Sequencing bugs

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

To restrict to a subsystem:
Chrcat(some_dir);
Chdir("/");

Ms

1. You cannot call “longjm” 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(Ms) \cap L(P) = \emptyset

The intersection is empty

Bad

L(Mp) L(P) L(Ms)
Theorem: $L(M_1) \cap L(M_2) = L(M_1) \times L(M_2)$
Metal Extension
- Test condition
- Mention data
- Track data state
- Not sound

```
Unlock()
lock()
Unlock()
Lock()
Unknown
lock()
unlock()
```

Diagram:
- Locked
- Unlocked
- Error
- Unknown
e.g. to get to the unknown state

lock(l);
   If(…)
       unlock(l);
   .
   .
   .
   If(isLocked(l))
       unlock(l);