



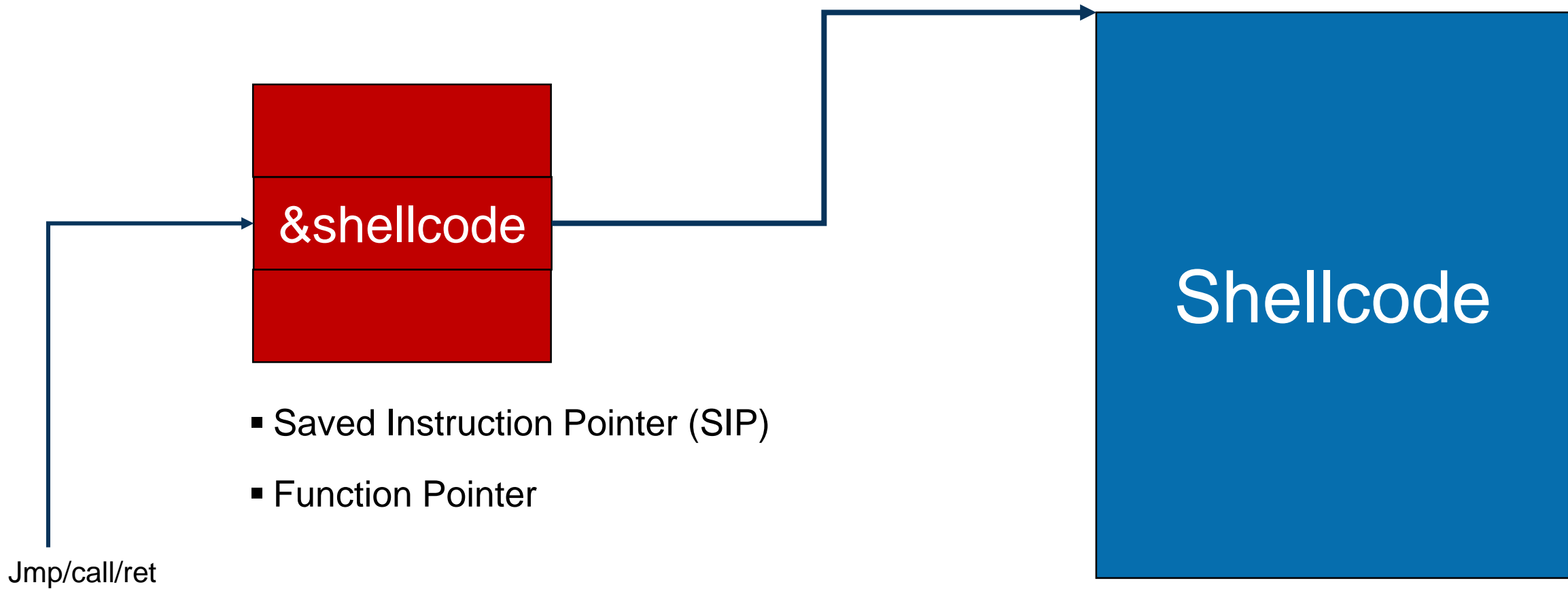
# Exploitation Techniques

Recap

# Exploitation Techniques

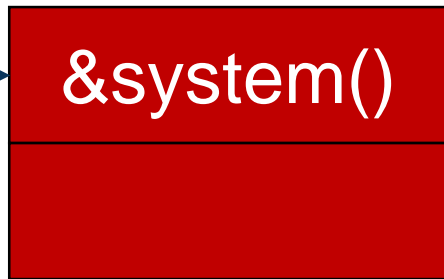
- Shellcode
- Ret2PLT
- ROP

# Shellcode

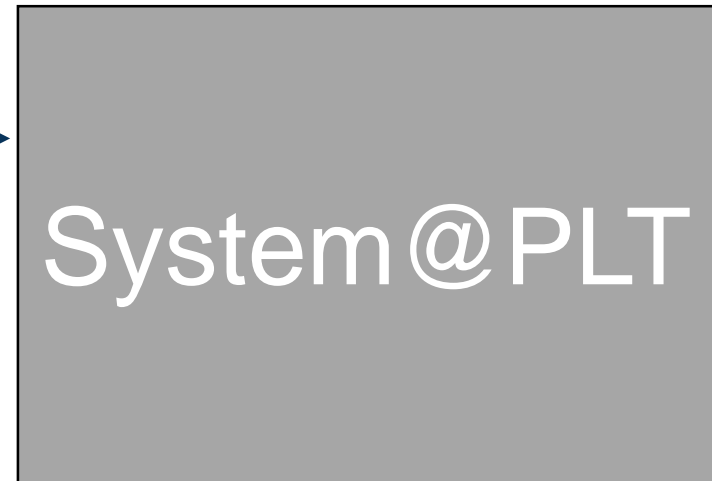


# Ret2PLT – RET/JMP

Stack  
Pointer

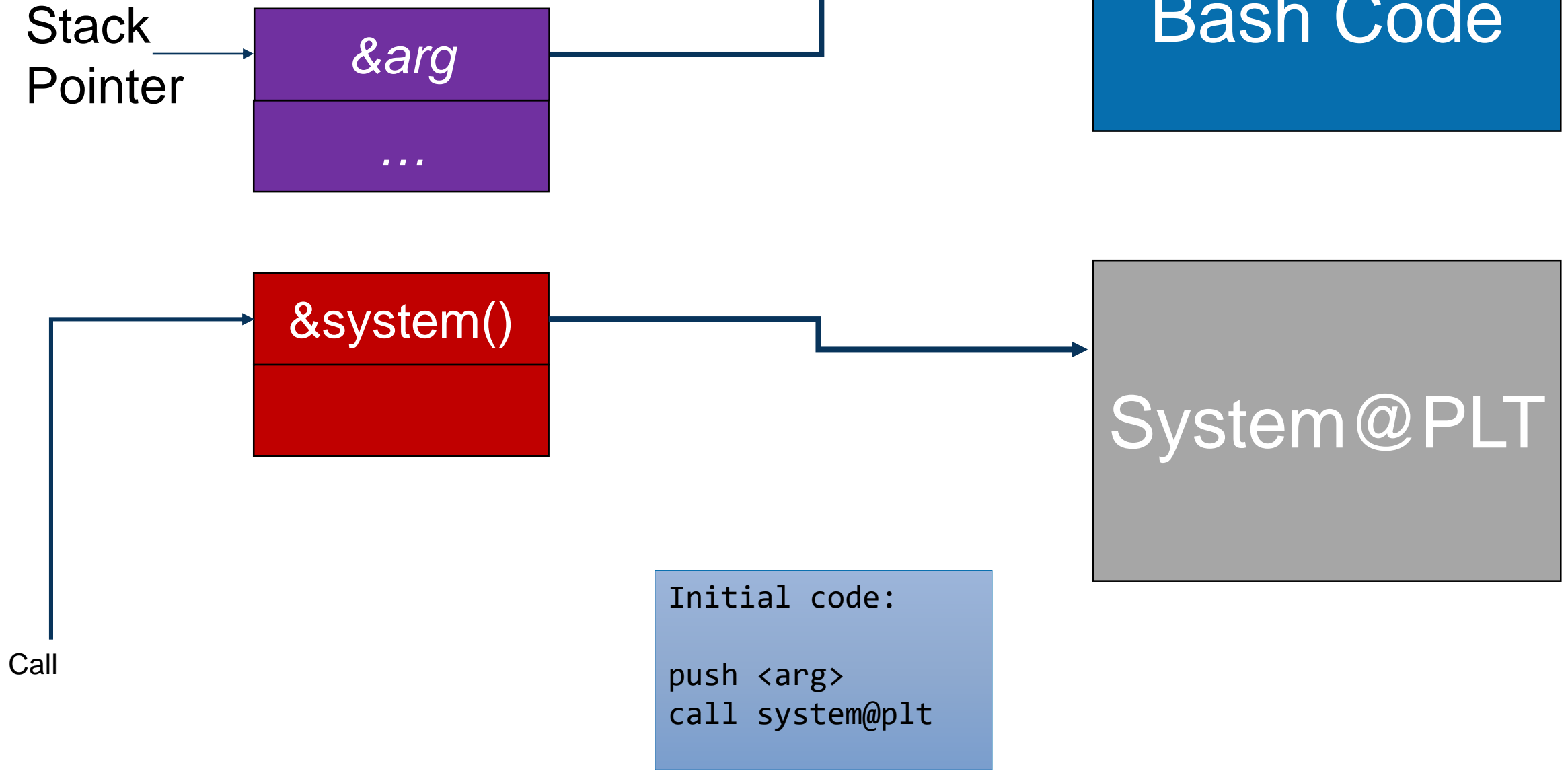


▪ Stack

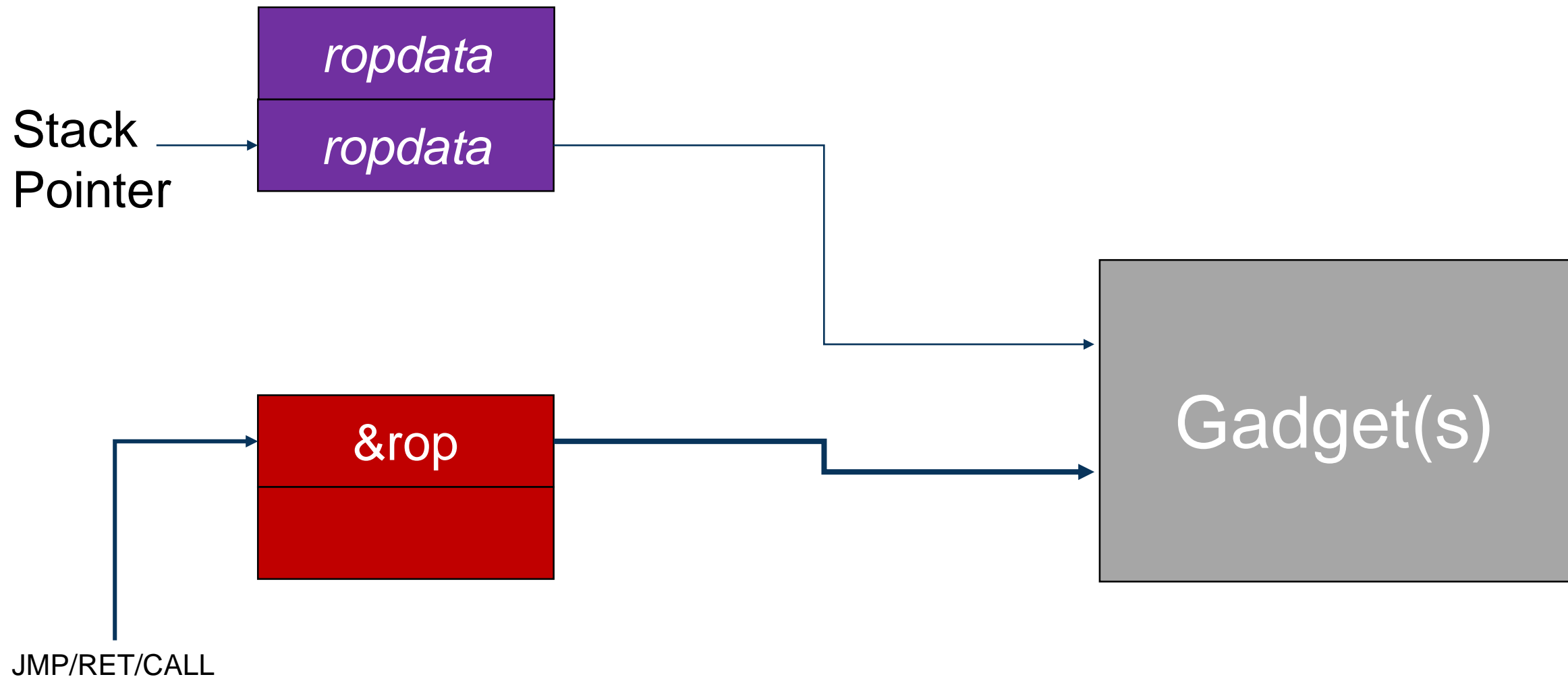


```
Initial code:  
push <arg>  
call system@plt
```

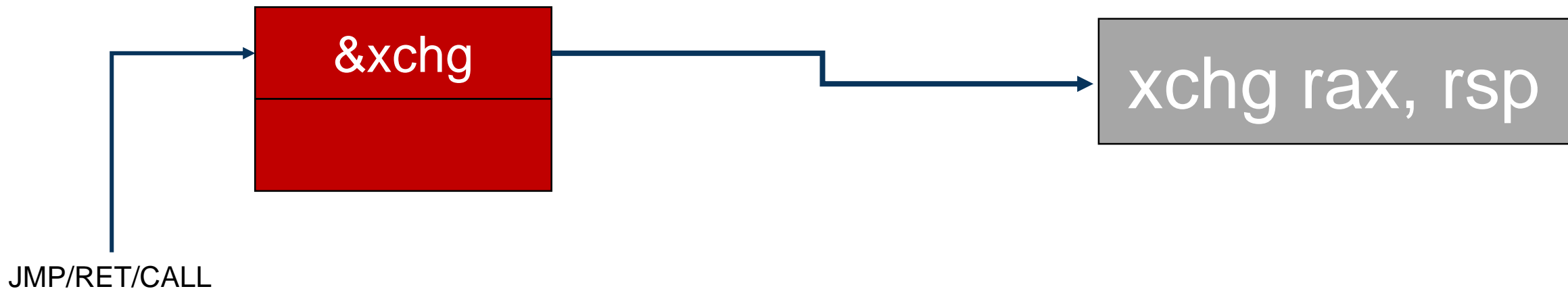
# Ret2PLT – Call



# ROP – ROPChain on stack



# ROP – ROPChain on heap



# ROP – ROPChain on heap

