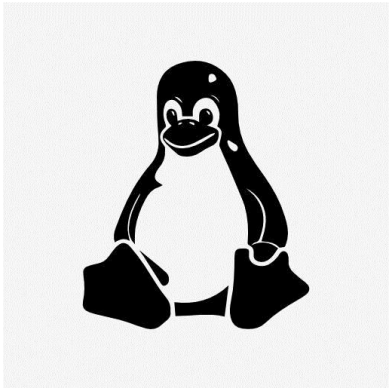
1.17 SeLinux

讲师：汪洋

目录

1 Selinux 前世今生



D C1 C2 B1 B2 B3 A1

《关于UNIX的安全》“首先要面对的事实是，UNIX的开发者并没有考虑安全问题，单单这一点就会引发大量的漏洞”

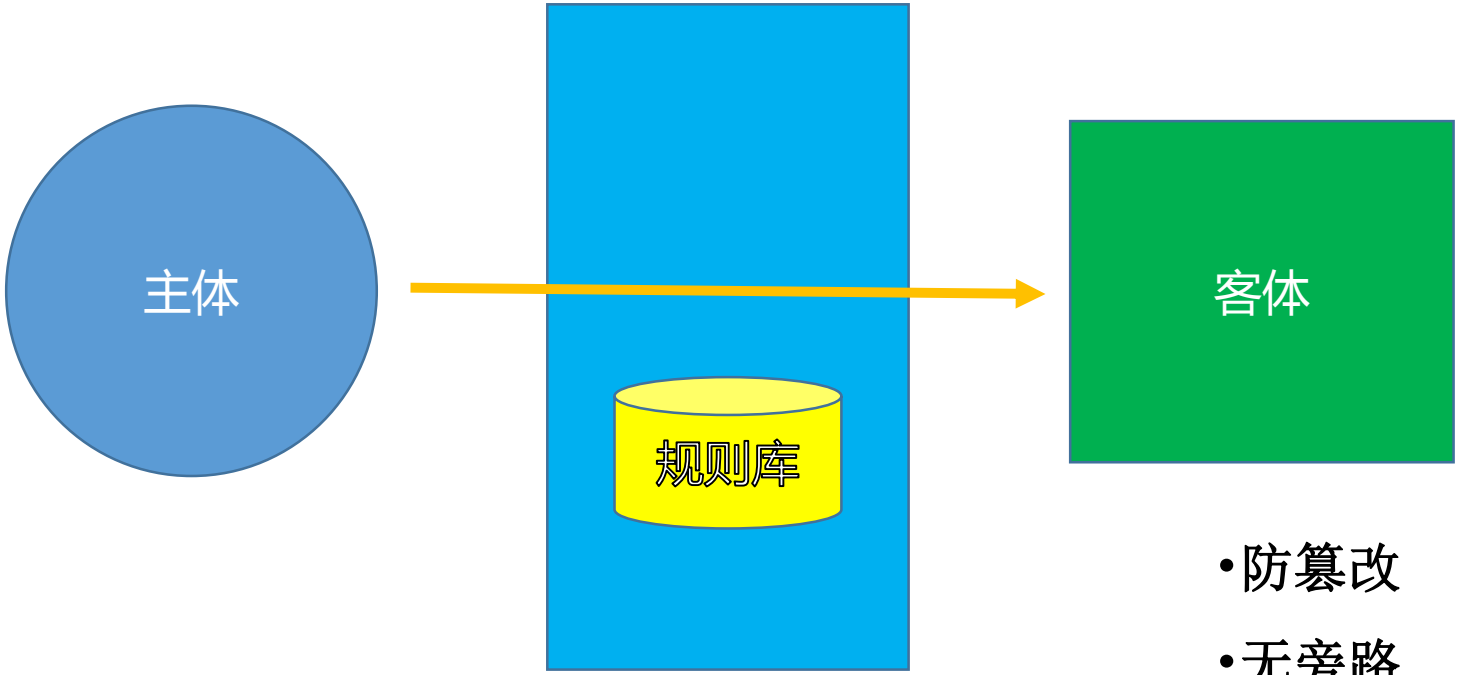
----- Dennis Ritchie

selinux

acl

iptables

tcp wrappers

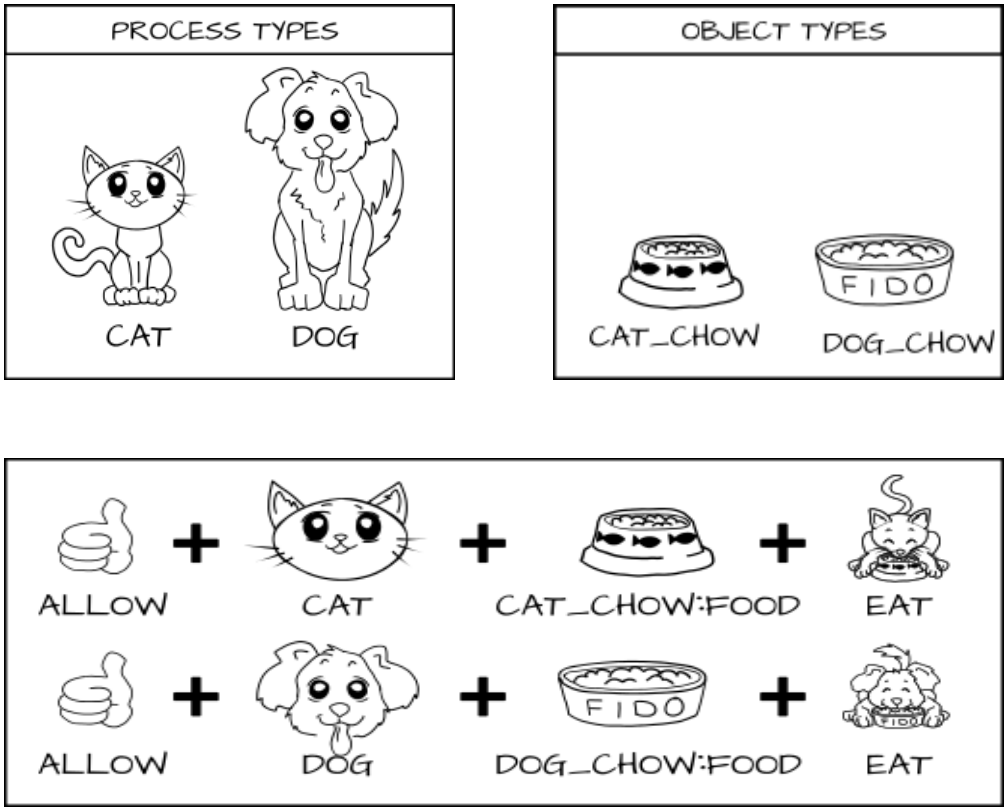


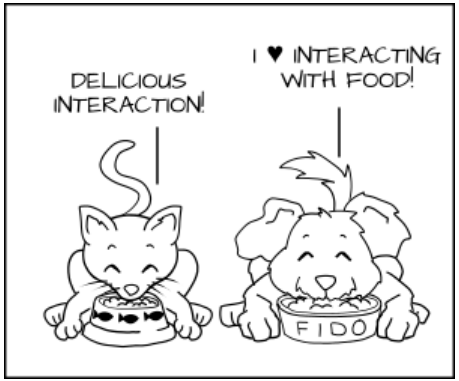
- 防篡改
- 无旁路
- 可验证

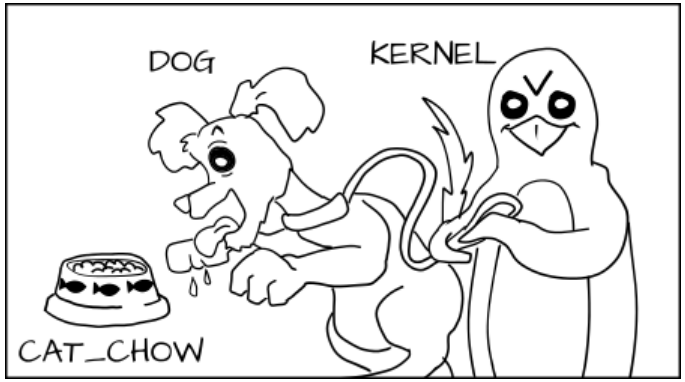
2.2→需要手动加载的一个外部模块

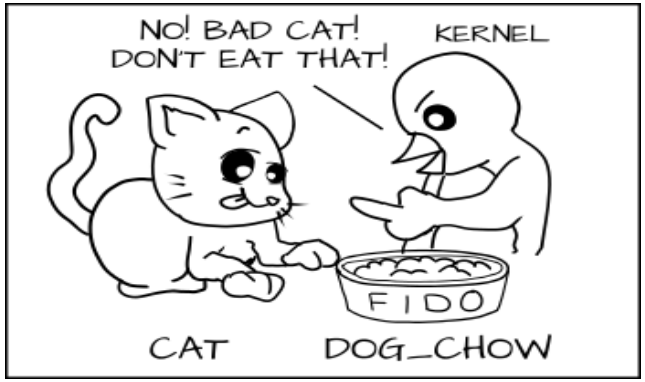
2.4→直接写到内核的一个模块

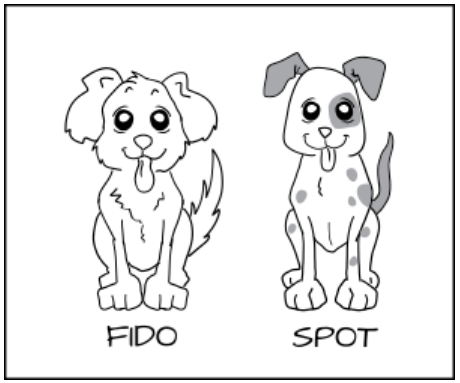
2.6→成为了一部分Linux发行版的内核的一部分


PROCESS TYPES
CAT
DOG
OBJECT TYPES
CAT_CHOW
FIDO
DOG_CHOW
ALLOW
CAT
CAT_CHOW:FOOD
EAT
ALLOW
DOG
FIDO
DOG_CHOW:FOOD
EAT

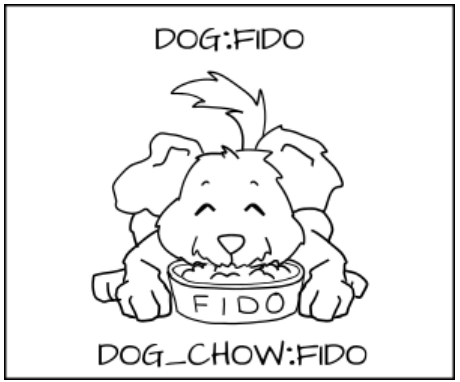

DELICIOUS INTERACTION!
I ♥ INTERACTING WITH FOOD!
FIDO

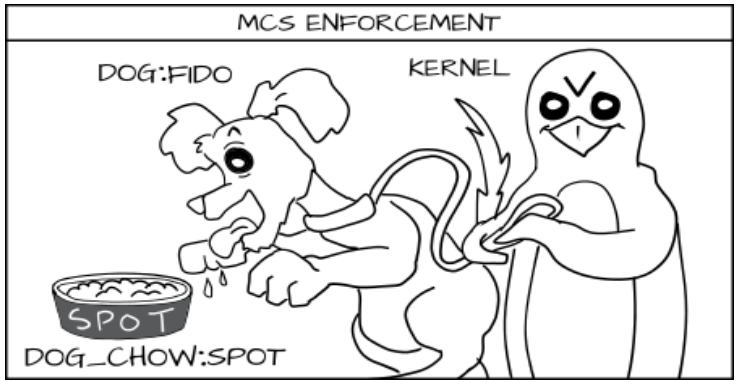

DOG
KERNEL
CAT_CHOW


NO! BAD CAT! DON'T EAT THAT!
KERNEL
FIDO
CAT
DOG_CHOW


FIDO
SPOT


FIDO
SPOT
DOG_CHOW:RANDOM1
DOG_CHOW:RANDOM2


DOG:FIDO
FIDO
DOG_CHOW:FIDO


MCS ENFORCEMENT
DOG:FIDO
KERNEL
SPOT
DOG_CHOW:SPOT

2 安全上下文

所有操作系统访问控制都是以关联的客体和主体的某种类型的访问控制属性为基础的。在 SELinux 中，访问控制属性叫做安全上下文。所有客体（文件、进程间通讯通道、套接字、网络主机等）和主体（进程）都有与其关联的安全上下文，一个安全上下文由三部分组成：用户、角色和类型标识符。常常用下面的格式指定或显示安全上下文：

用户:角色:类型

chcon [-R] [-t type] [-u user] [-r role] 文件

选项与参数：

-R ：连同该目录下的次目录也同时修改；

-t ：后面接安全性本文的类型字段！

-u ：后面接身份识别，例如 system_u；

-r ：后面接角色，例如 system_r；

restorecon 还原成原有的 SELinux type

格式：restorecon [-Rv] 档案或目录

选项与参数：

-R ：连同次目录一起修改；

-v ：将过程显示到屏幕上

3 Selinux 布尔值

Managing Boole（管理 SElinux布尔值）

Seliux 布尔值就相当于一个开关，精确控制 Selinux 对某个服务的某个选项的保护，比如samba服务

```
[root@localhost booleans]# getsebool -a | grep samba
samba_create_home_dirs --> off
samba_domain_controller --> off
samba_enable_home_dirs --> on
samba_export_all_ro --> off
samba_export_all_rw --> off
samba_portmapper --> off
samba_run_unconfined --> off
samba_share_fusefs --> off
samba_share_nfs --> off
sanlock_use_samba --> off
use_samba_home_dirs --> off
virt_use_samba --> off
```

getsebool -a命令列出系统中可用的SELinux布尔值。

setsebool命令用来改变SELinux布尔值

```
setsebool -p samba_enable_home_dirs=1
```

开启家目录是否能访问的控制