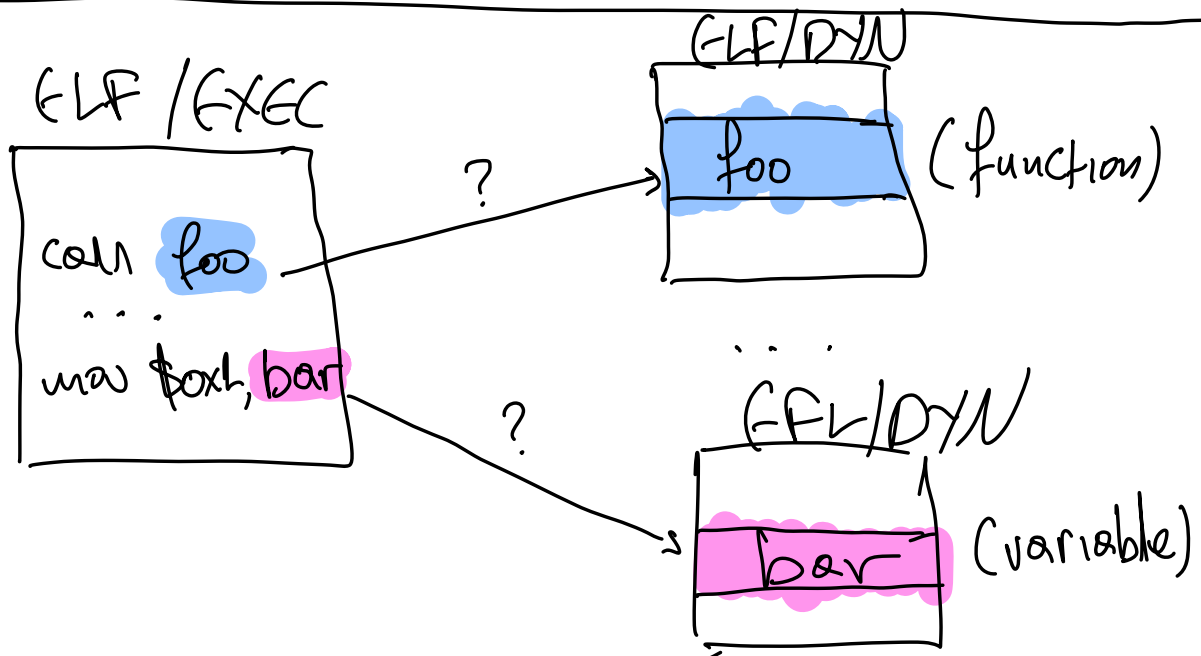
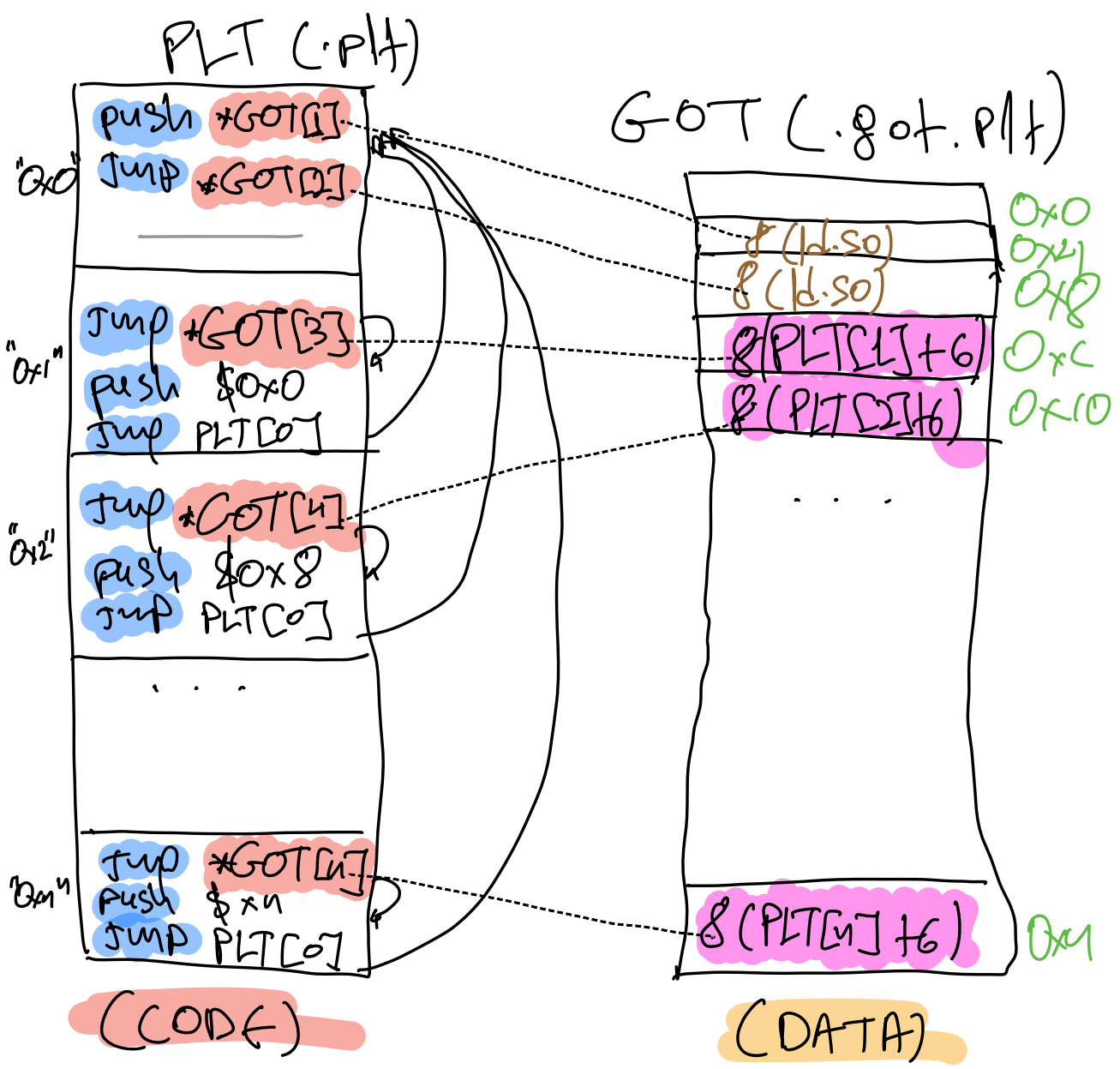


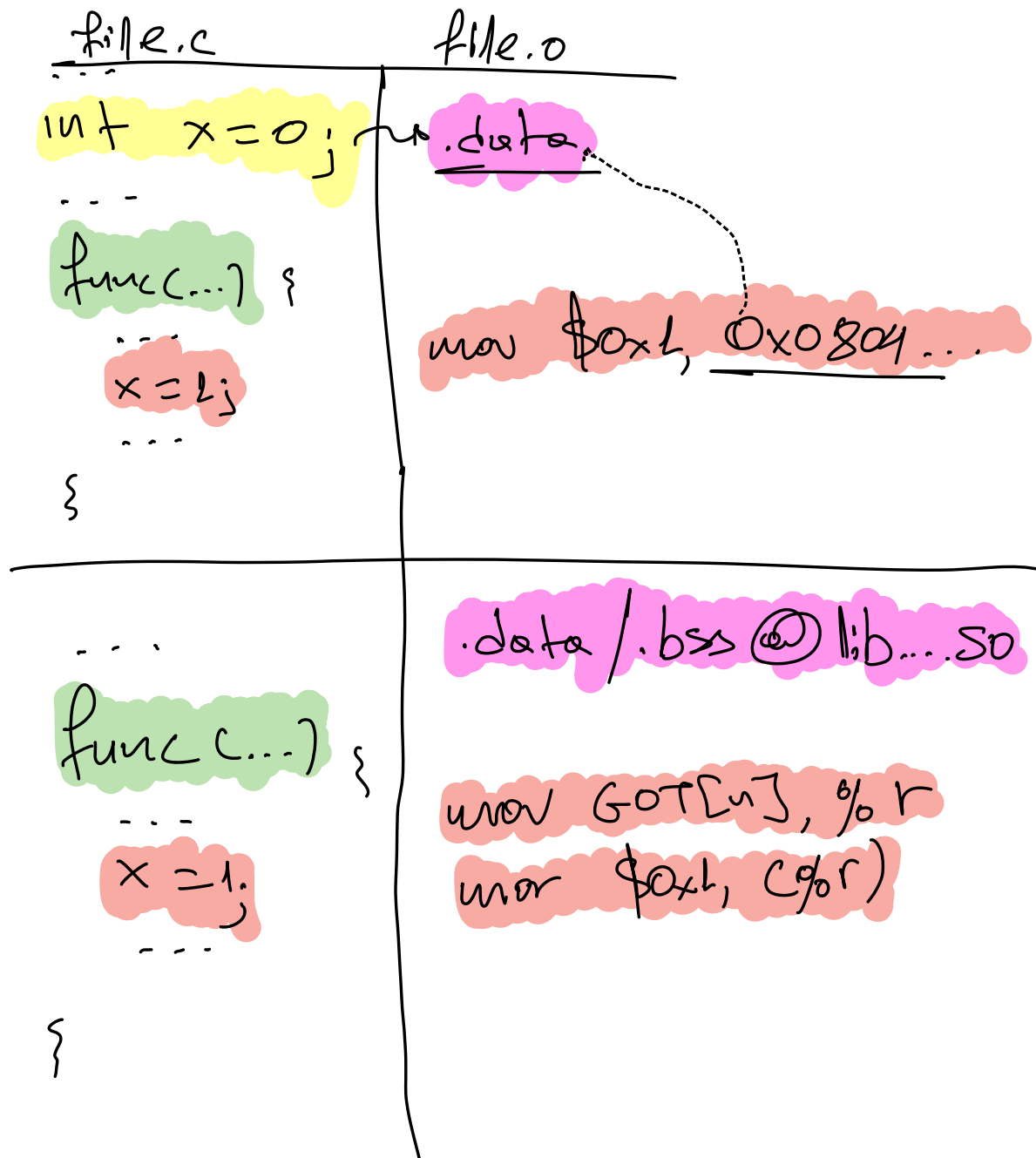
Dynamic Linking

↳ Procedure Linkage Table
(.PLT)

↳ Global Offset Table.
(.got)/(got.PLT)







RELRO - BIND NOW

↳ GOT hardening schemes

RELRO - BINDNOW

↳ GOT hardening schemes

RELRO (-z relro)

↳ .got is made read-only after initialization/loading

BINDNOW (-z now)

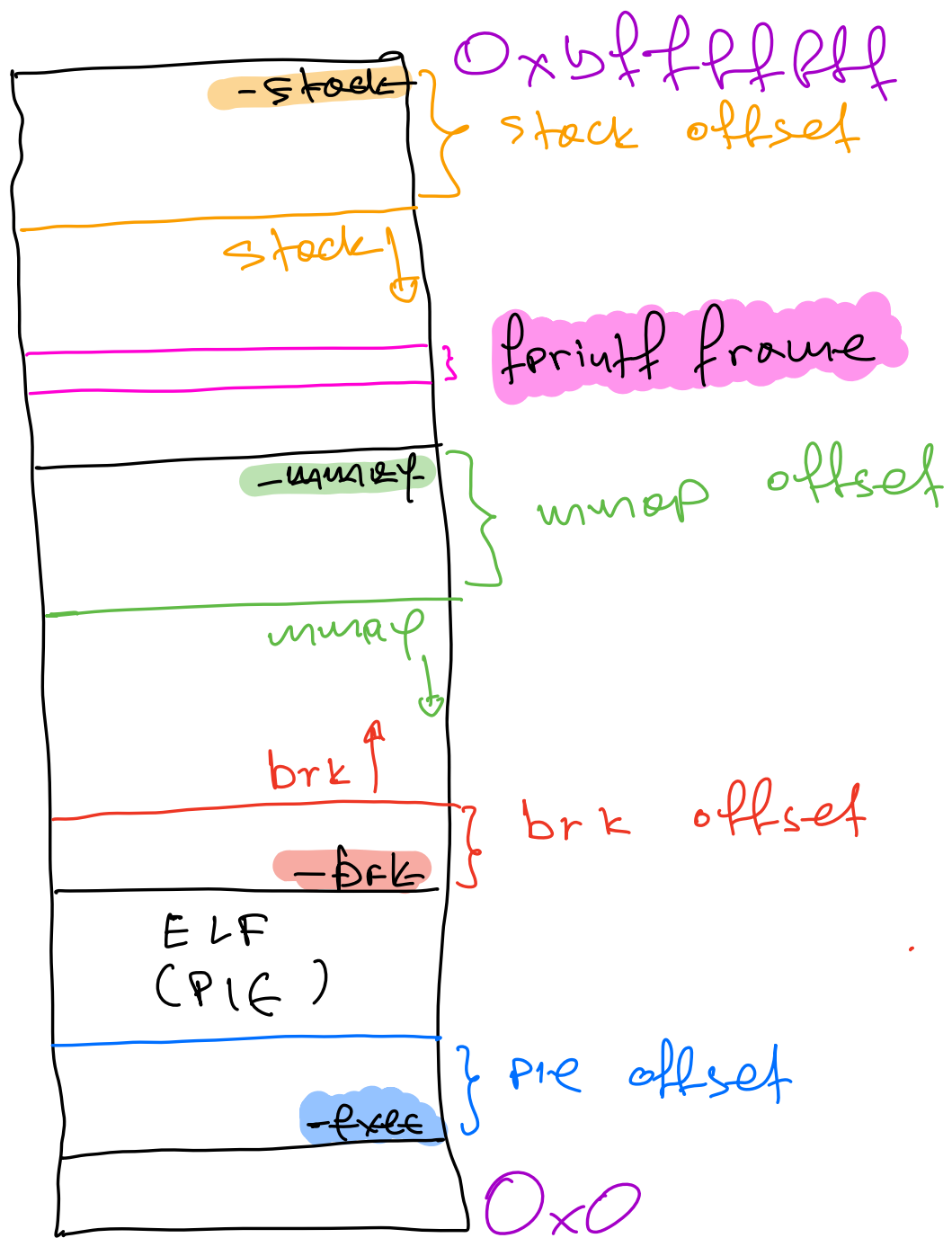
↳ .got.plt is merged with .got

↳ no lazy binding $\Rightarrow$ eager binding

↳ +RELRO

Advanced Memory Disclosure + Corruption

↳ arbitrary mem. disclosure
-||- -||- corruption



Mem. Disclosure - Format String Corruption Vuln.

⇒ %x %x %x ...

%p %p %p ...

⇒ %N\$x
%N\$p

leak a
value
relative
to printf's
frame in
the stack

Mem. Disclosure - Format String Vuln.

Corruption

⇒ %x %x %x ...

%p %p %p ...

⇒ %N\$x

%N\$p

leak a
value
relative
to printf's
frame in
the stack

⇒ %d, %o, %x, ... %P, ... %c
↳ non-pointer argument

⇒ %S

↳ pointer argument
(arbitrary mem. read)

⇒ %n

↳ pointer argument
(arbitrary mem. write)