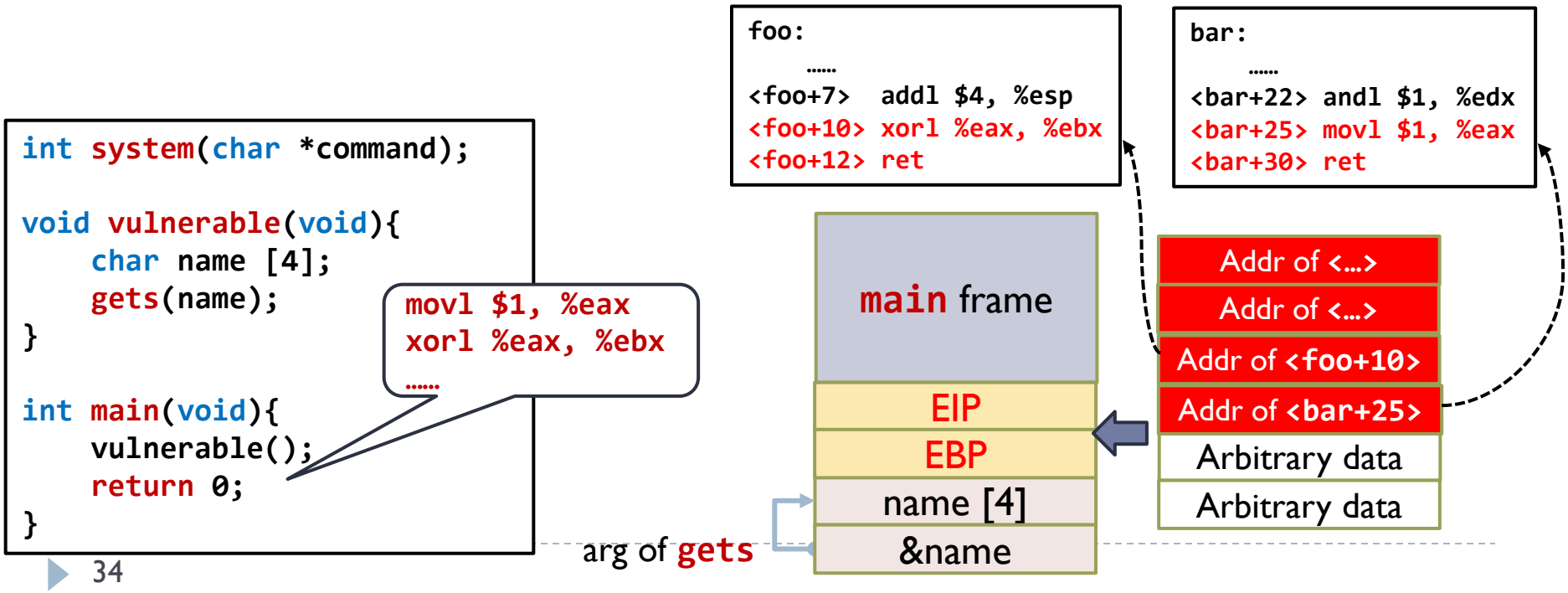
Insecurity of Non-Executable Memory

Return-Oriented Programming (ROP):

- Construct the malicious code by chaining pieces of existing code (gadget) from different programs.
- Gadget: a small set of assembly instructions that already exist in the system. It usually end with a return instruction (`ret`), which pops the bottom of the stack as the next instruction.



Limitations of Non-Executable Memory

Two types of executing programs

- Compile a program to the binary code, and then execute it on a machine (C, C++)
- Use an interpreter to interpret the source code and then execute it (Python)

Just-in-Time (JIT) compilation

- Compile heavily-used ("hot") parts of the program (e.g., methods being executed several times), while interpret the rest parts.
- Exploit runtime profiling to perform more targeted optimizations than compilers targeting native code directly

This requires executable heap

- Conflict with the Non-executable Memory protection