

[FlashDOT-intel~]\$

[HR • intel ~]\$

• /home/ivan/HR
→ Complaint Log

• /home/ivan/Events
→ Financial Documents

[Intel • intel ~]\$

• /home/gary/Research
→ Complaint Log

• /home/gary/Secret
→ Financial Documents

[IT • intel ~]\$

• /home/freddy/Security
→ Complaint Log

• /home/freddy/Support
→ Financial Documents

[Finance • intel ~]\$

• /home/frederick/Budget
→ Complaint Log

• /home/frederick/Payroll
→ Financial Documents

```
[FlashDOT-intel~]$ ls
```

```
Gary_Tsai  Ivan_Lugo  Freddy_Velez  Frederick_Chute
```

G.I.F.F CHART

NAME	CATEGORY							
GARY	c1				c5		c7	c8
IVAN		c2				c6		c8
FREDERICK			c3			c6		c8
FREDDY				c4	c5		c7	c8

		PRIVILEGE CHART			
		GARY	FREDERICK	FREDDY	IVAN
DEPARTMENT	DIRECTORY	~~~~~			
HR	HR				*
	EVENTS	*	*	*	*
IT	SECURITY	*		*	
	SUPPORT	*	*	*	*
FINANCE	BUDGET	*	*	*	*
	PAYROLL		*		*
INTEL	RESEARCH	*		*	
	SECRET	*			

Keys of who we are:

Intel=s0:c1

HR=s0:c2

Finance=s0:c3

IT=s0:c4

S= sensitivity

C = category

Keys of what we have:

Ticketing = c8

Payroll= c6

Budgeting =c8

HR= c2

Security = c5

Event = c8

Research= c7

Secret =c1

c8= Used to share among all departments

Multi-Category Security

```
[root@CentOS ~]# semanage login -l
```

Login Name	SELinux User	MLS/MCS Range	Service
__default__	user_u	s0	*
freddy	user_u	s0:c4,c5,c7,c8	*
frederick	user_u	s0:c3,c6,c8	*
gary	user_u	s0:c1,c5,c7,c8	*
garytsai	root	s0-s0:c0.c1023	*
guestuser	guest_u	s0	*
ivan	user_u	s0:c2,c6,c8	*
restricteduser	user_u	s0	*
root	system_u	s0-s0:c0.c1023	*
system_u	system_u	s0-s0:c0.c1023	*
tony	guest_u	s0	*

```
[root@CentOS ~]#
```

```
[root@CentOS ~]# semanage user -l
```

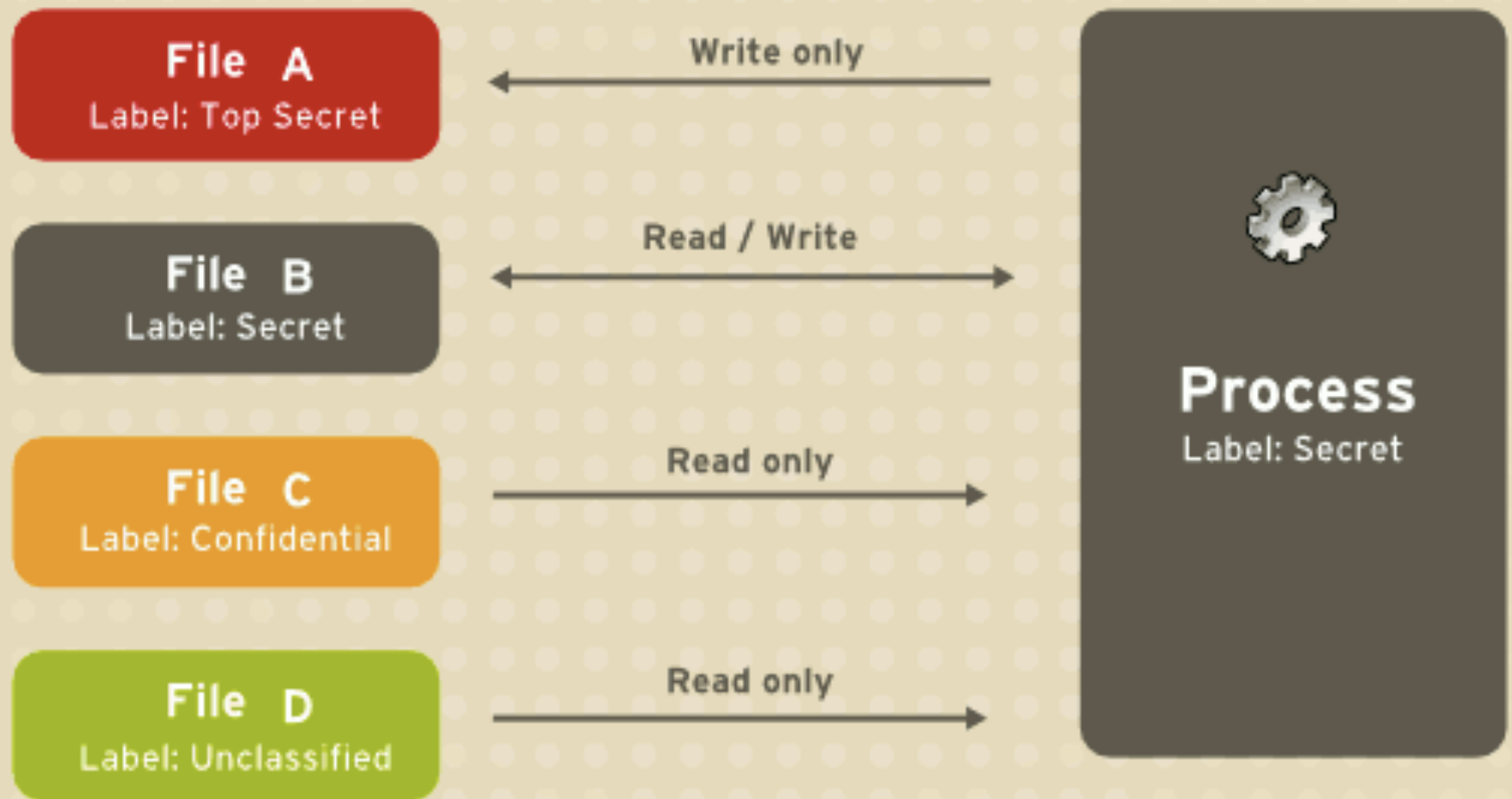
SELinux User	Labeling Prefix	MLS/MCS Level	MLS/MCS Range	SELinux Roles
guest_u	user	s0	s0:c0	guest_r
root	user	s0	s0-s0:c0.c1023	staff_r sysadm_r system_r unconfined_r
staff_u	user	s0	s0-s0:c0.c1023	staff_r sysadm_r system_r unconfined_r
sysadm_u	user	s0	s0-s0:c0.c1023	sysadm_r
system_u	user	s0	s0-s0:c0.c1023	system_r unconfined_r
unconfined_u	user	s0	s0-s0:c0.c1023	system_r unconfined_r
user_u	user	s0	s0-s0:c0.c1023	user_r
xguest_u	user	s0	s0	xguest_r

```
[root@CentOS ~]#
```


Multi-Level Security



Available data flows using an MLS system.



Processes can read the same or lower security levels but can only write to their own or higher security level.

tsudo: password for garytsar:

```
[root@centos ~]# semanage login -l
```

Login Name	SELinux User	MLS/MCS Range	Service
__default__	user_u	s0	*
fred	user_u	s1:c200	*
frederick	user_u	s2:c400	*
gary	user_u	s3:c500	*
ivan	user_u	s2:c300	*
root	root	s0-s15:c0.c1023	*
system_u	system_u	s0-s15:c0.c1023	*

```
[root@centos ~]# _
```

```
[root@centos ~]# semanage user -l
```

SELinux User	Labeling Prefix	MLS/MCS Level	MLS/MCS Range	SELinux Roles
guest_u	user	s0	s0	guest_r
root	user	s0	s0-s15:c0.c1023	auditad
staff_r	secadm_r	sysadm_r	system_r	
staff_u	user	s0	s0-s15:c0.c1023	auditad
staff_r	secadm_r	sysadm_r	system_r	
sysadm_u	user	s0	s0-s15:c0.c1023	sysadm_
system_u	user	s0	s0-s15:c0.c1023	system_
user_u	user	s0	s0-s15:c0.c1023	user_r
xguest_u	user	s0	s0	xguest_

```
[root@centos ~]# _
```