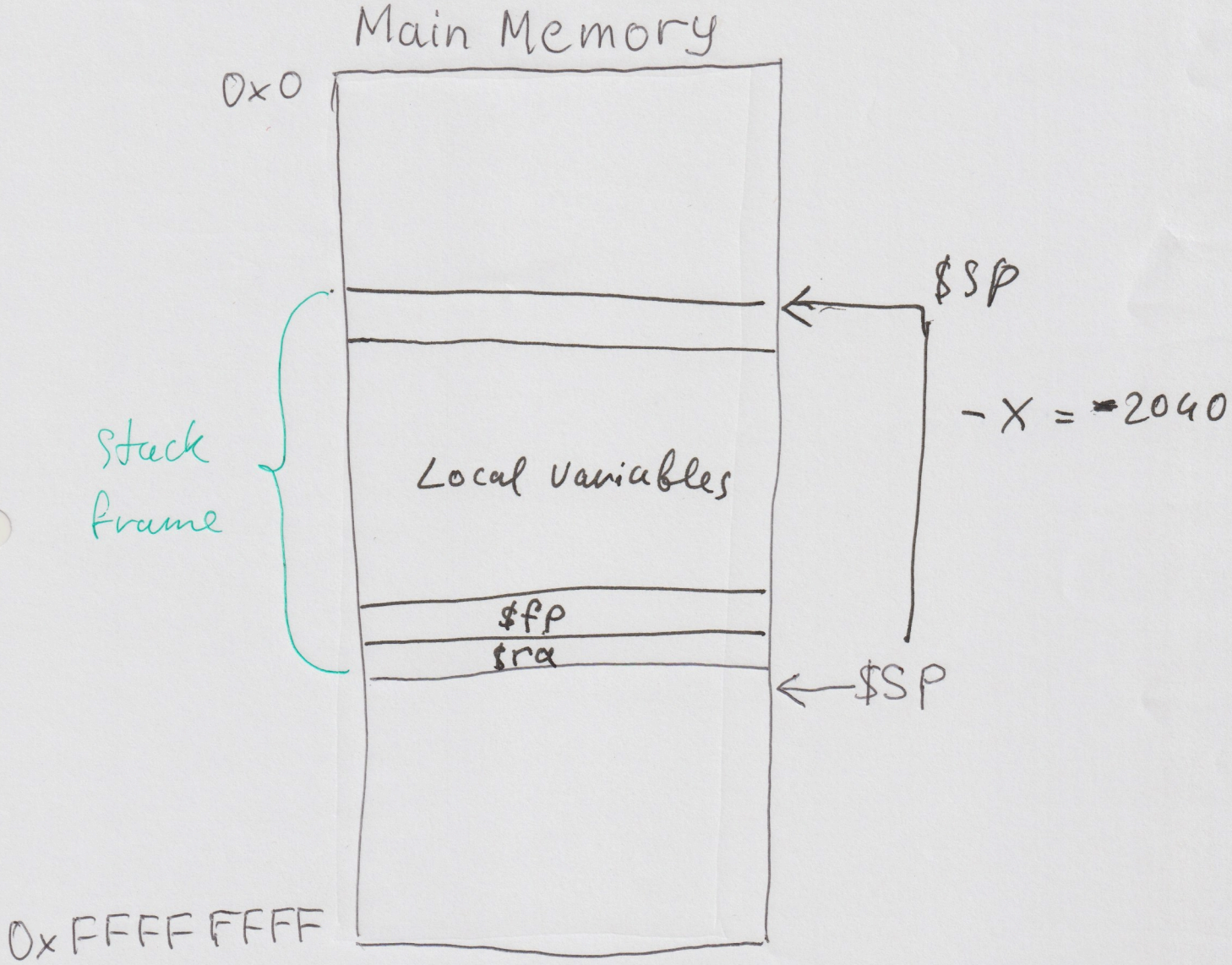
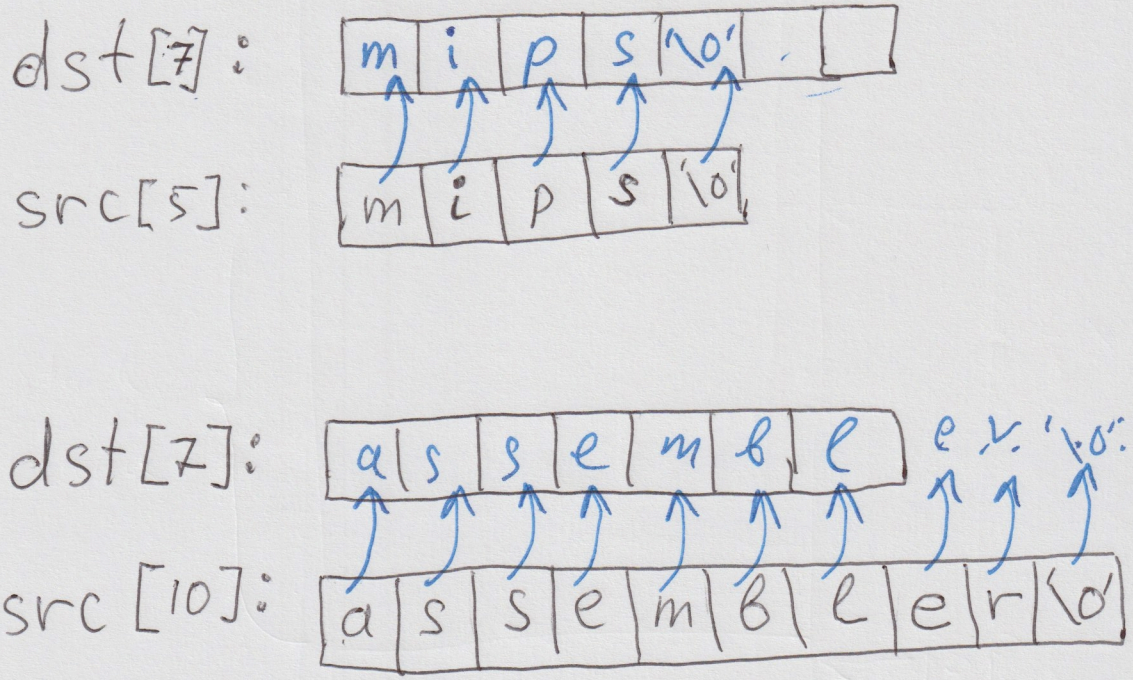
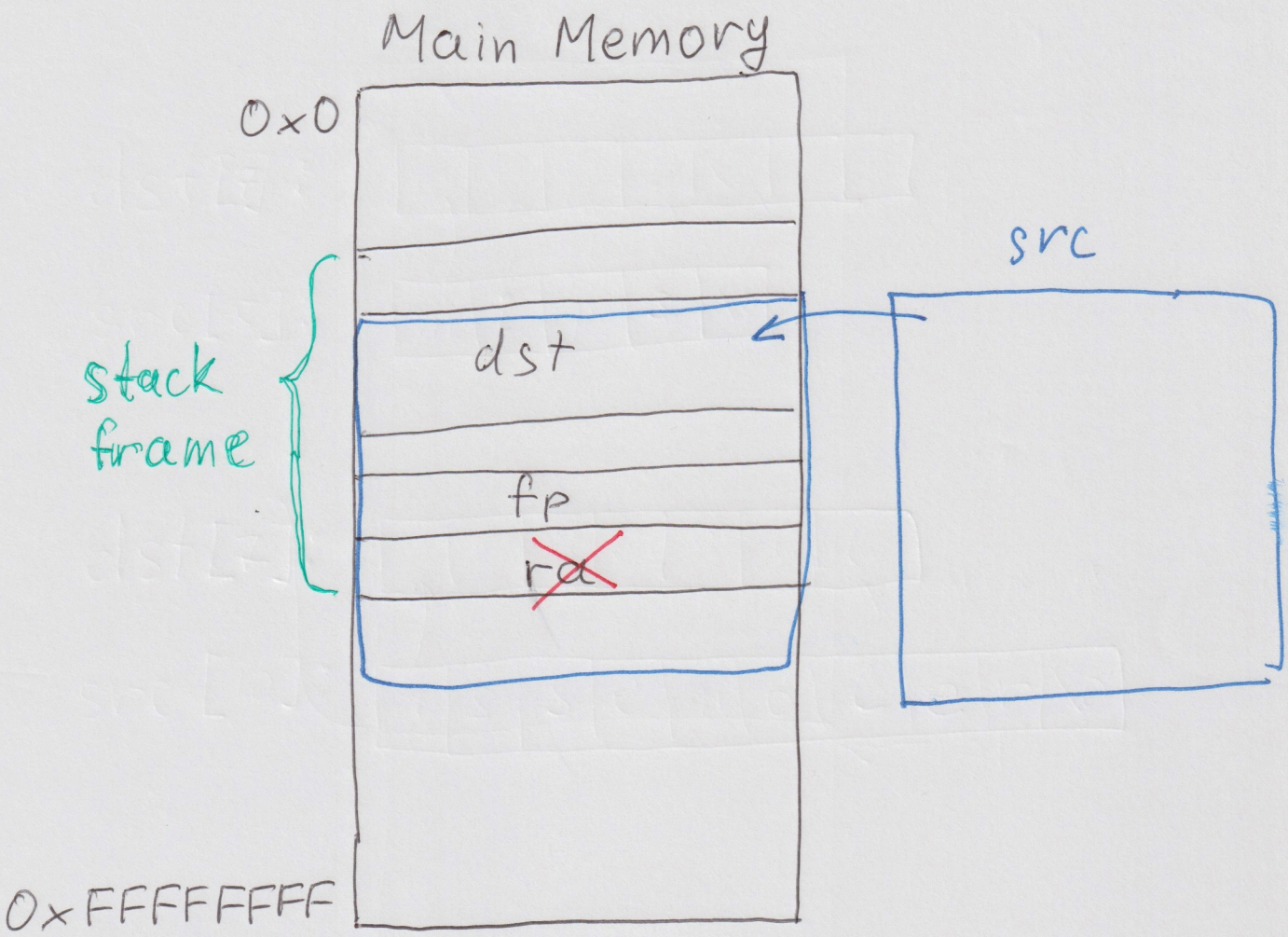
Stack Frame


Main Memory
0x0
$SP
-X = -2040
Stack Frame
Local Variables
$fp
$ra
$SP
0x FFFF FFFF

strcpy(dst, src);

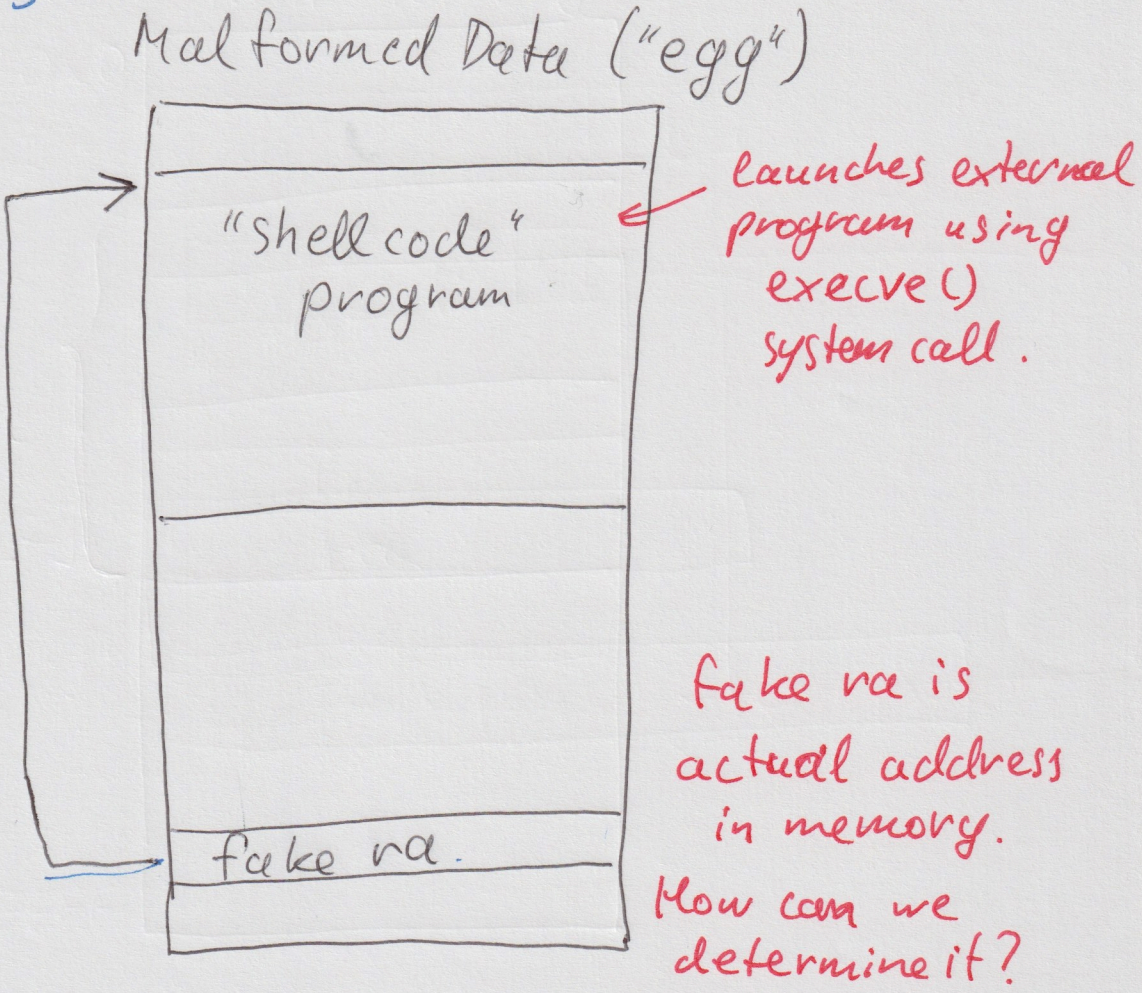


Buffer Overflow



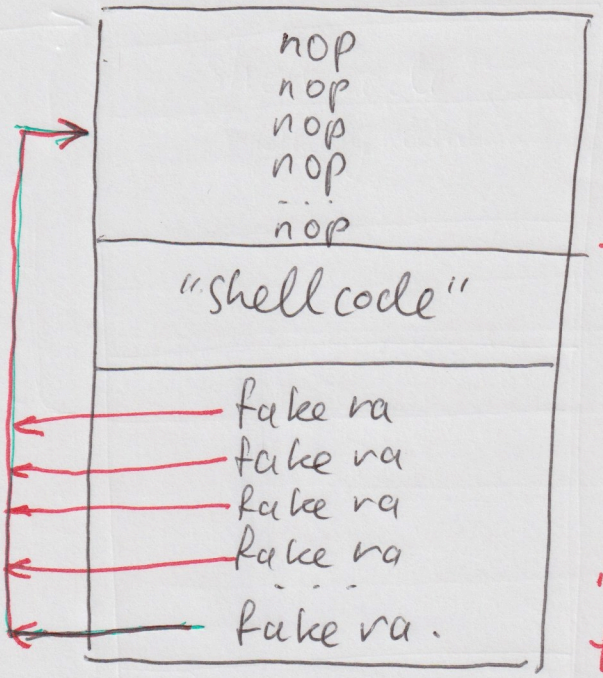
Buffer overflow exploit.

src



Exploit "egg"

More resilient to buffer address changes.



"catchment" area

fake return address points to the estimated "middle" of the catchment area.