




인증 기술

2024. 9

컴퓨터·소프트웨어공학과
이 형 효
(hlee@wku.ac.kr)

정보보호 목적(1)

- 비밀성(**C**onfidentiality, Secrecy) 
 - 비인가 사용자에게 의한 정보 조회 방지
- 무결성(**I**ntegrity) 
 - 비인가 사용자에게 의한 정보 변경 방지
 - 적법한 사용자에게 의한 부적절한 정보변경 방지
- 가용성(**A**vailability) 
 - 적법한 사용자에게 대한 서비스 거부 방지
 - The property that a product's services are accessible when needed and without undue delay

과도한, 심한, 지나친

정보보호 목적(2)

■ 책임성(Accountability)

- 자신이 수행한 작업에 대한 **책임 부과**
- 사용자가 실행한 작업의 내역(**로그, log**) 이용
- 일상생활에서 디지털 작업의 일상화로 그 중요성 증가

디지털포렌식(digital forensics)

전자적 증거물 등을 사법기관에 제출하기 위해
데이터를 수집, 분석, 보고서를 작성하는 일련의 작업

■ 신뢰성(Reliability)

- 불의의 사고, 고장에 대한 대처 기능

컴퓨터 보안 정의

■ Computer Security

- Computer security deals with the ^{다루다} **prevention** ^{방지} and **detection** ^{탐지} of **unauthorized actions by users** ^{허가되지 않은, 비인가된} of a computer system



■ 그러나

- 보안에 대한 유일한 정의는 존재하지 않음
- 책이나 문서마다 사용하는 정보보안에 대한 정의가 서로 다를 수 있음

컴퓨터 보안의 오버헤드 비용, 부담

- 컴퓨터 보안기능 실행 위한 컴퓨팅 자원 추가
 - CPU time, Memory, S/W 등
- 사용자에게 사용의 불편함 초래
 - Tradeoff between *security* and *ease-of-use* 교환, 거래 사용 편리성
- 보안 관리를 위한 비용
 - 우수한 GUI(Graphical User Interface)를 가진 보안 그래픽 사용자 인터페이스 제품 구입
- 보안은 이러한 오버헤드를 부담할 만한 가치가 있음

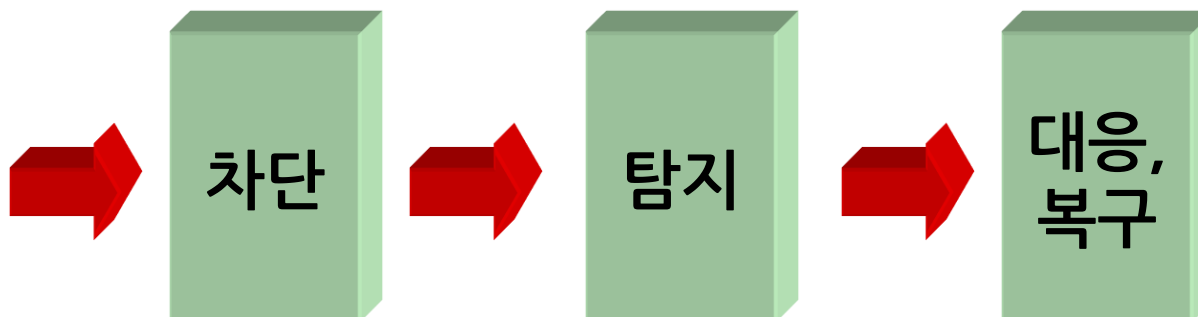
정보보호 조건

- 보호대상의 자산(**Asset**) 
 - 보호할 가치를 가진 보호대상이 존재
 - 컴퓨터, 통신망, 정보 등
- 시스템의 취약성(**Vulnerability**) 
 - 완전하지 않은 시스템의 보안
 - 하드웨어 또는 소프트웨어의 결함, 오작동, 관리부실
- 해커로부터의 위협(**Threats**) 
 - 보호대상에 대한 내부 또는 외부로부터의 위협 존재
 - 해커 또는 내부의 공격자

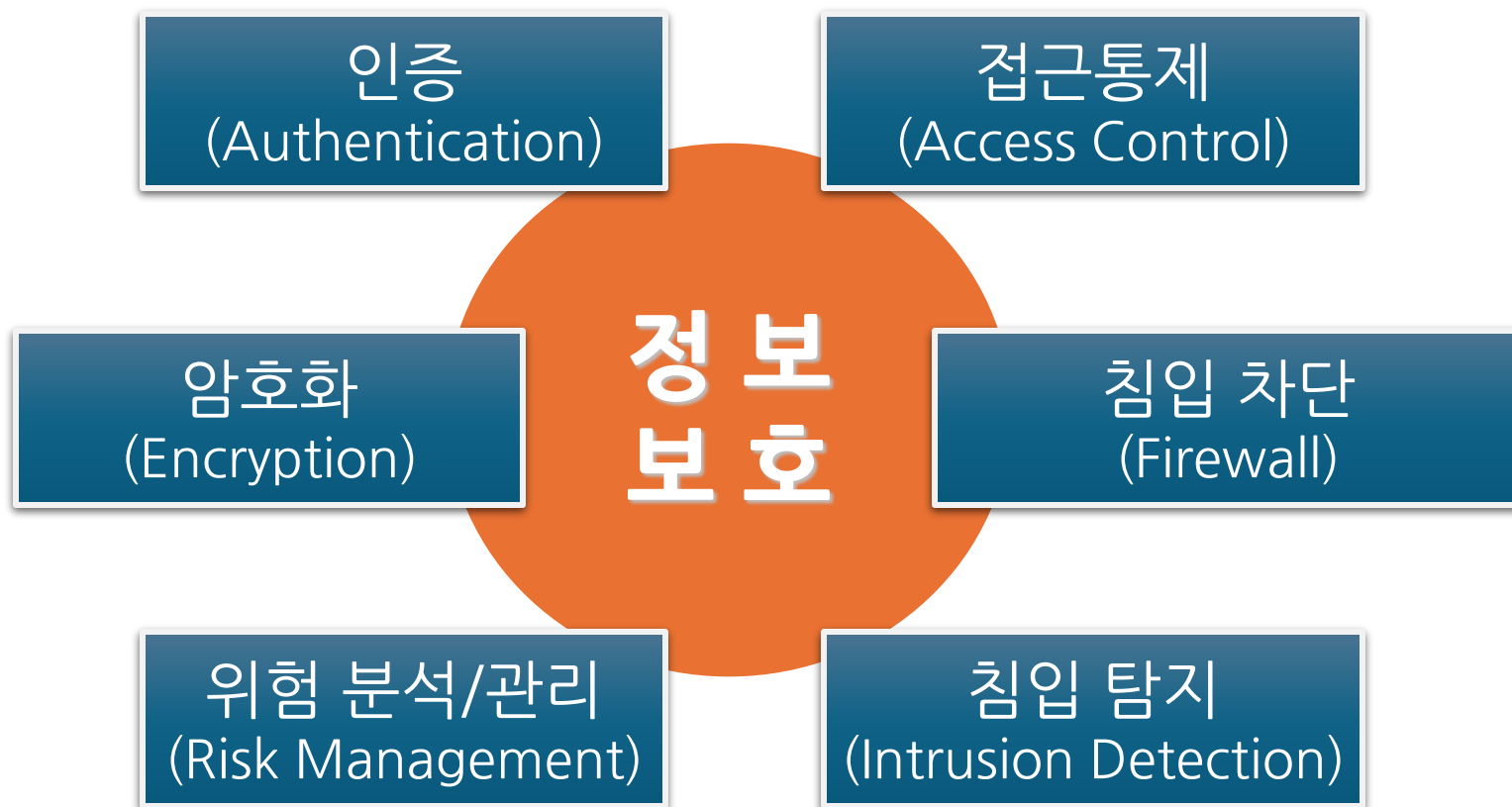
정보보호 방법, 절차

- 차단
 - 암호 기술, 방화벽(Firewall)
- 탐지(Detection)
 - 침입탐지시스템(IDS: Intrusion Detection System)
- 대응(Response), 복구(Recovery)
 - 침입 피해에 대한 대응 또는 복구

Hacker



정보보안 기술



정보보호 용어 정의(1)

- 인증(Authentication)
 - 사용자 신분 확인
- 접근통제(Access Control)
 - 신분이 확인된 사용자의 정보에 대한 접근권한 확인
- 암호화(Encryption)
 - 비인가 사용자가 정보를 조회할 수 없도록 자료를 다른 형태로 변형하는 작업
- 복호화(Decryption)
 - 암호화의 역과정

정보보호 용어 정의(2)

■ 침입차단시스템(Firewall)

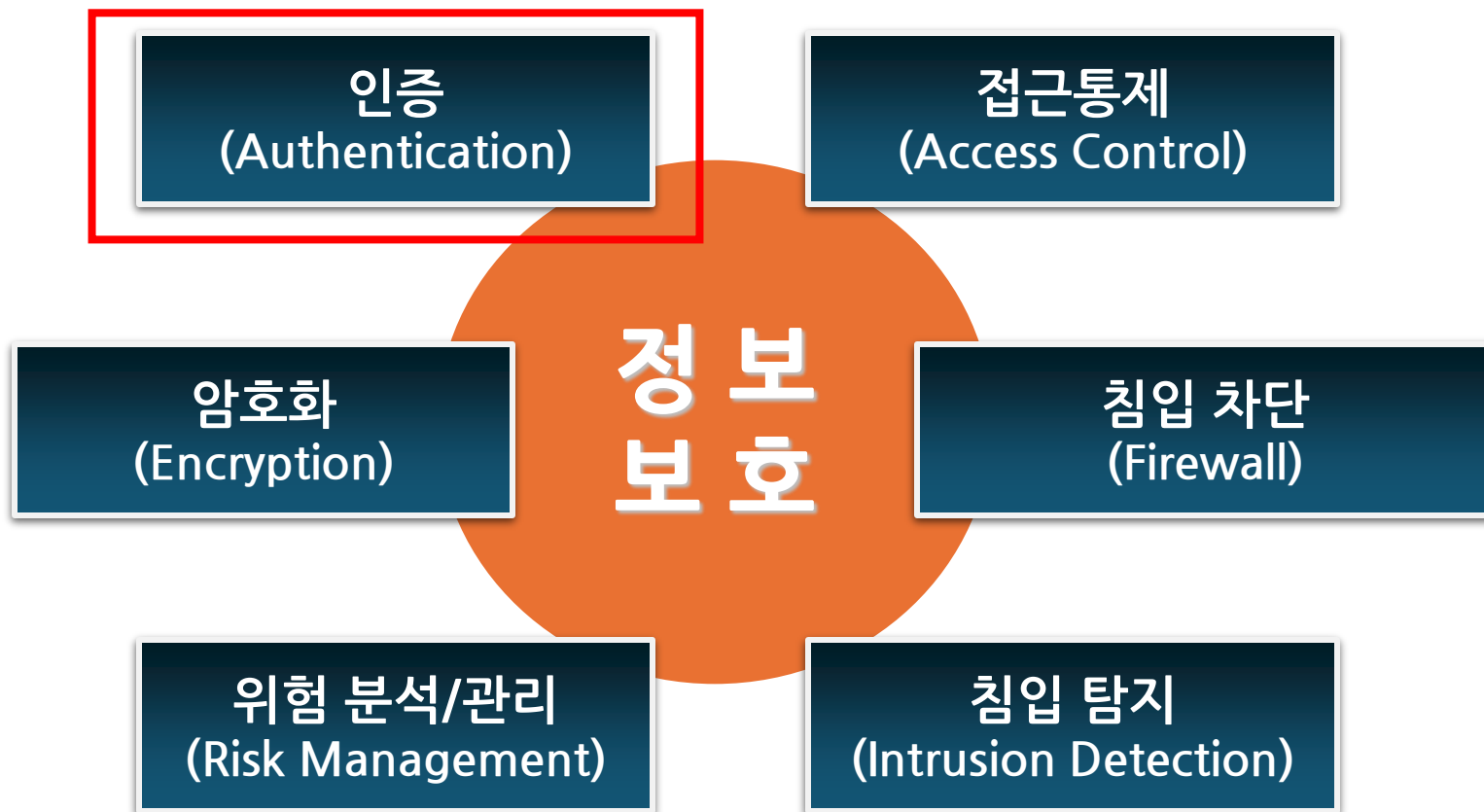
- 허용되지 않은 시스템으로부터의 접속 차단
- 하드웨어(H/W)와 소프트웨어(S/W)로 구성
 - ✓ 예: 라우터를 통한 패킷 필터링 방식

■ 침입탐지시스템(IDS)

- Intrusion Detection System
- 시스템에 침입한 불법 사용자를 탐지하여 경고 발생

인증 (Authentication)

정보보안 기술 - 인증



인증(Authentication)(1)

- 사용자의 신분을 확인하는 절차
- 필요성(인증결과의 활용)
 - 인증 이후 사용자의 권한을 확인하는 데 사용
 - 사용자의 사용기록(로그) 작성에 사용
- Identification vs. Authentication
 - Identification: announce who you are
 - Authentication: prove that you are who you claim to be

인증(Authentication)(2)

웹정보서비스

✉ 웹정보서비스 아이디

🔒 비밀번호

로그인

회원가입

아이디 찾기 | 비밀번호 찾기


원광대학교
WONKWANG UNIVERSITY

- 원광대학교 교내 소프트웨어설치 안내
- 불법소프트웨어 사용 및 지적재산권에 대한 안내
- 원광대학교 알리미 설치 안내
원광대 알리미는 구글 PLAY스토어나 애플 APPSTORE에서 다운로드 받으실 수 있습니다
- 웹메일(Office365) 사용안내

Identification?

Authentication?

14/48



인증 (Authentication)(3)

실생활에서의 식별 사례

실생활에서의 인증 사례

인증(Authentication)(4)

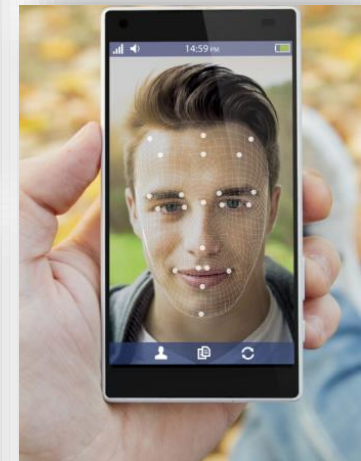
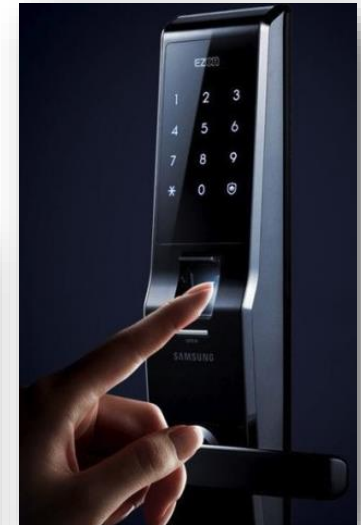
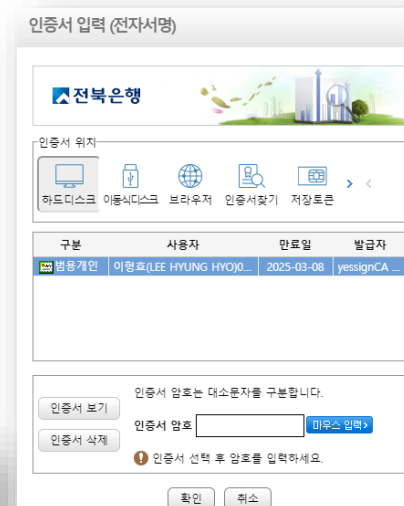
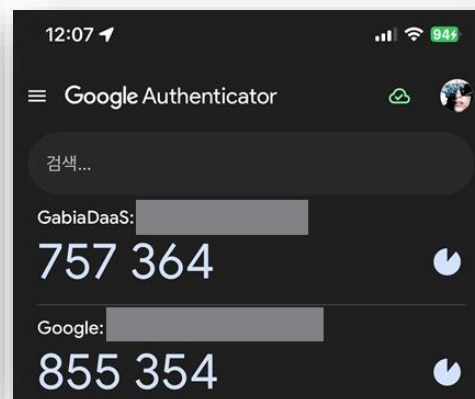
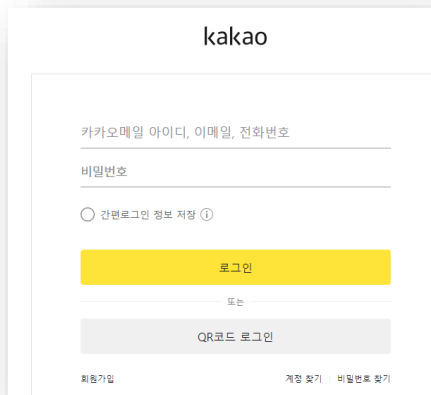
■ 인증 (Authentication)

- 컴퓨터 **사용자**의 **신원**을 **확인**하는 절차

✓ *something you **know***

✓ *something you **have***

✓ *something you **are***



인증 방식(1)

- 특별한 정보를 알고 있는지
 - Something you know
 - ID/PASSWORD
- 특별한 물건을 가지고 있는지
 - Something you hold (have)
 - 스마트폰, OTP 단말기, 열쇠, 신분증
- 특별한 신체적 특성을 가지고 있는지
 - Something(Who) you are
 - 지문, 홍채, 정맥, DNA, ... (생체인식 biometrics)

인증 방식(2)

- 특별한 행동특성을 보이고 있는지
 - What you do
 - 타이핑 속도와 시간 간격
- 특별한 장소에 있는지
 - Where you are
 - 사용자의 컴퓨터 접속 장소 (GPS 정보)

인증 방식(3)

■ 다중 요소 인증

- MFA(Multi-Factor Authentication)
- 2FA (2-Factor Authentication)
- 서로 다른 인증 방식 2개 이상을 적용한 인증 방식
 - ✓ (O) Something you **know** + Something you **have**
 - ✓ (O) Something you **know** + Something you **are**
 - ✓ (O) Something you **have** + Something you **are**
 - ✓ (O) Something you **know** + Something you **have** + Something you **are**
 - ✓ (X) Something you **know** + Something you **know**
 - ✓ (X) Something you **have** + Something you **have**

전통적 인증방식 취약점

- 물리적 신분증 조작/변조 사례



지문 인식 취약점(1)

- 지문 복제 사례



지문 인식 취약점(2)

- 가짜 손가락 이용 범죄 사례 (SBS, 2019)



홍채 인식 특징 및 취약점

■ 생체 인식 사례: 홍채(iris) 인식

- 홍채의 모양과 색, 모세혈관의 형태소를 분석하여 사람을 인식하는 기술
- 한 번 패턴이 완성되면 오랜 기간 동안 변하지 않은 특징
- 정확성이 우수한 생체기술로 평가



참고영상 (영화)

마이노리티 리포트
(2002)

독일 해커그룹(CCC),
사진으로 성 갤럭시 S8
홍채인식 뚫었다
(2017.5.24)

Username/Password 인증(1)

- 간단한 사용자 인증 방식
 - **Something you know** 방식
 - 정보보안의 첫 단계
 - 사용자에게 최소의 불편함 제공
 - 구현이 비교적 간단함
- Username 제시
 - Identification 과정
- Password 제시
 - Authentication 과정

Username/Password 인증(2)

■ 인증 과정

- 제시된 사용자ID/비밀번호 정보를 등록된 사용자ID/비밀번호 정보와 비교
- 패스워드 파일(Password file)
- Linux 시스템의 경우 /etc 디렉토리에 존재

■ 초기의 UNIX 계열 시스템

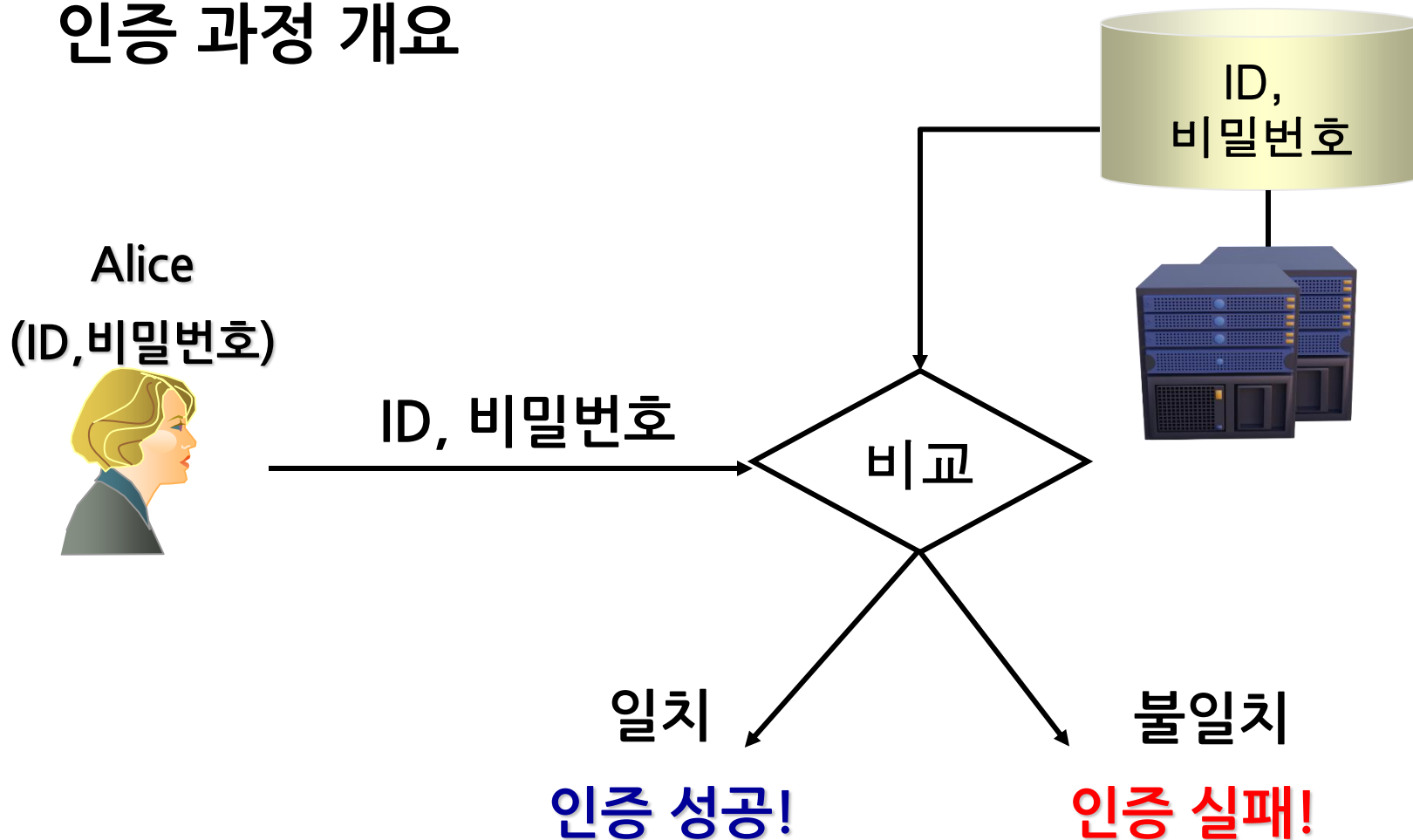
- 패스워드 파일 안에 암호화된 비밀번호 포함

■ 현재의 UNIX 계열, Linux 시스템

- 보안문제로 암호화된 비밀번호를 분리, 저장

Username/Password 인증(3)

- 인증 과정 개요



Username/Password 인증(4)

- 패스워드 파일 내용 예(/etc/passwd)

```
apache:x:48:48:Apache:/var/www:/bin/false
mailnull:x:47:47::/var/spool/mqueue:/dev/null
gdm:x:42:42::/home/gdm:/bin/bash
ident:x:98:98:pident user:/:/bin/false
rpc:x:32:32:Portmapper RPC user:/:/bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/bin/false
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
hlee:x:1001:1001:Lee, HyungHyo:/home/hlee:/bin/bash
[root@hlee hlee]#
```

사용자ID

Username/Password 인증(5)

- 암호화된 비밀번호가 저장된 파일 내용 예 (/etc/shadow)

```
ftp:!:11570:0:99999:7:::  
nobody:!:11570:0:99999:7:::  
nscd:!:11570:0:99999:7:::  
apache:!:11570:0:99999:7:::  
mailnull:!:11570:0:99999:7:::  
gdm:!:11570:0:99999:7:::  
ident:!:11570:0:99999:7:::  
rpc:!:11570:0:99999:7:::  
rpcuser:!:11570:0:99999:7:::  
xfs:!:11570:0:99999:7:::  
hlee:kCK9MAI6T5UEQ:11571:0:99999:7:::  
[root@hlee hlee]#
```

사용자ID

암호화된 비밀번호

Username/Password 인증(6)

- **일방 인증(Unilateral Authentication)**
 - 시스템 입장에서 사용자의 ID, 비밀번호만 점검
 - 사용자가 접속한 시스템에 대한 인증기능 없음
- **(참고) 상호 인증(Mutual Authentication)**
 - 시스템이 사용자를 인증하는 과정
 - 사용자가 시스템을 인증하는 과정
 - 속임 프로그램(spoofing program)에 대한 대응 방법

Username/Password 인증(7)

- 반복 인증(Repeated Authentication)
 - 세션의 시작뿐만 아니라 사용 중 일정기간마다 인증기능 수행
 - 예: 자동 화면잠금 후 비밀번호 입력 요구

Username/Password 인증(8)

- 보안 위협

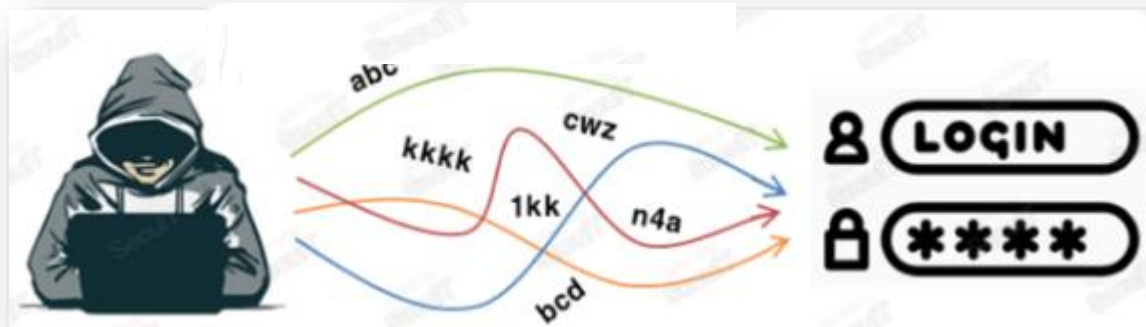
- 패스워드 추측(password guessing) 공격
- 로그인 프로그램 속임(login program spoofing) 공격

Username/Password 인증(9)

■ 패스워드 추측(password guessing) 공격

• Brute force 공격 (무차별 대입 공격)

- ✓ 가능한 모든 글자, 단어의 조합 이용



• 사전(Dictionary) 공격

- ✓ 사전(dictionary)에 나타난 모든 단어를 이용



Username/Password 인증(10)

- **패스워드 추측(password guessing) 공격 대응**
 - 모든 계정에 패스워드 설정
 - 긴 길이의 패스워드 사용
 - 대문자, 소문자, 숫자, 특수문자를 혼합한 패스워드 사용
 - 평범한 패스워드 사용 금지
 - ✓ 사전에 포함된 단어 사용 금지
 - 패스워드 aging (패스워드 유효기간 설정)
 - 로그인 시도 횟수 제한
 - 최종 로그인 성공시간, 접속 IP를 사용자에게 제공

Username/Password 인증(11)

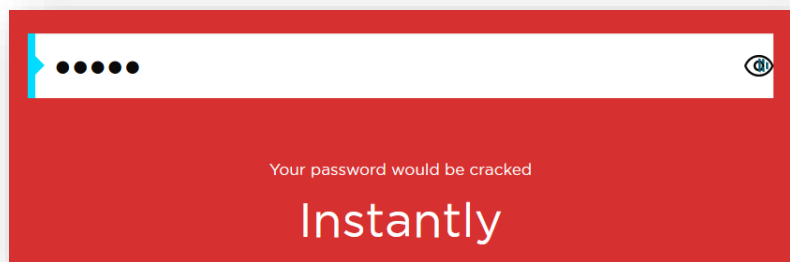
- 주어진 패스워드의 사전공격 취약점 점검 사이트
 - <https://www.security.org/how-secure-is-my-password/>



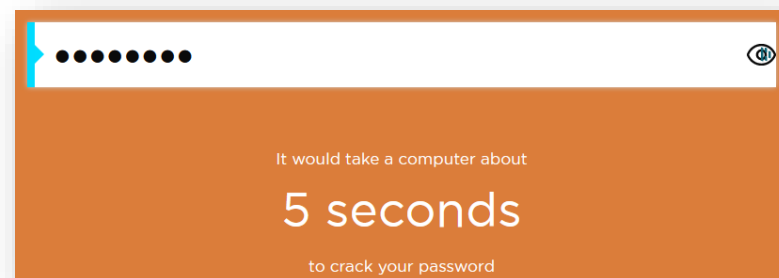
Username/Password 인증(12)

- 주어진 패스워드의 사전공격 취약점 점검 사이트

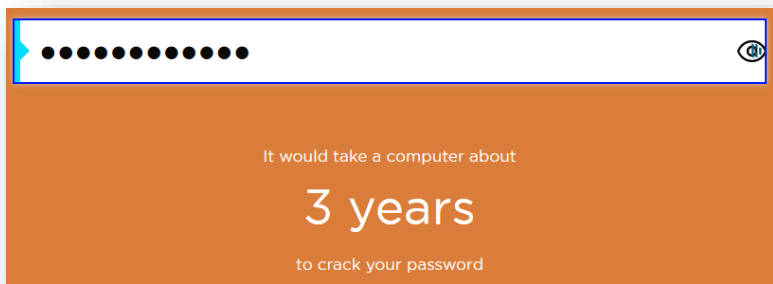
<apple>



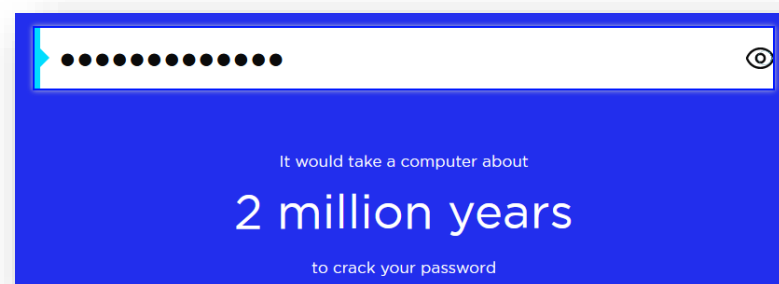
<wonkwang>



<wonkwang1234>



<HongGilDong@1>



Username/Password 인증(13)

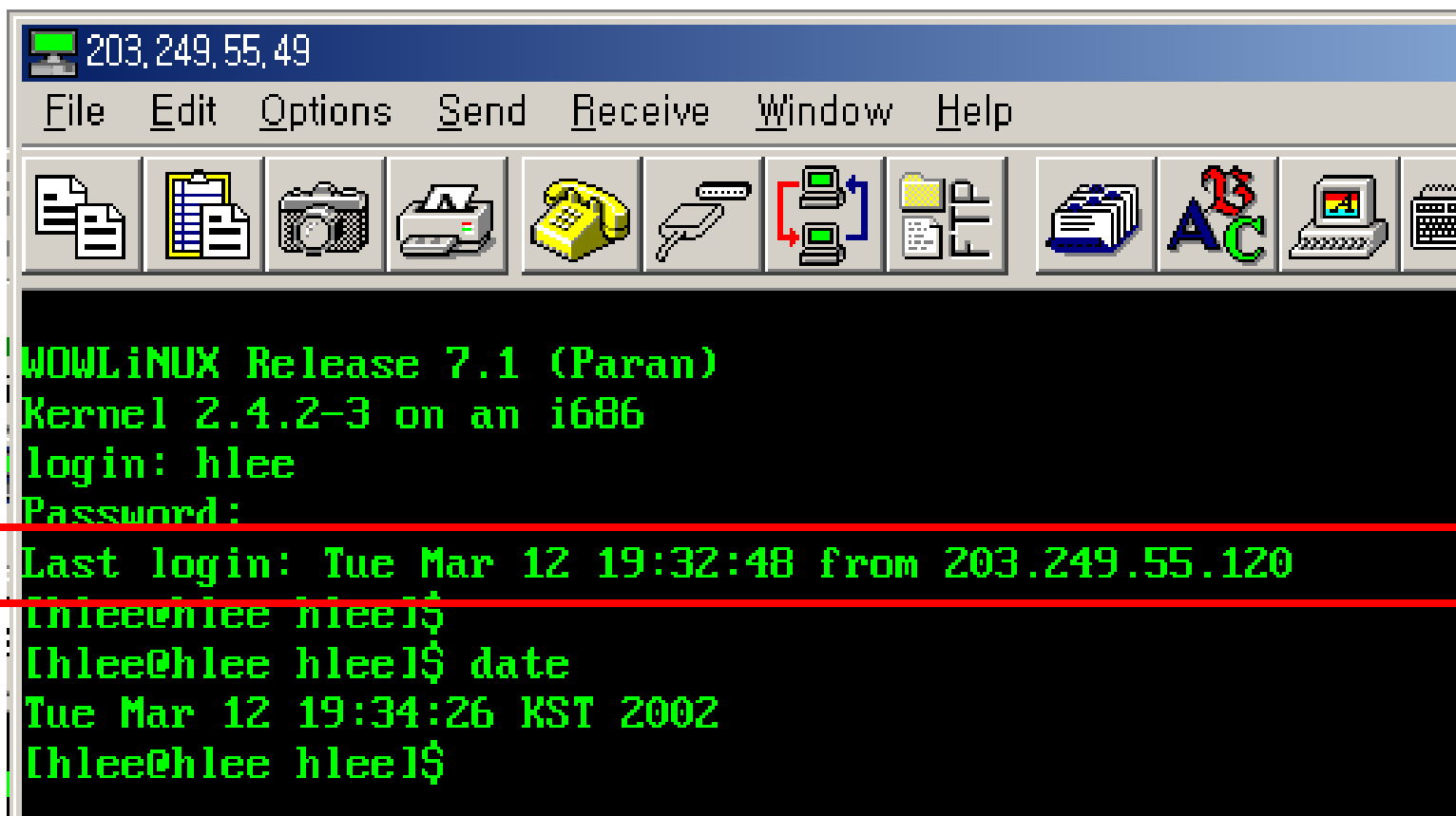
- Top weakest passwords

Top 10 Worst Passwords - Historic Analysis					
	2023	2015	2010	2005	2000
#1	123456	123456	123456	password	password
#2	123456789	password	password	123456	123456
#3	qwerty	12345	12345678	12345678	12345678
#4	password	12345678	qwerty	abc123	qwerty
#5	1234567	qwerty	abc123	qwerty	abc123
#6	12345678	1234567890	123456789	monkey	monkey
#7	12345	1234	111111	letmein	1234567
#8	iloveyou	baseball	1234567	dragon	letmein
#9	111111	dragon	iloveyou	111111	trustno1
#10	Covid	football	adobe123	baseball	dragon

© 2023 Copyright Janco Associates, Inc. – <https://e-janco.com>

Username/Password 인증(14)

- 패스워드 추측(password guessing) 공격 대응



```
203.249.55.49
File Edit Options Send Receive Window Help
[Icons: File, Edit, Options, Send, Receive, Window, Help, etc.]
WOWLinux Release 7.1 (Paran)
Kernel 2.4.2-3 on an i686
login: hlee
Password:
Last login: Tue Mar 12 19:32:48 from 203.249.55.120
[hlee@hlee hlee]$
[hlee@hlee hlee]$ date
Tue Mar 12 19:34:26 KST 2002
[hlee@hlee hlee]$
```

Username/Password 인증(15)

- 로그인 프로그램 속임(login program spoofing) 공격
 - Username/password를 확인하는 시스템(SW) 위장
 - ✓ 가짜 로그인 프로그램 실행
 - 사용자가 입력한 username/password 불법 취득
 - ✓ 사용자 패스워드 입수 후 가짜 로그인 프로그램 종료

Username/Password 인증(16)

로그인 프로그램 속임(login program spoofing) 공격



Username/Password 인증(17)

- 로그인 프로그램 속임(login program spoofing) 공격 대응
 - 로그인 성공 후 실패한 로그인 횟수 정보 제공
 - ✓ 로그인 실패 후 성공 한 세션에서 실패 로그인 횟수가 0이면
패스워드 속임 공격인지 의심, 점검 필요
 - 상호 인증(Mutual Authentication)
 - ✓ 사용자가 자신이 접속한 시스템을 인증하는 과정 추가

인증 종류

- **개체 인증(Entity Authentication)**
 - 사용자 또는 프로세스의 신분 확인
 - 예: Username/Password 인증
- **자료 출처 인증(Data Origin Authentication, Message Authentication)**
 - 자료의 전송자 또는 전송시스템 확인
 - 예: 전자서명(digital signature)

인증 기술 정리

- 인증의 정의
 - identification, authentication
- 인증을 수행하는 목적(필요성)
- 인증방식의 종류(분류) 및 특징
- ID/PW 방식의 인증 특징, 취약점 등
- 인증의 종류
 - 개체 인증, 메시지 출처 인증

간편 인증(1)

- 간편 인증 도입 배경

- 복잡한 공인인증서 발급 및 설치, 사용 문제점 보완(2020.12)



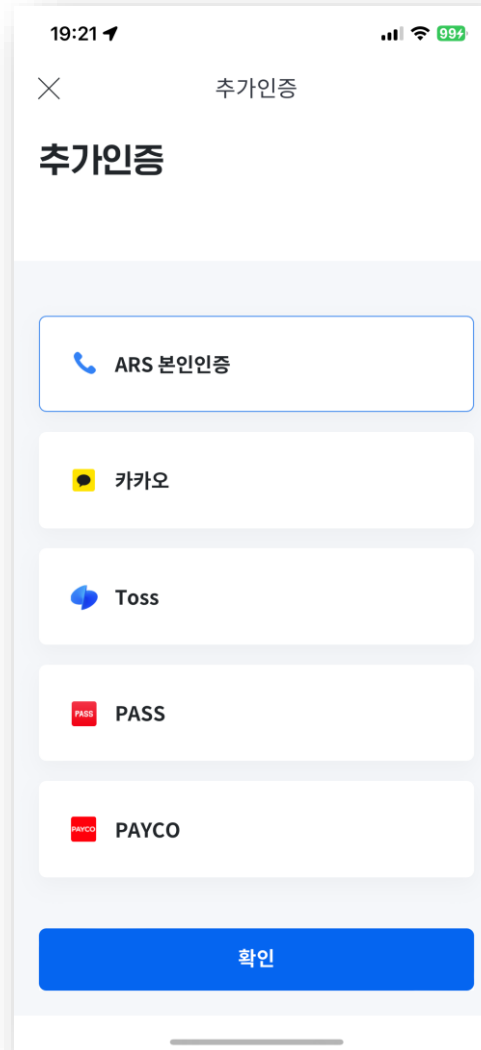
간편 인증(2)

■ 간편 인증 추진

- 2020.12: 전자서명법 개정 및 공인인증서 독점적 지위 폐지
- 2020.12: 공공분야 민간 전자서명 확대 도입, 5개 시범사업자
 - ✓ 카카오, 통신사PASS, 한국정보인증(삼성PASS), KB국민은행, NHN페이코 (5종)
- 2021.11: 네이버, 신한은행 추가 (5종 → 7종)
- 2022.2: 토스,뱅크샐러드 추가 (7종 → 9종)
- 2022.11: 드림인증, 하나은행, NH농협은행 (9종 → 12종)
- 2023.12: 카카오뱅크, 우리은행 (12종 → 14종)

간편 인증(3)

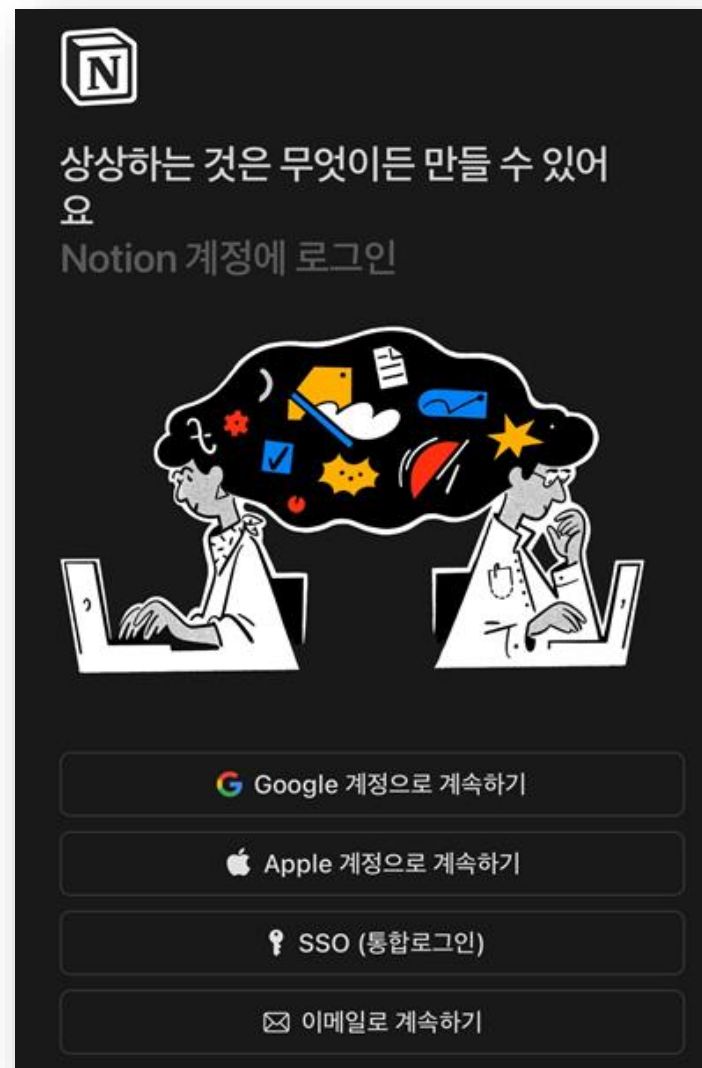
- 인터넷 뱅킹 시
추가 인증 화면(예)



소셜 인증(Social login/sign-in/sign-on)

■ 특징

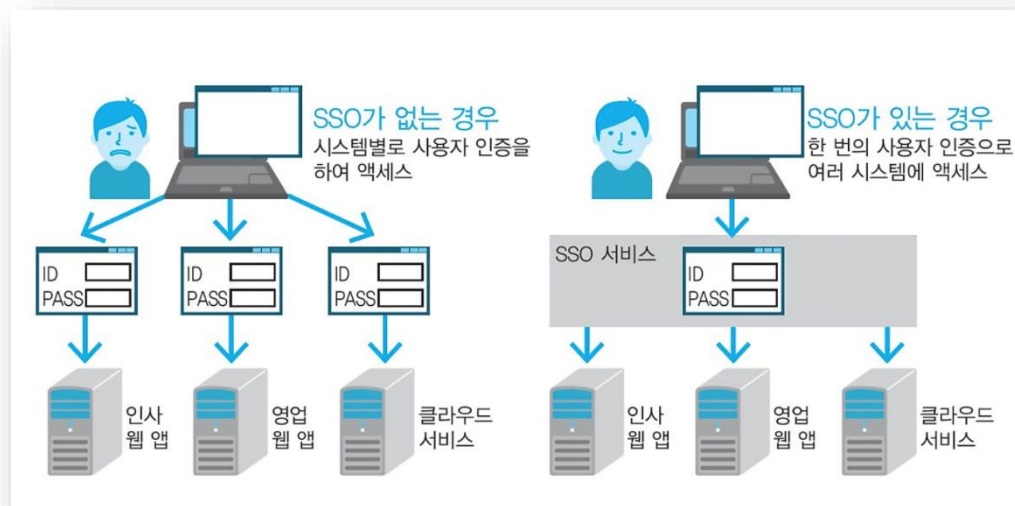
- 서비스 이용을 위해
- 해당 사이트가 제공하는 회원가입 절차 없이
- 주요 소셜 사이트에 인증 절차를 수행하고
 - ✓ 구글, 페이스북(메타), 애플, MS 등
- 서비스를 이용하는 방식



SSO(Single Sign-On)

■ 특징

- 한 사이트에 로그인 후
- 다른 사이트를 접속할 때
- 추가적인 로그인 없이
- 로그인 상태를 유지하는 서비스



■ 조건

- SSO 서비스 이용 사이트와 SSO 서비스 제공 사이트 간 사전 협약체결 및 SW 설치 필요

Q & A