Chapter 12
정보 보안

목차

학습목표

- 물리 보안과 정보 보안의 특징을 살펴본다.
- 악성 소프트웨어의 종류와 특징을 살펴본다.
- 악성 소프트웨어를 방지할 수 있는 방법들을 살펴본다.
- 해킹 의미를 살펴보고, 다양한 공격 방식을 알아본다.
- 다양한 인증 기술을 학습한다.
- 암호화 기술 방식과 특징을 학습한다.

물리 보안

보안

- 다양한 위협에서 자신의 신체나 재산을 지키는 일체의 행위

보안 기술

- 물리 보안 : 물리적인 위협을 막는 기술
- 정보 보안 : 온라인에서 발생하는 위협을 막는 기술

물리 보안

물리적인 위협의 종류

- 돈을 훔치는 도둑질, 강도 등 공격 행위
- 지폐나 유가증권을 위조하는 행위
- 원래 내용을 다른 내용으로 바꾸는 변조 행위
- 유사 제품을 제조 및 유통하는 행위
- CD나 음반 등 저작물을 무단으로 복제(저작권 침해)하는 행위

(a) 공격

(b) 위조

그림 12-1 물리적인 위협의 종류

피싱(phishing)

- 개인(private)과 낚시(fishing)의 합성어
- 보이스 피싱 사례
  - 은행, 검사, 경찰을 사칭하여 돈을 송금하게 함
  - 특정 장소에 돈을 보관하게 하여 착취
  - 자녀가 납치된 것처럼 가장하여 몸값을 요구

그림 12-2 보이스 피싱

물리 보안

물리적인 위협의 유형

- 공격, 위조/변조/저작권 침해, 사칭 등

물리적인 위협의 방지 대책

- 공격 : CCTV나 센서를 사용하여 외부 침입 감시
- 위조/변조/저작권 침해 : 위조 방지 기술을 사용하여 복제가 불가능하게 하거나, 복제하더라도 원본과 다르게 보이게 하는 기술 사용
- 사칭 : 직접 확인하는 방법 이외에 특별한 기술이 없어 개인적으로 주의가 요구됨

복사 방지 기술 사례 – 지폐

- 빛에 비추어야 보이는 그림
- 보는 각도에 따라 변하는 그림
- 형광 잉크를 입힌 그림
- 복사를 하면 검은색으로 보이게 하는 은선

(a) 형광 잉크

(b) 홀로그램

(c) 복사 방지용 은선

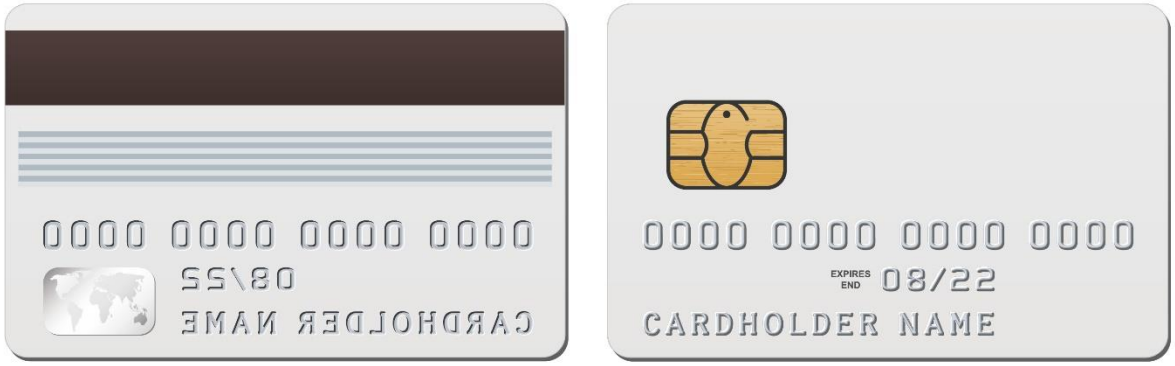
그림 12-3 지폐에 적용된 복사 방지 기술

물리 보안

신용카드, 출입카드 보안 기술

- 과거에는 카드 내 마그네틱에 정보를 넣어 읽는 방식 사용
- 마그네틱 방식이 쉽게 노출되자 암호화된 특수 칩과 RFID 기술을 사용하는 카드가 대중화됨
- RFID 기술을 이용한 보안 기술은 오프라인에서만 사용 가능

** 온라인에서는 인터넷 쇼핑 보안 대책으로 카드 만료 일자와 특수 숫자 사용



(a) 마그네틱 신용카드 (b) 암호화된 특수 칩이 내장된 신용카드

그림 12-4 신용카드 보안 기술

온라인에서 발생하는 불법 행위

- 컴퓨터나 스마트폰 등 시스템을 공격하여 파괴하는 경우
- 다른 사람의 데이터를 가로채는 경우
- 데이터를 위조하거나 다른 사람의 데이터를 도용하여 무단으로 사용하는 경우
- 기업이나 기관을 사칭하여 개인정보를 입력하도록 유도한 후 모은 개인 데이터를 다른 범죄에 악용하는 경우(인터넷 피싱)
- 디지털 데이터를 불법 복제하는 경우
- 비방이나 인식 공격 등 비윤리적 행위를 하는 경우

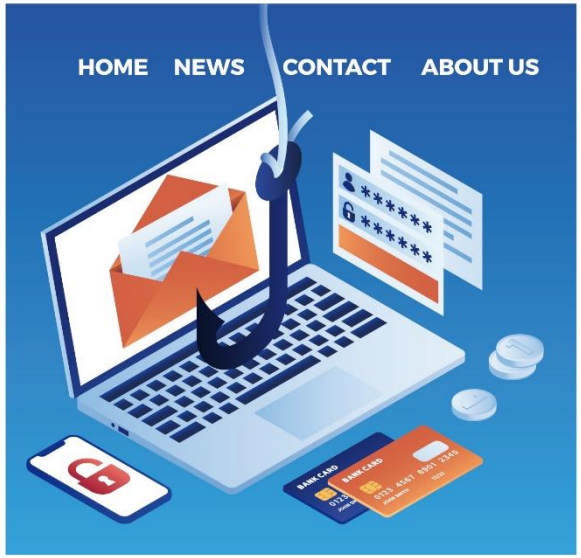


그림 12-5 인터넷을 이용한 피싱

정보 보안

정보 보안의 필요성

- 디지털 복제는 들킬 염려가 없다는 생각 때문에 일반인 사이에서도 불법 복제가 줄지 않음
- SNS 이용이 늘어나면서 직접 만나지 않고도 의사 전달이 가능해짐에 따라 비방이나 인식 공격 등 비윤리적 행위도 늘어남

정보 보안의 정의

- 수집하고 가공한 정보를 송수신 및 저장하는 과정에서 발생할 수 있는 훼손, 변조, 유출 등 불법적인 행위를 차단하는 방법

융합 보안

융합 보안

- 물리 보안과 정보 보안을 결합한 형태
- 현대 보안 기술은 물리 보안과 정보 보안 영역을 따로 보지 않고 하나의 영역으로 봄
- 사례
  - 사람 얼굴을 인식하여 범죄자를 자동으로 찾아주는 CCTV 기술
  - 교통법규 위반의 경우 자동차번호판을 자동으로 인식하고 벌금을 부과하는 기술

악성 소프트웨어

악성 소프트웨어의 특성

- 악의적인 행위를 할 목적으로 만들어 유포시킨 소프트웨어
- 종류와 감염 경로가 다양
- 과거에는 소프트웨어를 복사하는 과정에서 악성 소프트웨어에 감염
- 최근에는 웹 사이트 방문, 이메일 첨부 파일 다운로드, 스마트폰 메시지 클릭만으로도 감염
- 악성 소프트웨어에 감염되면 시스템이 느려지거나 아예 파괴될 수 있음
- 개인정보 유출, 설정 변경, 원치 않은 광고 노출 등 다양한 피해가 발생

악성 소프트웨어

컴퓨터 바이러스

- 대표적인 악성 소프트웨어
- 컴퓨터 속의 자료를 없애거나 시스템을 정지하려고 만든 파괴적인 소프트웨어
- 자기 자신을 복제하는 능력이 있어 주변 컴퓨터까지 감염 및 확산
- 시스템 파일을 감염시키고, 파일들을 지우거나 하드디스크를 포맷해서 컴퓨터를 사용할 수 없게 만듦

그림 12-6 컴퓨터 바이러스가 시스템 파괴

악성 소프트웨어

컴퓨터 바이러스 감염 경로

- 불법 다운로드 웹 사이트를 사용하는 경우
- 토렌트 같은 파일 다운로드 프로그램을 사용하는 경우
- 다른 컴퓨터에서 감염된 파일을 복사한 경우

■ 바이러스 감염 예방을 위한 주의사항

- 비정상적인 경로로 파일을 다운로드 시 xx.exe나 yy.com처럼 모르는 실행 파일이 있을 때는 절대로 실행해서는 안 됨(대부분 실행 파일로 감염)
- 안전하지 못한 웹 사이트 방문 시 <허용> 버튼 절대 누르지 말 것

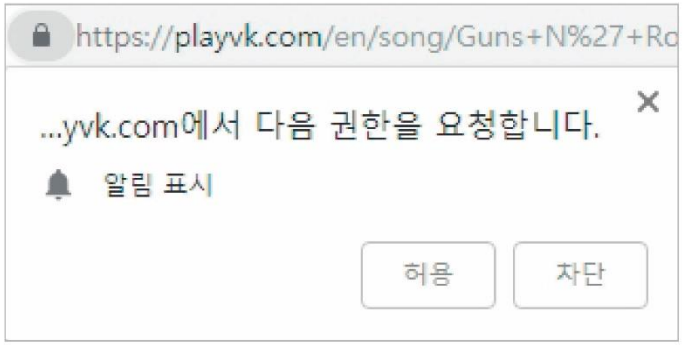


그림 12-7 바이러스에 감염될 수 있는 메시지 창

악성 소프트웨어

트로이목마

- 컴퓨터 바이러스보다는 조금 약하지만 악성 소프트웨어
- 컴퓨터 바이러스와 달리 자기복제 능력이 없음(해당 컴퓨터만 감염)
- 트로이목마라는 이름은 트로이전쟁 중 목마에 군인을 숨겨 적군에 침투시킨 후 전쟁을 끝낸 그리스 로마 신화에서 따옴
- 대부분 유용해 보이는 소프트웨어에 몰래 숨겨 놓음

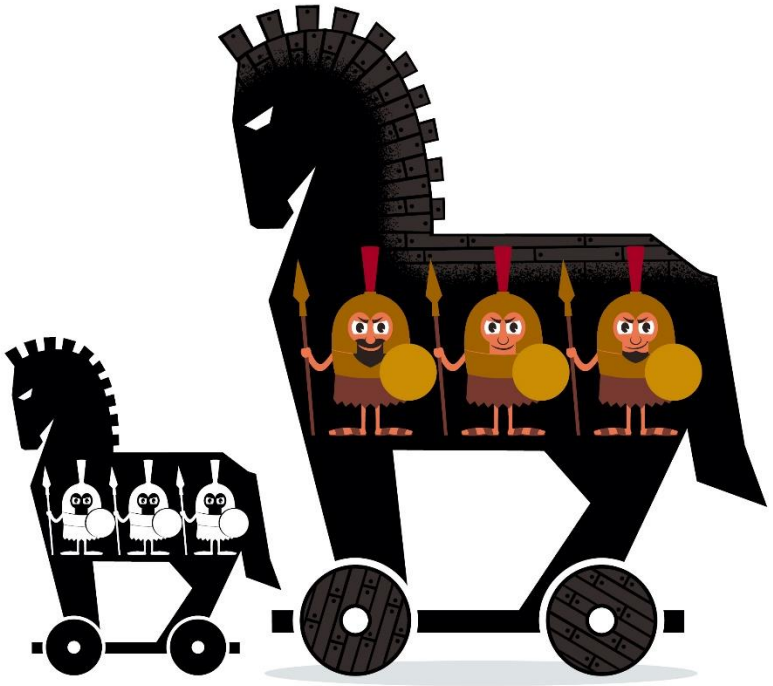


그림 12-8 트로이목마 바이러스

악성 소프트웨어

매크로 바이러스

- 엑셀, 워드, 파워포인트는 프로그램 자체에 외부 파일을 실행할 수 있는 매크로 기능이 있음(동영상 또는 음악 재생 등)
- 매크로 바이러스는 엑셀, 워드, 파워포인트 문서 같은 데이터 파일에 포함해서 배포
- 데이터 파일에 포함해서 유포하기 때문에 상대적으로 사용자가 의심하지 않고 파일을 열 확률이 더 높음
- 잘 모르는 웹 사이트에서 다른 사람이 쓴 리포트 파일, 잘 모르는 사람에게 받은 이메일에 첨부된 파일을 다운로드하여 파일을 열면 매크로 바이러스에 감염

악성 소프트웨어

랜섬웨어(ransomware)

- 돈을 지불해야만 컴퓨터 자료를 볼 수 있게 하는 악성 소프트웨어
- 감염되면 컴퓨터 내 모든 파일에 암호가 걸려 파일을 열 수 없게 됨
- 사진이든 문서든 간에 전혀 열리지 않고 해커에게 몸값을 요구하는 메시지가 나타나고, 돈을 지불하지 않으면 영영 데이터를 사용할 수 없게 됨

그림 12-9 랜섬웨어에 걸린 화면

악성 소프트웨어

■ 기타 악성 소프트웨어

- 애드웨어
  - 사용자 화면이나 웹 사이트 초기 화면에 사용자 동의 없이 광고를 띄움
  - 웹 브라우저의 시작 화면을 자신의 협찬사 웹 페이지로 강제로 바꾸기도 함

- 스파이웨어
  - 사용자 동의 없이 방문하는 웹 사이트, 사용 패턴, 개인정보 같은 정보를 몰래 훔쳐 가는 프로그램

그림 12-10 사용자 동의 없이 광고를 보여 주는 애드웨어

악성 소프트웨어

■ 무료 소프트웨어와 같이 설치되는 프로그램

- 무료 소프트웨어를 다운로드하여 설치할 때는 추가로 설정 또는 부수적인 프로그램을 같이 설치하지 않는지 확인 필요

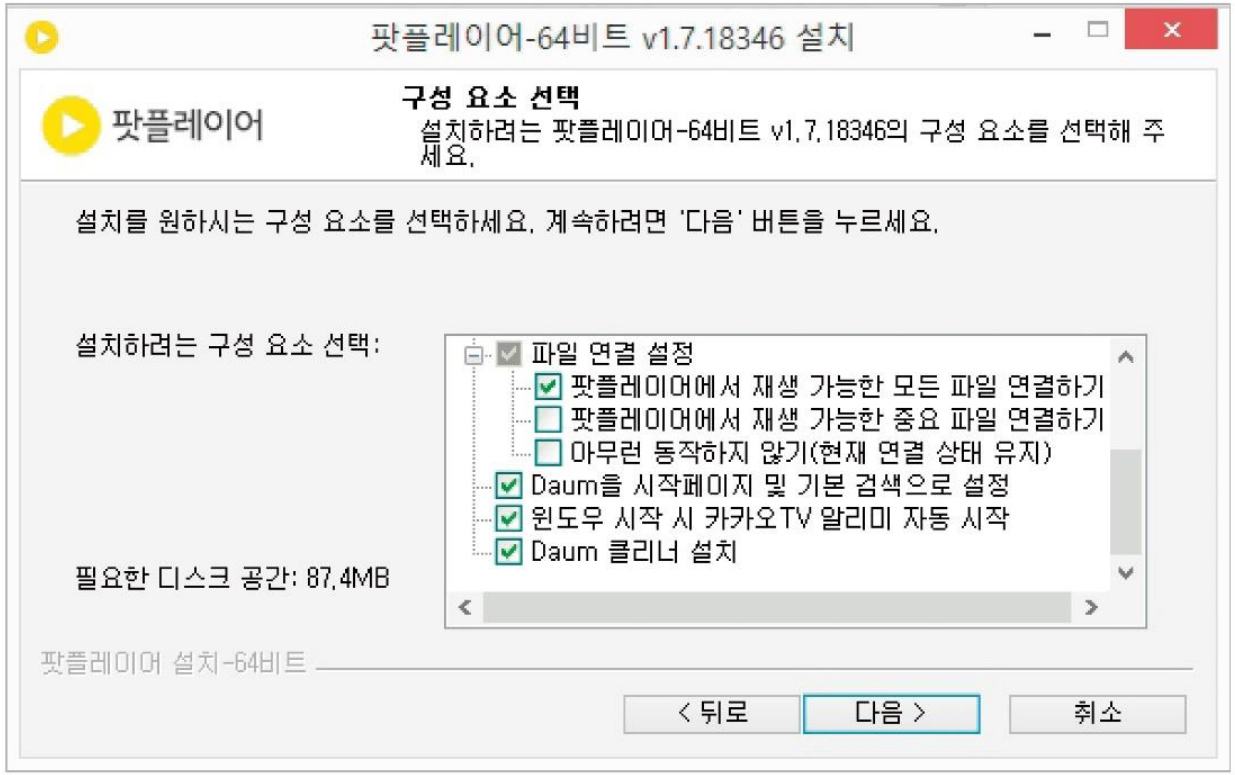


그림 12-11 부가 프로그램 설치에 체크된 설치 화면

악성 소프트웨어

백신

- 악성 소프트웨어를 예방하려면 백신을 설치해야 함
- 백신 소프트웨어는 주기적으로 업데이트할 것
- 의심이 가는 파일을 다운로드했다면 백신 프로그램을 사용하여 검사를 진행한 후 실행

해킹

- 전자회로나 컴퓨터의 하드웨어, 소프트웨어, 네트워크, 웹 사이트 등 각종 정보 체계가 본래 의도와는 다른 동작을 일으키도록 하는 행위
- 아이폰에서는 MP3 파일을 자유자재로 사용할 수 없는데, 탈옥 프로그램으로 MP3 파일을 마음대로 쓸수 있게 하면 해킹

크래킹

- 불법적으로 시스템에 접근하는 것은 해킹과 같으나, 시스템이나 통신을 마비시키거나 파괴하는 행위까지 포함
- 악성 소프트웨어는 사용자 실수로 시스템에 침투하여 불법 행위를 일으키는 것

** 크래킹 혹은 해킹은 시스템 외부에서 침투하려는 모든 시도를 가리킴

해커

- 일반적으로 '해커'는 부정적인 의미로 쓸 때가 많은데, 원래는 컴퓨터 내의 시스템이나 프로그래밍에 관해 전문지식을 가진 사람을 의미함
- 해커 중 범죄를 일으키는 사람을 크래커(cracker, 파괴자)라고 함
- 크래커에게서 시스템을 지키는 사람을 화이트 해커라고 함
- 일반적으로 크래커를 '해커'로 인식하고 있기 때문에 시스템 파괴자를 해커라 칭함

해킹 피해 사례

- 페이스북 : 3,000만 명에 달하는 개인정보가 유출(2018년 10월 미국)
- 가상화폐거래소 빗썸 : 약 190억 원의 가상화폐 도난(2018년 6월 국내)
- 가상화폐거래소 자이프 : 약 670억 원의 가상화폐 도난(2018년 9월 일본)

그림 12-12 해킹 공격의 유형

해킹의 변화

- 컴퓨터 운영체제가 점점 안정화되고 방화벽이나 침입 탐지 시스템 같은 해킹에 대비한 소프트웨어들을 개발하면서 해커들이 외부에서 침입하기가 점점 어려워짐
- 사용자 패스워드를 탈취하거나 바이러스나 이메일 첨부 파일을 사용하여 시스템 내부의 사용자 정보를 불법 취득하는 쪽으로 바뀌고 있음
- 조직 내부에서 단 한 명의 정보만 획득해도 해당 아이디로 컴퓨터에 침입하여 시스템을 파괴하기가 더 쉽기 때문

도스(Denial of Service, DoS)

- 클라이언트/서버 구조의 가장 큰 단점은 서버 과부하
- 도스라 불리는 서비스 거부 공격은 서버 쪽에 많은 양의 패킷을 보내어 다른 사람이 서버를 이용하지 못하도록 막음
- 도스 공격은 공격하는 컴퓨터가 몇 대 되지 않기 때문에 해당 컴퓨터만 차단하면 공격이 종료됨

디도스(Distributed DoS, DDoS)

- 해킹 중 가장 잘 알려진 방법으로 분산형 서비스 거부 공격
- 디도스에서 공격자는 일반인 컴퓨터를 감염시켜 자신이 조정할 수 있는 컴퓨터로 만들고(좀비 컴퓨터), 수백 대의 좀비 컴퓨터가 감염되면 공격자는 같은 시간에 한 서버를 공격하도록 명령을 내림
- 도스와 달리 여러 곳에서 공격하기 때문에 방어하기가 매우 어려움

그림 12-13 디도스 공격

디도스(Distributed DoS, DDoS) 피해

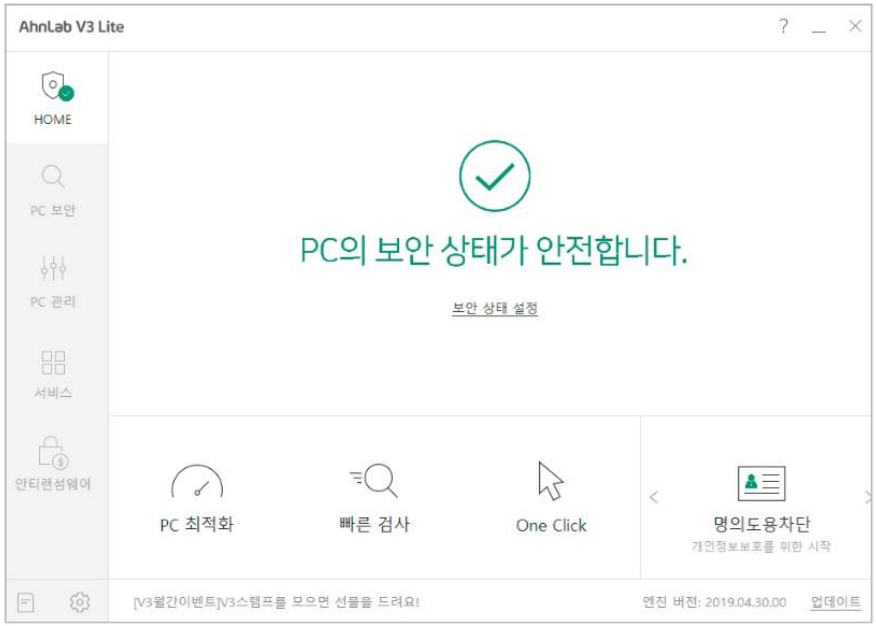
- 2016년 10월 디도스 공격으로 웹 사이트 마비
  - 미국 : 아마존, 트우이터, 넷플릭스 등 1,200여 개 웹 사이트
  - 국내 : 아프리카 TV 등
  - 서아프리아(라이베리아) : 국가 전체 인터넷 마비

- 디도스 공격이 점점 지능화되면서 많은 보안업체가 이 디도스 공격을 회피하는 기술들을 선보이고 있음

정보 보호 방법

백신

- 악성 소프트웨어에서 자신의 컴퓨터나 스마트폰을 지키는 데 사용하는 프로그램
- 악성 소프트웨어를 차단하고 찾아서 치료
- 우리나라 최초의 백신인 V3를 비롯하여 무료로 배포하는 백신 프로그램을 설치해서 사용

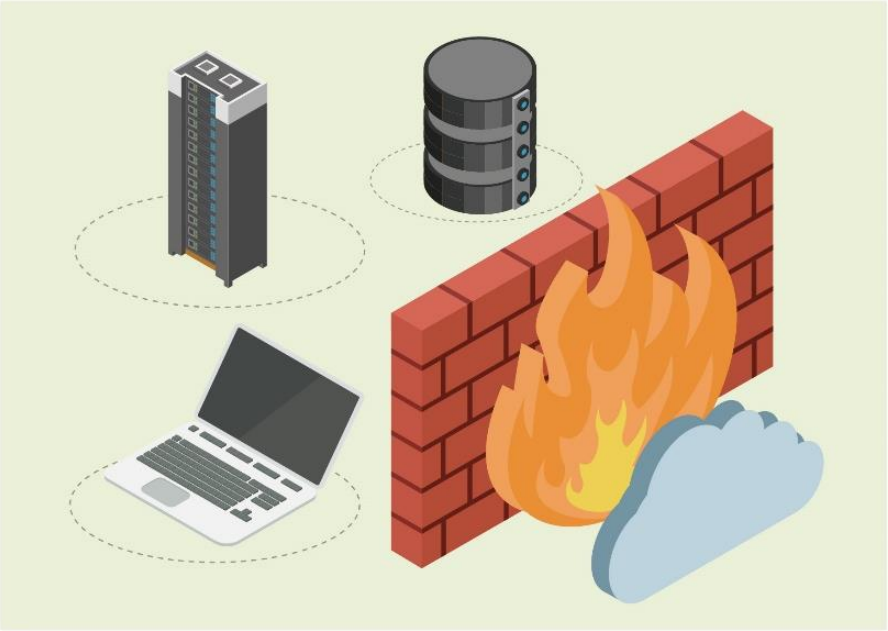


(a) V3 백신 화면

정보 보호 방법

방화벽

- 네트워크로 전송되는 데이터를 검사하여 악성 소프트웨어나 해킹이 내부로 침투하지 못하게 막는 소프트웨어
- 시스템 내부에 있는 정보가 불법적으로 외부로 나가지 못하게 막는 기술도 포함
- 요즘은 운영체제가 자체적으로 방화벽 소프트웨어를 동작시킴



(b) 방화벽

인증 기술

패스워드 인증

- 패스워드는 사용자가 본인임을 입증하는 가장 기본적인 방법
- 패스워드는 대문자, 소문자, 숫자를 조합하여 어렵게 만들어야 하며, 해킹에 대비하여 6개월에 한 번씩은 변경해야 함

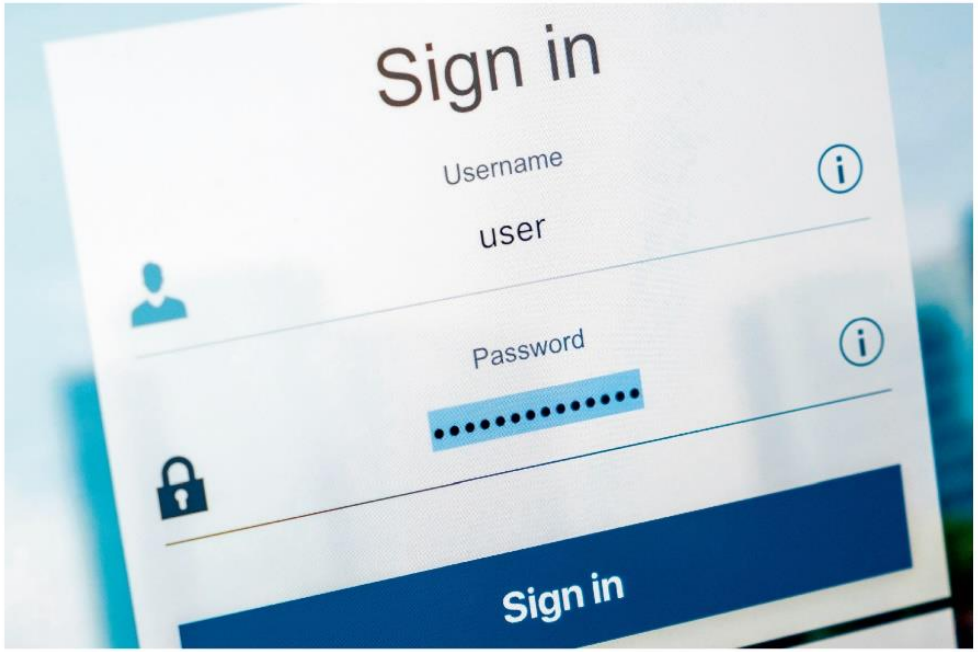
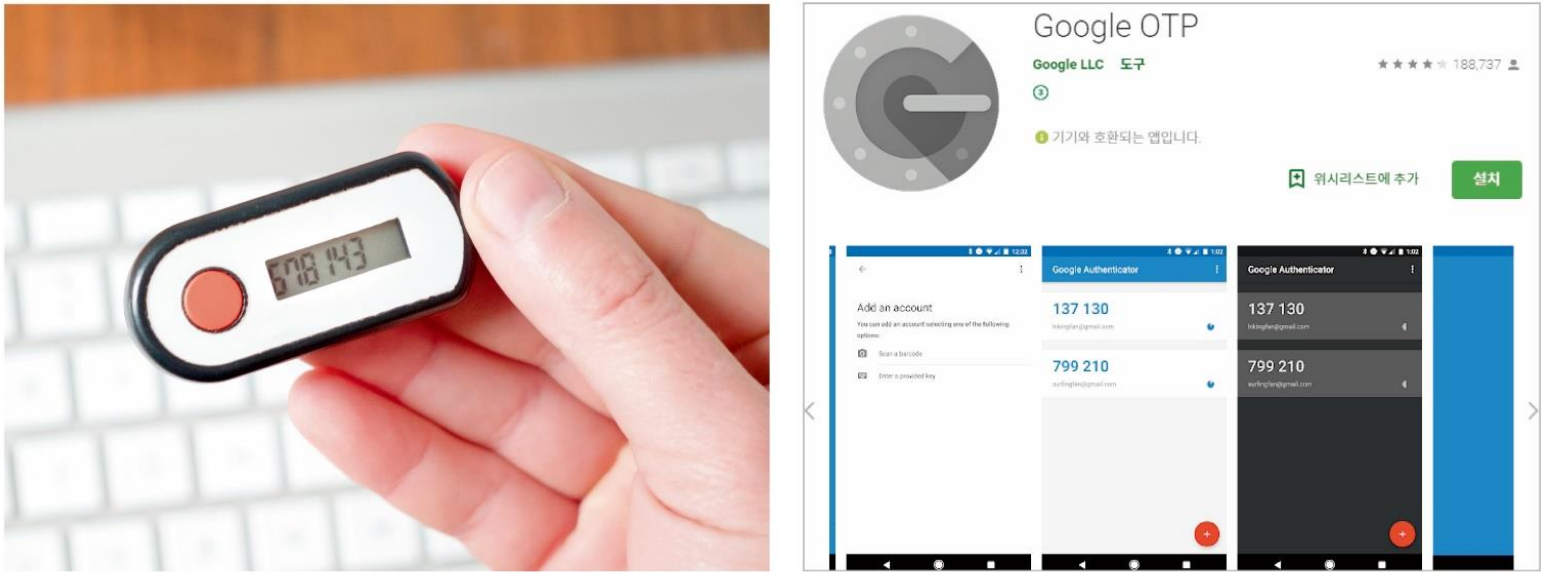


그림 12-15 패스워드 인증

인증 기술

OTP(One Time Password)

- 일정 시간만 쓰고 버리는 패스워드
- 은행거래에서 가장 흔하게 볼 수 있음
- 일정한 알고리즘에 따라 암호 생성하며 스마트폰용 OTP도 있음



(a) 배터리형 OTP　　(b) 구글 OTP

그림 12-16 OTP의 종류

인증 기술

■ 바이오 인증

- 지문 인식, 안면 인식, 홍채 인식처럼 신체를 이용하여 인증하는 방식
- OTP와 달리 휴대가 불필요, 복사가 어려워 미래 기술로 각광을 받고 있음
- 국내 은행 웹 사이트뿐 아니라 해외 대형 은행들도 바이오 인증을 도입

(a) 지문 인식 (b) 안면 인식

그림 12-17 바이오 인증 기술

인증 기술

공인인증서

- 공인된 기관에서 인증한 전자서명
- 우리나라는 은행이나 쇼핑몰 사이트를 이용할 때 공인인증서를 요구

그림 12-18 공인인증서 화면

인증 기술

공인인증서

- 외국의 대형 웹 사이트에서는 공인인증서를 전혀 사용하지 않음
- 대신 미국 등 선진국은 'https://'라는 보안 웹 사이트를 개발
  - s는 secure(보안)를 의미
  - 외국에서는 패스워드와 OTP만으로도 거래가 가능
  - 한류 열풍이 불어 외국인이 국내 웹 사이트에서 거래하고 싶어도 공인인증서가 없기 때문에 거래를 하지 못하는 현상이 발생

콘텐츠 유출 방지 기술

DRM(Digital Rights Management)

- 디지털 콘텐츠를 무단으로 사용하는 것을 막는 방지 기술
- DRM은 적법한 콘텐츠 사용은 허락하지만 그 외는 사용을 막는 기술
- DRM 기술은 회사의 문서를 관리하는 데 적용

그림 12-19 DRM과 관련한 연관 단어

콘텐츠 유출 방지 기술

워터마크(watermark)

- 어떤 파일에 관한 저작권을 식별할 수 있도록 특수하게 삽입된 패턴
- 물로 쓴 글씨처럼 평상 시에는 보이지 않다가 특수한 처리를 하면 나타나는 마크(mark)라는 의미로 워터마크라고 함
- 원 저작자가 자신의 작품임을 증명하는 데 사용

그림 12-20 피카소 사인

암호화 기술

암호화

- 원본 데이터를 풀기 어려운 패턴으로 변형하여 허가받은 사용자 외에는 볼 수 없게 하는 기술

복호화

- 암호문을 원문으로 돌리는 것
- 복호화를 하려면 키를 반대로 사용

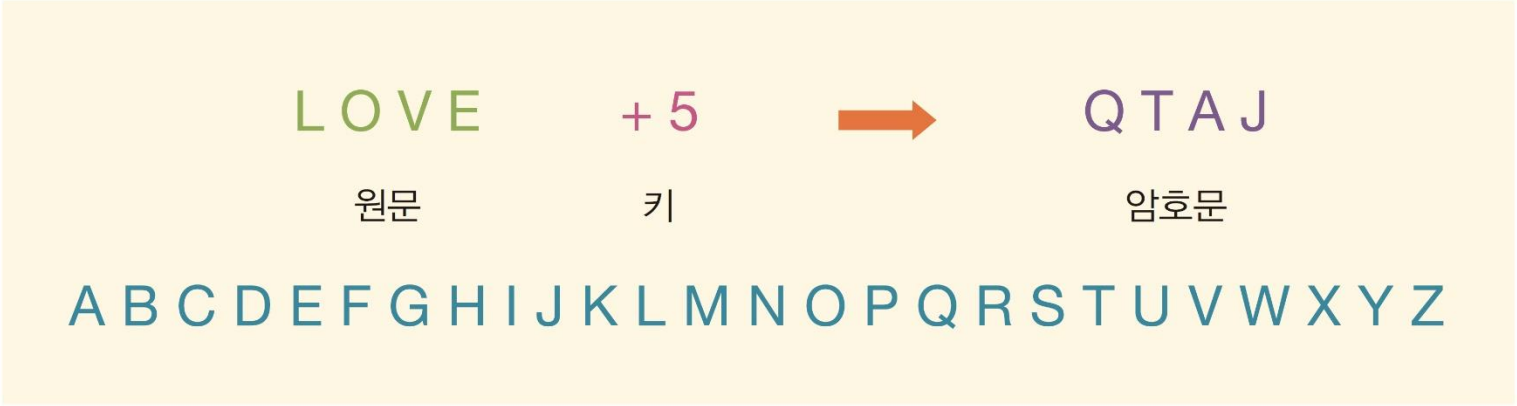


그림 12-21 암호화의 예

암호화 기술

대칭(단일)키 암호화

- 하나의 키로 암호화 혹은 복호화하는 방식
- DES(Data Encryption Standard)
  - 암호화하고 해독하는 데 하나의 키만 사용하는 대표적인 방법
  - 1977년 미국에서 국가 표준으로 지정한 방식으로 56비트 키 사용
- AES(Advanced Encryption Standard)
  - 2000년도에 더 강력한 단일키 암호화 방식인 AES로 대체
  - AES 방식은 키로 128비트를 사용하며, 전 세계에서 널리 활용

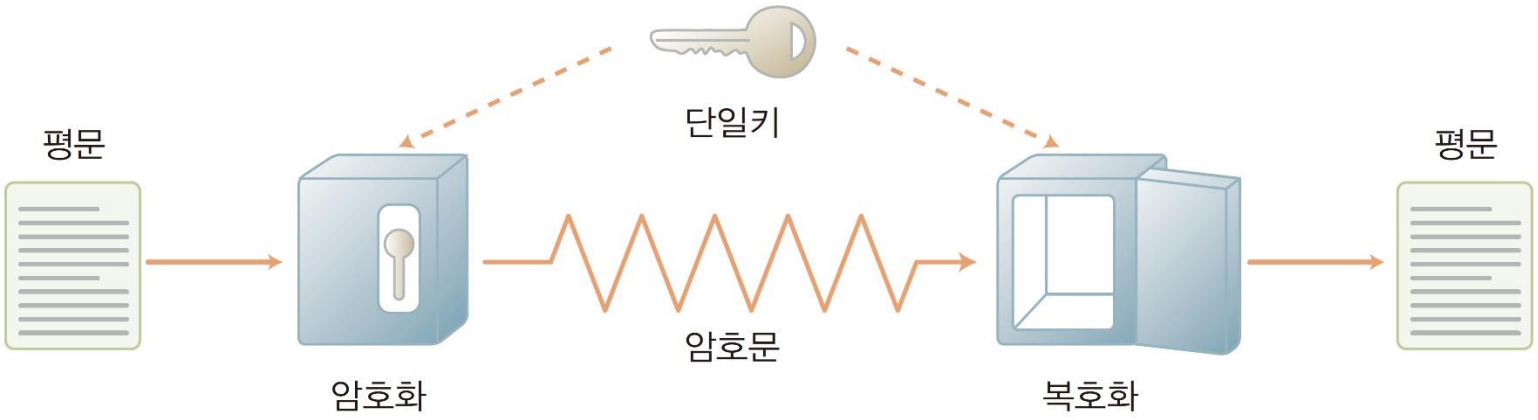


그림 12-22 대칭키 암호화

암호화 기술

대칭(단일)키 암호화의 단점

- 암호로 만든 결과물과 함께 키도 같이 전달해야 함
- 암호를 해독하려면 당연히 키를 상대방에게 전달해야 함
  - 전달 과정에서 다른 사람에게 노출되면 암호문이 깨질 수 있음
  - 키를 소유한 사람이 나쁜 마음을 먹는다면 해당 키를 다른 암호문을 해독하는 데 사용할 수도 있음

암호화 기술

공개키(비대칭 암호화) 기술

- 공개키와 비밀키의 쌍으로 키를 구성
- 공개키
  - 암호문을 만들려는 사람에게 공개하는 키
  - 암호를 만들 때는 사용할 수 있지만, 암호를 해독할 수는 없음
- 비밀키
  - 암호를 해독하는 키
  - 공개키가 노출되거나 탈취되어도 암호를 해독하지 못하는 장점이 있음

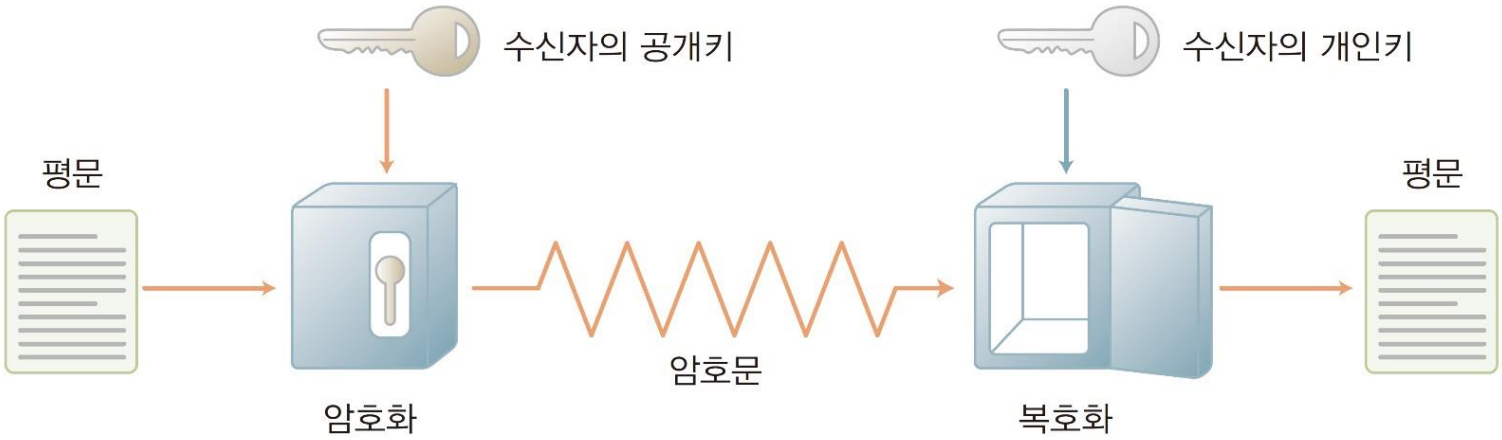


그림 12-23 비대칭키 암호화

Thank you!

한빛아카데미 Hanbit Academy, Inc.