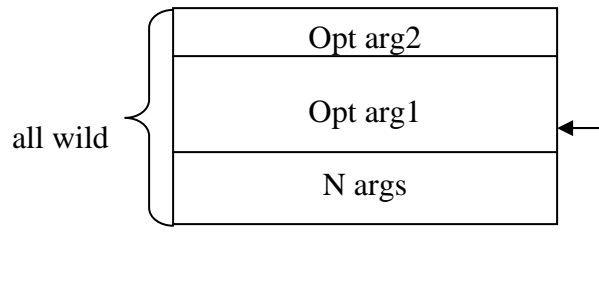
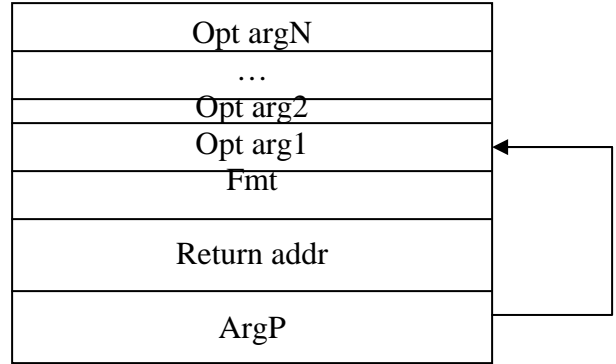


CSE 509 CLASS NOTES (3/20)

CCured and format string bugs

```
Printf(const char *fmt, ...);
Printf(tainted_string);
```

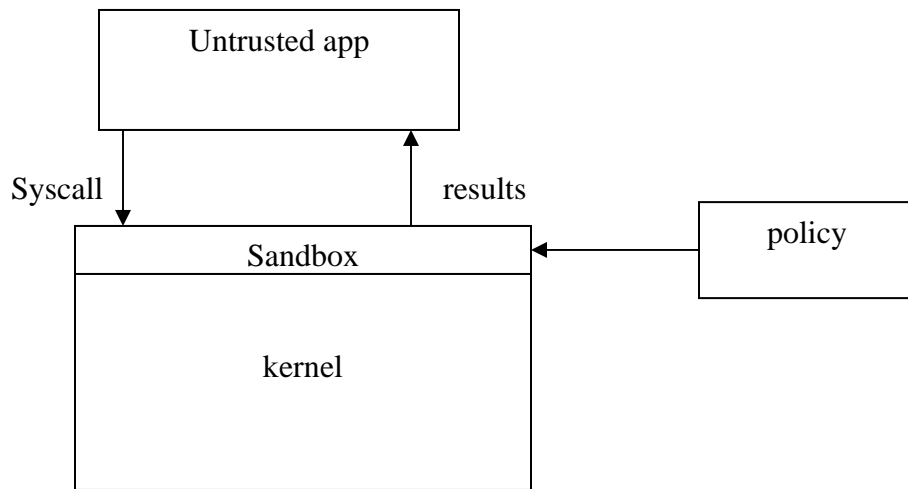
If CCured printf does not know the number of Args, attacks still possible (but probably much harder)



Ostia (sandboxing)

- don't trust code
- want to run it safely
- system call monitoring

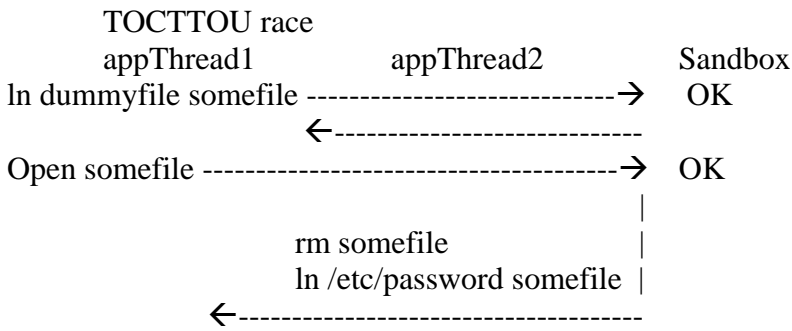
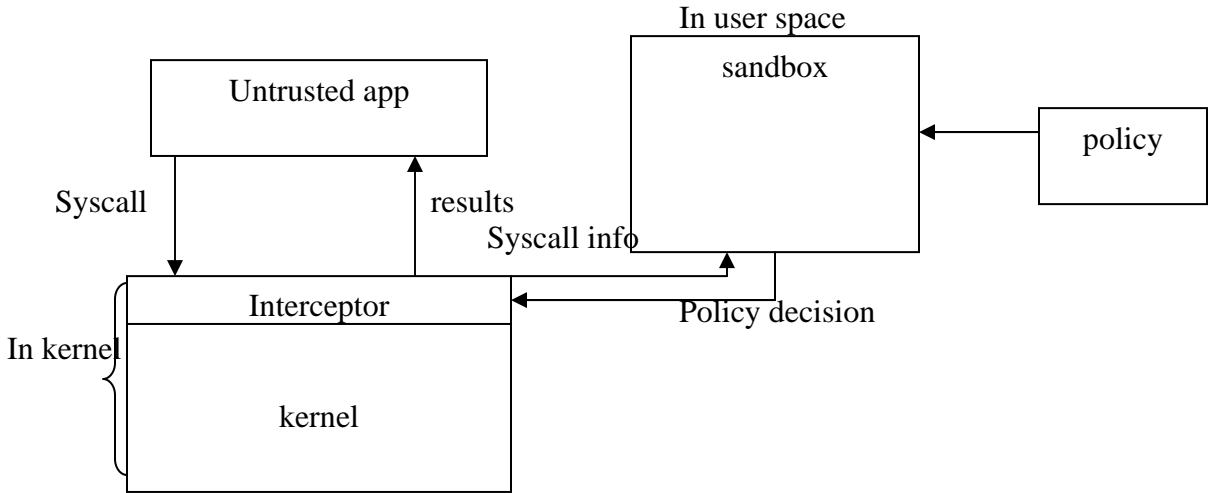
- how do we implement this
 1. IDEA 1 : in kernel



Big picture

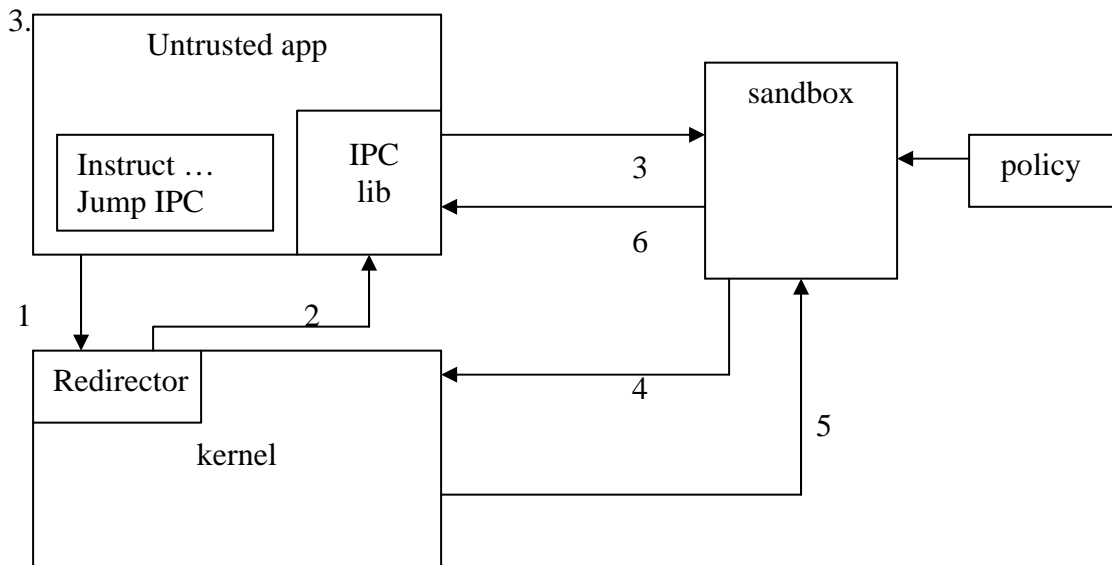
Privilege separation == sandboxing == IDS
 Idea 1 may introduce bugs.

2. IDEA 2 : hybrid



Races

- memory races
- os races



1. syscall
 2. redirect
 3. syscall request
 4. syscall
 5. results
 6. results
- Delegating architecture
 - o makes memory races go away
 - o makes it possible to do policy checks in racefree manner
 - o performance?
 - Many syscall unmediated
 - Patch code to use IPC lib
 - o IPC lib is not trusted
 - race-free policy enforcement
 - o suppose policy is :
 - can only open files in “/var/tmp”
 - o what about
/var/tmp/foo/../../ha
 - canonicalize?
 - o races?
 - walk the filename by hand