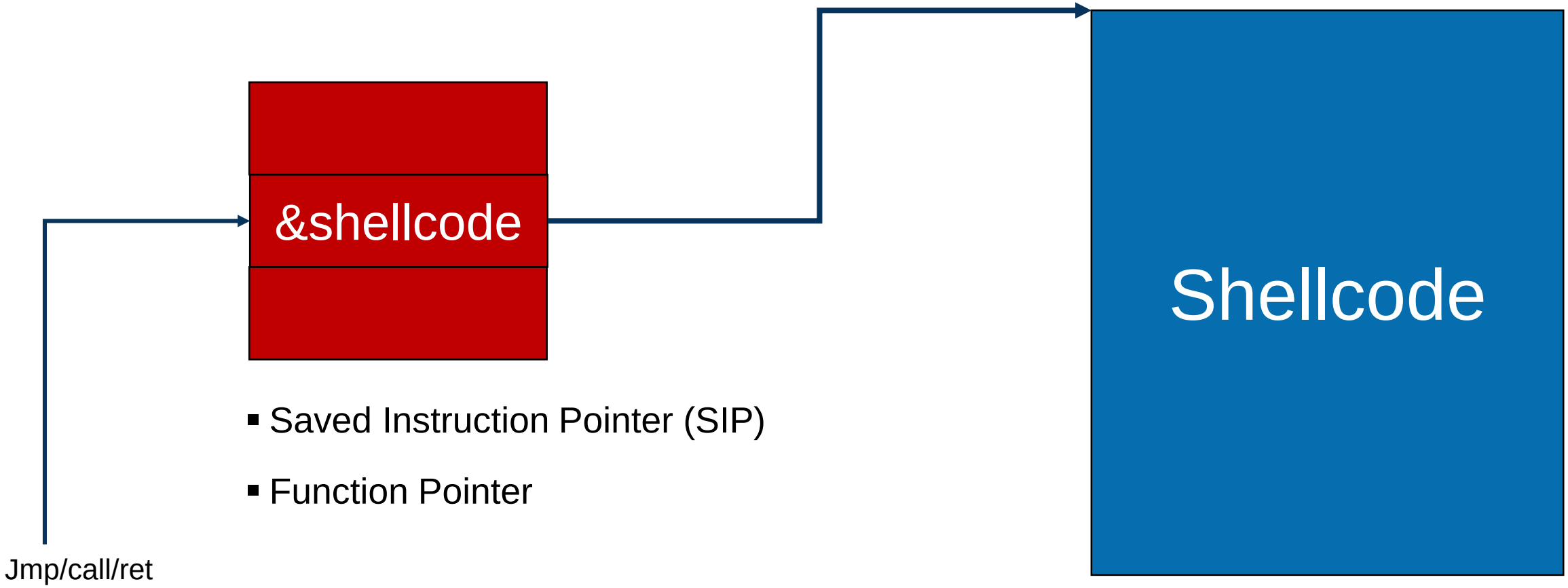
Exploitation Techniques

Recap

Exploitation Techniques

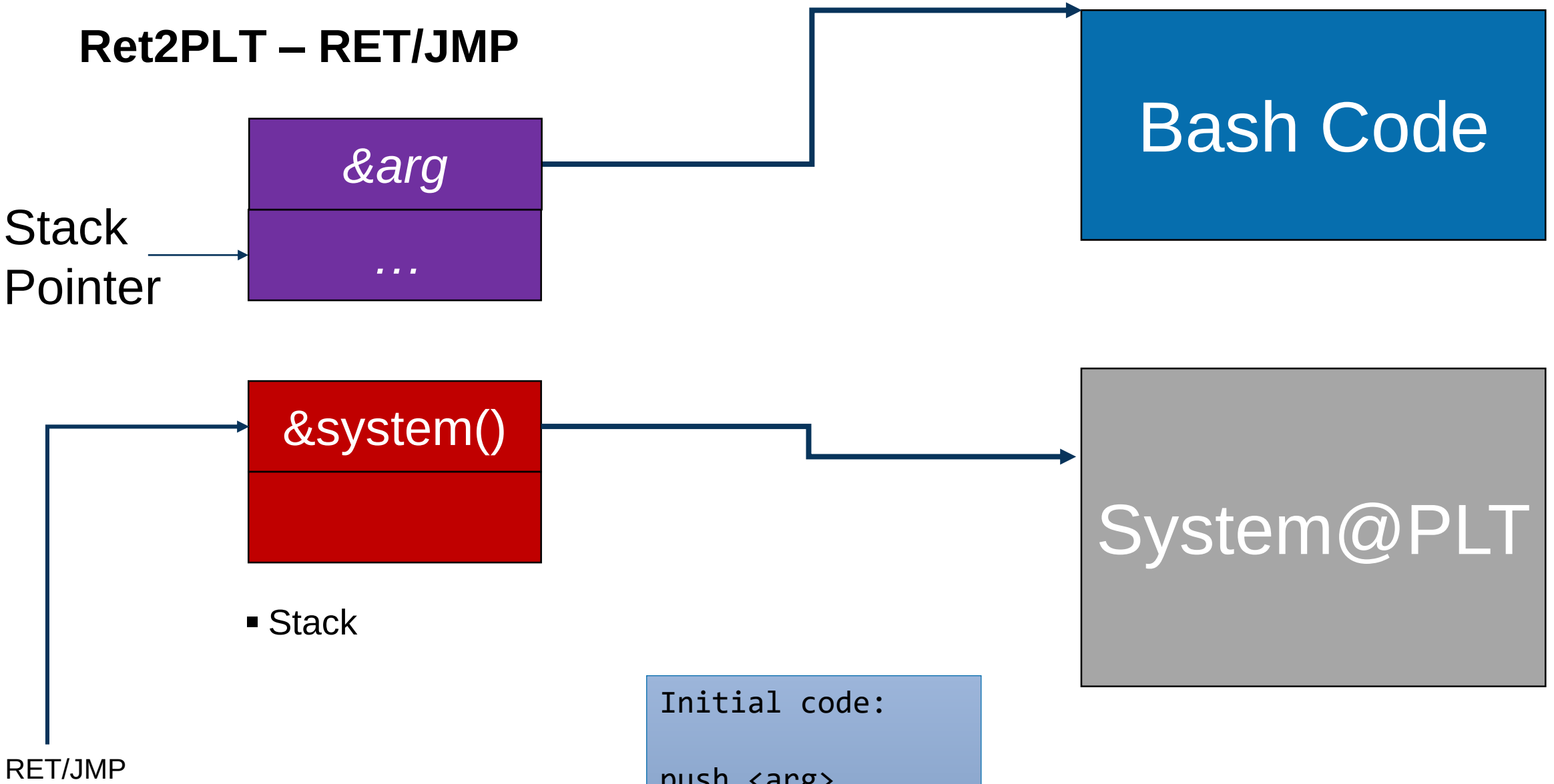
- Shellcode
- Ret2PLT
- ROP

Shellcode

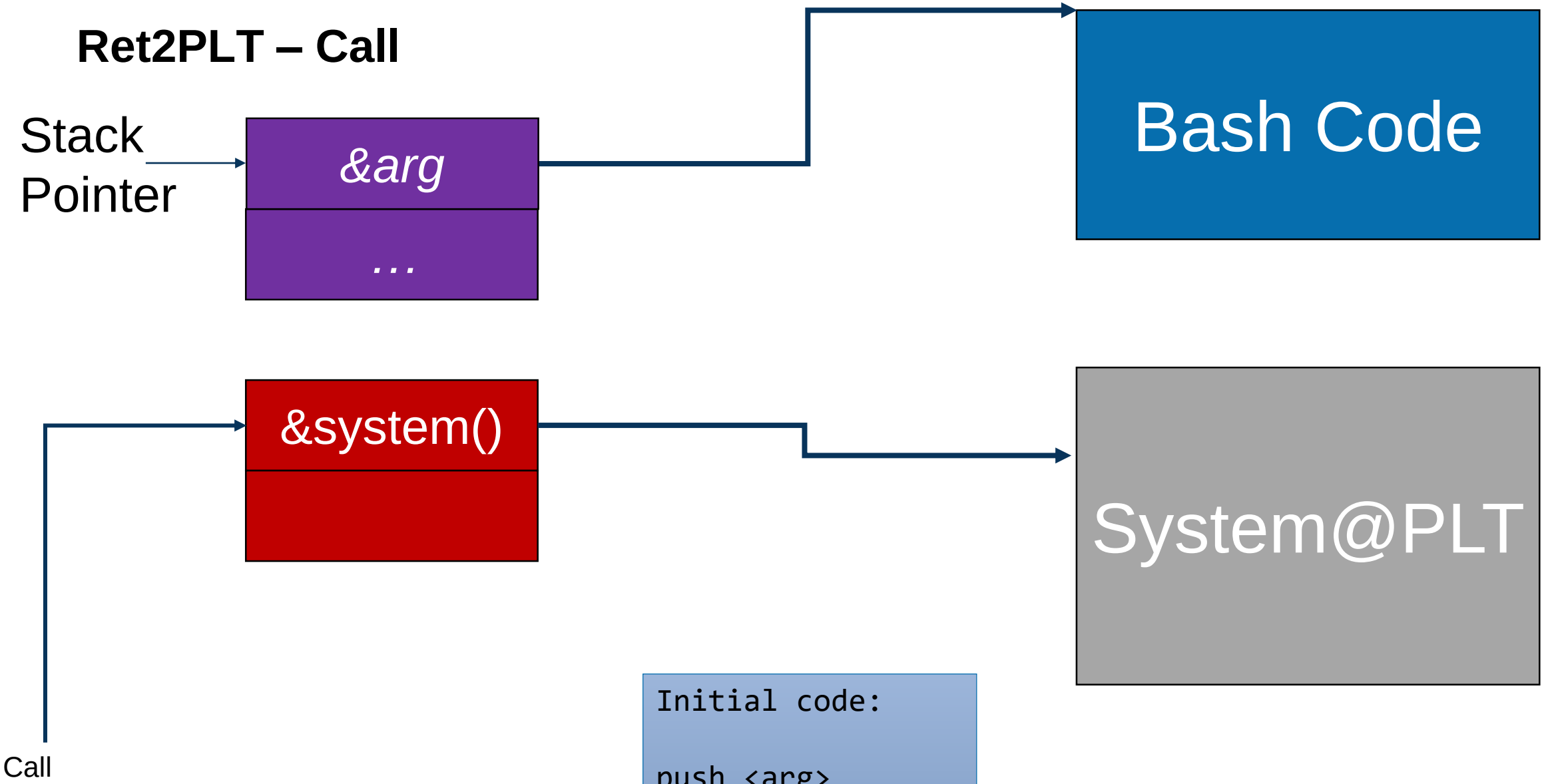


- Saved Instruction Pointer (SIP)
- Function Pointer

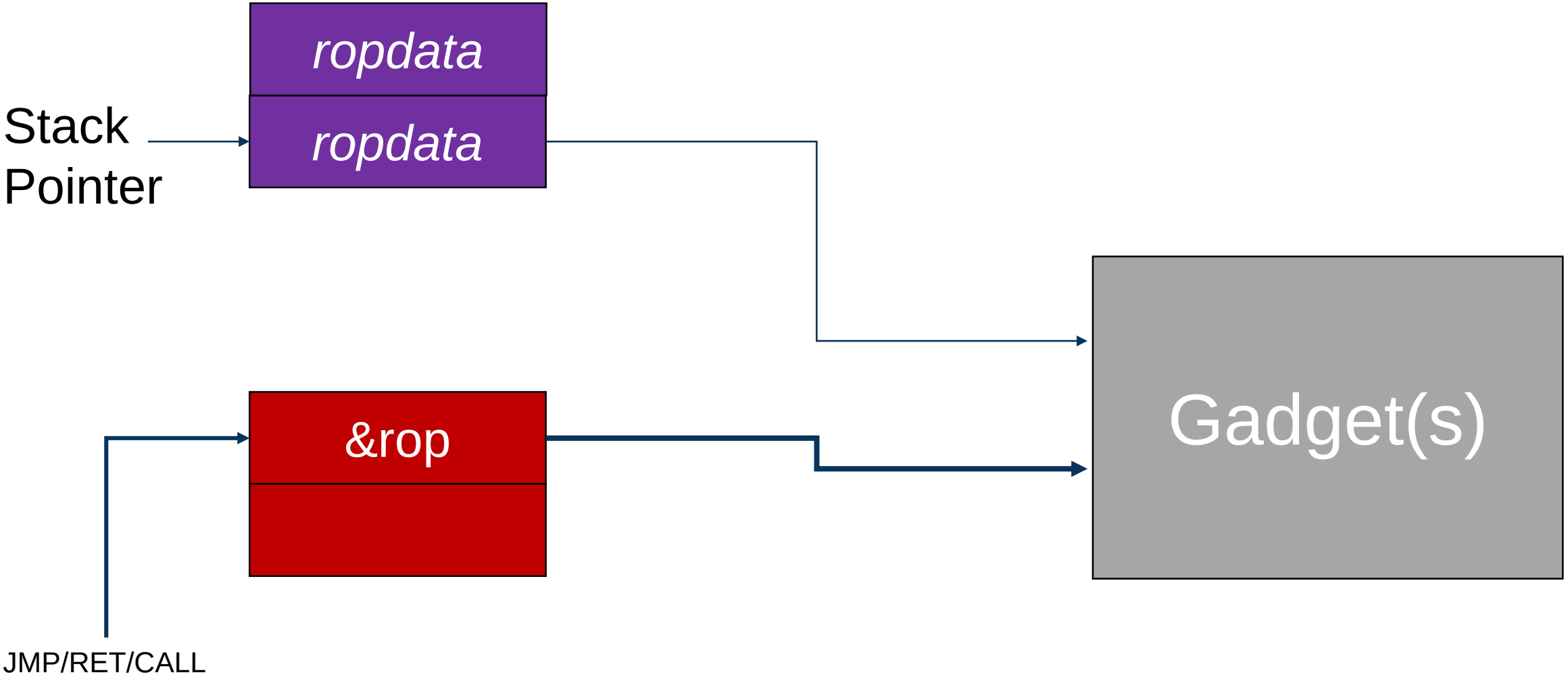
Ret2PLT – RET/JMP



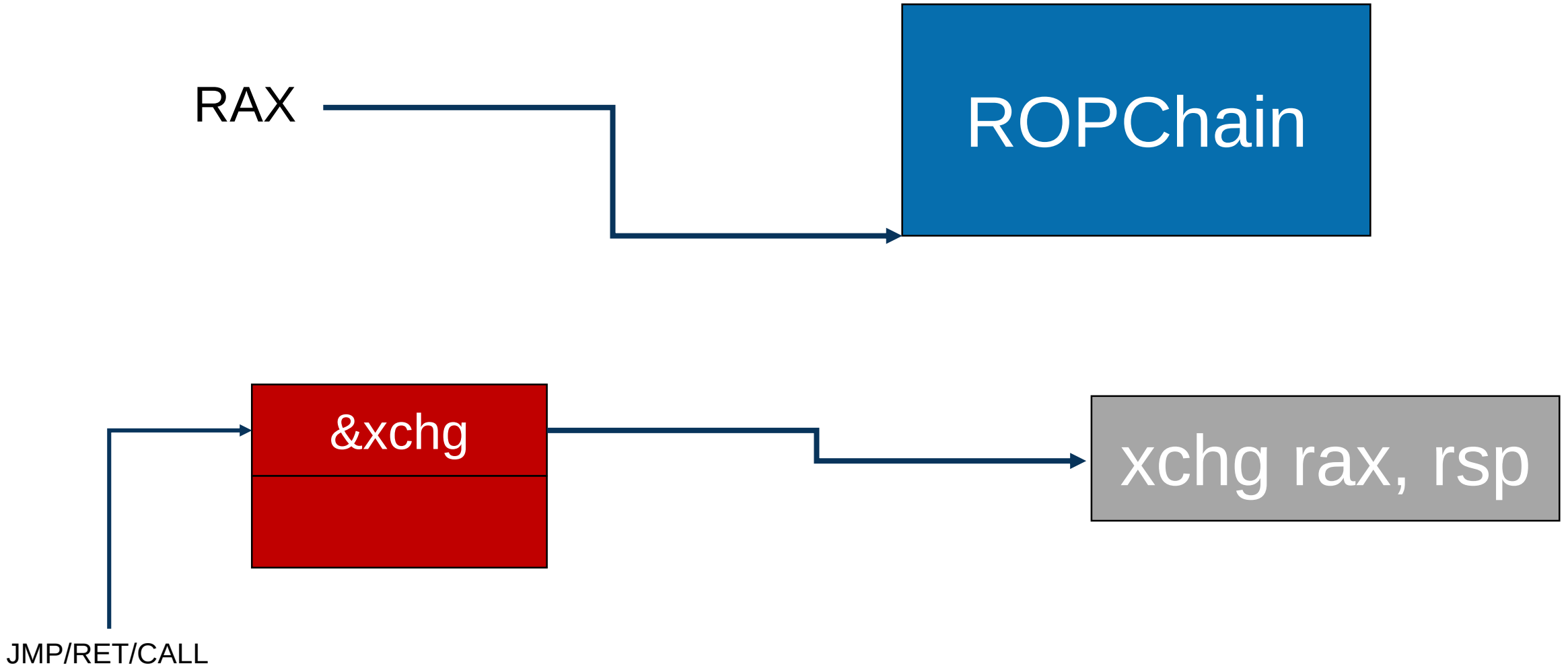
Ret2PLT – Call



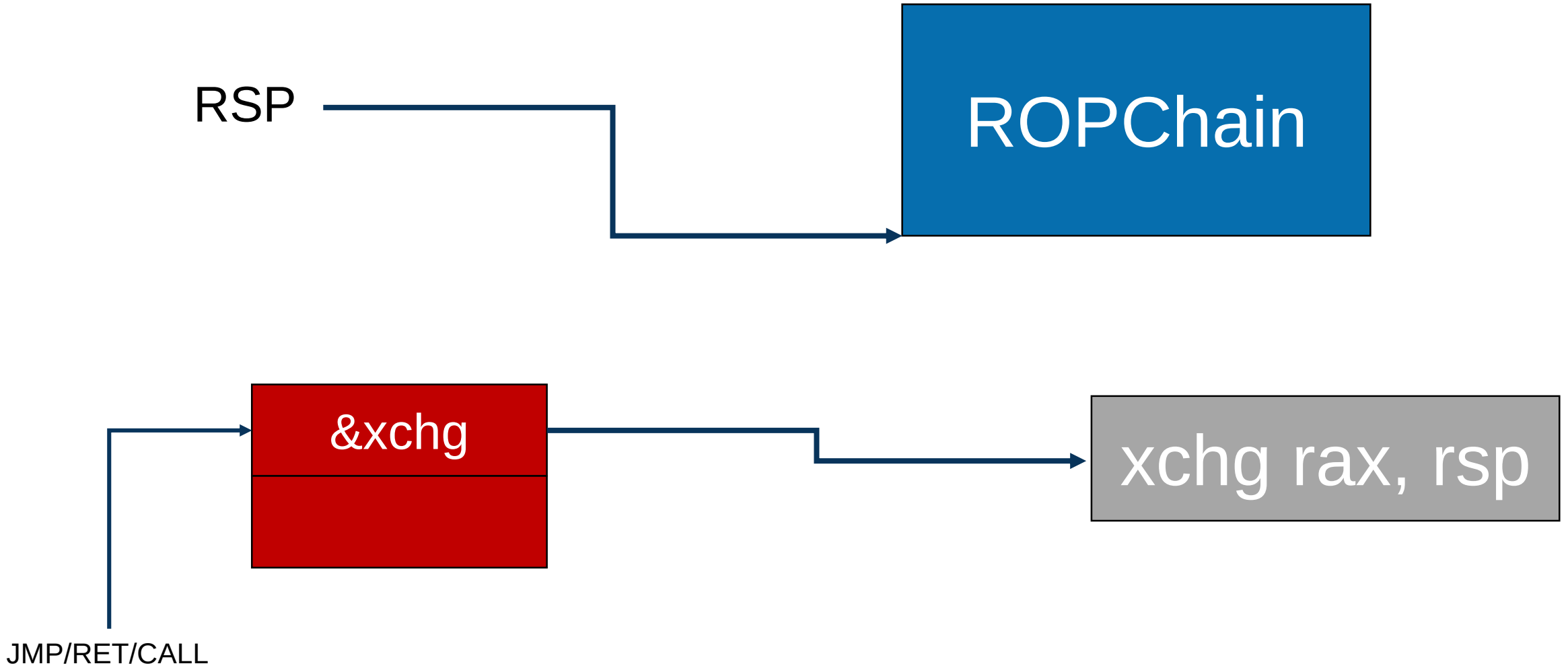
ROP – ROPChain on stack



ROP – ROPChain on heap



ROP – ROPChain on heap




COMPASS
SECURITY