정보 보안 개론

Guardian@SNU

2019 Fall

목차

1 정보 보안

1.1 해킹의 정의

- **국어사전**: 다른 사람의 컴퓨터 시스템에 침입하여 장난이나 범죄를 저지르는 일
- **영한사전**: 컴퓨터 조작을 즐기기, 무엇이나 숙고하지 않고 실행하기
- **영영사전**: Hacking is about finding inventive solutions using the properties and laws of a system in ways not intended by its designer

1.2 정보 보안의 역사

- **1950년대 이전**: 암호화 기계 에니그마, 최초의 컴퓨터 콜로서스 (앨런 튜링)
- **1960년대**: 최초의 미니컴퓨터 PDP-1, 최초의 컴퓨터 연동망(네트워크) ARPA, Unix 운영체제 개발, 전화망 해킹으로 무료 장거리 전화 시도
- **1970년대**: 최초의 이메일 전송, Microsoft 설립, 최초의 데스크톱 솔, 애플 컴퓨터 탄생, C 언어 개발
- **1980년대**: 베이직과 도스 개발, 네트워크 해킹 시작, 카오스 컴퓨터 클럽, GNU와 리처드 스톨먼, 케빈 미트닉, 모리스 웜, 해커 선언문
- **1990년대**: 데프콘 해킹 대회, 리눅스 0.01, 리눅스 FreeBSD 1.0, 윈도우 NT 3.1, 넷스케이프, 트로이 목마, 백 오리피스
- **2000년대**: DDoS 공격, 웜 삼총사, 개인 정보 유출과 도용, 전자상거래 교란, 지능적 지속 위협 (APT) 공격에 의한 금융 해킹
- **2010년대**: 농협 사이버 테러, 스마트폰 보안

1.3 보안의 3대 요소

- **기밀성**: 인가된 사용자만이 정보 자산에 접근할 수 있도록 하는 것
- **무결성**: 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것
- **가용성**: 정보 자산에 대해 필요한 시점에 접근이 가능하도록 하는 것

1.4 보안 전문가의 지식 소양

- **운영체제**
- **네트워크**: TCP/IP 프로토콜의 동작에 대한 정확한 이해

- **프로그래밍**: C 프로그래밍, 웹 프로그래밍에 대한 이해
- **서버**: 웹, 데이터베이스, WAS, FTP, SSH, Telnet 등, 인증 및 접근 제어, 암호화 수준, 암호화 여부 이해
- **암호**: 대칭키 및 비대칭키 알고리즘의 종류와 강도, 공개 키 기반 구조의 이해
- 보안 시스템, 모니터링 시스템 등

1.5 보안 관련 법

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 정보통신기반 보호법
- 개인정보 보호법
- 통신비밀보호법
- 저작권법

2 시스템 보안

2.1 시스템의 이해