데이터통신과 네트워킹

Data Communication & Networking Ch. 16

동아대학교 컴퓨터AI 공학부
S03 301-01호실 (이양민 교수 연구실)
2024.12 (Kakao ID: yanwenry)

CHAPTER

16

보안

Section

SECTION 01

해킹과 보안

1. 보안의 정의

- **정보보안**은 수집하고 가공한 정보를 송수신 및 저장하는 과정에서 발생할 수 있는 훼손, 변조, 유출과 같은 불법적인 행위를 차단하는 방법.
- 정보통신기술을 이용하여 시스템을 파괴하거나 정보를 탈취하는 행위를 해킹hacking이라 부르고 이러한 행위를 하는 자를 해커hacker라 부름.
- 해킹의 기본은 특정한 시스템을 공격하는 것이다. 해커는 서버나 네트워크의 약한 부분을 공격하여 시스템에 침투하거나 패스워드를 탈취하여 시스템을 장악.

그림 16-1 뉴스기사: 엔비디아의 소스코드가 해커에 의해 탈취(출처: https://thehackernews.com)

SECTION 01

해킹과 보안

2. 악성 소프트웨어

- 악성 소프트웨어의 대표적인 경우가 **컴퓨터 바이러스**.
- 컴퓨터 바이러스는 컴퓨터 속의 자료를 파괴하거나 시스템을 정지시키기 위해 만들어진 소프트웨어.
- 자기 자신을 복제하는 능력을 가지고 있어서 주변 컴퓨터까지 감염시킴.

그림 16-2 악성 사이트 차단 메시지 창

SECTION 01

해킹과 보안

- **트로이 목마**는 컴퓨터 바이러스와 달리 자기 복제 능력이 없기 때문에 해당 컴퓨터만 감염 -> 개인정보를 탈취하거나 좀비 컴퓨터로 만들어 다른 시스템을 공격할 수 있는 상태로 만듦.
- 매크로 바이러스는 엑셀, 워드 혹은 파워포인트 문서 같은 데이터 파일에 포함되어 배포.
- **랜섬웨어**ransomware는 돈을 지불해야만 컴퓨터의 자료를 볼 수 있게 해주는 악성 소프트웨어 -> 랜섬웨어에 감염되면 컴퓨터 내 모든 파일이 암호가 걸려 파일을 열 수 없게 됨 -> 랜섬웨어는 악성 소프트웨어로 돈을 벌 수 있기 때문에 점점 많이 퍼지고 있음.

그림 16-3 랜섬웨어에 걸린 화면

SECTION 01

해킹과 보안

- 애드웨어의 AD는 광고를 의미하며, 사용자의 화면이나 홈페이지 화면에 사용자의 동의 없이 광고를 띄움.
- 스파이웨어는 사용자의 동의 없이 방문하는 사이트, 사용 패턴, 개인정보와 같은 정보를 몰래 훔쳐가는 프로그램.

그림 16-4 사용자 동의 없이 광고를 보여주는 애드웨어

SECTION 01

해킹과 보안

3. 피싱

- 피싱은 개인Private과 낚시Fishing의 합성어로 개인정보를 낚는다는 의미 -> 보이스 피싱은 전화와 같은 통신 매체를 이용하여 은행, 검사, 경찰을 사칭하여 돈을 송금하게 하거나, 특정 장소에 돈을 보관하게 하여 착취하는 수법.
- 정보통신을 이용한 피싱은 가짜의 이메일 주소나 가짜 웹사이트를 이용하여 돈을 요구하거나 개인정보를 탈취.

그림 16-5 피싱(phishing)과 가짜 사이트

SECTION 01

해킹과 보안

- **파밍**pharming은 씨를 뿌려 한번에 수확하는 농사Farming에서 유래한 신조어 -> 네트워크 정보를 변조하여 가짜 사이트로 유도하는 기법.
- 파밍은 네트워크 정보를 변조하여 가짜 사이트로 유도하기 때문에 사용자는 진짜 사이트라고 믿고 정보를 입력하게 됨.
- 파밍에서는 바이러스를 사용하여 사용자의 컴퓨터를 감염시킴 -> 사용자가 특정 사이트를 방문하려 하는 경우 가짜 사이트의 주소로 DNS 정보를 변경 -> 사용자는 DNS의 정보가 변경되었다는 사실을 모른 체 가짜 사이트를 이용하기 때문에 자신의 개인정보가 쉽게 노출 됨.

그림 16-6 파밍(pharming)

SECTION 01

해킹과 보안

- DNS의 정보를 변경하는 해킹 기법을 **스푸핑**Spoofing이라 부름.
- 스푸핑은 여러 가지 의미로 사용되는데, 파밍과 같이 가짜 웹사이트를 만들어 놓고 사용자들의 방문을 유도하거나, TCP/IP의 구조적 결함을 이용해 사용자의 정보를 탈취하는 해킹 기법을 의미.
- DNS를 변경하는 것을 DNS 스푸핑이라고 하며, MAC 주소를 속여 네트워크의 정보를 탈취하는 방법을 ARP 스푸핑이라 부름. IP 주소를 속여 패킷을 탈취하는 기법을 IP 스푸핑이라 부름.

- 피싱과 파밍의 차이점

표 16-1 피싱과 파밍의 차이

	피싱(phishing)	파밍(pharming)
수법	사용자를 속여 가짜 사이트에 접속하도록 유도하거나 돈을 지불하게 하는 방법	DNS를 변경하여 가짜 사이트에 접속
수단	이메일 발송	DNS 변조
피해	사용자의 자각에 의해 피해를 막을 수 있음	사용자가 자각할 수 없어 피해규모가 큼

SECTION 01

해킹과 보안

- **스미싱**smshing은 문자메시지 SMS와 phishing이 결합된 피싱기법이다. 주로 스마트폰의 문자 메시지를 통해 가짜 사이트로 유도.
- 용자가 문자 메시지에 포함된 주소를 클릭하게 되면 가짜 사이트로 이동하여 개인정보를 입력 시키거나, 스마트폰에 해킹용 소프트웨어를 설치하여 개인정보를 탈취.
- 스미싱과 유사한 피싱 방식으로 인터넷 전화VoIP를 이용하여 사용자의 개인정보를 탈취하는 해킹 수법을 비싱vishing(VoIP + phshing)이라 부름.

표 16-2 스미싱 메시지의 예

스미싱 메시지의 예
• 당신의 카드가 해외에서 $540불 결제되었습니다. 내용을 확인하려면 아래 주소를 클릭하세요.
• 사건번호 23453번 고소장이 접수되었습니다. 고소장 내용을 아래 주소에서 확인할 수 있습니다.
• 작년에 내신 세금 중 환급금이 있습니다. 환급금 명세는 아래 주소에서 확인할 수 있습니다.

SECTION 01

해킹과 보안

4. 디도스

- 도스Denial of Service; DoS라 일컫는 서비스 거부 공격은 서버 쪽에 많은 양의 패킷을 보내어 다른 사람이 서버를 이용하지 못하도록 막는 해킹수법.
- 분산형 서비스 거부 공격, 디도스(DDOSDistributed DoS)는 일반인들의 컴퓨터를 바이러스에 감염시켜 자신이 조정할 수 있는 좀비 컴퓨터로 만든 후, 수백 대의 좀비 컴퓨터가 감염되면, 공격자는 같은 시간에 한 서버를 공격하도록 명령을 내림.
- 도스와 달리 디도스의 경우 여러 곳에서 공격하기 때문에 이를 방어하기가 매우 어려움.

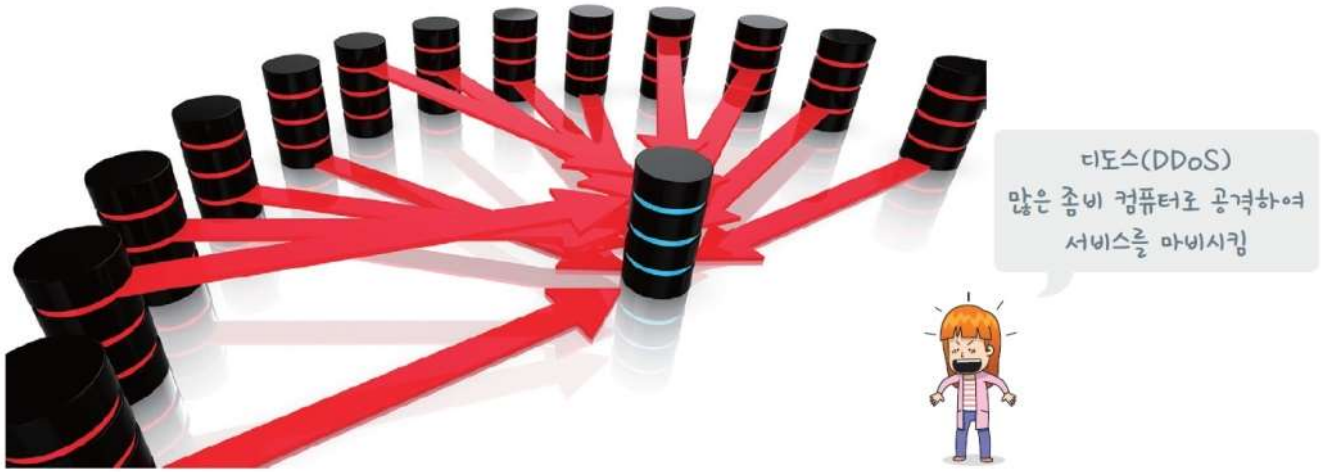


그림 16-7 디도스 공격

SECTION 01

해킹과 보안

5. 위조 및 변조

- 오프라인에서는 위조/변조/저작권 침해에 대한 방지책으로 복사 방지 기술이 사용.
- 신용카드나 출입카드에도 복사 방지 보안 기술이 적용됨. 과거에는 카드 내 마그네틱에 정보를 넣어 이를 읽는 방식을 사용했으나 현재는 암호화된 특수 칩과 RFID 기술을 사용하는 카드가 대중화되었음.

(a) 형광 잉크 (b) 홀로그램 (c) 복사 방지용 은선

그림 16-8 지폐에 적용된 복사 방지 기술

(a) 마그네틱 신용카드 (b) 암호화된 특수 칩이 내장된 신용카드

그림 16-9 신용카드 보안 기술

SECTION 02

암호화와 프로토콜

1. 암호화 이해하기

- **암호화**encryption란 원래의 데이터를 풀기 어려운 패턴으로 변형시켜서 허가받은 사용자 외에는 볼 수 없게 만드는 기술.
- 암호화에는 평문plaintext(원문)과 암호문ciphertext을 만들기 위한 키key가 필요 -> 평문에 키를 적용시키면 암호문 -> 암호문을 푸는 키를 적용시키면 평문으로 돌아오는데 이를 복호화decryption라 부름.
- 'LOVE'라는 단어를 암호화하는 경우 각 문자에 +5를 하여 암호를 만들면 'QTAJ'가 됨. 이때 +5는 키.
- 복호화를 위해서는–5를 연산을 하면 평문인 'LOVE'가 됨.

그림 16-10 암호화와 복호화

SECTION 02

암호화와 프로토콜

- 암호화 기술은 크게 대칭키 암호화와 비대칭키 암호화로 나눔.
- **대칭키 암호화**는 하나의 키로 암호화 혹은 복호화 하는 방식 -> 단일키 암호화 혹은 비밀키 암호화라고도 부름.
- 하나의 키만 사용하는 대표적인 알고리즘으로 DES(Data Encryption Standard)가 있음 -> 더 강력한 단일키 암호화 방식인 AES(Advanced Encryption Standard)로 대체 됨.
- 대칭키(단일키) 암호화 방식의 가장 큰 단점은 암호화로 만들어진 결과물(암호문)과 함께 키도 같이 전달해야 한다는 것 -> 키가 다른 사람에게 노출될 경우 암호문이 깨질 수 있음 -> 키를 소유한 사람이 나쁜 마음을 먹는다면 해당 키로 다른 암호문을 해독하는 데 사용할 수도 있음.

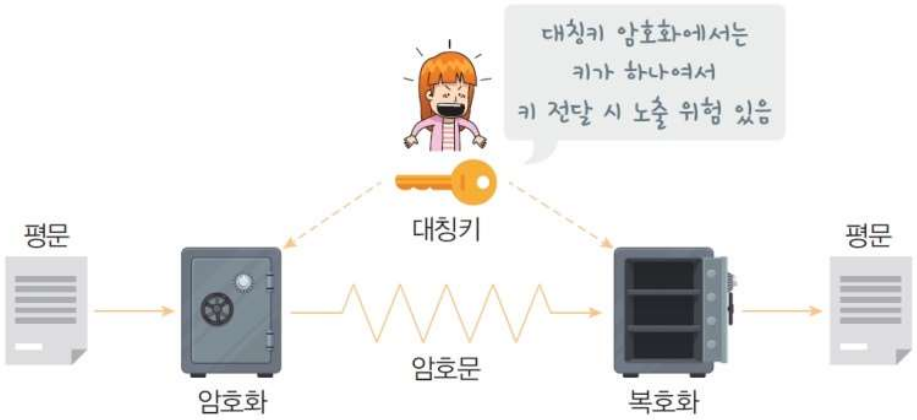


그림 16-11 대칭키 암호화

SECTION 02

암호화와 프로토콜

- **비대칭키 암호화**에서는 공개키public key와 개인키private key의 두 개의 쌍으로 키가 구성 -> **공개키 암호화**라고 부름.
- 개키는 암호문을 만들려는 사람에게 공개해주는 키->암호를 해독할 수는 없음 -> 암호를 해독하는 키는 개인키로만 가능 -> 공개키 암호화는 암호를 만드는 키와 암호를 푸는 키가 서로 다르기 때문에 비대칭 방식이라 부름 -> 대칭키 방식에서의 키를 안전하게 나눠주는 문제를 해결.
- 비대칭 암호화 알고리즘으로 RSA 방식이 있으며 전자서명 등에 광범위하게 활용되고 있음.
- 비대칭 키의 단점은 계산량이 월등히 많아 컴퓨터 자원을 많이 소비한다는 것.

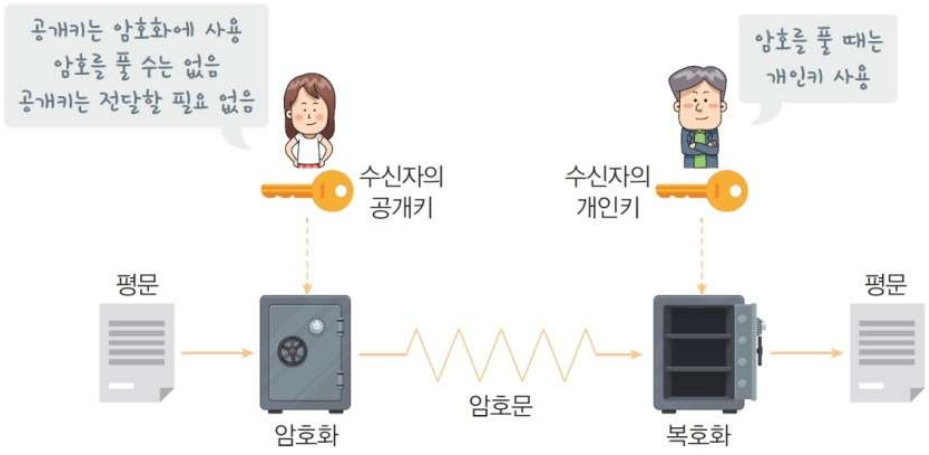


그림 16-12 비대칭키 암호화

SECTION 02

암호화와 프로토콜

2. 암호화 알고리즘

- **치환암호**substitution cipher는 문자를 다른 문자로 대치하는 암호 방식이다. 앞서 'LOVE'에 +5를 'QTAJ'를 만들었는데 이것이 치환암호 -> 덧셈연산(+5)을 사용하였기 때문에 이를 **덧셈암호**additive cipher 혹은 **쉬프트 암호**shift ciper라고 부름.
- 로마의 황제였던 줄리어스 시저Julius Caesar가 사용해서 유명해졌기 때문에 시저암호라고도 불림.

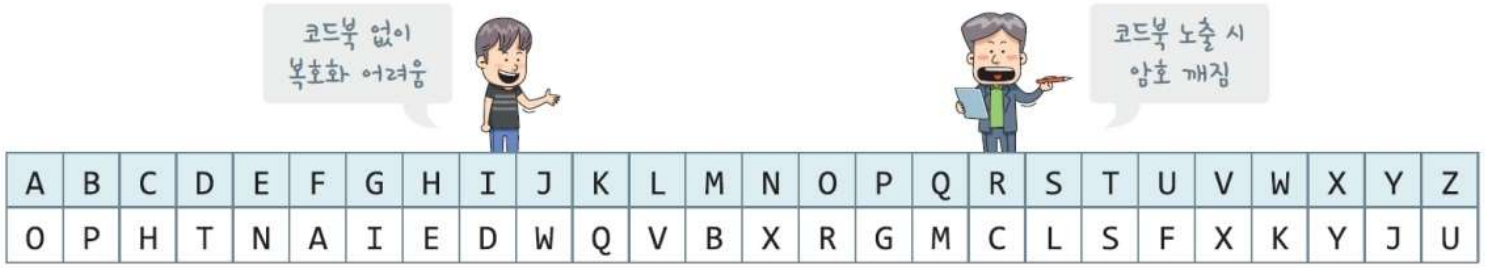
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

그림 16-13 덧셈 암호(시프트 암호)

SECTION 02

암호화와 프로토콜

- **코드북 암호**code book ciper은 다음 표와 같이 무작위로 만들어진 코드북을 서로 공유하여 암호화 및 복호화를 하는 방식.
- 단일키의 역할을 하는 코드북이 없다면 암호를 푸는 것은 상당히 어려움 -> 그러나 코드북이 노출되는 경우, 쉽게 암호가 풀리는 단점이 있음.



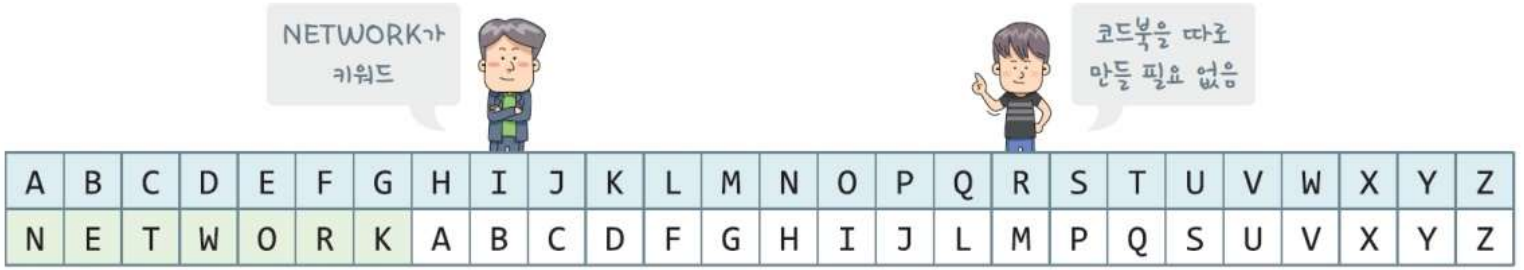
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	P	H	T	N	A	I	E	D	W	Q	V	B	X	R	G	M	C	L	S	F	X	K	Y	J	U

그림 16-14 코드북 암호

SECTION 02

암호화와 프로토콜

- 코드북 방식을 보완하는 다양한 치환암호 방식이 개발 되었음.
- 키워드 암호화는 양쪽이 아는 키워드를 사용하여 문자를 암호문자로 변환하는 방법.
- 다음 그림 은 NETWORK 키워드를 사용하여 만들어진 문자 변환표 -> 맨 앞에 NETWORK 워드를 배치하고, 나머지 알파벳으로 채워짐.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	E	T	W	O	R	K	A	B	C	D	F	G	H	I	J	L	M	P	Q	S	U	V	X	Y	Z

그림 16-15 키워드 암호

SECTION 02

암호화와 프로토콜

- **전치암호**transposition cipher는 문자의 위치를 변경하여 암호를 만드는 방식이며, 위치암호라고도 부름.
- 전치암호에서 키는 바뀌는 위치정보.
- 다음 그림은 COMPUTERNETWORK를 5개씩 나누어 전치 암호방식으로 암호화 및 복호화 과정을 나타냄.

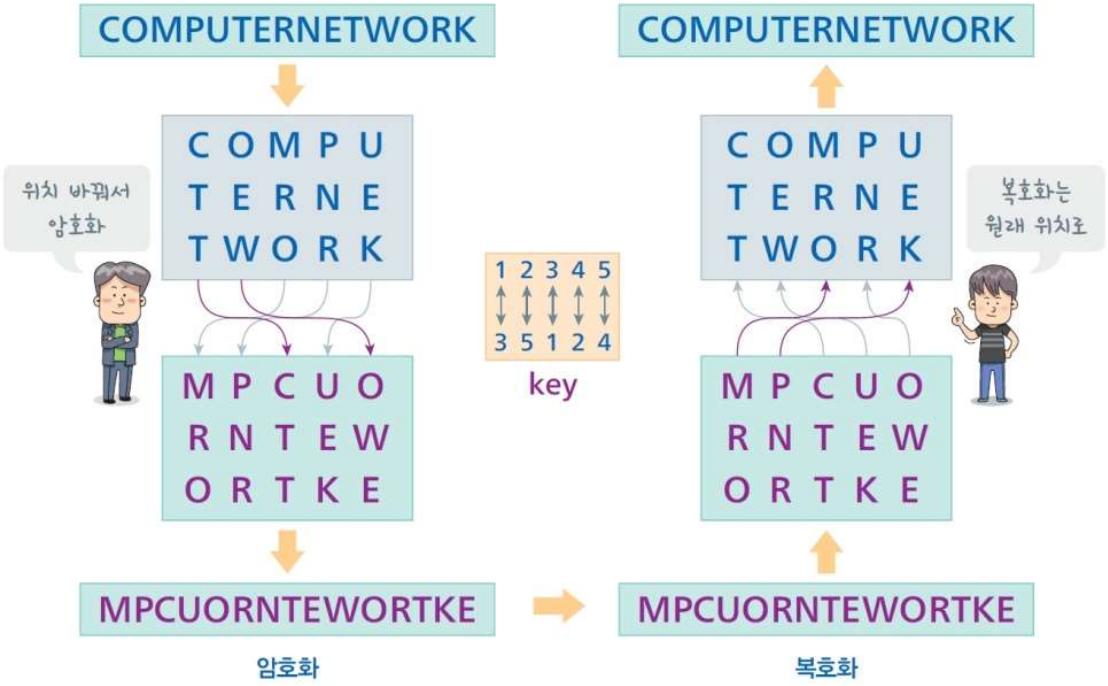


그림 16-16 전치 암호

SECTION 02

암호화와 프로토콜

3. 보안 프로토콜

- 웹은 연구자들이 연구결과를 공유하거나 정보교환 목적으로 만들어졌기 때문에 모든 데이터를 암호화할 필요성이 없었음. 그래서 웹에서 오고가는 데이터는 쉽게 그 내용을 확인 할 수 있음 -> 보안 프로토콜을 사용하여 전체 네트워크의 안전을 지키는 추세로 발전.
- 통신의 기본이 되는 것은 소켓이다. 공개키 암호화를 사용하여 사용자를 인증하고, 소켓의 데이터를 암호화 하는 프로토콜이 **SSL**이며, Secure Sockets Layer의 약자.
- TLS Transport Layer Security은 SSL 보다 강화된 보안 프로토콜.
- SSL이 보안 프로토콜의 시초였으며, 많은 사람들이 아직도 SSL을 표준으로 알고 있기 때문에 웹에서 사용하는 암호화 프로토콜을 SSL이라 부르지만 실제로는 TLS가 업계의 표준. 따라서 TLS 대신 SSL이라 부르기도 하고 SSL/TLS를 같이 표시하기도 함.

SECTION 02

암호화와 프로토콜

- **HTTPS**는 TTPS는 HTTP with Secure 혹은 HTTP with SSL의 약자이며, HTTP를 보안 프로토콜 위에 구축하여 안전한 웹 사용을 가능하게 만들어줌.
- HTTP의 경우 전송되는 데이터가 암호화 되지 않기 때문에 해커들이 모든 데이터를 확인 할 수 있음 -> HTTPS가 보안문제 해결.
- A클라이언트와 통신을 하는 도중에 해커가 마치 A클라이언트가 보낸 데이터인 것처럼 패킷을 만들어 서버에게 전송할 수 있음으로 A클라인언트가 보낸 데이터라는 것을 서버가 확인 할 수 있어야 함 -> HTTPS는 디지털 서명을 교환함으로써 데이터의 무결성을 확인.
- HTTPS는 사설 인증기관Certificate Authority(CA)을 통해 방문한 사이트가 진위여부 확인.

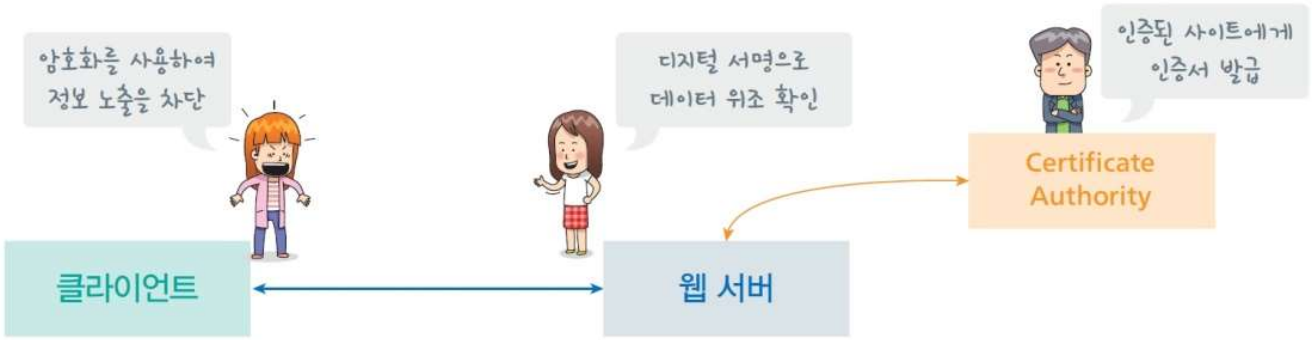


그림 16-17 HTTPS의 역할

SECTION 02

암호화와 프로토콜

SSL의 동작과정은 핸드쉐이트(협의) -> 세션 시작 -> 세션종료.

1. 클라이언트가 서버에게 Hello 메시지를 보냄. 메시지에는 클라이언트가 임의로 생성한 데이터(임의 데이터 1)와 클라이언트가 사용 가능한 암호화 방식 후보가 명시되어 있음.

2. 서버는 클라이언트에게 Server Hello 메시지를 보냄. Server Hello 메시지에는 서버가 임의로 생성한 데이터(임의 데이터 2)와 앞으로 사용할 암호화 방식을 결정하여 보내줌. 또한 CA로부터 받은 인증서를 클라이언트에게 전달.

3. 클라이언트는 서버로부터 받은 인증서가 유효한지를 확인.

그림 16-19 SSL 동작 과정

SECTION 02

암호화와 프로토콜

- SSL에서 통신에 사용하는 암호화 알고리즘으로 대칭키 방식을 사용 -> pre master secret key.
- 암호문과 pre master secret key를 묶어서 다시 공개키로 암호화 하여 서버에게 전달.
- 인증서를 확인한 이후에 그 안에 있는 공개키를 사용하여 암호문과 pre master secret key를 다시 암호화 한 후 서버에게 전달 -> 서버는 클라이언트로부터 전달 받은 데이터를 개인키로 암호화.
- pre master secret key를 사용하여 암호문을 복호화 하여 평문(임의 데이터 1 + 임의 데이터 2)이 얻어지는지를 확인.
- 정상적으로 복호화 되었다면 클라이언트와 서버사이에 오고가는 모든 데이터는 pre master secret key로 암호화되고 또한 복호화 됨.

그림 16-20 SSL의 핸드쉐이크 단계에서의 암호화 방법

SECTION 03

보안 기술

1. 인증 기술

- 인증은 대표적인 보안 기술로 자기 자신을 증명하는 기술이다. 인증기술의 대표적인 경우가 패스워드이며 본인임을 입증하는 가장 기본적인 방법임.
- 구글 크롬의 [설정] - [보안 및 개인정보 보호] 페이지에서 유출된 비밀번호를 확인 할 수 있음.

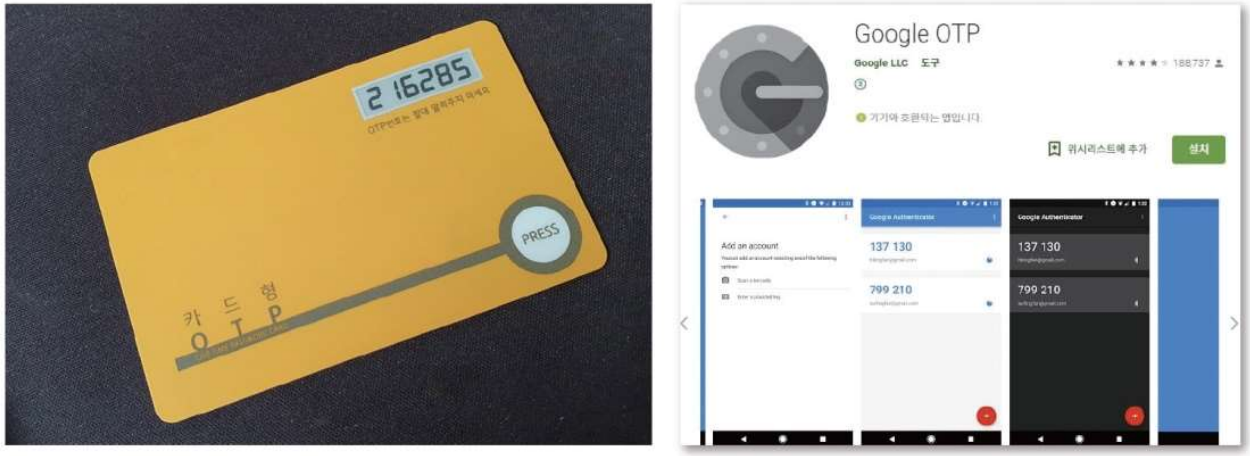
그림 16-21 패스워드 인증

그림 16-22 크롬의 유출된 비밀번호 확인 페이지

SECTION 03

보안 기술

- 개인이 아무리 노력한다고 해도 시스템의 정보가 노출된 경우 패스워드도 같이 노출될 가능성이 있음.
- 이러한 문제를 해결하는 방법으로 일정 시간만 쓰고 버리는 패스워드가 **OTP**One Time Password



(a) 배터리형 OTP (b) 구글 OTP

그림 16-23 OTP의 종류

SECTION 03

보안 기술

- 바이오 인증이란 지문 인식, 안면 인식, 홍채 인식과 같이 사람의 신체를 이용하여 인증하는 방식.
- 바이오 인증방식은 OTP와 같이 특수한 장치를 따로 휴대할 필요가 없고, 복사가 어려워 미래 기술로 각광을 받고 있음.
- 금융과 관련된 기술을 '금융FINancial+기술Technology=핀테크'라 부르는데, 바이오 인증 분야는 핀테크 기술의 핵심 기술로 각광을 받고 있음.

(a) 지문 인식 (b) 안면 인식

그림 16-24 바이오 인증 기술

SECTION 03

보안 기술

- **공동인증서**란 한국에서 금전거래를 할 때 공인된 기관에서 인증한 전자서명을 가리킨다. 앞서 SSL에서 설명한 인증서는 인증기관(CA)이 사이트에게 발행해 주는 인증서.
- 과거에는 공인인증서라 불렀으며 인터넷 뱅킹이나 인터넷 쇼핑몰에서의 실시간 결제에 주로 사용됨.

그림 16-25 공인인증서 화면

SECTION 03

보안 기술

2. 보안 관련 소프트웨어

백신은 악성 소프트웨어로부터 자신의 컴퓨터나 스마트폰을 지키기 위해서 사용하는 프로그램.

그림 16-26 백신 성능 테스트 사이트(https://av-test.org)

SECTION 03

보안 기술

- **방화벽**, 영어로 firewall은 미리 정의된 보안 규칙을 사용하여 네트워크에서 전송되는 데이터들을 점검하고 제어하는 네트워크 보안 시스템.
- 방화벽이라는 용어는 원래 건물 내 화재가 번지는 것을 막기 위해 설치된 방벽을 의미 -> 방화벽의 역할은 신뢰 수준이 낮은 네트워크로(보통의 경우 인터넷)부터 오는 해로운 트래픽이 신뢰 수준이 높은 네트워크(내부 망)로 들어오지 못하게 막는 것.

그림 16-27 방화벽

SECTION 03

보안 기술

- 초창기 방화벽은 패킷 자체만을 살펴보고, 미리 설정된 정책에 따라 허용 또는 거부를 결정하는 패킷필터 방식 -> 모든 패킷을 검사하므로 검사규칙이 많아질수록 처리속도가 느려지는 단점.
- 패킷필터 방식의 단점을 해결하는 스테이트 풀state full 검사방식이 개발 됨.
- 기존의 패킷 필터 기반 방식에서 더 나아가 애플리케이션에 어떠한 영향을 미칠지를 분석하는 방화벽도 출현하였음.
- 많은 방화벽은 네트워크 주소 변환Network Address Translation; NAT 기능을 가짐 -> 내부 네트워크에서 사용하는 IP 주소와 외부에 드러나는 주소를 다르게 유지하여 내부 네트워크를 숨김.

그림 16-28 윈도우 방화벽 설정 화면

SECTION 03

보안 기술

- 키보드가 버퍼를 사용하는데 버퍼 내용 중 아이디, 패스워드, 계좌 정보와 연관된 데이터를 해커에게 전달하기 위하여, 바이러스나 트로이목마와 같은 악성 소프트웨어들은 키보드 버퍼를 훔쳐봄 -> 이를 막기 위하여 Touch EN과 같은 키보드 보안 프로그램이 설치 됨.
- 인증서 암호를 입력할 때에 키보드의 보안을 위하여 버퍼를 사용하지 않는 가상 키보드를 제공하기도 함.

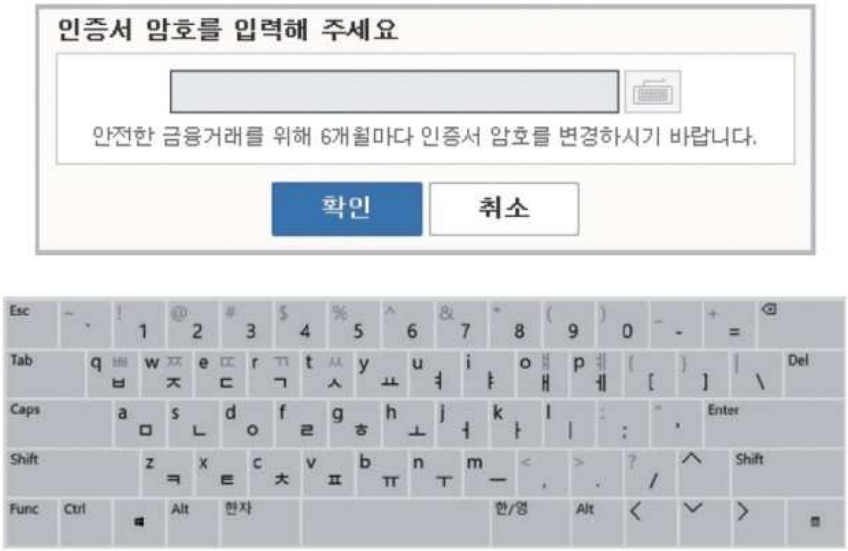


그림 16-29 가상 키보드 화면

SECTION 03

보안 기술

3. 콘텐츠 유출 방지 기술

- **DRM**Digital Rights Management이라 불리는 디지털 권리 관리 기술은 디지털 콘텐츠를 무단으로 사용하는 것을 막기 위한 보안기술 -> DRM은 적법한 콘텐츠의 사용은 허락하지만, 그 외의 사용을 막는 기술
- DRM 기술은 회사의 문서 관리에 많이 적용됨. 문서에 대한 권한이 있는 사용자를 구분하여 문서에 대한 작업을 제한하는 것이 DRM.
- 멀티미디어 데이터에도 DRM이 사용된다. 인터넷을 통해 구매한 음악 파일이나 영화 파일의 경우, DRM 기술이 적용되어 허가되지 않는 컴퓨터나 기기에서 볼 수 없게 막아 놓았음.
- 디지털 워터마크란 어떤 파일에 관한 저작권을 식별할 수 있도록 특수하게 삽입된 패턴을 의미.

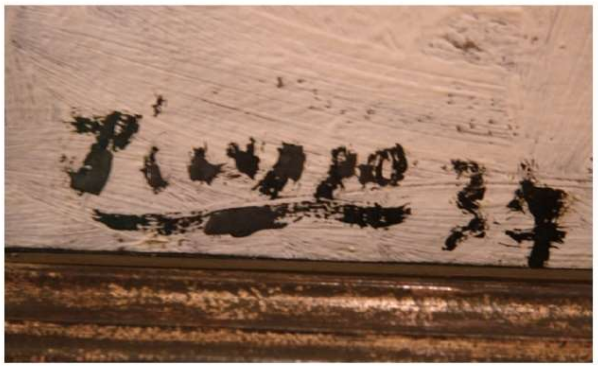


그림 16-30 피카소의 사인