



Definition of SELinux

MAC





~~80:20:DE:AD:BE:EF~~

Mandatory

Access

Control

... refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target.

```
var subject = [  
    'process',  
    'thread'  
];
```

```
var object = [  
  'file',  
  'directory',  
  'port',  
  'shm'  
];
```

SELinux adheres to the concept of least privilege, which gives a process exactly the rights it needs to perform it's given task.

Yes, that
includes
almighty
Rook!

Short History of SELinux

1992 = First concepts
by NSA



2001 = Intro at Linux
Kernel Summit
by the NSA.

Work on Linux
Security Modules
begins

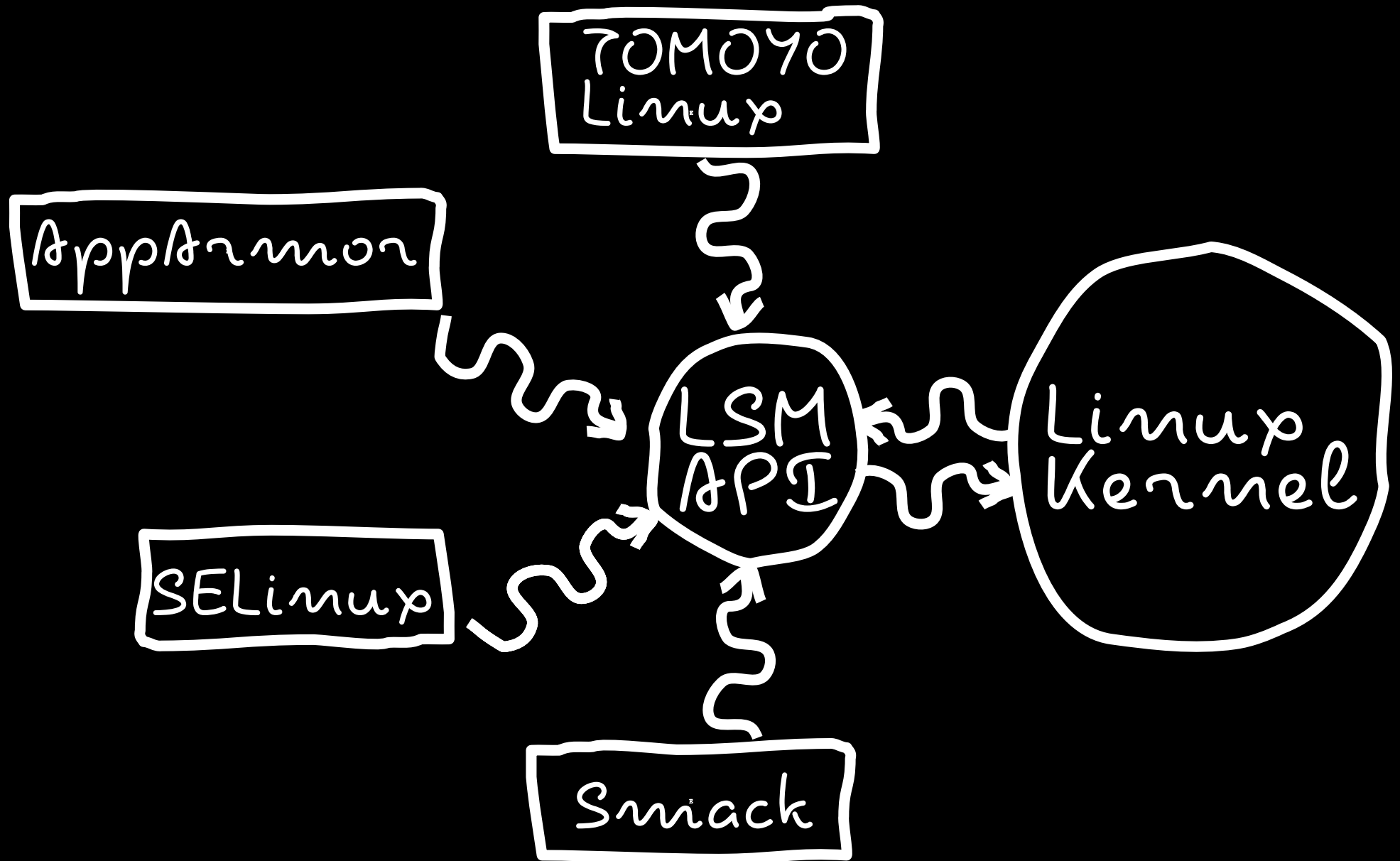
2002 = Integration into
Kernel 2.4 via
module.

2003 = Release of Linux
Kernel 2.6 with
LSM.

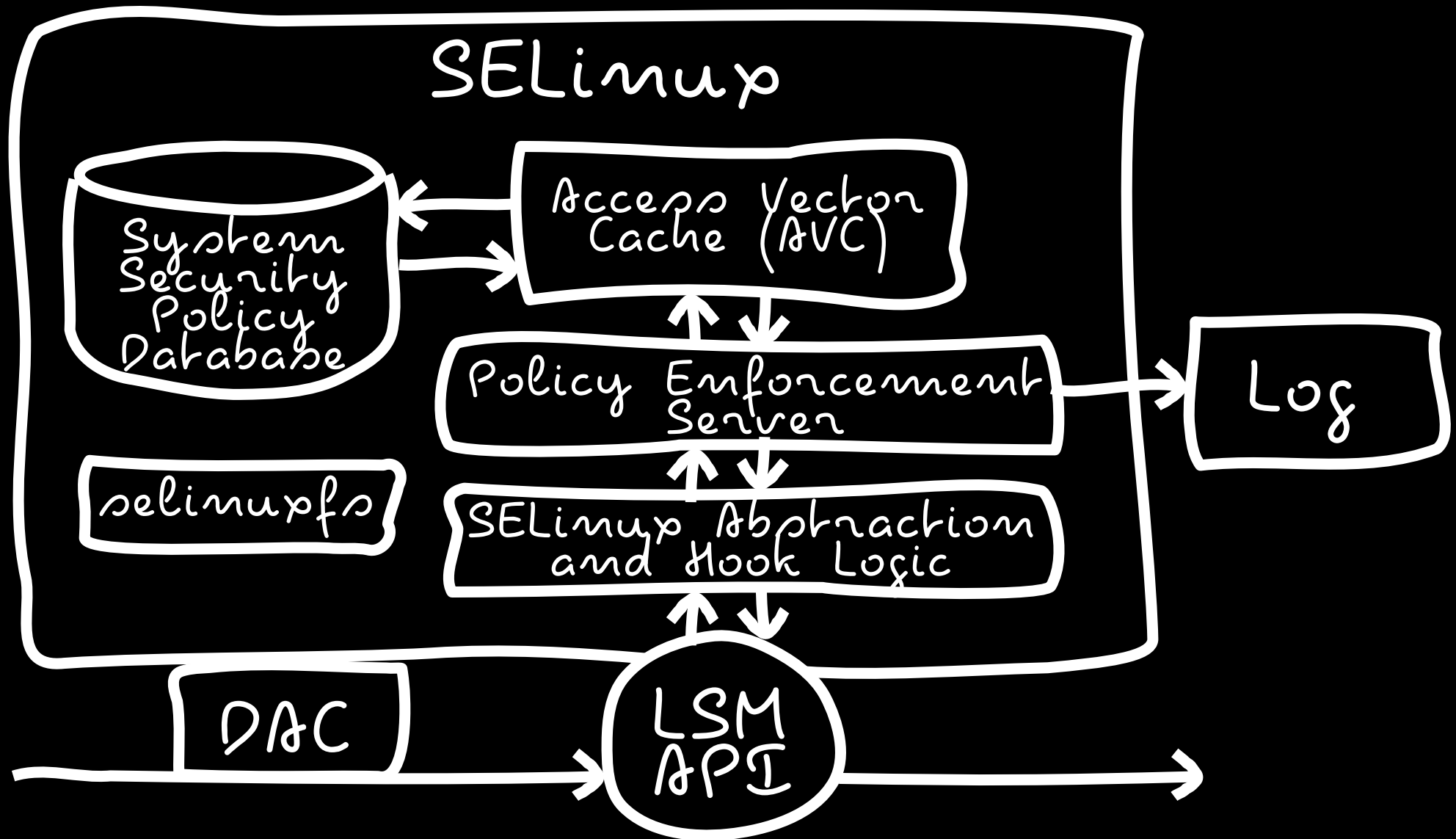
2005 = Inclusion of 
SELinux in RHEL 4

Architecture Overview

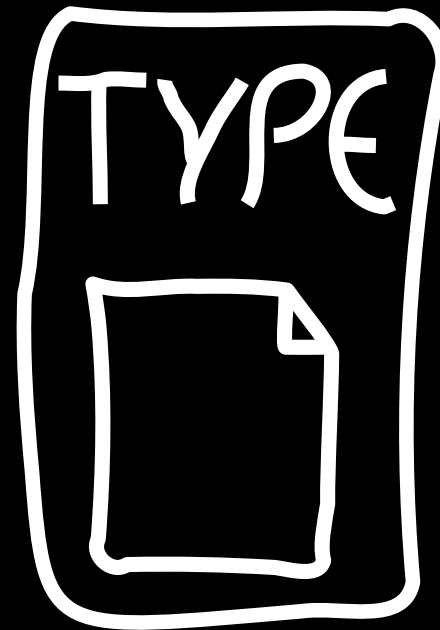
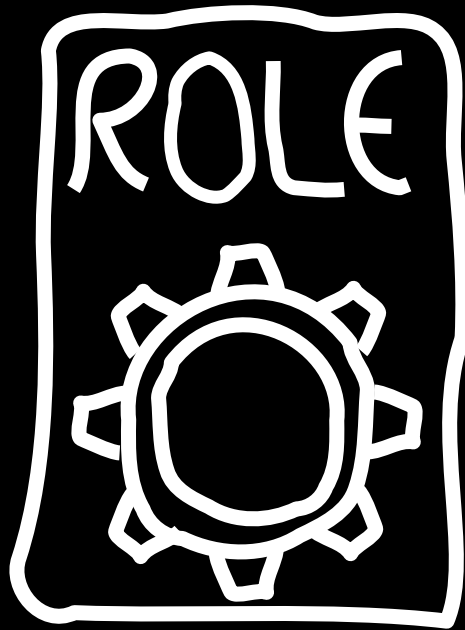
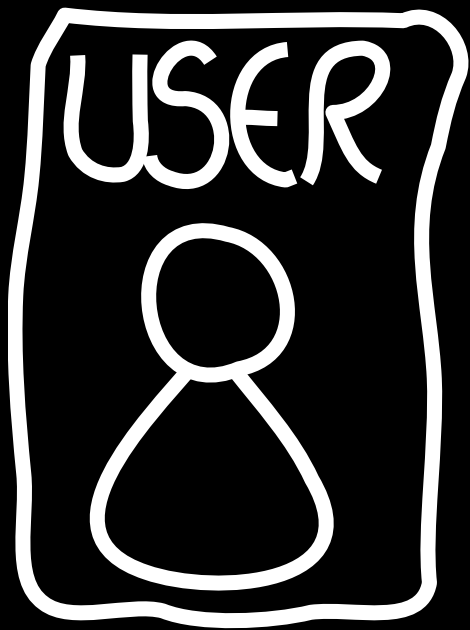
Linux Security Modules



SELinux Components



Security Context

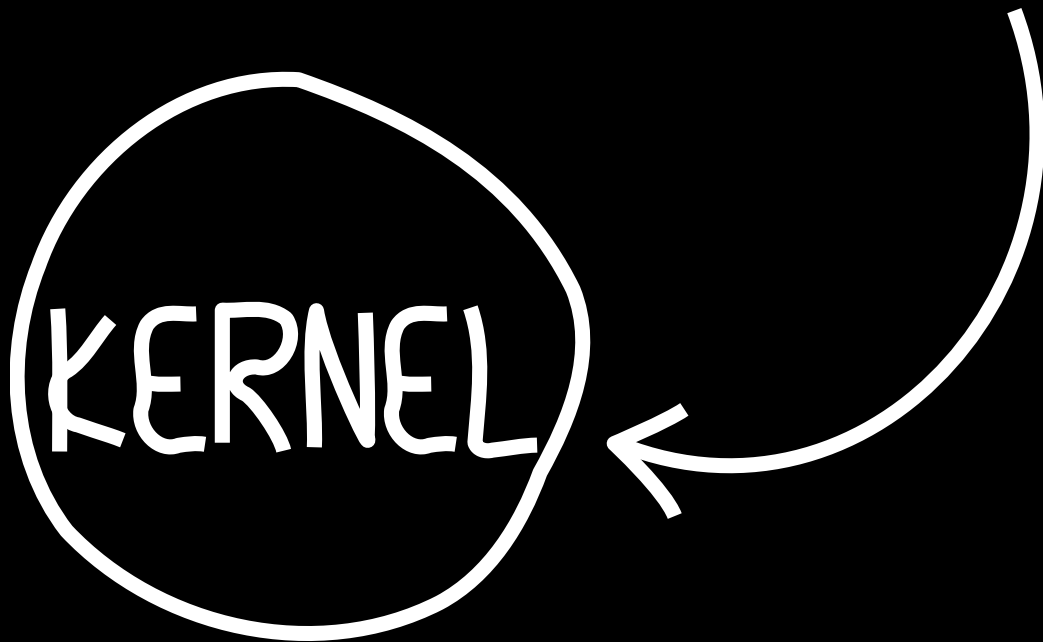


Prerequisites

XATTR

CONFIG_AUDIT

CONFIG_SECURITY_SELINUX



Confirm **Kernel** features

```
# egrep "CONFIG_(.*SELINUX|AUDIT)|XATTR" \  
/boot/config-2.6.18-348.4.1.el5
```

CONFIG_AUDIT_ARCH=y

CONFIG_AUDIT=y

CONFIG_AUDITSYSCALL=y

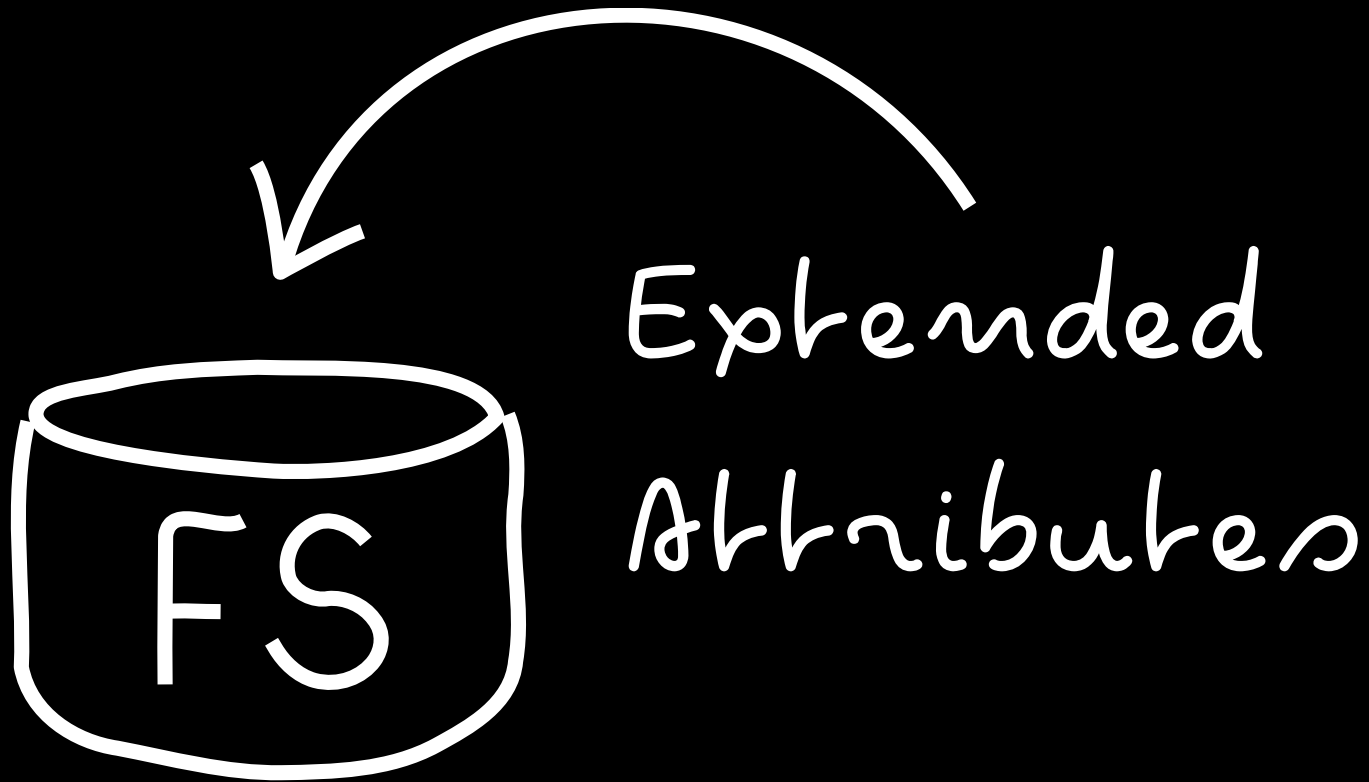
CONFIG_EXT2_FS_XATTR=y

CONFIG_EXT3_FS_XATTR=y

CONFIG_EXT4_FS_XATTR=y

CONFIG_CIFS_XATTR=y

CONFIG_SECURITY_SELINUX=y



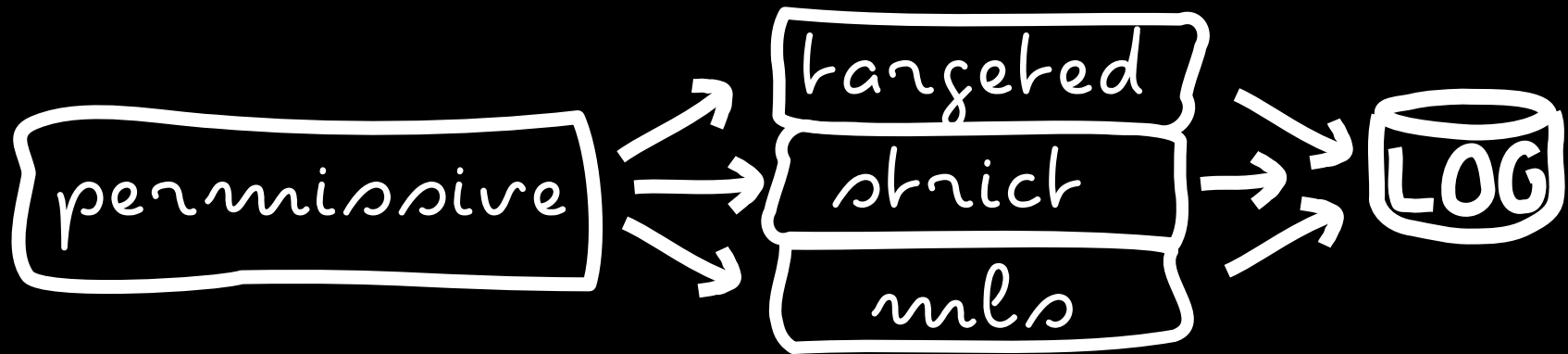
Confirm extended attributes

```
# tune2fs -l /dev/sda1 | grep features:  
Filesystem features:    ... ext_attr ...
```

Enough theory
already,
bring
on
the
goods!



/etc/selinux/config



Check current status

```
# sestatus
```

```
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:        enforcing
Policy version:                21
Policy from config file:      targeted
```

Mid flight **mode** change

getenforce

Enforcing

Check

setenforce 0

getenforce

Permissive

Disarm

setenforce 1

getenforce

Enforcing

Re-enable

My role in this?

```
# secon
```

```
user: user_u
```

```
role: system_r
```

```
type: unconfined_t
```

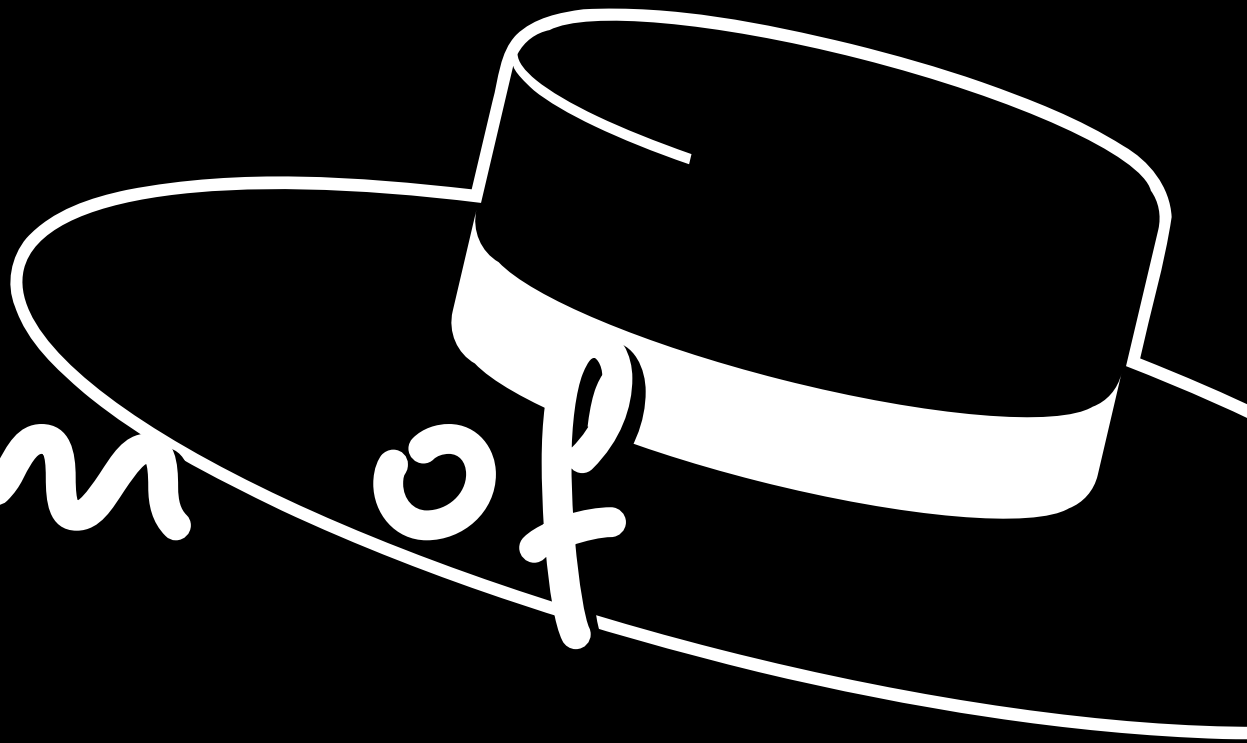
```
Sensitivity: s0
```

```
Clearance: s0
```

```
Mls-range: s0
```

The

Option of



SELinux enabled utilities

ls

ps

id

netstat

find -context

lsof (RHEL 6)

Sample output

```
# ls -Z
```

```
drwxr-xr-x  root root system_u:object_r:default_t foo
```

```
# ps -Z
```

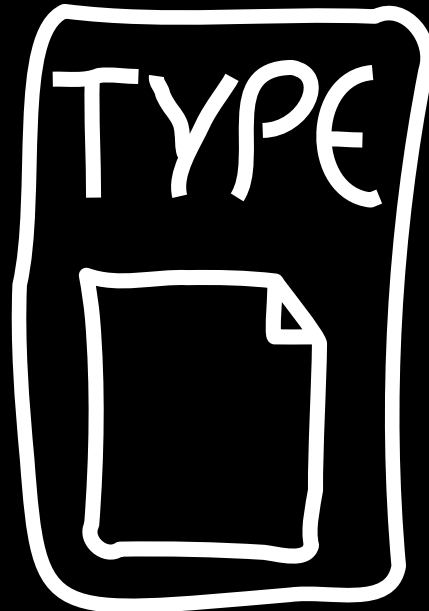
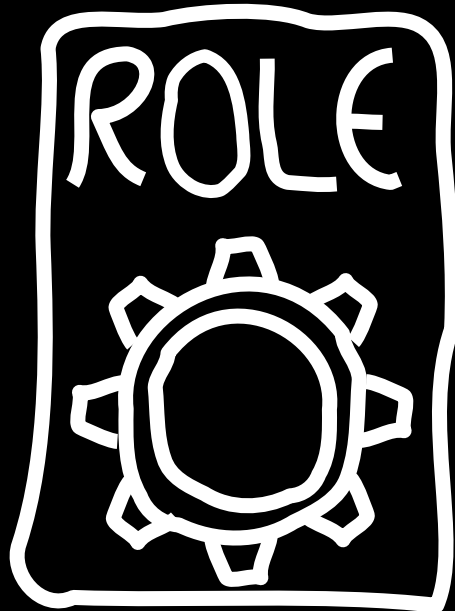
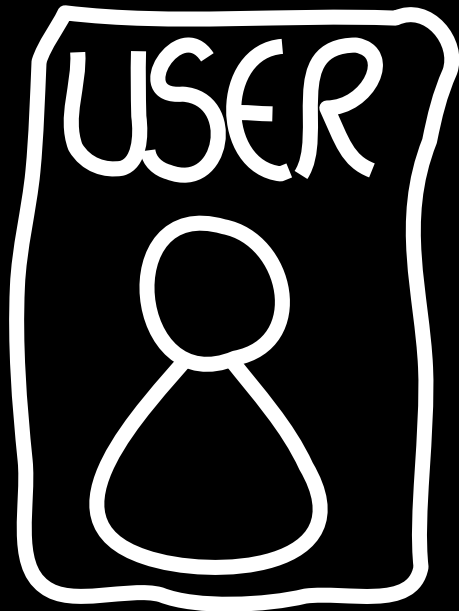
LABEL	PID	TTY	TIME	CMD
user_u:system_r:unconfined_t	2508	pts/0	00:00:07	sudo

```
# id -Z
```

```
user_u:system_r:unconfined_t
```

Output to Context

system_u:object_r:file_t:s0



Making
changes

SELinux tools

getsebool
setsebool
chcon
semanage
restorecon

List booleans

```
# getsebool -a
NetworkManager_disable_trans --> off
aisexec_disable_trans --> off
allow_aisexec_rw_tmpfs --> off
allow_console_login --> off
allow_cvs_read_shadow --> off
allow_daemons_dump_core --> on
allow_daemons_use_tty --> on
```

Toggle value

```
# setsebool NetworkManager_disable_trans on  
# getsebool NetworkManager_disable_trans  
NetworkManager_disable_trans --> on
```

Change context

```
# cd /var/tmp/foo
# ls -Z bar
-rw-r--r-- root root user_u:object_r:tmp_t:s0 bar

# chcon -t file_t bar
# ls -Z bar
-rw-r--r-- root root user_u:object_r:file_t:s0 bar
```

Manage context

```
# semanage fcontext -a -t default_t /var/tmp/foo/bar
```

```
# ls -Z bar
```

```
-rw-r--r-- root root user_u:object_r:file_t:s0 bar
```

```
# restorecon /var/tmp/foo/bar
```

```
# ls -Z bar
```

```
-rw-r--r-- root root user_u:object_r:default_t:s0 bar
```

Restore context

```
# cd /var/tmp/foo
# ls -Z bar
-rw-r--r-- root root user_u:object_r:file_t:s0 bar

# restorecon bar
# ls -Z bar
-rw-r--r-- root root user_u:object_r:tmp_t:s0 bar
```

Trouble
shooting

Auditing tools

audit2allow
audit2why

Aggregating audit log

```
# audit2allow -a
```

```
#===== restorecon_t =====  
allow restorecon_t syslogd_t:dir relabelto;  
allow restorecon_t syslogd_t:file relabelto;
```

```
#===== syslogd_t =====  
allow syslogd_t default_t:file append;
```

Babelfishing the log

```
# audit2why < /var/log/audit/audit.log  
type=AVC msg=audit(1355080647.280:69): avc: denied \  
  { relabelto } for  pid=3699 comm="restorecon" \  
  name="log" dev=loop0 ino=7905 \  
  scontext=user_u:system_r:restorecon_t:s0 \  
  tcontext=system_u:object_r:syslogd_t:s0 tclass=dir
```

Was caused by:

Missing or disabled TE allow rule. \
Allow rules may exist but be disabled \
by boolean settings; check boolean settings. \
You can see the necessary allow rules by \
running audit2allow with this audit message \
as input.

Resources

< <http://selinuxproject.org> >

< <http://en.wikipedia.org/wiki/SELinux> >

< <https://fedoraproject.org/wiki/SELinux> >



Thank you

