인덕대학교

운영체제 보안
- 사용자 계정

컴퓨터소프트웨어학과

김병국 교수

학습목표

- 다중 사용자 운영체제의 개념을 안다.
- 사용자 계정의 관리를 위한 파일의 구성을 안다.
- 계정을 관리할 수 있다.

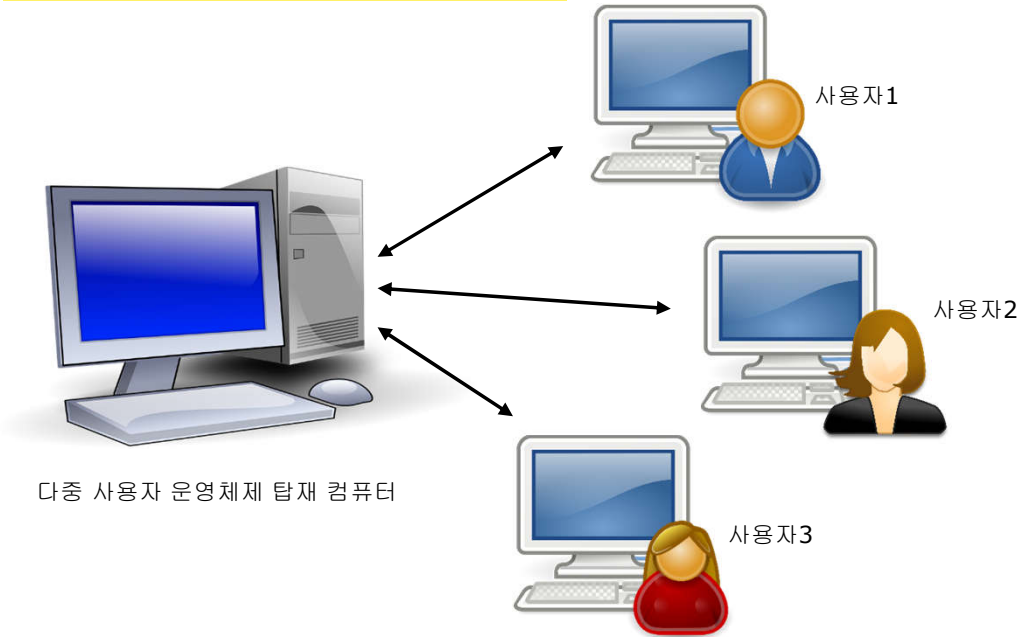
목차

- 다중 사용자 운영체제
- 사용자 계정
- 계정 관리

1. 다중 사용자 운영체제 [1/3]

❑ 개념

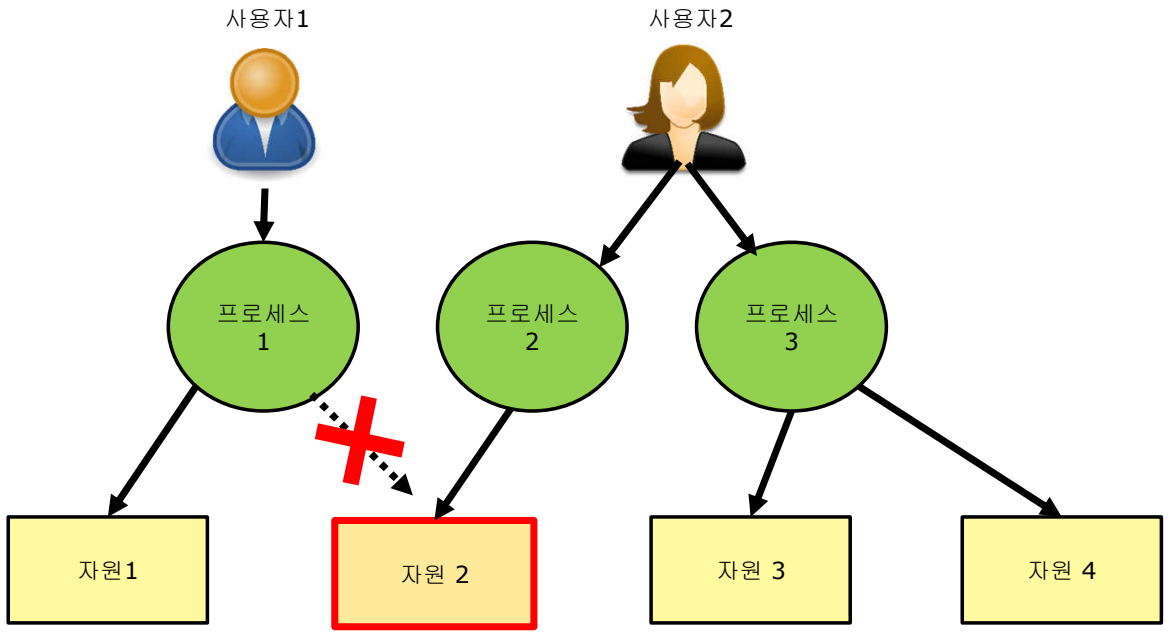
- 하나의 운영체제내 다수 사용자의 접근 및 작업을 지원
- 사용자 별 UI를 위한 창(터미널)을 제공
- 멀티태스크 환경 필요



1. 다중 사용자 운영체제 [2/3]

❑ 유닉스 운영체제

- 다중 사용자/프로세스를 위한 서버/워크스테이션용 운영체제
- 사용자 개인 자료(데이터, 프로세스)에 대한 타 계정과의 침해를 방지
  - 보안기능이 필수



1. 다중 사용자 운영체제 [3/3]

❑ 보안(Security)

- 운영체제는 인증된(authorized) 사용자만 접근이 가능하도록 동작
- 자원(프로세스, 데이터 등)을 보호(protect)하기 위해 사용되는 방법
  - 사용자 별 자원 접근의 권한을 부여

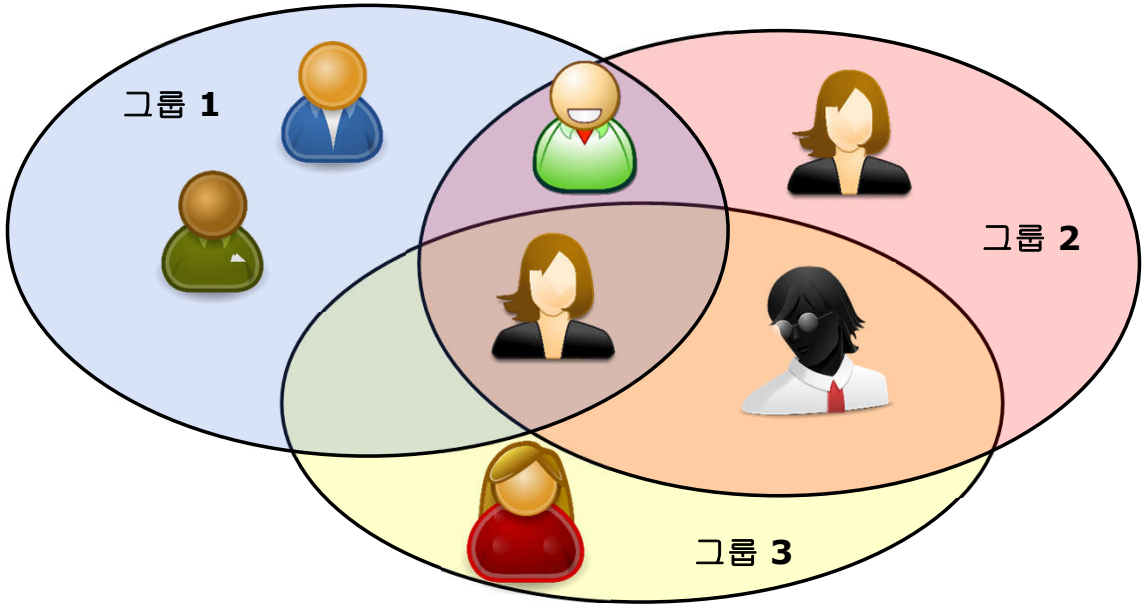
❑ 보호(Protection)

- 위험 요소로 부터 피해를 방지
  - 위험 요소: vulnerability, asset, threat 등
- 내부 피해로 인한 내상(internal injury)과 유출에 따른 외상(external injury)이 존재

2. 사용자 계정 (1/3)

❑ 계정 정책

- 시스템 접근(로그인)을 위해서는 계정(account)이 필요
- 운영체제는 계정별 자원(프로세스, 파일 등)에 할당된 접근 권한으로 운영을 허용
- 운영체제는 사용자(user)별 접근 권한 및 그룹(group)별 접근 권한을 지원
- 시스템 내 모든 계정은 그룹에 포함



2. 사용자 계정 (2/3)

❑ 계정 정보 (1/2)

- 파일: /etc/passwd
  - 각 행 별 사용자 계정(user account)을 정의
  - root(ID: 0)는 시스템 관리자 계정

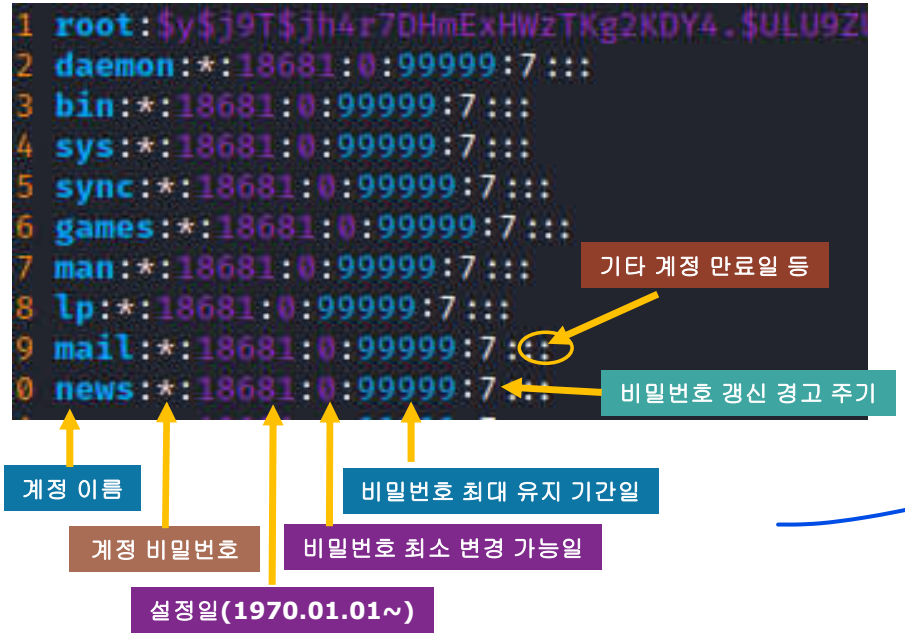
```
1 root:x:0:0:root:/root:/usr/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
...
49 geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
50 lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
51 king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
52 kali:x:1000:1000:Kali,,,:/home/kali:/usr/bin/bash
53 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

계정 이름 | 계정 비밀번호 | 사용자 ID | 그룹 ID | 부가 정보 | 홈 경로 | 최초 실행파일

2. 사용자 계정 (3/3)

❑ 계정 정보 (2/2)

- 파일: /etc/shadow
  - 사용자 계정 별 비밀번호를 관리(백업파일: /etc/shadow-)
  - 파일은 시스템관리자(root)만 접근이 가능
  - 비밀번호는 암호화되어 관리됨("!" 문구가 앞에 있으면 접근 불가 상태가 됨)



3. 계정 관리 (1/3)

인덕대학교

❑ 사용자 보기

- 명령어: id [계정명] 또는 finger [계정명]
  - 지정한 계정명의 세부 정보(ID, 기본 그룹, 확장 그룹)를 출력

```
kali@kali:~$ id kali
uid=1000(kali) gid=1000(kali) groups=1000(kali),24(cdrom),25(floppy),
27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(blue
tooth),133(scanner),142(kaboxer)
kali@kali:~$
kali@kali:~$ finger kali
Login: kali                             Name: Kali
Directory: /home/kali                   Shell: /usr/bin/bash
On since Mon May  3 17:59 (KST) on tty7 from :0
   1 hour 27 minutes idle
No mail.
No Plan.
kali@kali:~$
```

[명령어 실행결과]

3. 계정 관리 (2/3)

❑ 사용자 추가 및 비밀번호 설정

- 명령어: adduser [계정명] (또는 useradd [계정명])
  - 지정한 이름의 사용자의 계정(이름: 계정명)을 추가
  - 생성된 계정의 홈 경로는 "/home/[계정명]" 으로 생성됨
  - 단, useradd 명령어는 홈디렉토리를 생성하지 않음
  - 해당 명령은 시스템관리자(root) 권한으로만 실행이 가능
    - 시스템 관리자 권한으로 해당 명령을 실행하기 위해서는 "sudo" 명령을 함께 사용
    - 단, "sudo" 명령은 허가된 계정만 사용이 가능("kali" 는 허가되어있음)

- 명령어: passwd {계정명}
  - 지정한 계정의 비밀번호를 설정(관리자 전용)
  - 일반 사용자는 자신의 비밀번호만 변경이 가능

3. 계정 관리 (3/3)

❑ 사용자 삭제

- 명령어: deluser [계정명] (또는 userdel [계정명])
  - 지정한 이름의 사용자의 계정(이름: 계정명)을 삭제
  - 홈 디렉토리 삭제 시:
    - deluser 명령어 : deluser --remove-home [계정명]
    - userdel 명령어 : userdel -r [계정명]
  - 해당 명령은 시스템관리자(root) 권한으로만 실행이 가능

수고하셨습니다.