7주차 3차시 정보보안과 정보보호

【학습목표】

1. 정보보안 방법과 정책을 살펴보고 설명할 수 있다.
2. 정보보호 방법과 정책을 살펴보고 설명할 수 있다.

학습내용1 : 정보보안

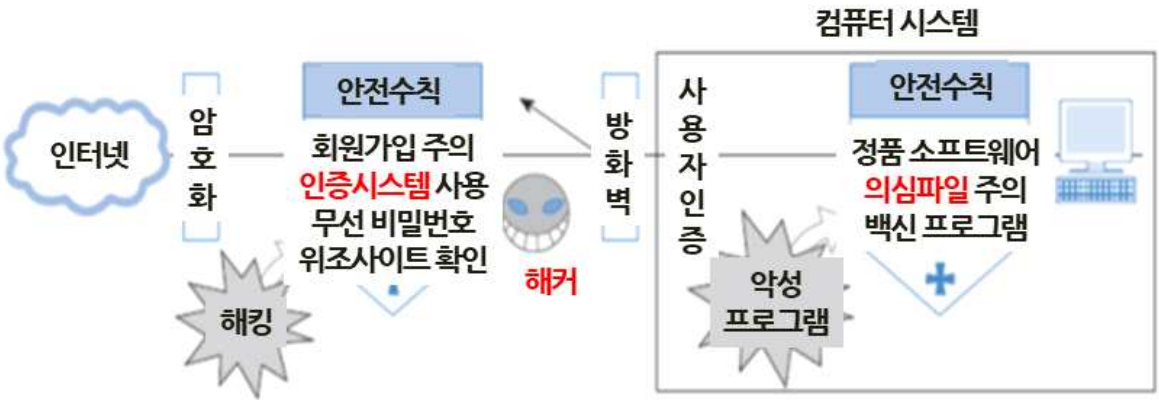
- 컴퓨터 바이러스와 해킹은 우리 주변에서 흔히 일어날 수 있는 상황으로, 이를 대처할 수 있는 방안을 강조

1. 정보보안의 개념

1) 정보보안이란?
- 잘못된 정보의 관리로 인해 많은 피해, 규칙을 지키고 보안 관련 프로그램을 사용하여 정보를 안전하게 지키고 사용하는 것

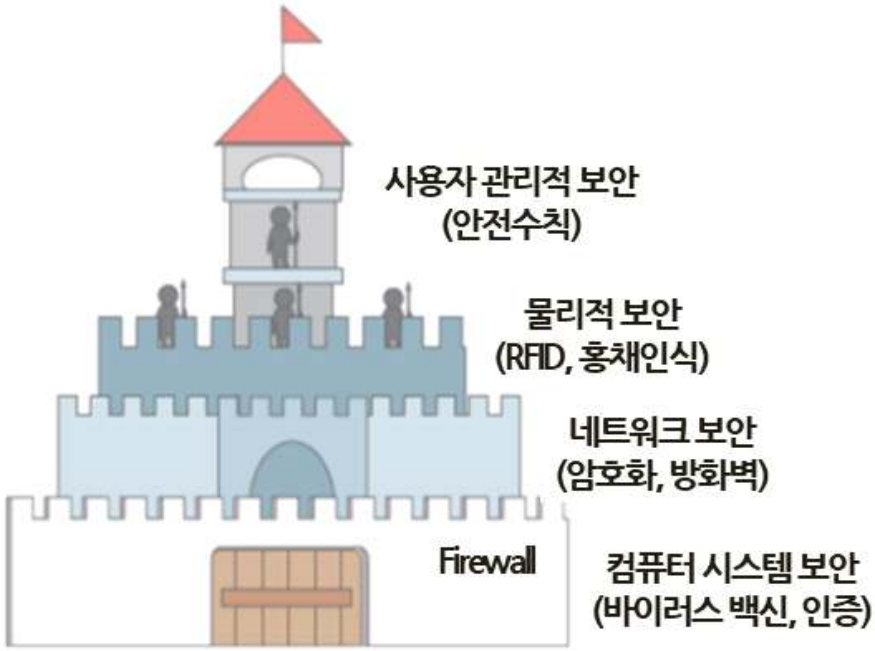
2) 정보보안 환경
- 암호화 기술, 전자서명, 방화벽 설치
- 백신 프로그램, 스파이웨어 제거 프로그램 등 설치

[정보보안의 환경 구축]



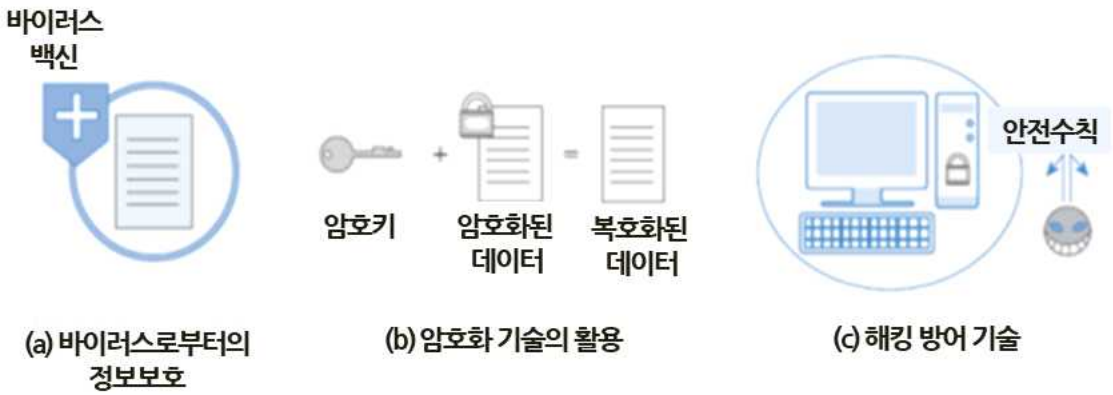
3) 정보보안 서비스의 유형
- 정보보안 서비스는 외부의 공격이나 침입으로부터 시스템을 보호
- 정보보안의 4가지 유형과 계층 - 컴퓨터 시스템의 보안, 네트워크 보안, 컴퓨터에 대한 물리적 보안, 사용자 관리적 보안

[정보보안 서비스의 유형]



① 컴퓨터 시스템 보안
- 악성/유해 프로그램으로부터의 정보보호(백신 주기적으로 사용)
- 인증에 의한 정보보안 서비스(패스워드 사용)
- 불법적 해킹에 의한 내부 시스템에 대한 정보보호 서비스(안전수칙)

[컴퓨터 시스템 보안을 위한 방법]

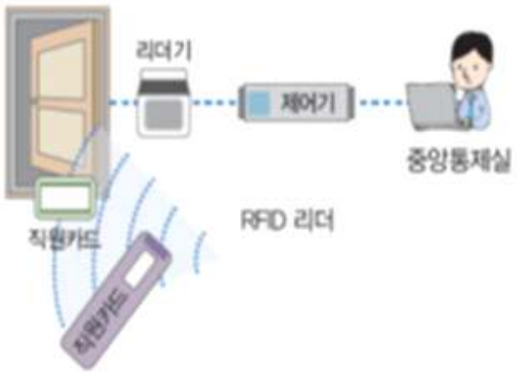


② 네트워크 보안
- 네트워크 보안은 정보가 이동하는 경로보안, 암호화 기법 사용
- 방화벽 사용 : 소프트웨어 방식(소규모 방화벽으로 윈도우 방화벽),
- 하드웨어 방식 (회사 네트워크와 같이 규모가 큰 경우 프록시 서버(Proxy Server)에 방화벽을 설치하여 네트워크를 감시)

③ 물리적 보안
- 물리적 장소에 있는 컴퓨터 시스템의 접근을 막음, 허가 받지 않은 사람의 출입을 통제
- RFID 출입증, 정맥 인식, 지문인식, 홍채인식, 얼굴인식 등으로 출입자 확인

[물리적 보안 시스템]

(a) 지문인식 시스템



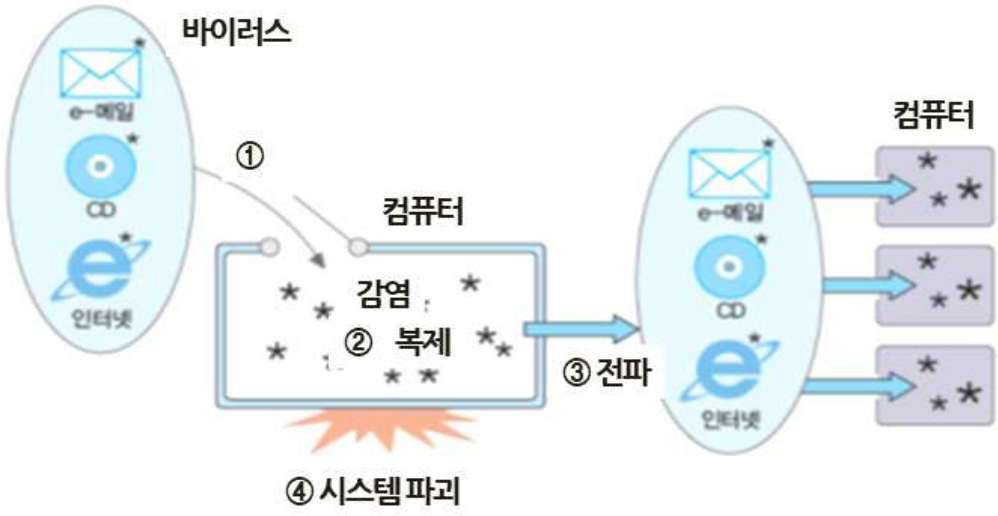
(b) RFID를 이용한 출입통제 시스템

④ 사용자 관리적 정보보안
- 컴퓨터 시스템을 안전하게 관리하기 위한 정보보호 관리 수칙
- 예) 패스워드의 주기적 교체, 컴퓨터 시스템 내 정보의 주기적 백업
- 불의의 정보 사고에 대한 예방을 통해 피해의 최소화

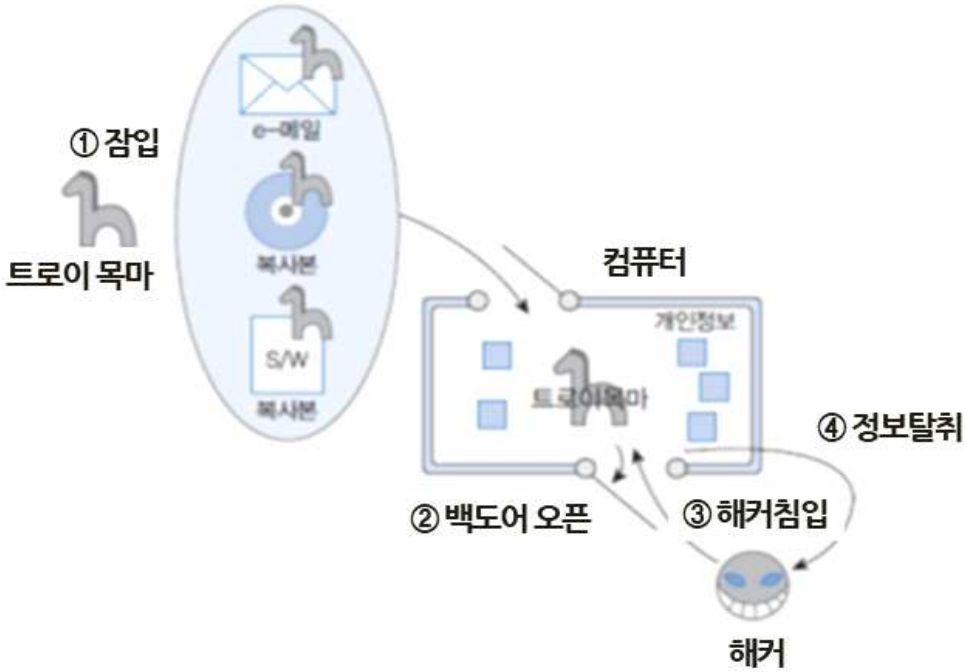
2. 컴퓨터 악성 프로그램 및 해킹

1) 컴퓨터 악성/유해 프로그램
- 악성 프로그램 : 컴퓨터 시스템 파괴 등 나쁜 의도를 갖고 만들어진 경우의 코드
- 유해 프로그램 : 시스템을 파괴하지는 않지만 개인자료를 수집하려는 특정 목적을 위해서 만들어진 것으로, 사용자에게 정신적 피해를 줌

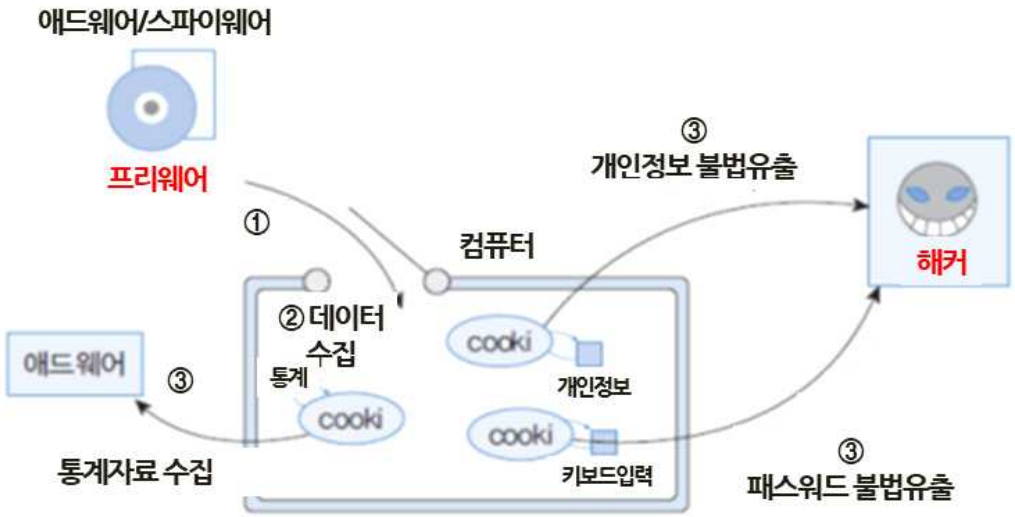
① 컴퓨터 바이러스(Computer Virus)
- e-메일이나 불법 소프트웨어 등을 통해서 컴퓨터 시스템에 침투하는 악성/유해 프로그램
- 일단 바이러스에 감염되면 복제, 전파 또는 데이터 파괴가 발생하며, 양성 바이러스(Benign Virus)는 복제 후 전파코드만 갖고 전파만하고, 악성 바이러스(Malignant Virus)는 컴퓨터 시스템에 직접적 피해를 주는 바이러스



② 트로이목마(Trojan)
- 컴퓨터 시스템에 몰래 들어와 백 도어(뒷문)를 만드는 유해성 프로그램
- 해커는 백도어로 시스템에 침투하여 불법 접근한 뒤 자료삭제, 정보 탈취



③ 스파이웨어 및 애드웨어(Spyware and Adware)
- 스파이웨어 : 사용자의 컴퓨터에 몰래 숨어 있다가 정보를 빼가는 악성/유해 프로그램으로,
- 주로 개인 및 시스템정보, 인터넷의 사용 습관 등을 수집하는 스파이 행위로 개인의 정보를 불법적으로 도용
- 애드웨어: “Advertise”와 “Software”의 합성어, 마케팅 목적을 위해 사용자 기호 데이터를 수집하는 정당한 행위
- 스파이웨어와 애드웨어는 쿠키(Cookie)(= 홈 페이지에 접속할 때 생성되는 임시 파일) 형태로 컴퓨터 시스템 내부에 들어오고,
- 쿠키를 이용하여 컴퓨터 내부에 있는 각종 데이터 수집하여, 외부로 반출



2) 해킹과 크래킹(Hacking and Cracking)

* 해킹: 네트워크의 취약한 부분을 이용하여 컴퓨터 시스템에 불법 침입하여 특정 사이트를 공격하는 행위,

- 해킹은 원래 시스템에 취약한 부분을 점검하기 위한 목적으로 사용하고, 범죄 행위에 사용될 경우에는 크래킹

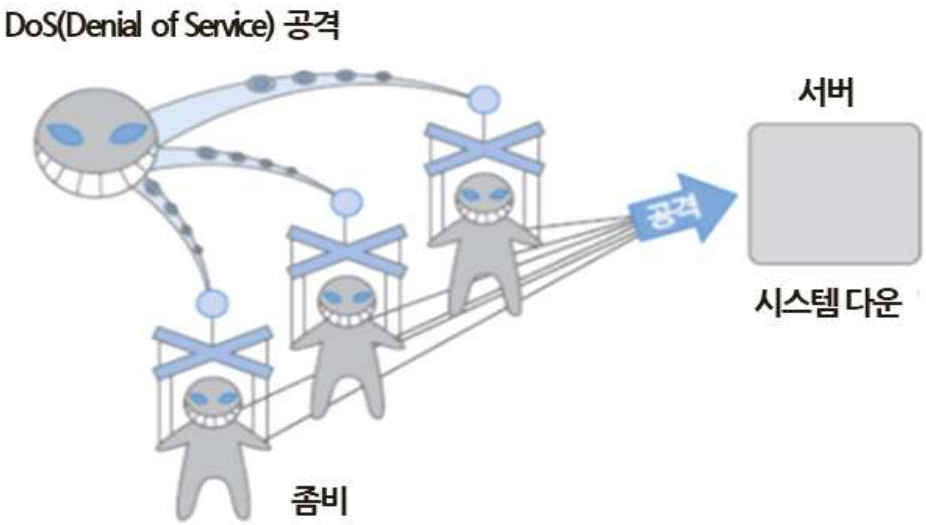
* 크래킹: 해킹이 범죄에 사용될 경우를

① 네트워크 취약점을 이용한 불법 침입

- 해커는 정보 수집 단계에서 네트워크 정보, 시스템 OS 정보, 방화벽 정보 등을 수집하여 취약점을 분석, 수집된 정보를 통하여 취약한 부분을 공격

② 서비스 거부공격(DoS: Denial of Service)

- 바이러스와 같이 시스템을 파괴하지는 않으나 정보 시스템의 정상적인 수행을 정지시킴으로써 사용자에게 불편을 초래
- 해커는 네트워크에 연결된 다수의 컴퓨터를 불법으로 이용하여 공격 목표가 되는 서비스 서버에 동시 다발적으로 시도, 이로 인하여 서버는 부하가 걸리고 특정 사이트가 마비됨
- 좀비(Zombie): DoS 공격에 보안이 취약한 컴퓨터를 불법적으로 이용하는데 이때 사용된 컴퓨터



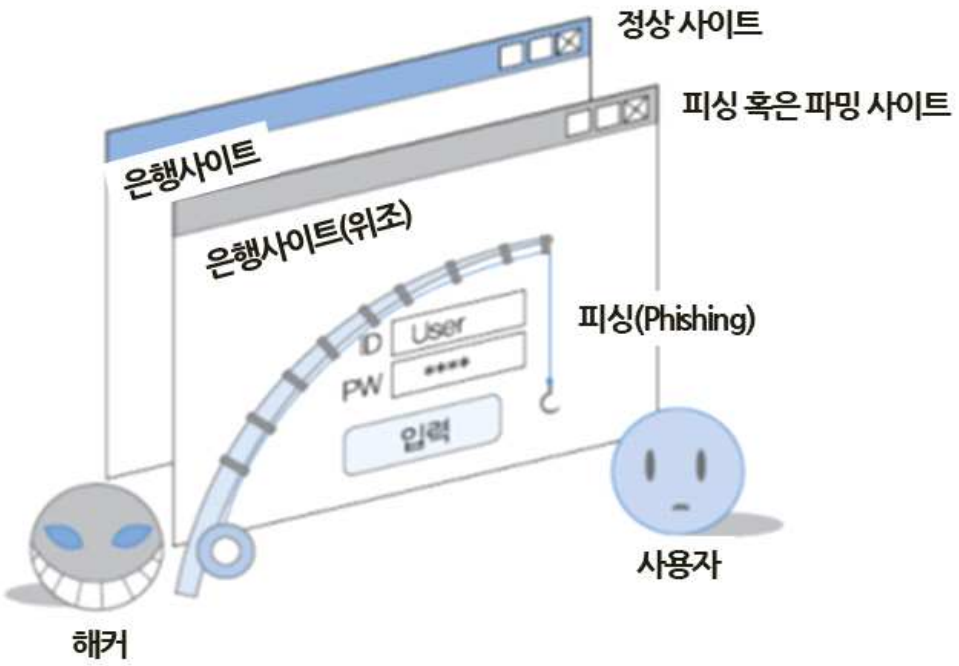
* 피싱(Phishing) 및 파밍(Pharming)

① 피싱

- 개인의 정보(사용자 계정, 패스워드, 신용카드 호)의 ID를 불법적으로 취득하여 범죄에 사용하는 해킹 기술,
- 위조 사이트(eBay,온라인쇼핑, 온라인 뱅킹)를 개설한 뒤 정보를 불법적으로 취득하여 범죄 이용

② 파밍

- 피싱과 비슷한 해킹 유형으로 인터넷 주소창에 방문하고자 하는 사이트의 URL을,
- 가짜 사이트(도메인 자체를 중간에 바꾸는 방식)로 이동시키는 해킹 기술



3) 스팸 메일

- 불특정 다수에게 동일한 내용을 대량으로 보내는 e-메일, 일명 정크 메일
- 스팸 메일 발신자들은 채팅 사이트, 해킹, 바이러스 등에 의해 불법적으로 수집한 리스트를 사용(e-메일 필터링 유틸리티로 스팸메일 차단과 멤버십가입과 유해 사이트 방문시 유의)

[매일같이 쏟아지는 스팸 메일]

학습내용2 : 정보보호

- 내 신변에 관련된 정보를 보호하기 위한 방안에 중점을 두어 강조

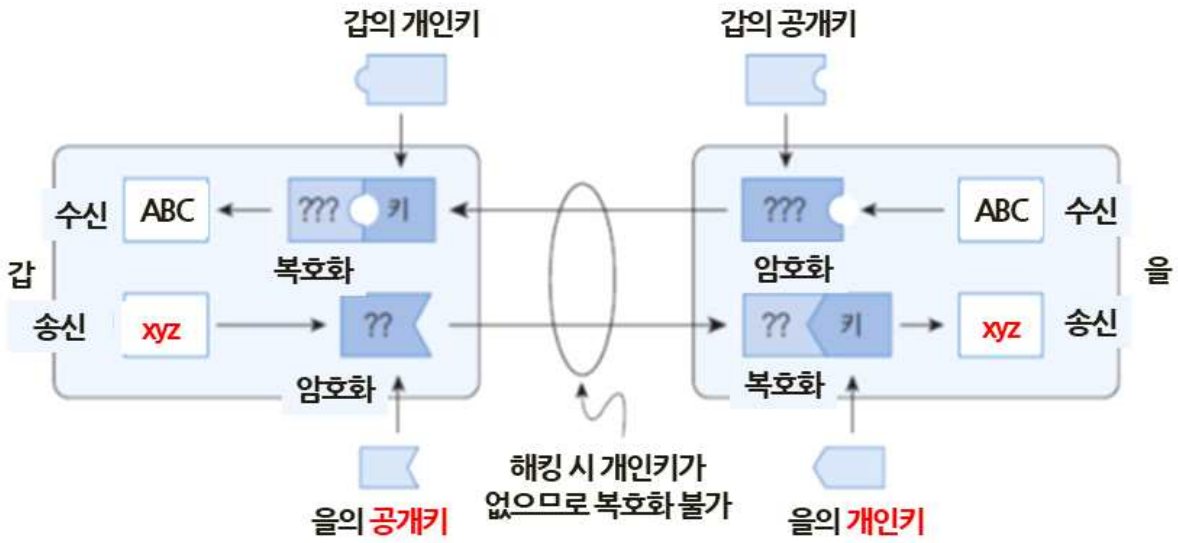
1. 정보보호를 위한 암호화 및 인증

1) 암호화 기술
- 컴퓨터 암호화(Cryptography)란 글자의 배열 순서를 바꾸거나 ,특정한 키(Key) 값을 설정하여 문자의 조합을 혼합시켜, 암호화하는 방식

- 대칭키(Symmetric Key) 방식과 공개키(Public Key) 방식

① 대칭키 암호화 방식
- 송신 측과 수신 측 컴퓨터에서 동일한 암호 키를 이용하여 암호화하는 기법
- 복호화 는 암호화 된 정보를 키 값을 이용하여 원문으로 변환하는 과정
- 송수신 측이 동일한 암호 키를 가지는 것이 중요,
- 그냥 수신하면 해커에 노출될 수 있기 때문에 키 전송과 생성에 어려운 점이 있음

② 공개키 암호화 방식
- 공개 키와 개인 키(Private Key)라는 두 비대칭적인 키를 이용하여 메시지를 암호화
- 공개키는 모두에게 알려져 있으며 메시지를 암호화 하는데 사용,
- 암호화된 메시지는 개인 키를 가진 사람만이 복호화하여 열어 볼 수 있음(매우 안정적인 방식)
- 중간에 유출되더라도 수신자의 개인 키를 알 수 없기 때문에 메시지를 열어볼 수 없음
- 가장 보편적인 공개키 방식으로는 RSA 알고리즘이 사용



2) 인증(Authentification)
* 컴퓨터 간에 교환되는 정보 위변조 및 사용자의 진위 여부를 확인하는 과정
- 사용자 인증: 비밀번호 설정, RFID나 스마트카드 등을 활용한 카드 인증, 생체인식 방법
- 메시지 인증: 전자서명 사용, 문서에 서명한 사람이 누구인지, 전자 문서의 변조 여부를 알 수 있음

[인증(Authentication)의 기술]

(a) 패스워드


(b) 지문인식 마우스


(c) 전자서명

【학습정리】

1. 물리적 보안
- 물리적 장소에 있는 컴퓨터 시스템의 접근을 막음, 허가받지 않은 사람의 출입을 통제할 때는 RFID 출입증, 정맥 인식, 지문인식, 홍채인식, 얼굴인식 등

2. 트로이목마(Trojan)
- 컴퓨터 시스템에 몰래 들어와 백 도어(뒷문)를 만드는 유해성 프로그램으로 해커는 백도어로 시스템에 침투하여 불법 접근한 뒤 자료삭제하고 정보 탈취하는 행위

3. 스파이웨어(Spyware)
- 사용자의 컴퓨터에 몰래 숨어 있다가 정보를 빼가는 악성/유해 프로그램, 주로 개인 및 시스템정보, 인터넷의 사용 습관 등을 수집하는 스파이 행위로 개인의 정보를 불법적으로 도용

4. 파밍(Pharming)
- 파싱과 비슷한 해킹 유형으로 인터넷 주소창에 방문하고자 하는 사이트의 URL을 가짜 사이트(도메인 자체를 중간에 바꾸는 방식)로 이동시키는 해킹 기술