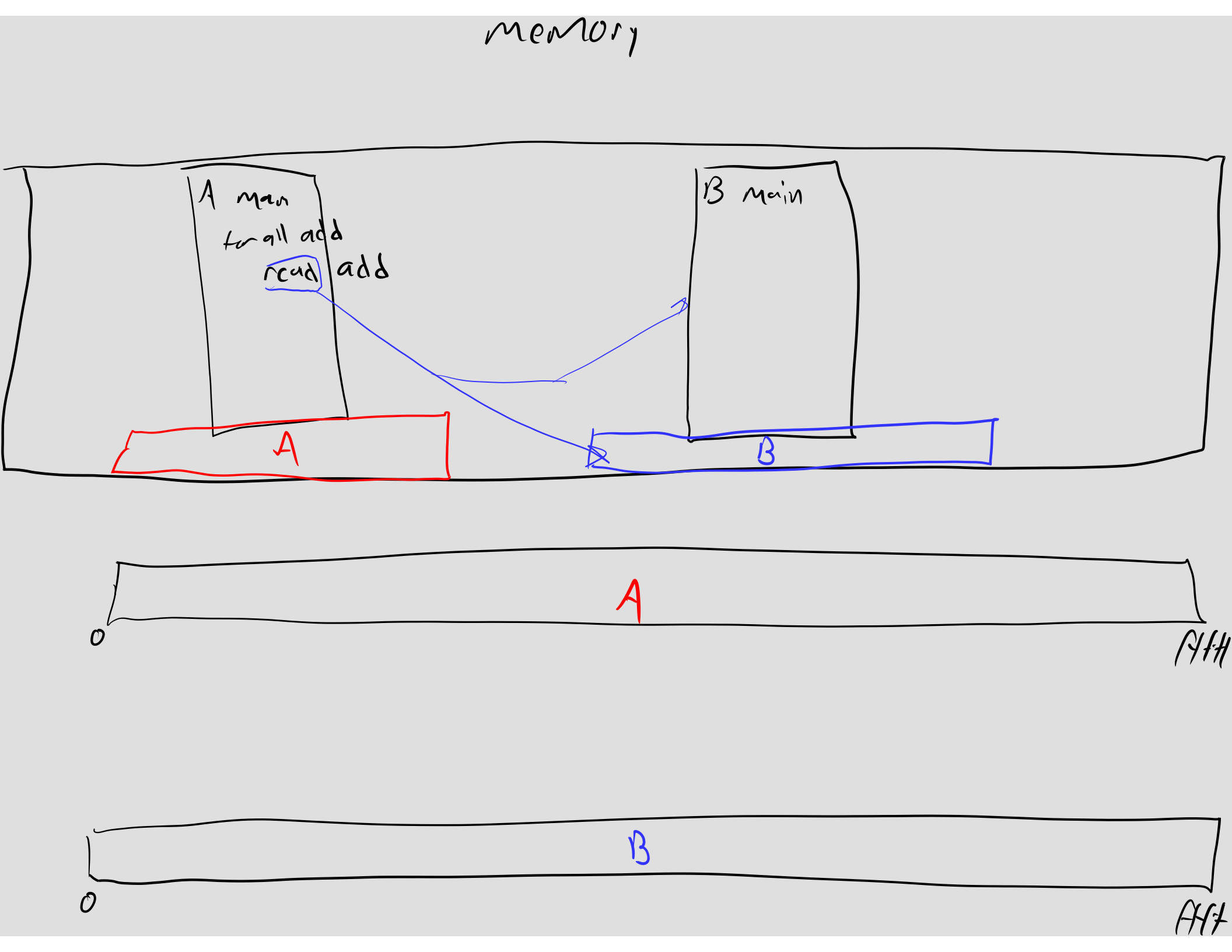
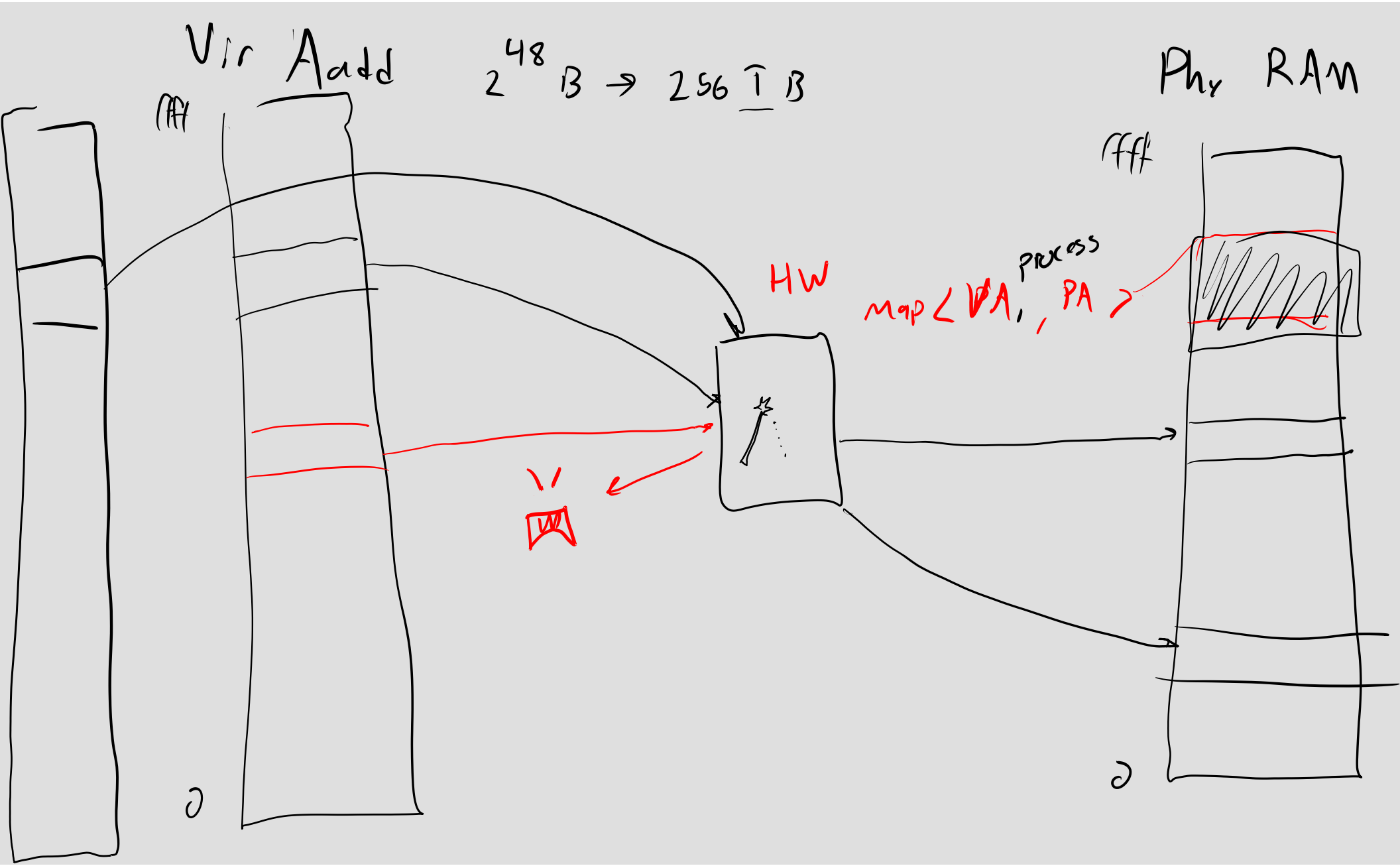
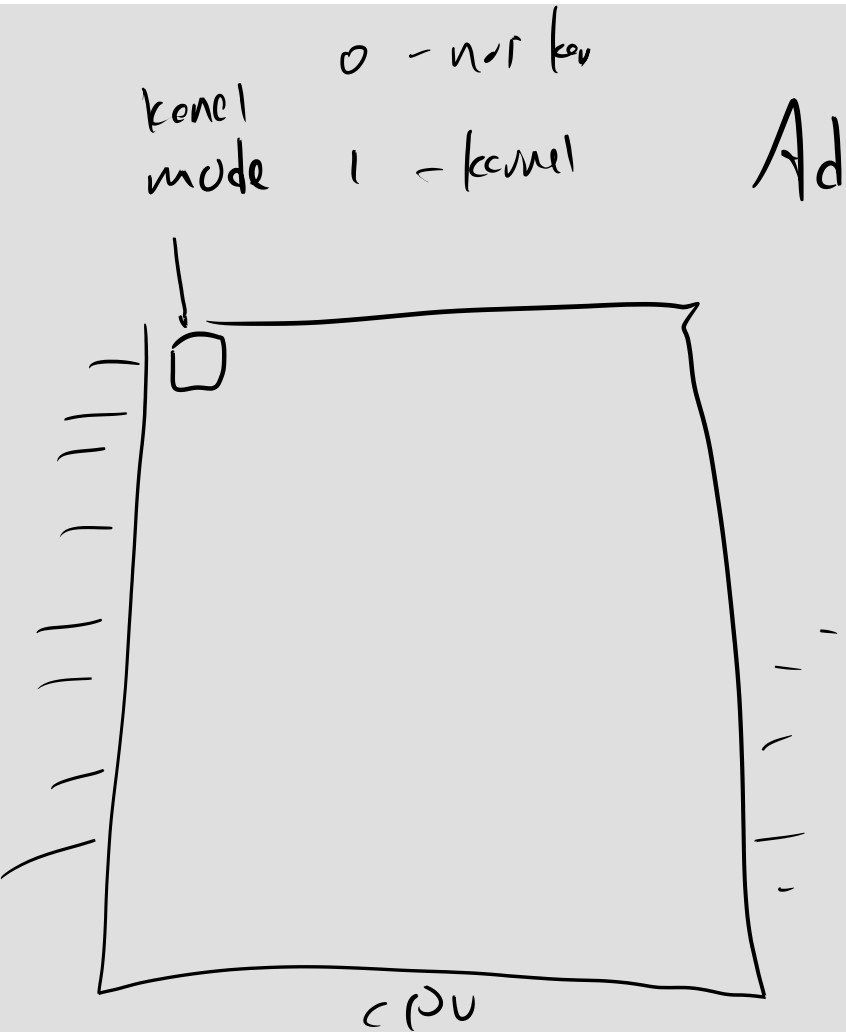
Things proc A should not be able to do bcs proc B exists

- chan B's mem or wifi or disk or...
- chan B
- → stop B w/o permission
- use all mem / CPU / etc
- read B's mem
- chang OS mem
- shut down comp
- access mem / disk
- use wifi directly


memory
A main
for all add
rcvd add
B main
A
B
A
0
FFFF
B
0
FFFF


Vir Aadd
2^48 B → 256 T B
Phy RAM
HW
map < VA, PA, process >
0
0



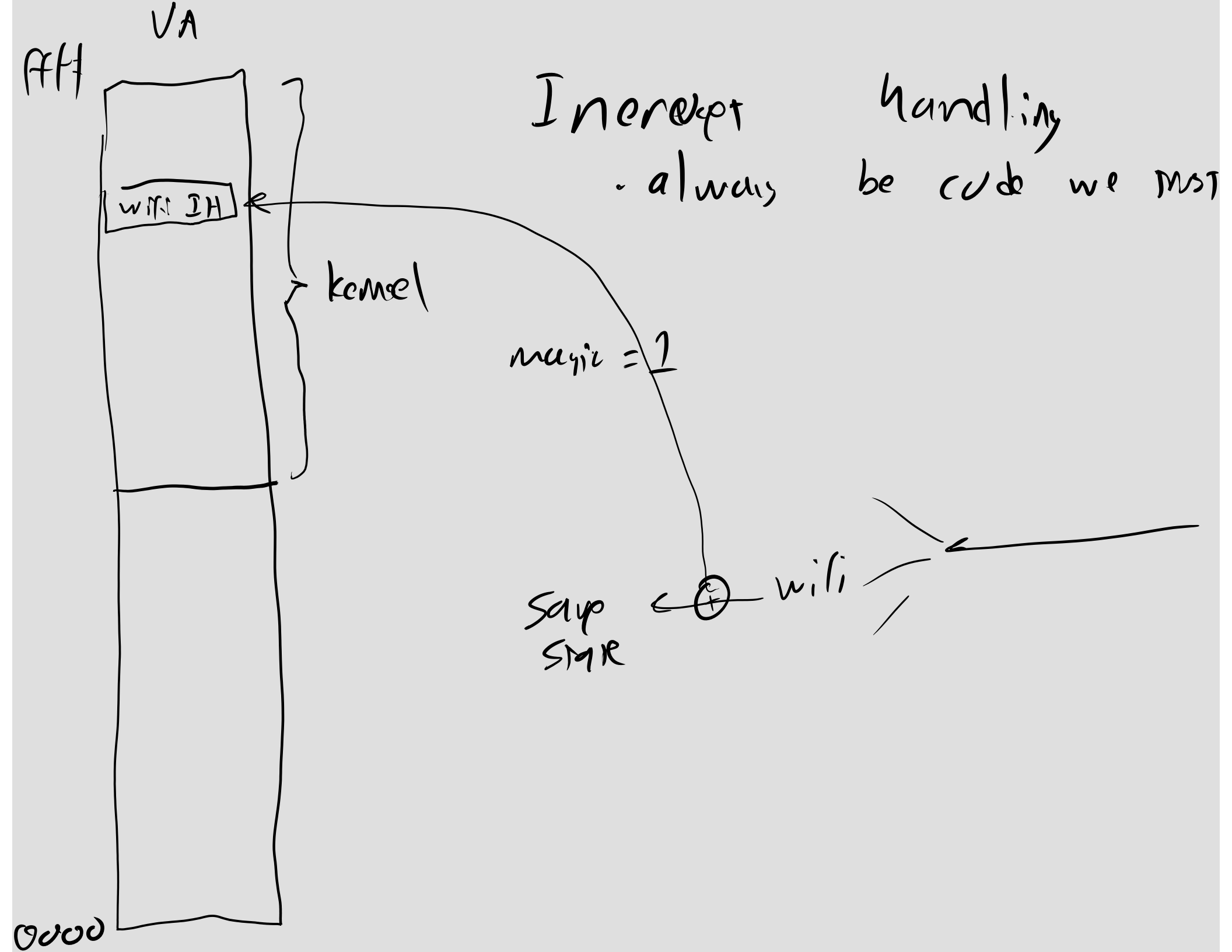
Add Trans DS

- only written by trusted SW

OS (SW) kernel (HW mode for OS)

Privileged Instr:

- change ATDS (Page table)
- set mode to 1



Interrupt handling

- always be code we must