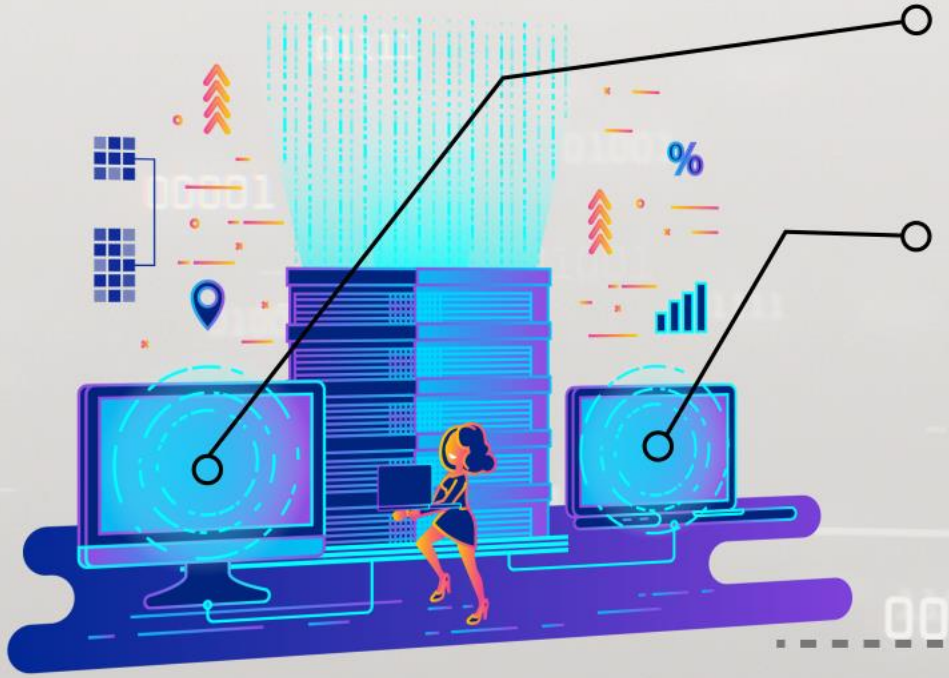
北京郵電大學
Beijing University of Posts and Telecommunications



SUID权限

蒋砚军 北京邮电大学计算机学院

三级权限存在的问题

问题

- 系统中任一个用户，要么对文件的全部内容具有访问权，要么不可访问文件。有的情况下，很不方便。

三级权限存在的问题举例

- 用户修改口令，文件/etc/passwd和/etc/shadow
- 用户liu的文件list.txt：希望用户liang，只能读取行首为#的行和与他有关的行。

```
#=============================================================
# 登录名    工作证号    姓名      月份      工资      奖金      补助      扣除      总额
#-------------------------------------------------------------
   tian      2076     田晓星     03       4782      4500      200       175      8307
   liang     2074     梁振宇     03       4560      4400      180        90      8050
   sun       3087     孙东旭     03       4804      4218      106       213      7915
   tian      2076     田晓星     04       4832      4450      230       245      8267
   liang     2074     梁振宇     04       4660      4450      230        70      8270
   sun       3087     孙东旭     04       4700      4310      283       270      8023
#=============================================================
# 注：燃气费自本年度开始不再从工资中扣除。
```

用户liu的程序query.c

```
int main(void)
 {
    FILE *f;
    char line[512], name[64], *username;

    if ((f = fopen("list.txt", "r")) == NULL) {
        printf("*** ERROR: Open file \"list.txt\": %m\n");
        exit(1);
    }

    username = getlogin();
    while (fgets(line, sizeof(line), f)) {
        if (line[0] == '#')
            printf("%s", line);
        else if (sscanf(line, "%s", name) > 0 && strcmp(name, username) == 0)
            printf("%s", line);
    }
}
```

简单的三级权限的问题

用户liu

源程序经过编译后，生成可执行文件query。为了保密用户liu将文件list.txt的权限设为rw-------，文件query的权限为rwx--x—x

```
$ chmod 600 list.txt
$ chmod 711 query
$ ls -l list.txt query
-rw-------   1 liu   leader     722 Dec 10 23:04 list.txt
-rwx--x--x   1 liu   leader   56134 Dec 10 23:07 query
$
```

用户liang执行命令query

```
$ query
*** ERROR: Open file "list.txt" : Permission denied
$ cat list.txt
cannot open list.txt: Permission denied
```

SUID权限

- 文件query的文件主liu给文件query增加SUID权限

```
$ chmod u+s query
$ ls -l query
-rws--x--x   1 liu   leader   56134 Dec 10 23:07 query
```

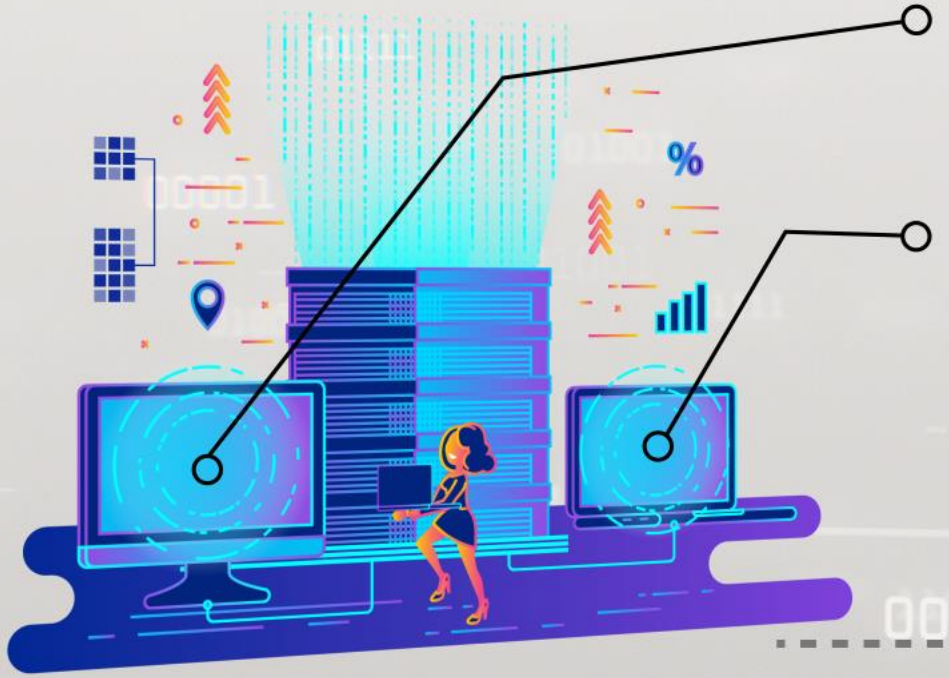
- 用户liang通过query命令查询只许liu可读的文件list.txt

```
$ ls -l list.txt query
-rw-------   1 liu   leader     722 Dec 10 23:04 list.txt
-rws--x--x   1 liu   leader   56134 Dec 10 23:07 query
$ query
#=============================================================
# 登录名 工作证号 姓名     月份    工资    奖金    补助    扣除    总额
#-------------------------------------------------------------
   liang    2074    梁振宇    03     4560    4400     180      90    8050
   liang    2074    梁振宇    04     4660    4450     230      70    8270
#=============================================================
# 注：燃气费自本年度开始不再从工资中扣除。
$ cat list.txt
cannot open list.txt: Permission denied
```

进程实际UID/有效UID

- 一般情况下，进程的实际UID和有效UID相等。
- 打开文件open()时，系统根据进程的有效UID，与文件所有者UID之间的关系和文件的权限进行访问合法性验证
- 可执行程序具有SUID权限，进程的实际UID和有效UID不再相等。实际UID是当前用户，而有效UID为可执行文件的文件主。
- SUID使得用户可以通过文件主提供的程序，以文件主的权限访问文件，但这种访问依赖于文件主提供的程序，进行有限的访问。

北京郵電大學
Beijing University of Posts and Telecommunications



谢 谢