Сигурност на операционни системи

Принципи на защита и сигурност

- **Принцип на най-малките привилегии** – на програмите, потребителите и системите трябва да бъдат дадени единствено привилегии, достатъчни за изпълнение на техните задачи.

Техники за компютърна сигурност

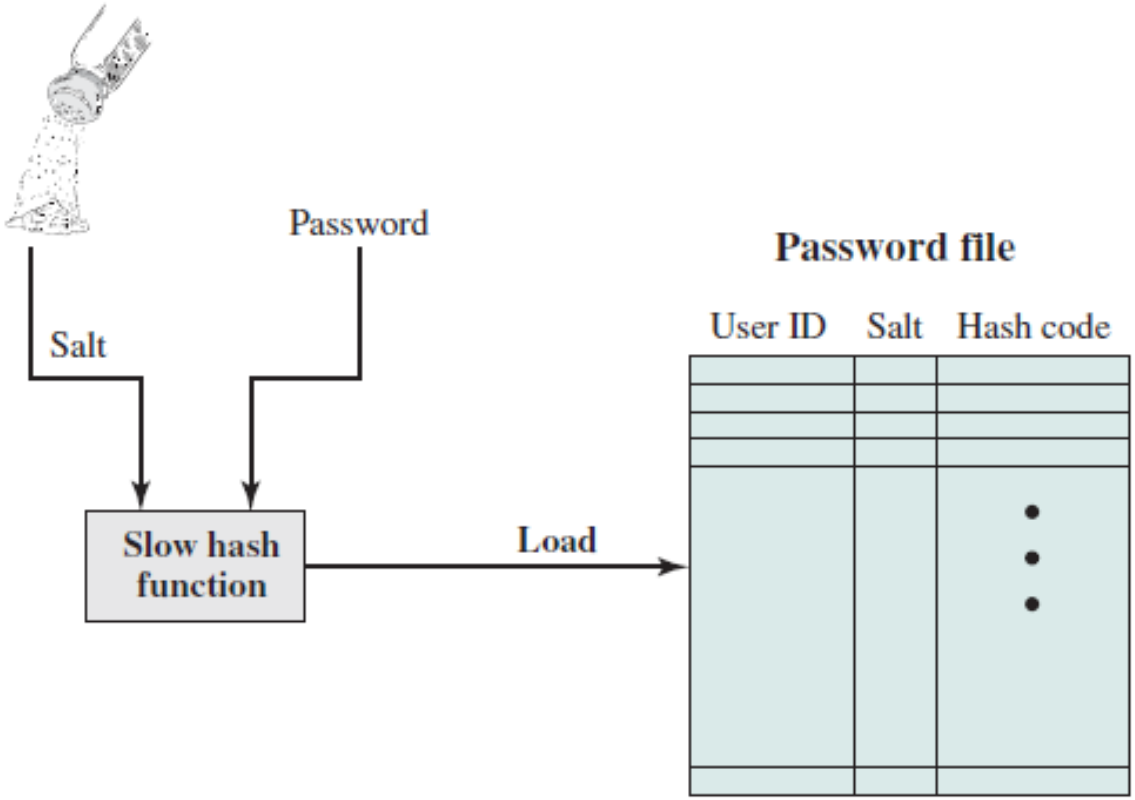
- Автентикация
- Контрол на достъп
- Защита от зловреден софтуер

Автентикация, базирана на пароли

- Паролата се хешира с псевдослучайно число – salt.
- Типично за Linux се използва MD5 хеш алгоритъм и 48 бита salt стойност.

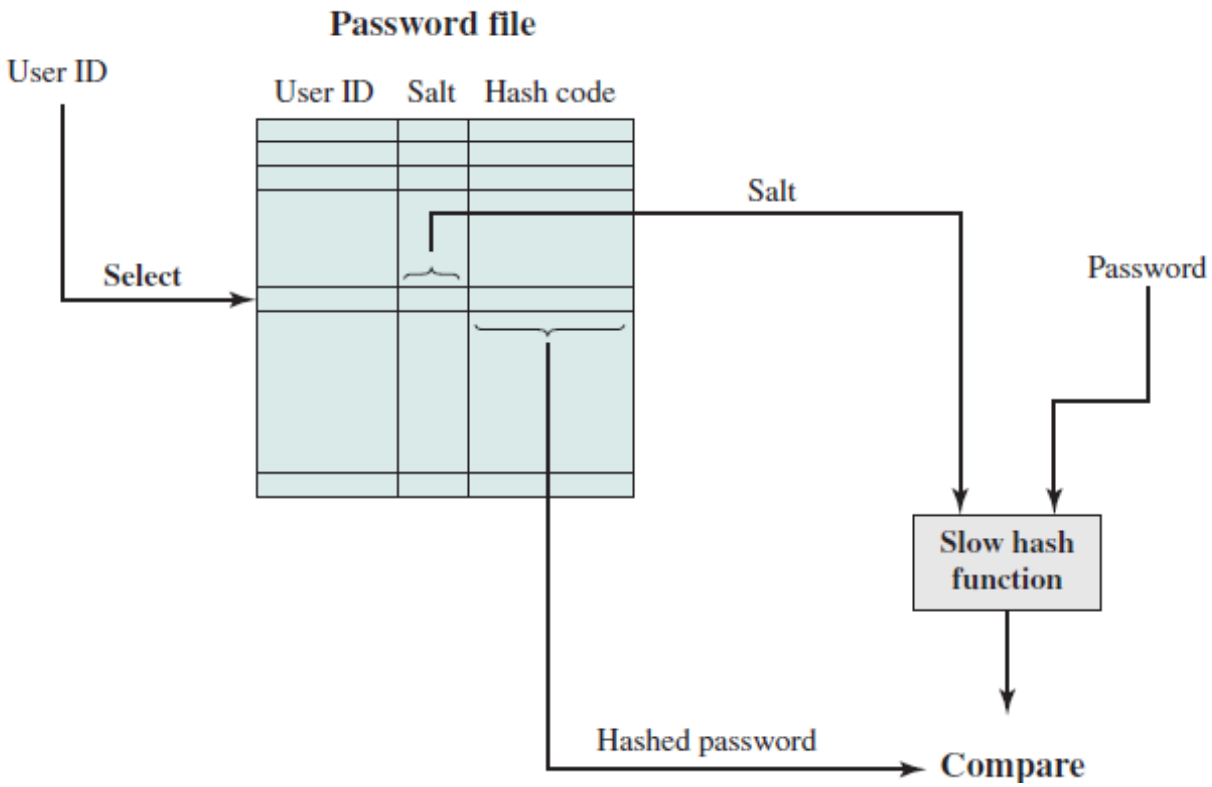
Автентикация, базирана на пароли

Въвеждане на нова парола



Автентикация, базирана на пароли

Проверка на парола



Автентикация, базирана на токени

- Memory card – карти с памет, съхраняващи код за достъп.
- Smart card – малко устройства с вграден микропроцесор, памет и интерфейс и поддържат протоколи за автентикация.
- Биометрична автентикация – персонална автентикация на базата на уникални физически характеристики на потребител.

Pluggable Authentication Modules

- PAM - пакет от споделени библиотеки, даващи възможност за избор на автентикация на потребители.
- Въвежда Middleware слой между приложението и автентикационния механизъм.
- Може да подържа данни за сесията.
- Разширява възможностите на Linux да бъде от класа на enterprise OS.

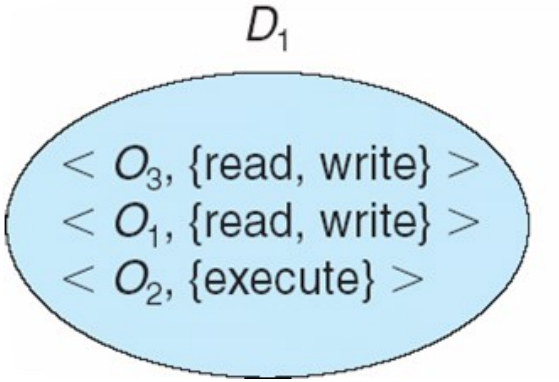
Контрол на достъпа

Политиките за контрол на достъпа указват какви типове на достъп за разрешени, при какви условия и за кого:

- Discretionary access control (DAC) – контрол базиран на идентичността на заявителя и на правила на негов достъп. Може да се предоставят права на други субекти.
- Role-based access control (RBAC) – контрол базиран на ролята на потребителите в системата и на права на достъп за съответната роля.
- Mandatory access control (MAC) – контролът се определя от администратора.

Discretionary access control (DAC)

- Компютърната система се разглежда като съвкупност от процеси и обекти
- Процесите оперират в защитена област (домейн), описваща до кои ресурси има достъп
- Възможността за изпълнение на операция върху обект- право на достъп
- Домейн – колекция от права на достъп, всяко във вида <обект, множество права>



Реализация на домейн

Домейн може да бъде:

- Потребител. Възможните обекти за достъп зависят от идентичността на потребителя.
- Процес. Възможните обекти за достъп зависят от идентичността на процеса.
- Процедура. Възможните обекти за достъп съответстват на локалните променливи, дефинирани в процедурата.

В Linux домейн се асоциира с потребител.

Матрица на достъп

Защитата се разглежда като матрица:

- Редовете представят домейните
- Колоните представят обектите
- Access(i, j) е множество от операции, което процес, изпълняващ се в домейн i, може да изпълни върху обект j.

domain \ object	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

Използване на матрица на достъп

- Ако процес в домейн **Di** се опита да изпълни операция **op** върху обект **Oj**, то операцията **op** трябва да бъде в матрицата за достъп
- Потребителят, създал обекта, може да дефинира колона за достъп до този обект

Използване на матрица на достъп

Матрицата за достъп разделя механизма на прилагане от политиката:

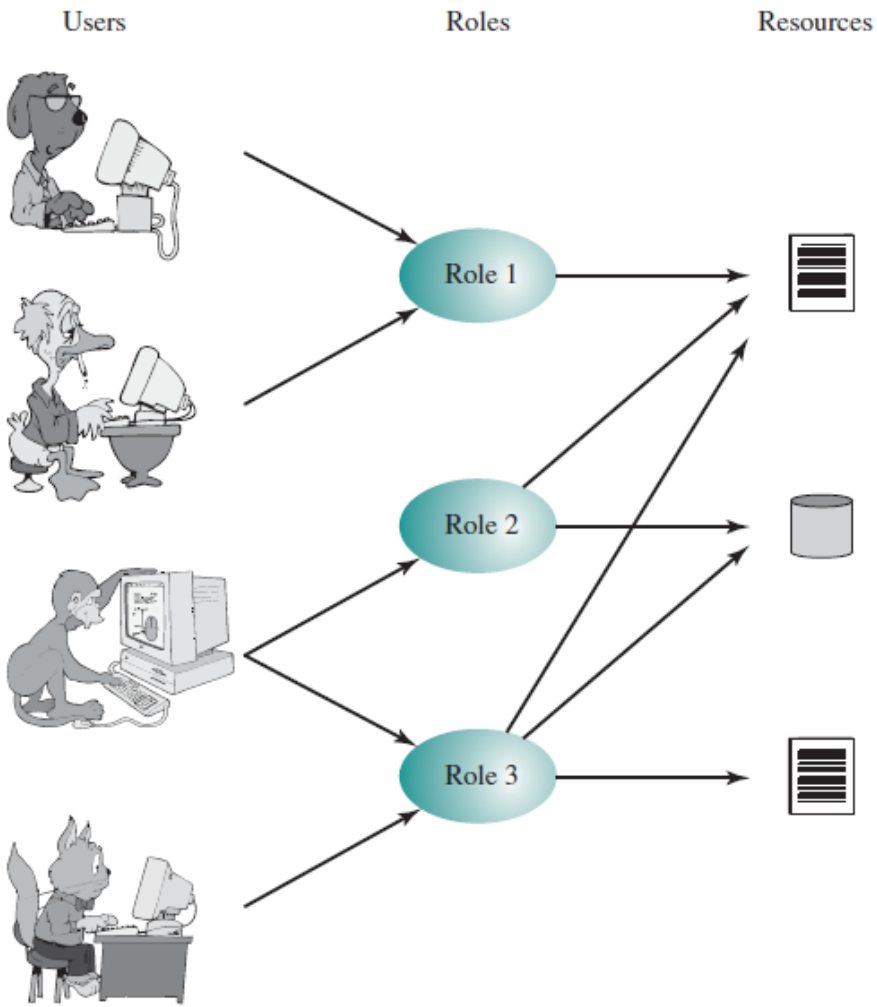
- Механизъм – операционната система предоставя матрицата и правата. Тя осигурява манипулирането с матрицата да бъде само от оторизирани компоненти.
- Политика – потребителят определя политиката. Кой и в какъв режим може да достъпва даден обект.

Role-based access control (RBAC)

RBAC е контрол, базиран на роли, които потребителят може да заема в системата, вместо на неговата идентичност.

- Правата се присвояват на роли, вместо на индивидуални потребители.
- Потребителите се свързват към определени роли (най-често в зависимост от работата им в организацията).

Role-based access control (RBAC)



Role-based access control (RBAC)

Потребител може да заема множество роли и множество потребители могат да заемат една и съща роля:

	R_1	R_2	...	R_n
U_1	×			
U_2	×			
U_3		×		×
U_4				×
U_5				×
U_6				×
⋮				
U_m	×			

Role-based access control (RBAC)

Всяка роля има специфични права на достъп до един или няколко ресурса. Роля може да се третира като обект – възможност за йерархии на роли.

Roles \ Objects	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
• • •									
R_n			control		write	stop			

Модел на сигурност в Linux

- Системните извиквания са единственият начин за взаимодействие с ОС;
- Всеки потребител или негов процес се идентифицира с user-ID (UID).

Супер потребител

ROOT user

Потребители

- /etc/passwd
- **`useradd, usermod, userdel`**

Групи

- /etc/group
- **`groupadd, groupmod, gropudel`**

Пароли

```
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:/bin/false
news:x:9:13:news:/usr/lib/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucppublic:/bin/false
operator:x:11:0:operator:/root:/bin/bash
games:x:12:100:games:/usr/games:/bin/false
ftp:x:14:50::/home/ftp:/bin/false
```

/etc/passwd

```
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
sshd:*:9797:0:::::
```

/etc/shadow

Контрол на достъп в Linux

- Режими на достъп: read, write, execute
- Три класа потребители в Unix / Linux:
  - owner
  - group
  - public
- За всеки файл и поддиректория има 9 защитни бита: 3 за owner, 3 за group, 3 за public.

Листинг на директория в Linux

```
6291458 -rw-------  1 root root  1198 May 13  2019 .xinitrc
6295287 -rw-------  1 root root 20516 May 14  2019 .xorgxrdp.10.log
6291459 -rwx--x--x  1 root root  1198 May 13  2019 .xsession*
6295293 drwx--x--x  2 root root  4096 May 14  2019 Desktop/
6295297 drwx--x--x  2 root root  4096 May 14  2019 Documents/
6295294 drwx--x--x  2 root root  4096 Sep  9  2019 Downloads/
6295298 drwx--x--x  2 root root  4096 May 14  2019 Music/
6295299 drwx--x--x  2 root root  4096 May 14  2019 Pictures/
6295296 drwx--x--x  2 root root  4096 May 14  2019 Public/
6295295 drwx--x--x  2 root root  4096 May 14  2019 Templates/
6295300 drwx--x--x  2 root root  4096 May 14  2019 Videos/
6297287 -rw-r--r--  1 root root    12 Apr 14 13:47 file1
6295357 drwx--x--x 14 root root  4096 Apr  2 11:08 oslab/
6297123 drwxr-xr-x  2 root root  4096 Mar 26 12:23 rmos/
6297285 lrwxrwxrwx  1 root root     5 Apr 14 13:47 softlink1 -> file1
6291462 drwx--x--x  3 root root  4096 May 14  2019 vmtools/
6295285 drwx--x--x  2 root root  4096 May 14  2019 xrdp/
root@LinuxOS:~#
```

Тип на файла

Разрешения на достъп

```
6291458 -rw-------  1 root root  1198 May 13  2019 .xinitrc
6295287 -rw-------  1 root root 20516 May 14  2019 .xorgxrdp.10.log
6291459 -rwx--x--x  1 root root  1198 May 13  2019 .xsession*
6295293 drwx--x--x  2 root root  4096 May 14  2019 Desktop/
6295297 drwx--x--x  2 root root  4096 May 14  2019 Documents/
6295294 drwx--x--x  2 root root  4096 Sep  9  2019 Downloads/
6295298 drwx--x--x  2 root root  4096 May 14  2019 Music/
6295299 drwx--x--x  2 root root  4096 May 14  2019 Pictures/
6295296 drwx--x--x  2 root root  4096 May 14  2019 Public/
6295295 drwx--x--x  2 root root  4096 May 14  2019 Templates/
6295300 drwx--x--x  2 root root  4096 May 14  2019 Videos/
6297287 -rw-r--r--  1 root root    12 Apr 14 13:47 file1
6295357 drwx--x--x 14 root root  4096 Apr  2 11:08 oslab/
6297123 drwxr-xr-x  2 root root  4096 Mar 26 12:23 rmos/
6297285 lrwxrwxrwx  1 root root     5 Apr 14 13:47 softlink1 -> file1
6291462 drwx--x--x  3 root root  4096 May 14  2019 vmtools/
6295285 drwx--x--x  2 root root  4096 May 14  2019 xrdp/
root@LinuxOS:~#
```

Owner

Разрешения на достъп

```
6291458 -rw-------  1 root root  1198 May 13  2019 .xinitrc
6295287 -rw-------  1 root root 20516 May 14  2019 .xorgxrdp.10.log
6291459 -rwx--x--x  1 root root  1198 May 13  2019 .xsession*
6295293 drwx--x--x  2 root root  4096 May 14  2019 Desktop/
6295297 drwx--x--x  2 root root  4096 May 14  2019 Documents/
6295294 drwx--x--x  2 root root  4096 Sep  9  2019 Downloads/
6295298 drwx--x--x  2 root root  4096 May 14  2019 Music/
6295299 drwx--x--x  2 root root  4096 May 14  2019 Pictures/
6295296 drwx--x--x  2 root root  4096 May 14  2019 Public/
6295295 drwx--x--x  2 root root  4096 May 14  2019 Templates/
6295300 drwx--x--x  2 root root  4096 May 14  2019 Videos/
6297287 -rw-r--r--  1 root root    12 Apr 14 13:47 file1
6295357 drwx--x--x 14 root root  4096 Apr  2 11:08 oslab/
6297123 drwxr-xr-x  2 root root  4096 Mar 26 12:23 rmos/
6297285 lrwxrwxrwx  1 root root     5 Apr 14 13:47 softlink1 -> file1
6291462 drwx--x--x  3 root root  4096 May 14  2019 vmtools/
6295285 drwx--x--x  2 root root  4096 May 14  2019 xrdp/
root@LinuxOS:~#
```

Group

Разрешения на достъп

```
6291458 -rw-------  1 root root  1198 May 13  2019 .xinitrc
6295287 -rw-------  1 root root 20516 May 14  2019 .xorgxrdp.10.log
6291459 -rwx--x--x  1 root root  1198 May 13  2019 .xsession*
6295293 drwx--x--x  2 root root  4096 May 14  2019 Desktop/
6295297 drwx--x--x  2 root root  4096 May 14  2019 Documents/
6295294 drwx--x--x  2 root root  4096 Sep  9  2019 Downloads/
6295298 drwx--x--x  2 root root  4096 May 14  2019 Music/
6295299 drwx--x--x  2 root root  4096 May 14  2019 Pictures/
6295296 drwx--x--x  2 root root  4096 May 14  2019 Public/
6295295 drwx--x--x  2 root root  4096 May 14  2019 Templates/
6295300 drwx--x--x  2 root root  4096 May 14  2019 Videos/
6297287 -rw-r--r--  1 root root    12 Apr 14 13:47 file1
6295357 drwx--x--x 14 root root  4096 Apr  2 11:08 oslab/
6297123 drwxr-xr-x  2 root root  4096 Mar 26 12:23 rmos/
6297285 lrwxrwxrwx  1 root root     5 Apr 14 13:47 softlink1 -> file1
6291462 drwx--x--x  3 root root  4096 May 14  2019 vmtools/
6295285 drwx--x--x  2 root root  4096 May 14  2019 xrdp/
root@LinuxOS:~#
```

Public

Собственици на файл

```
6291458 -rw-------  1 root root  1198 May 13  2019 .xinitrc
6295287 -rw-------  1 root root 20516 May 14  2019 .xorgxrdp.10.log
6291459 -rwx--x--x  1 root root  1198 May 13  2019 .xsession*
6295293 drwx--x--x  2 root root  4096 May 14  2019 Desktop/
6295297 drwx--x--x  2 root root  4096 May 14  2019 Documents/
6295294 drwx--x--x  2 root root  4096 Sep  9  2019 Downloads/
6295298 drwx--x--x  2 root root  4096 May 14  2019 Music/
6295299 drwx--x--x  2 root root  4096 May 14  2019 Pictures/
6295296 drwx--x--x  2 root root  4096 May 14  2019 Public/
6295295 drwx--x--x  2 root root  4096 May 14  2019 Templates/
6295300 drwx--x--x  2 root root  4096 May 14  2019 Videos/
6297287 -rw-r--r--  1 root root    12 Apr 14 13:47 file1
6295357 drwx--x--x 14 root root  4096 Apr  2 11:08 oslab/
6297123 drwxr-xr-x  2 root root  4096 Mar 26 12:23 rmos/
6297285 lrwxrwxrwx  1 root root     5 Apr 14 13:47 softlink1 -> file1
6291462 drwx--x--x  3 root root  4096 May 14  2019 vmtools/
6295285 drwx--x--x  2 root root  4096 May 14  2019 xrdp/
root@LinuxOS:~#
```

User name

Group name

Промяна на разрешения

- За всеки отделен файл или поддиректория се дефинира подходящ достъп
- Задаване на защитата - chmod
- Компоненти:
- Потребител – [ugoa] u – собственик, g – група, o – други, a – всички
- Добавяне/премахване – [+ -]
- Разрешения – r, w, x

```
# chmod u+x test.c
# chmod +w test.c
# chmod g-x test.c
```

Промяна на разрешения

- Прилагане на специфично множество от разрешения
- Използва се числово представяне

Стойност	rwx
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Промяна на разрешения

- `# chmod 751 test.c`
- `# chmod 240 test.c`

Промяна на разрешения за директории

- R – четене съдържанието на директорията
- W – създаване на файлове и поддиректории в нея
- X – възможност за влизане в директорията

Промяна на собственост на файл

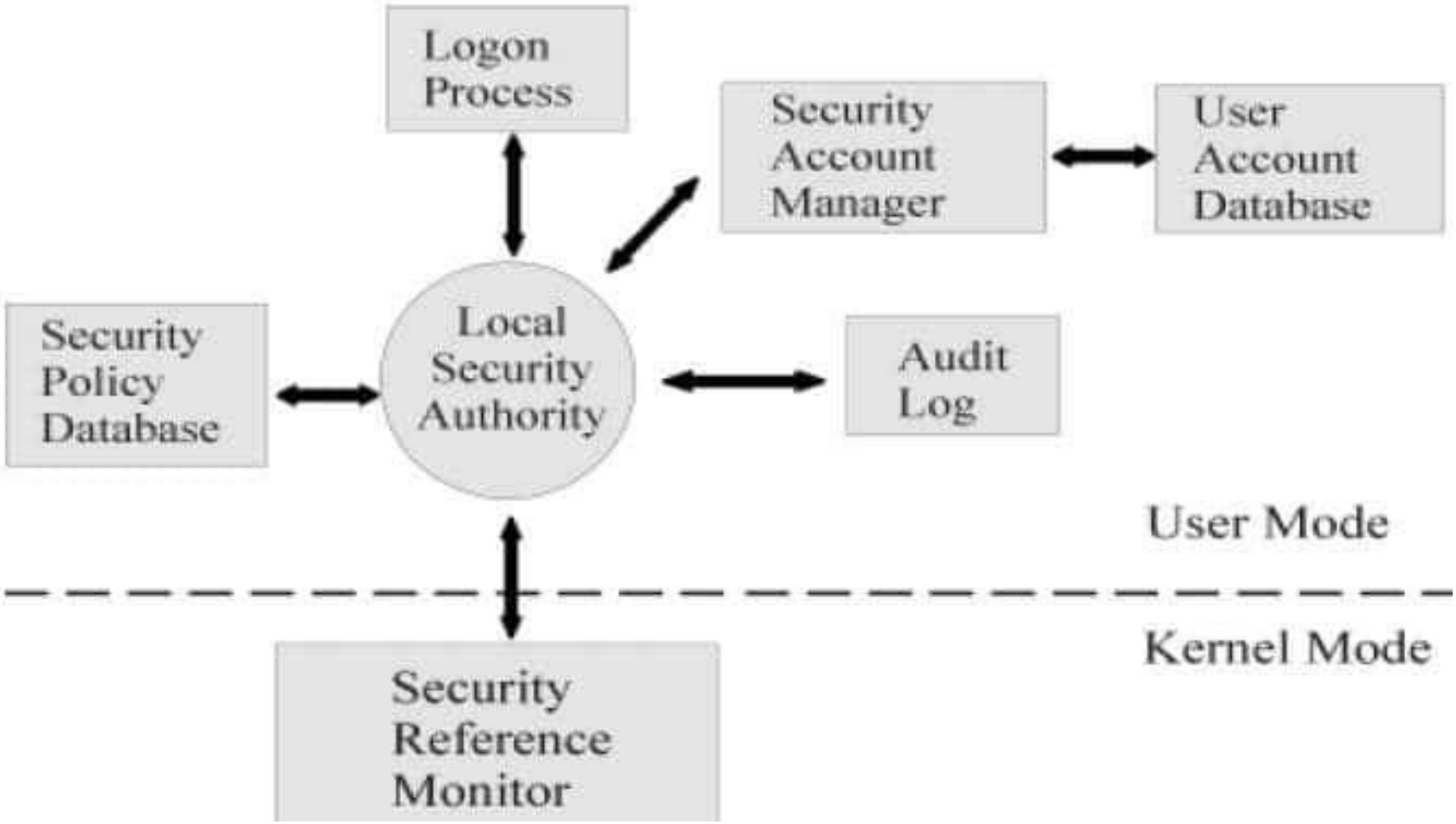
```
# chown <user>:<group> <file>
```

```
# chown ivan:users test.c
```

Модел на сигурност в Windows

- Security Reference Monitor – проверка на достъпа, генериране на лог файлове и манипулиране с права на достъп.
- Local Security Authority – прилагане на локалната политика за сигурност и управление на интерактивния логон.
- Security Account Manager – локална база данни с информация за акаунтите. Използва се за локален достъп.

Модел на сигурност в Windows

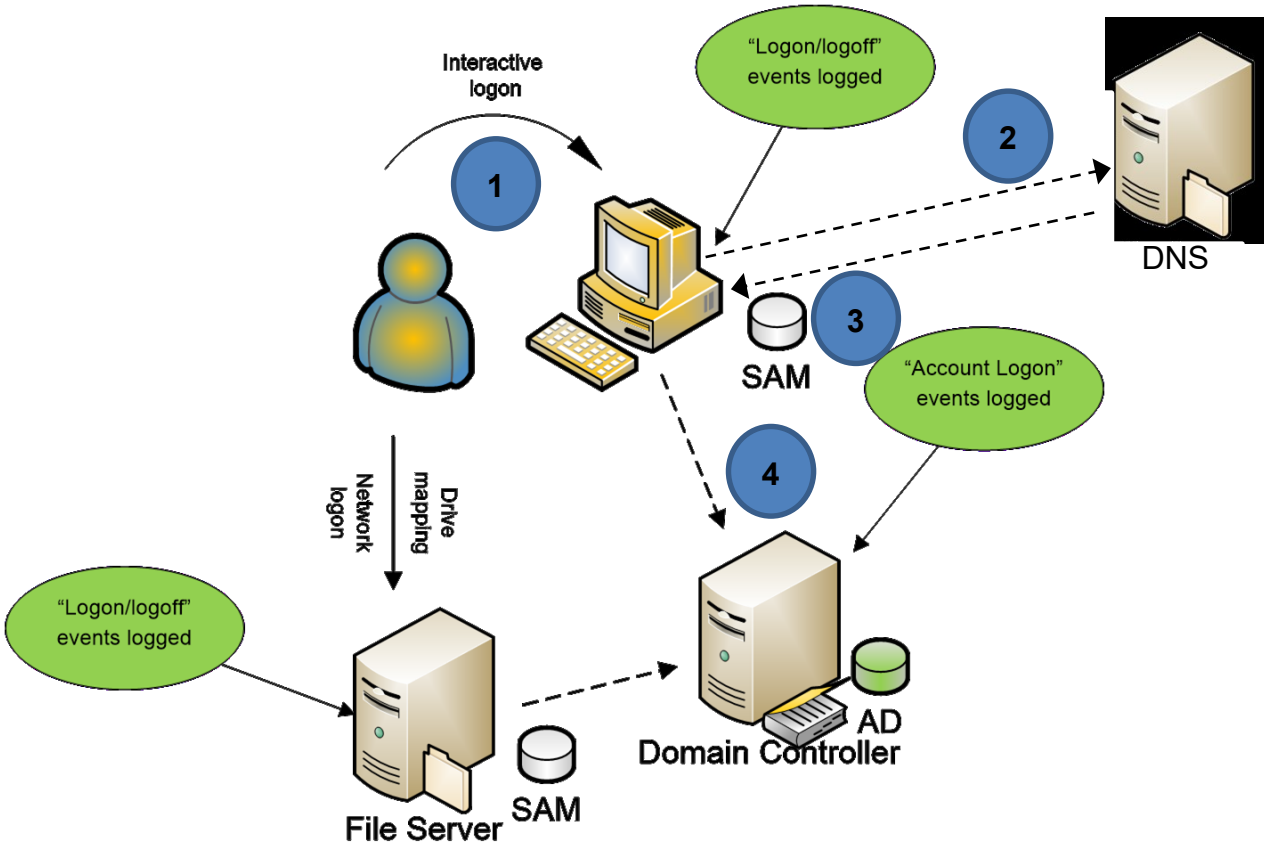


Windows Active Directory

- Използва се протокол LDAP.
- Автентициране при логване в домейн.
- Креденциалите се изпращат през мрежата.
- Netlogon.

Процес на логване на потребител в домейн

1. Изпраща се заявка към *netlogon* процеса.
2. Netlogon запити
DC на изисквания
3. DNS връща IP а
на домейн контро
4. Клиентът изпра
заявки към DC по
протокол.



Windows Access Control Lists (ACL)

Списък от контролни записи (ACE). Всеки ACE идентифицира потребител и указва права на достъп.

- Discretionary ACL (DACL)
- System ACL (ACL)

Security Descriptor

- Даннова структура всеки обект, съдържаща собственик, DACL, SACL и др.

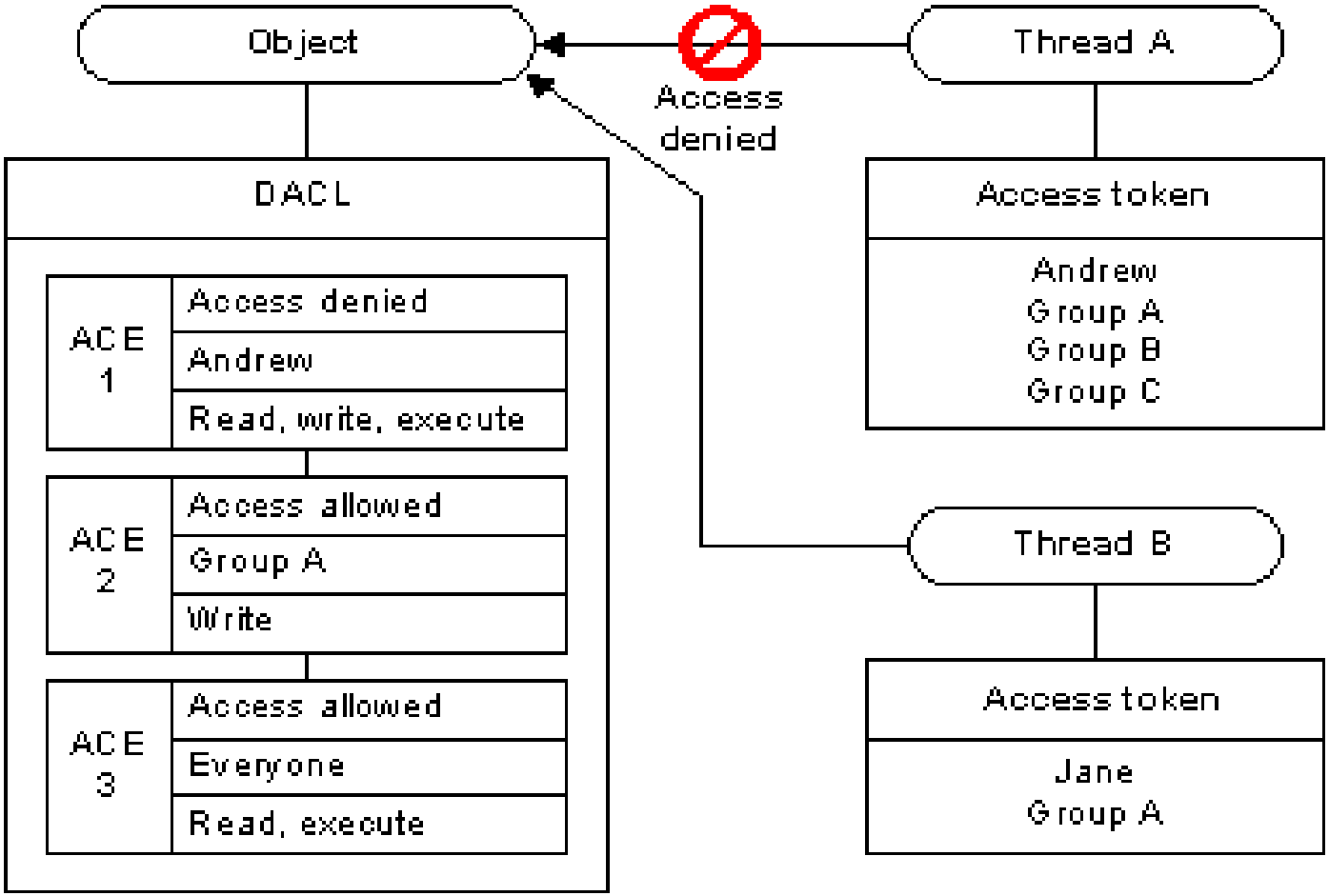
Owner: CORP\Blake

ACE[0]: Allow CORP\Paige Full Control

ACE[1]: Allow Administrators Full Control

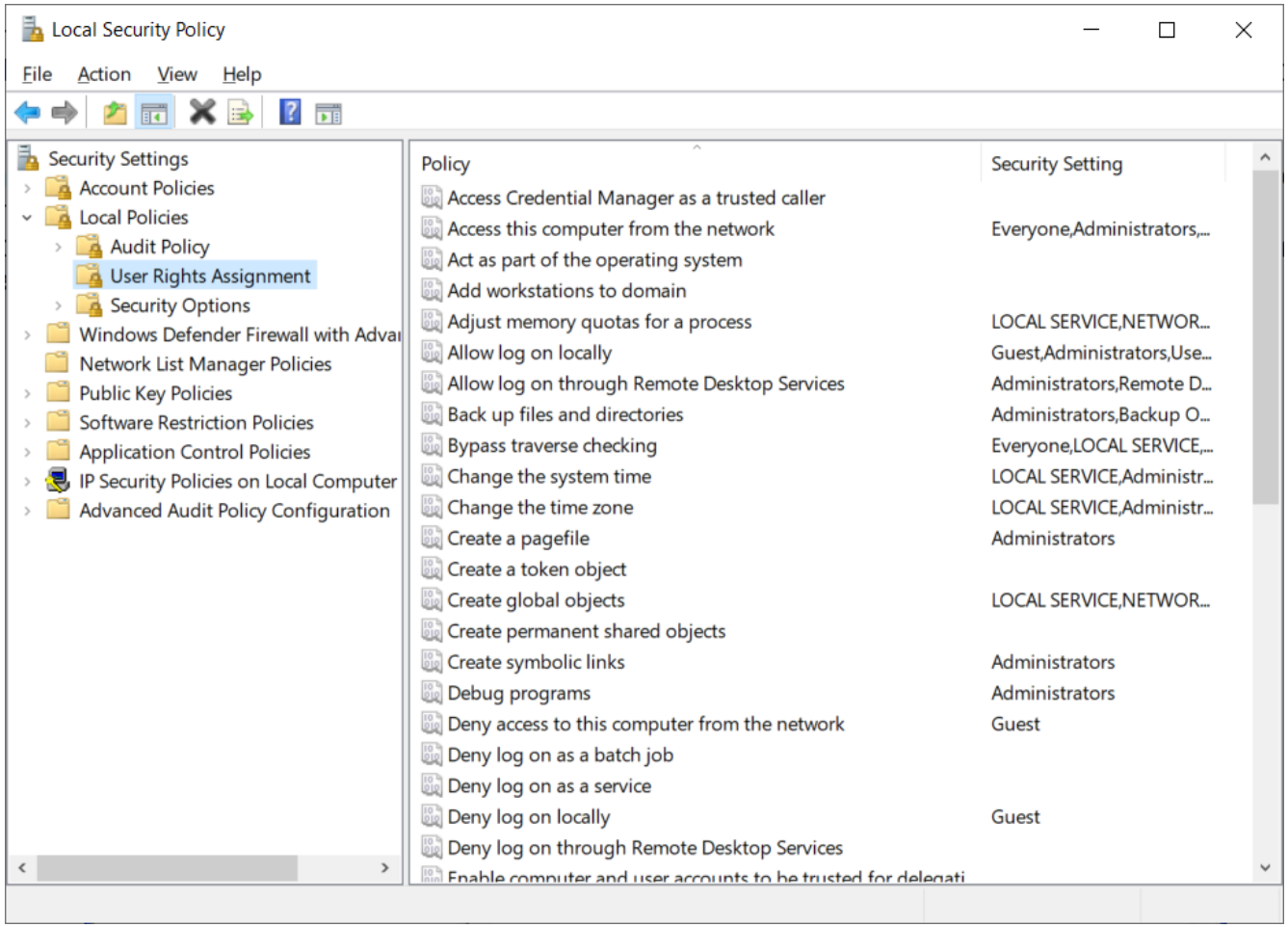
ACE[2]: Allow CORP\Cheryl Read, Write and Delete

Security Descriptor

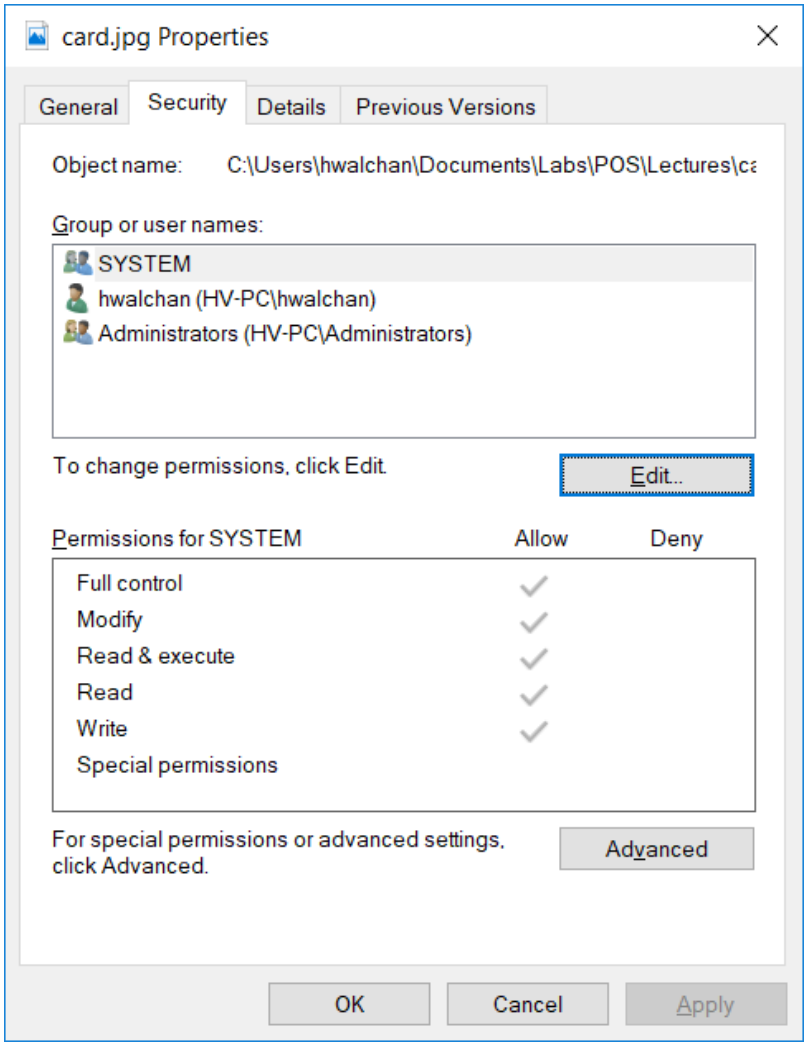


Windows привилегии

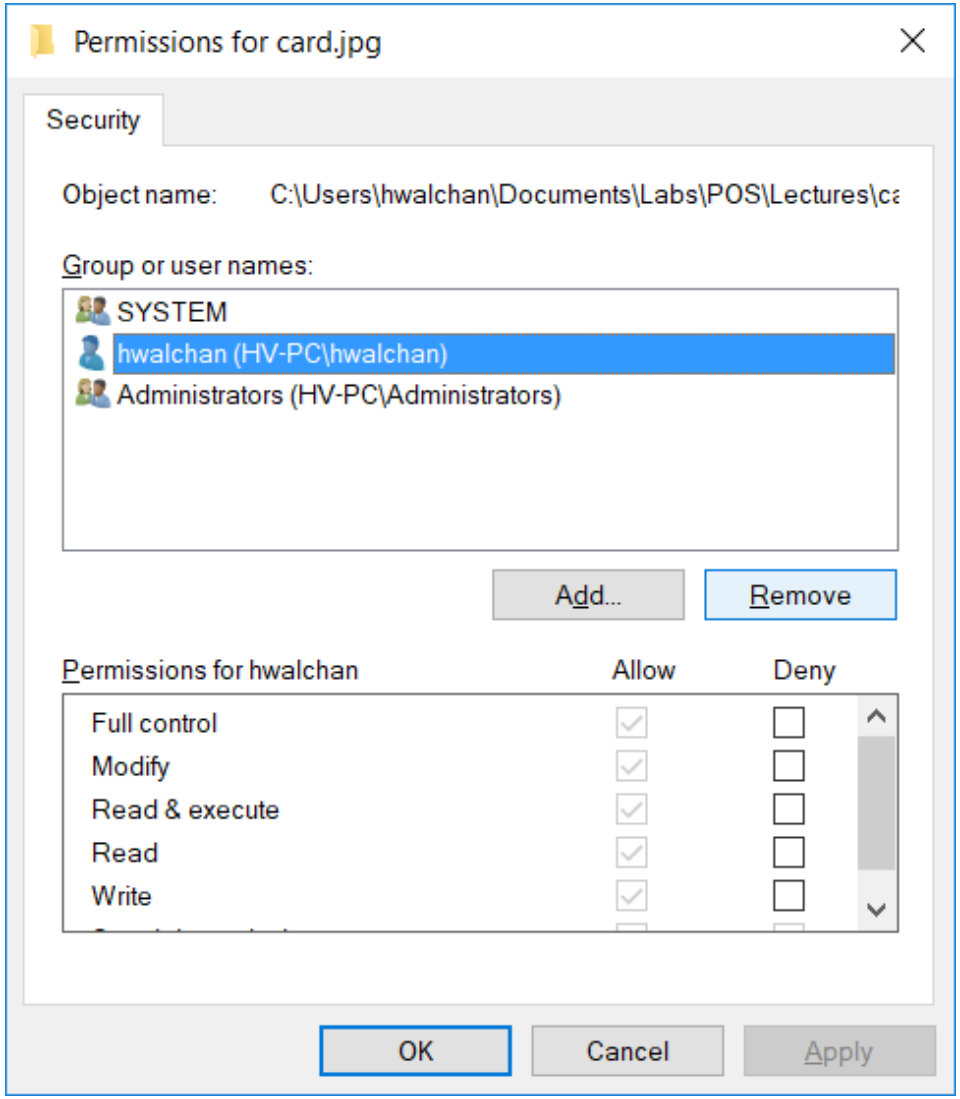
- Какво потребител може да изпълнява.



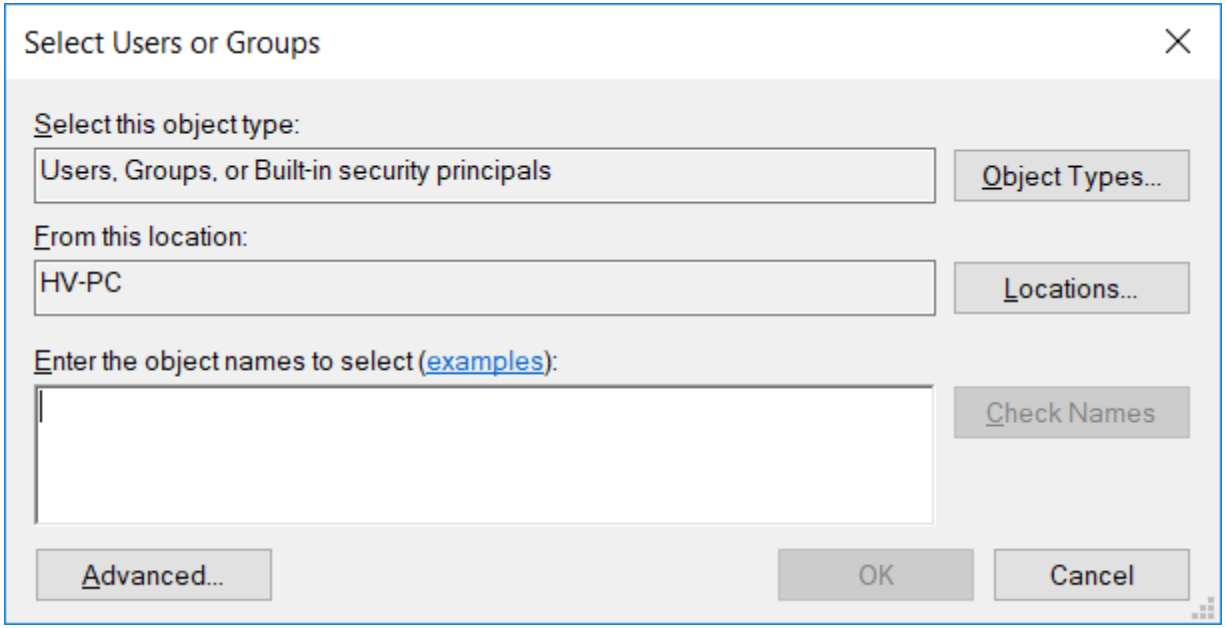
Управление на достъп в Windows



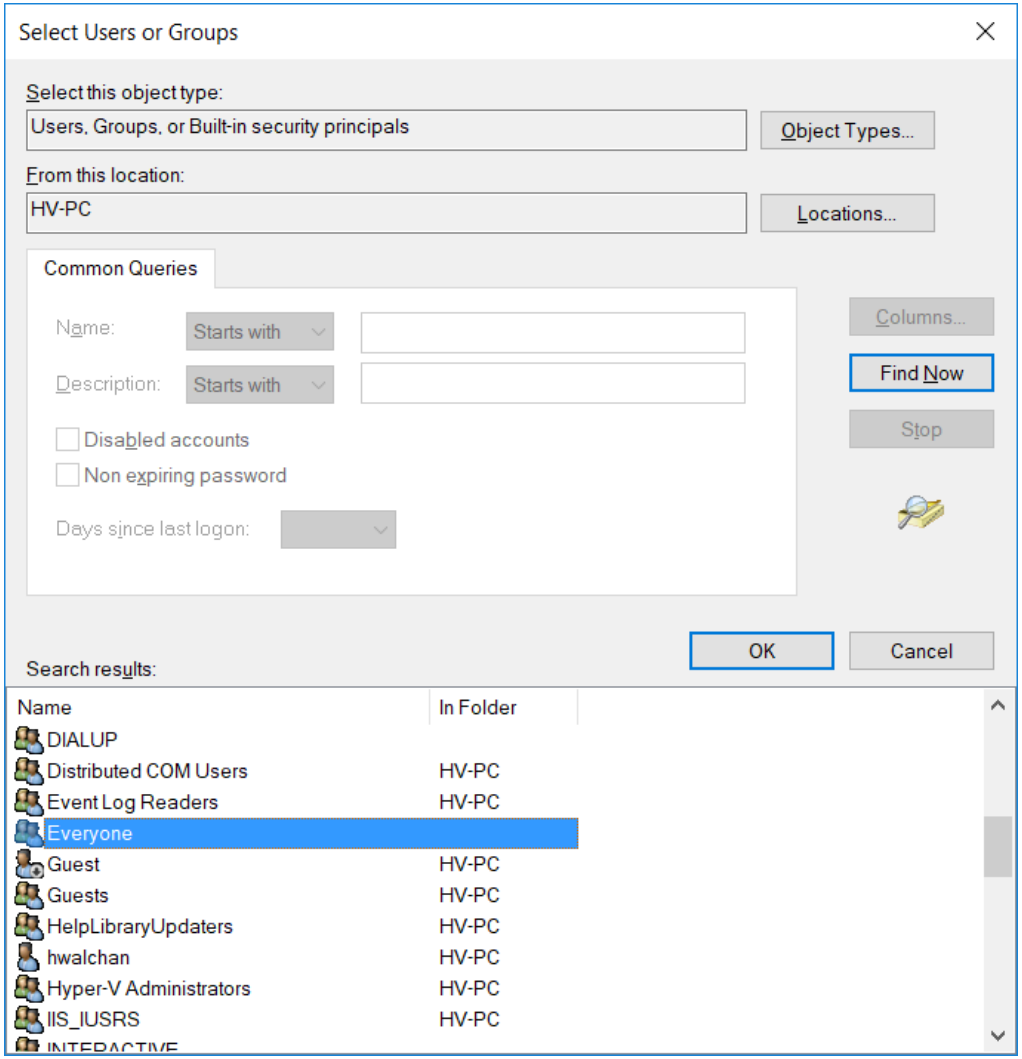
Управление на достъп в Windows



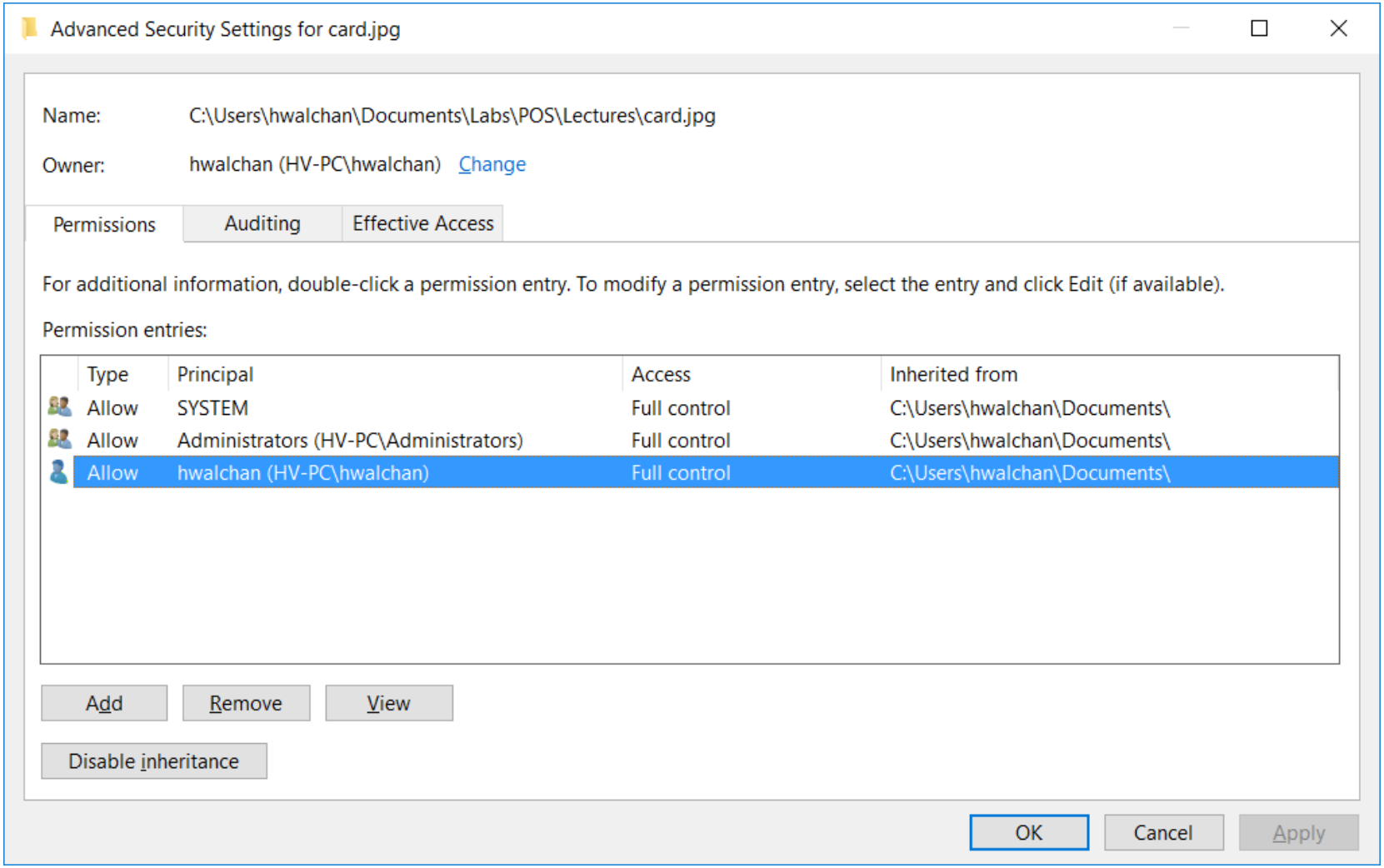
Управление на достъп в Windows



Управление на достъп в Windows



Управление на достъп в Windows



Защита от зловреден софтуер

- Обновяване на операционната система
- Премахване на уязвимости (patching)
- Антивирусен софтуер

Въпроси ?