을 가진 프로그램 (Malware)

**악성코드의 증상**

1. 시스템 정보 변경
2. 시스템 재부팅
3. 전자우편 자동 발송
4. 네트워크 속도 저하
5. 파일 삭제 및 손상
6. 화면 출력
7. 특정음 발생

**악성코드의 발전 역사**

1999년도 : E-mail 사용

2000년대 : 소프트웨어 취약점을 활용하는 악성코드들 발생

최근 : 이메일 및 여러 가지 취약점 등 공격 가능한 루트로 발생

**악성코드 개발 목적**

일반적으로는 특정 목적을 가진 **지능적인 사이버 범죄자에 의해** 악성코드 개발

주요 목표에는

비밀번호 훔치기, 인증번호 수집, 스팸메일 발송, 디도스 공격등이 있다.

최근에는 랜섬웨어라는 악성코드가 유행

랜섬웨어 : 암호화된 파일들을 복호화해주는 대가로 돈을 요구

악성코드 개발자 : **개인, 조직, 정부**

**악성코드 생명 주기**

악성코드 **생성** -> **감염**시킴 -> **활동** -> 악성코드 **인지** -> 대책들 **반영** -> **박멸**

**보호 및 대응방안**

1. 신뢰받는 기업에서 만들어진 안티 바이러스 설치, 항상 최근 엔진으로 업데이트
2. 윈도우 보안 패치들을 최신으로 유지
3. 출처가 불분명한 파일 다운로드 x
4. 공유폴더 사용 제한 or 사용시 읽기 전용으로만
5. 패스워드 다양한 기호, 대소문자, 숫자로 조합한 패스워드 사용