

窦轶////yi.dou@njupt.edu.cn

O p e r a t i n g   S y s t e m s

# 操作系统



# 文件安全

Linux  
Android  
Linux  
OpenStack  
Mac OS  
Windows



# 文件安全

## 本讲内容

1. 文件安全的基本要求
2. 文件存取控制矩阵
3. 文件存取控制表
4. 口令和密码

# 文件安全的基本要求

文件保护：防止用户破坏文件内容

文件保密：防止非法用户访问文件

# 文件安全的基本要求

## 1 文件安全需求

- ①保证有权限的合法用户对文件的各种合法操作
- ②防止没有权限的用户对文件进行的各种非法操作
- ③防止非法用户冒充合法用户对文件进行各种操作
- ④防止有权限的合法用户对文件的非法违规操作

# 文件安全的基本要求

## 2 存取控制验证模块

①验证用户的身份、权限

②比较用户权限和本次存取要求是否相符

③若有冲突，则拒绝本次文件存取操作



# 文件安全

## 本讲内容

1. 文件安全的基本要求
2. 文件存取控制矩阵
3. 文件存取控制表
4. 口令和密码

# 文件存取控制矩阵

- 存取控制矩阵是利用一个二维矩阵来实现文件的存取控制
- 一维列出使用文件系统的全部用户，一维列出系统中的全部文件
- 每一项表示用户对文件的存取权限
- 存取权限包括读（Read）、写（Write）和执行（eXecute）
- 存取控制验证模块比较存取控制矩阵与本次存取，如果不匹配，就拒绝执行

权 限 文件	用户	Huang	Zhang	Lee	...
Print		RWX	RX	X	...
Hello.c		RW	W	R	...
count		R	RWX	X	...
...		...	...	...	...



# 文件存取控制矩阵

权 限 文 件	用 户	Huang	Zhang	Lee	...
Print		RWX	RX	X	...
Hello.c		RW	W	R	...
		---	---	--	
Hello.c		RW	W	R	...
count		R	RWX	X	...
...		...	...	...	...

# 文件安全

## 本讲内容

1. 文件安全的基本要求
2. 文件存取控制矩阵
3. 文件存取控制表
4. 口令和密码


# 文件存取控制表

## 1 基于用户分组

文件主

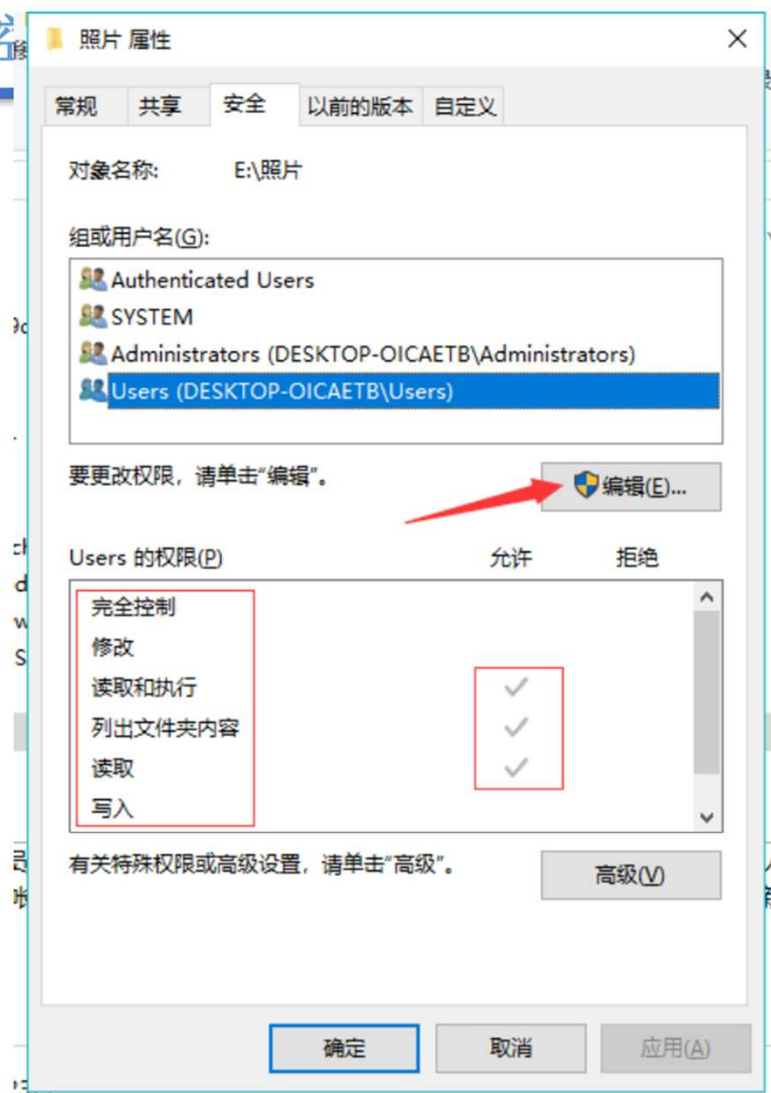
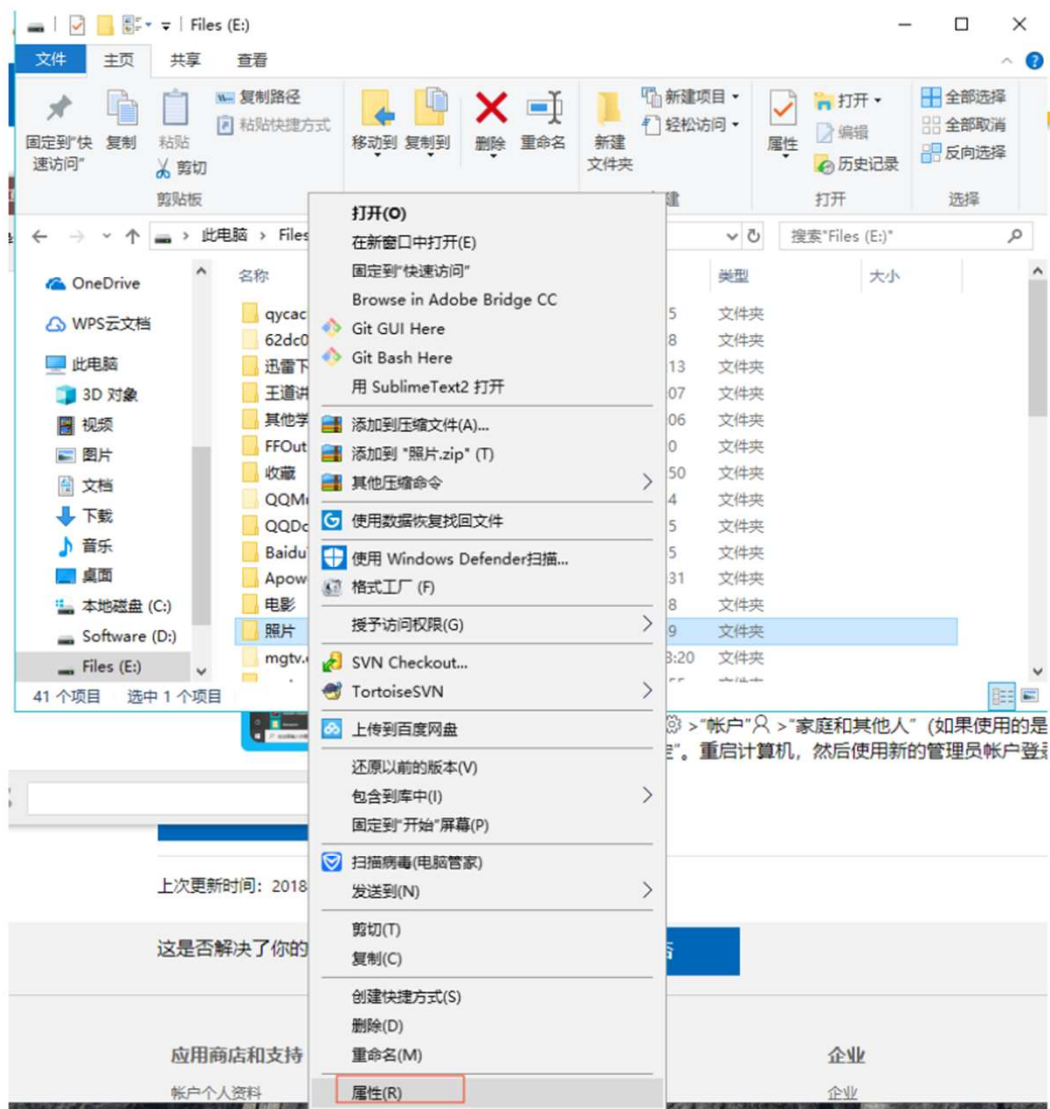
文件主同组用户

其他用户

 系统为每个文件建立一个存取控制表，表中记录各类用户对该文件的存取权限

文件 A 的存取控制表

用户类别	权限
文件主	{RWX}
同组用户	{RX}
其他用户	{X}



# 文件存取控制表

## 2 UNIX/LINUX

- 📖 用户分为文件主、同组用户、其他用户三类，定义存取权限可读r、可写w、可执行x，文件属性

- rwx rwx rwx



```

jyin@jyin: ~/folder1$ ll
total 48
drwxr-xr-x 3 jyin jyin 4096 Apr 25 22:41 ./
drwxr-xr-x 8 jyin jyin 4096 Apr 24 11:11 ../
-rwxr-xr-x 1 jyin jyin 16688 Apr 23 22:18 a.out*
-rw-r--r-- 2 jyin jyin 6 Apr 23 22:16 file1.txt
-rw-r--r-- 1 jyin jyin 50 Mar 15 10:44 file2.txt
-rw-r--r-- 2 jyin jyin 6 Apr 23 22:16 file3.txt
lrwxrwxrwx 1 jyin jyin 9 Apr 25 22:26 file4.txt -> file1.txt
drwxr-xr-x 2 jyin jyin 4096 Apr 25 22:41 folder2/
-rw-rw-rw- 1 jyin jyin 73 Apr 23 22:18 hello.c
jyin@jyin: ~/folder1$ _

```

文件类型	链接数	所属组	最后修改时间	文件名
-rw-rw-r--	1	stu	0	common
文件权限	拥有者	大小		



-rw-rw-r--.	1	stu	stu	0	Jul	12	19:08	common	普通文件
lrwxrwxrwx.	1	stu	stu	6	Jul	12	19:09	link -> common	链接文件
drwxrwxr-x.	2	stu	stu	4096	Jul	12	19:08	list	目录文件
prw-rw-r--.	1	stu	stu	0	Jul	12	19:09	tunnel	管道文件
crw-rw----.	1	root	root	1, 11	Jul	12	19:01	kmsg	字符设备文件
srw-rw-rw-.	1	root	root	0	Jul	12	19:02	log	套接字设备文件
brw-rw----.	1	root	disk	7, 0	Jul	12	19:01	loop0	块设备文件

字段 1: 表示文件类型

字段 2: 文件所有者对该文件的权限

字段 3: 文件所属组的权限

字段 4: 其他用户的权限（既不是文件所有者也不是文件所属组的用户）

# 文件安全

## 本讲内容

1. 文件安全的基本要求
2. 文件存取控制矩阵
3. 文件存取控制表
4. 口令和密码

## 口令保护



为文件设置一个“口令”（如：abc112233），用户请求访问该文件时必须提供“口令”。

文件控制块（FCB）

口令一般存放在文件对应的 FCB 或索引结点中。用户访问文件前需要先输入“口令”，操作系统会将用户提供的口令与FCB中存储的口令进行对比，如果正确，则允许该用户访问文件

# 口令和密码

## 1 口令

📖 创建文件时，  
为该文件设置  
的口令，**口令**  
**存放于文件说**  
**明中，不够安**  
**全**

**优点：**

简单，易实现

**缺点：**

保密性相对较差

改变存取控制不方便

存取权限控制粗粒度

# 口令和密码

## 2 密码

- ❏ 在用户创建文件后写入存储设备时对文件进行编码加密
- ❏ 读取文件时，根据用户提供的代码键将文件进行译码解密，将其还原为源文件
- ❏ 文件写入时的编码工作及读出时的译码都由系统存取控制验证模块来承担



# 文件安全

Linux  
Android  
Linux  
OpenStack  
Mac OS  
Windows

