

운영체제 보안

- 사용자 전환 및 그룹 계정

컴퓨터소프트웨어학과

김병국 교수



- 프로세스의 계정 정보를 추출하는 프로그램을 만들 수 있다.
- 사용자 및 그룹 계정을 전환할 수 있다.
- 그룹 계정의 관리를 위한 파일의 구성을 안다.
- 그룹 계정을 변경할 수 있다.



목차

□프로세스의 계정 정보 추출

□사용자 전환

□그룹 계정

□그룹 관리

□그룹 전환

□관련 실습



1. 프로세스의 계정 정보 추출 (1/3)

□ 사용자 정보 추출

- 함수: getuid() & getgid()
 - getuid() : 현재 프로세스의 사용자 ID값을 추출
 - getgid() : 현재 프로세스의 그룹 ID값을 추출
- 함수: getlogin() & getlogin_r()
 - 시스템에 로그인한 현재 사용자 계정을 추출
 - 인자(getlogin_r()):
 - *buf : 저장될 주소
 - bufsize : buf의 크기
 - 결과값:
 - 성공: getlogin() → 문자열 포인터 값, getlogin_r() → 문자열의 길이
 - 실패: getlogin() → null, getlogin_r() → -1

```
#include <unistd.h>

uid_t getuid(void);

uid_t geteuid(void);

char *getlogin(void);

int getlogin_r(char *buf, size_t bufsize);
```

【함수의 프로토타입】



1. 프로세스의 계정 정보 추출 (2/3)

□ 사용자 정보 추출

■ 함수: getpwuid()

- 주어진 사용자 ID에 해당하는 사용자 계정 정보를 추출
- 추출값은 passwd 구조체형 포인터를 가짐
- 인자:
 - uid : 사용자 ID
- 결과값:
 - 성공: struct passwd 구조체형 포인터 변수
 - 실패: null

```
#include <sys/types.h>
#include <pwd.h>

struct passwd *getpwnam(const char *name);
struct passwd *getpwuid(uid_t uid);
```

[getpwuid() 함수의 프로토타입]

```
/* A record in the user database. */
struct passwd
{
    char *pw_name;           /* Username. */
    char *pw_passwd;         /* Hashed passphrase, if shadow database
                             not in use (see shadow.h). */
    __uid_t pw_uid;          /* User ID. */
    __gid_t pw_gid;          /* Group ID. */
    char *pw_gecos;          /* Real name. */
    char *pw_dir;            /* Home directory. */
    char *pw_shell;          /* Shell program. */
};
```

[passwd 구조체]



1. 프로세스의 계정 정보 추출 (2.1/3)

□ 사용자 정보 추출

■ 함수: getpwnam()

- 주어진 사용자명에 해당하는 사용자 계정 정보를 추출
- 추출값은 passwd 구조체형 포인터를 가짐
- 인자:
 - *name : 사용자명
- 결과값:
 - 성공: struct passwd 구조체형 포인터 변수
 - 실패: null

```
#include <sys/types.h>
#include <pwd.h>

struct passwd *getpwnam(const char *name);

struct passwd *getpwuid(uid_t uid);
```

[getpwnam() 함수의 프로토타입]

```
/* A record in the user database. */
struct passwd
{
    char *pw_name;           /* Username. */
    char *pw_passwd;         /* Hashed passphrase, if shadow database
                             not in use (see shadow.h). */
    __uid_t pw_uid;          /* User ID. */
    __gid_t pw_gid;          /* Group ID. */
    char *pw_gecos;          /* Real name. */
    char *pw_dir;            /* Home directory. */
    char *pw_shell;          /* Shell program. */
};
```

[passwd 구조체]



1. 프로세스의 계정 정보 추출 (3/3)

□ 실습

■ 사용자 정보 추출

```
1  #include <stdio.h>
2  #include <sys/types.h>
3  #include <pwd.h>
4  #include <unistd.h>
5
6  int main(int argc, char* argv[])
7  {
8      struct passwd *stPasswd;
9
10     if (argc != 2)
11     {
12         printf("Usage: %s <username>\n", argv[0]);
13         return -1;
14     }
15
16     printf("LogIn Account: %s\n", getlogin());
17
18     stPasswd = getpwnam(argv[1]);
19     if (stPasswd == NULL)
```

```
20     {
21         printf("There is no %s", argv[1]);
22         return -1;
23     }
24
25     printf("Name: %s\n", stPasswd->pw_name);
26     printf("UID: %d\n", stPasswd->pw_uid);
27     printf("GID: %d\n", stPasswd->pw_gid);
28     printf("Additonal : %s\n", stPasswd->pw_gecos);
29     printf("Home : %s\n", stPasswd->pw_dir);
30     printf("Shell : %s\n", stPasswd->pw_shell);
31
32     return 0;
33 }
```

[파일명: get_userinfo.c]

사용자 정보 추출

2. 사용자 전환 (1/2)

□ 사용자 전환

■ 명령어: su {계정명}

- su: **S**ubstitute **U**ser
- 지정한 사용자 계정으로 현재 작업자의 계정을 전환
- 전환 시 반드시 해당 계정의 비밀번호를 입력해야 함
 - 단, 시스템관리자(root)는 다른 계정으로 전환 시 비밀번호 필요 없음
- 옵션:
 - -(없음), -l, --login : 지정한 계정으로 새로 로그인 한 것처럼 동작



2. 사용자 전환 (2/2)

□ 대리 실행

- 명령어: `sudo {-u user} [명령어]`

- 지정된 사용자 계정으로 명령어를 실행

- 지정된 계정이 없을 경우 입력된 명령어는 시스템 관리자(root) 계정으로 실행됨
- 지정된 명령어만 해당 계정으로 동작함
- 프로세스 종료 후 원래 계정환경으로 복귀
- sudo 명령어는 시스템에서 별도 지정된 계정만 이용할 수 있음
 - kali 계정은 이미 시스템에서 이미 설정된 상태
 - 관련 파일: `/etc/sudo.conf`, `/etc/sudoers`, `/etc/sudoers.d/*`

- su와 sudo의 차이점

- su는 지정된 사용자 계정으로 자신을 변경
- sudo는 지정된 사용자 계정으로 명령어를 실행



3. 그룹 계정

□ 그룹 정보

- 파일: /etc/group & /etc/gshadow
 - 그룹별 비밀번호를 관리(백업파일: /etc/gshadow-)
 - 파일은 시스템관리자(root)만 접근이 가능

비밀번호는 암호화되어 관리됨

```
1 root:x:0:
2 daemon:x:1:
3 bin:x:2:
4 sys:x:3:
5 adm:x:4:
```

```
16 fax:x:21:
17 voice:x:22:
18 cdrom:x:24:kali
19 floppy:x:25:kali
20 tape:x:26:
21 sudo:x:27:kali
22 audio:x:29:pulse,kali
```

그룹 이름

그룹 ID

그룹 비밀번호

그룹 멤버

[파일: /etc/group]

```
33 video:*::kali
34 sasl:*::
35 plugdev:*::kali
36 staff:*::
37 games:*::
38 users:$6$xzZYUzJUnTSBNyU/$Uw
39 nogroup:*::
```

그룹 비밀번호

그룹 관리자

그룹 멤버

[파일: /etc/gshadow]

시정



4. 그룹 관리 (1/2)

□ 그룹 추가 및 삭제

- 명령어: `addgroup [그룹명]`

- 지정한 이름의 그룹을 추가
- 추가된 그룹은 `/etc/group`와 `/etc/gshadow`에 기록
- 해당 명령은 시스템관리자(root) 권한으로만 실행이 가능

- 명령어: `delgroup [그룹명]`

- 지정한 이름의 그룹을 삭제



4. 그룹 관리 (2/2)

□ 그룹 관리

- 명령어: `gpsswd {옵션} [그룹명]`

- 그룹의 속성(비밀번호, 멤버, 관리자 등)을 수정

- 대표적인 옵션:

- (없음) : “그룹명”의 비밀번호를 설정

- `-a [계정]` : “계정”을 “그룹명”의 멤버로 추가

- `-d [계정]` : “계정”을 “그룹명”의 멤버에서 제거

- `-A [계정1, 계정2, ...]` : “그룹명”의 관리자들을 설정

- `-r` : “그룹명”의 비밀번호를 삭제



5. 그룹 전환

□ 그룹 전환

- 명령어: newgrp [그룹명]

- 지정한 그룹으로 자신의 기본 소속을 변경
- 지정한 그룹이 자신의 확장 그룹에 포함되어 있으면, 바로 변환됨
- 그렇지 않으면, 지정한 그룹의 비밀번호를 입력해야 함

- 명령어: sg [그룹명] [명령어]

- 지정한 그룹으로 명령어를 실행



수고하셨습니다.

