

Sequencing bugs

```
seteuid(0)  
.  
.  
.  
seteuid(getuid())
```

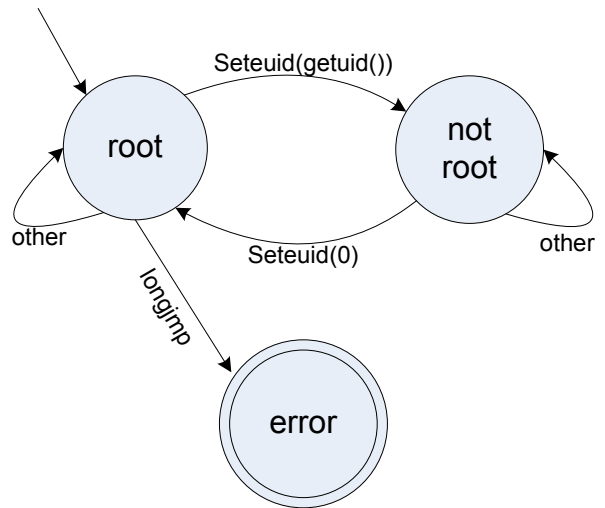
To restrict to a subsystem:

```
Chract(some_dir);  
Chdir("/");
```

Ms

1. You cannot call "longjmp" as root

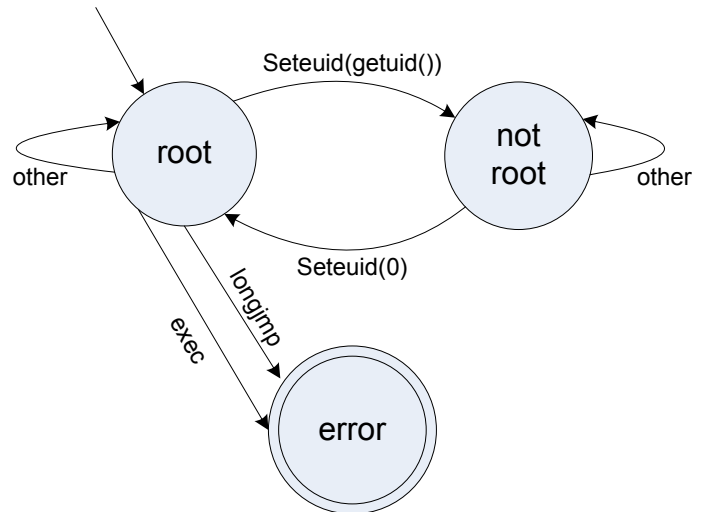
In term of FSA



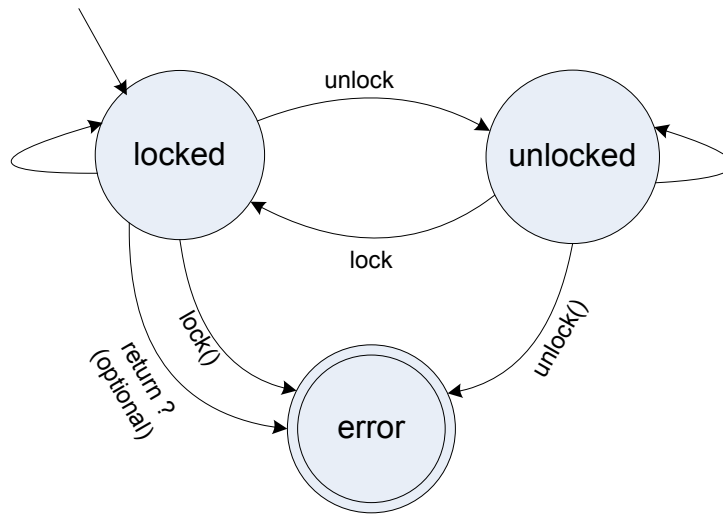
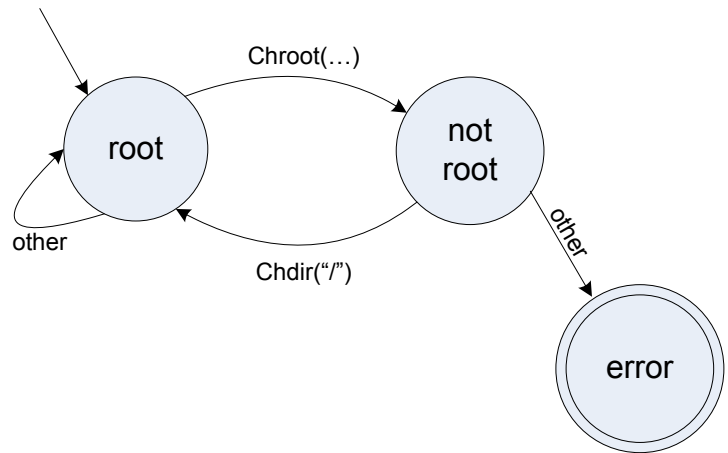
2. Do not call "exec" as root

E.g: bad thing to do

```
seteuid(0)  
.  
.  
.  
exec(helper_program);
```



3. chroot must always be followed by chdir



MOPS: 12 bugs. 70 false possibilities

Model checking

P

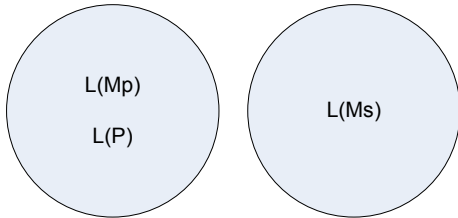
```
Int main(...)  
{  
  seteuid(0);  
  dummy();  
  if(...)  
    setuid(getuid())  
  dummy();  
  exec();  
}
```

L(M) = language generated/accepted by M

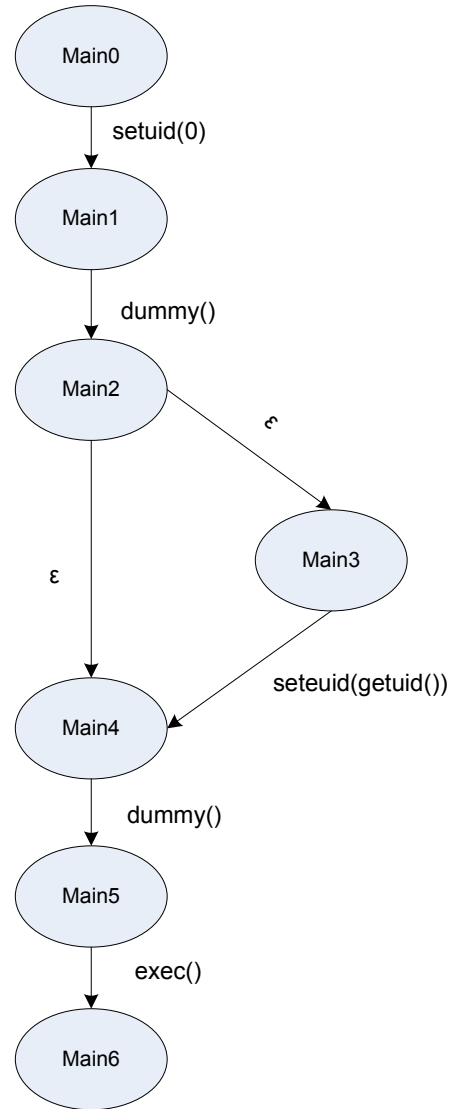
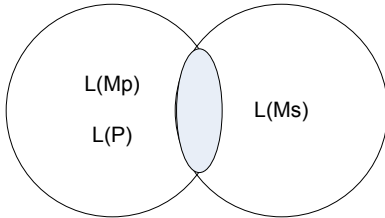
Goal

$$L(M_s) \cap L(P) = \emptyset$$

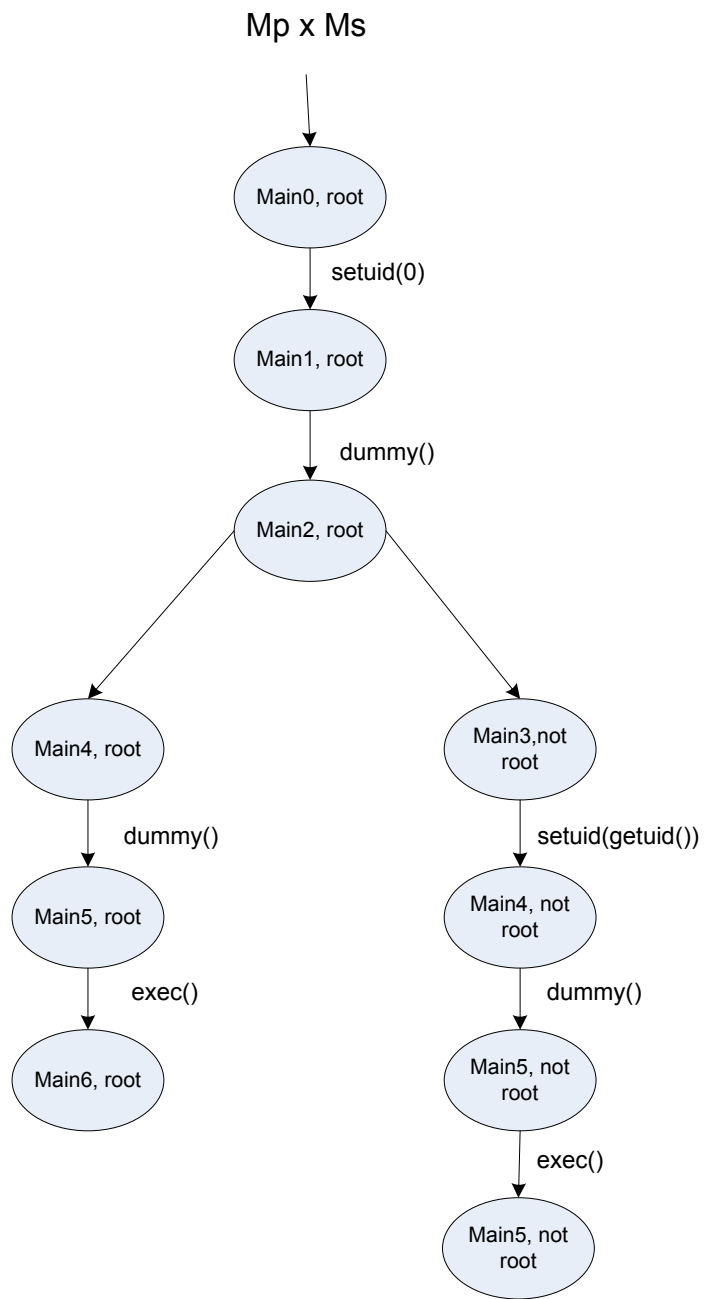
The intersection is empty



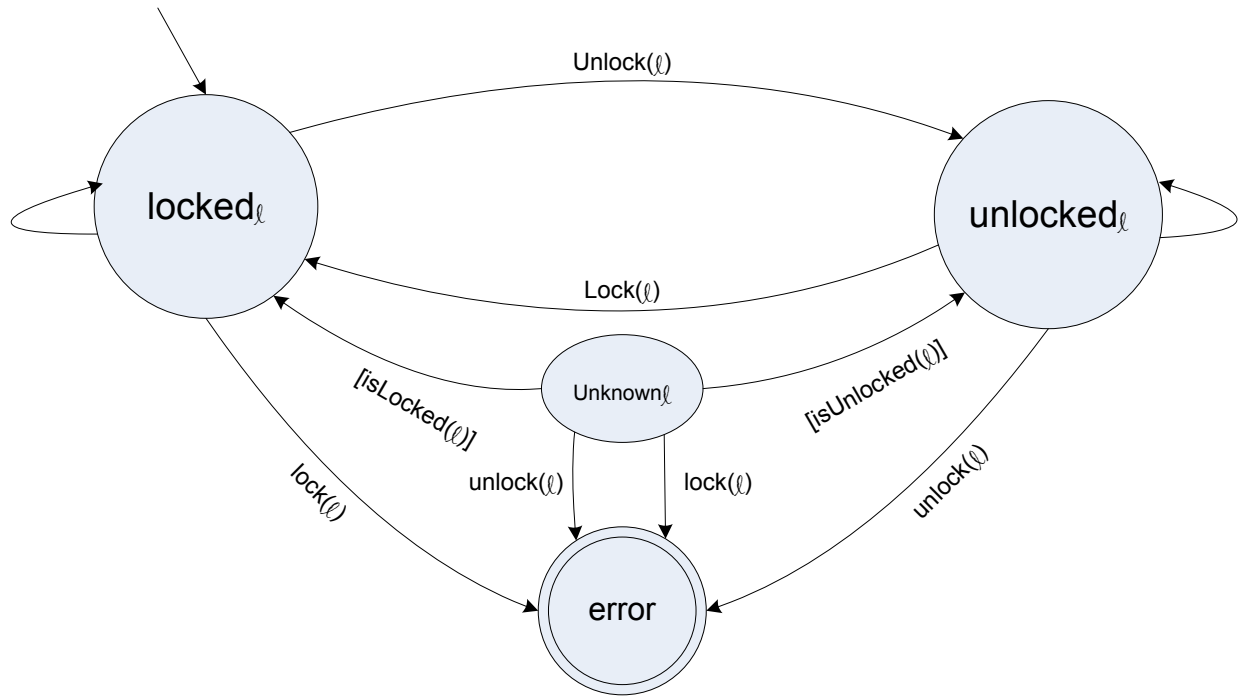
Bad



Theorem: $L(M1) \cap L(M2) = L(M1) \times L(M2)$



- Metal Extension
- Test condition
 - Mention data
 - Track data state
 - Not sound



e.g. to get to the unknown state

```
lock(l);  
if(...)  
  unlock(l);  
.  
.  
.  
if(isLocked(l))  
  unlock(l);
```

