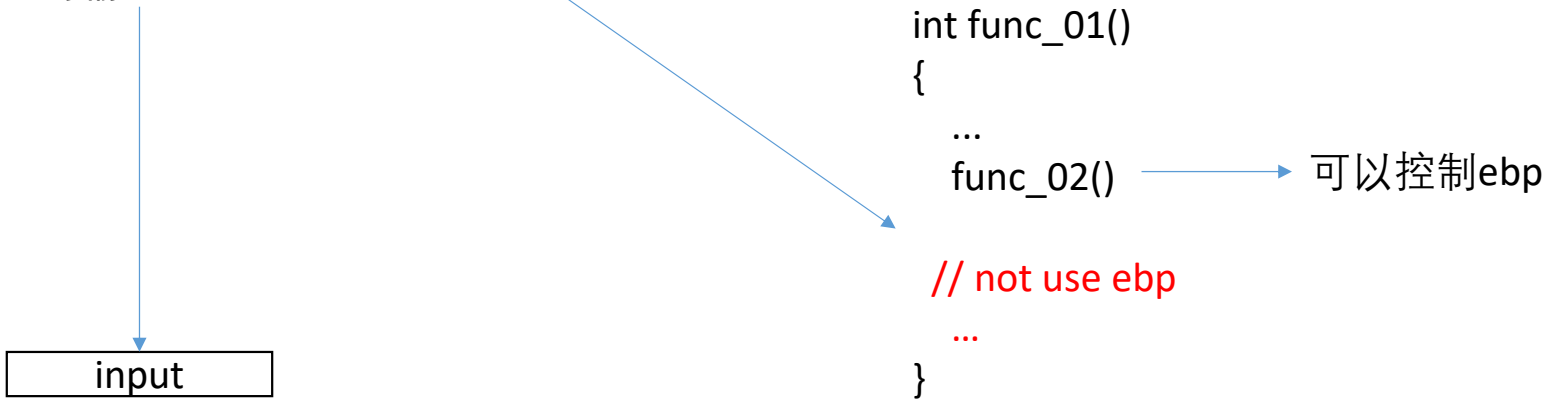
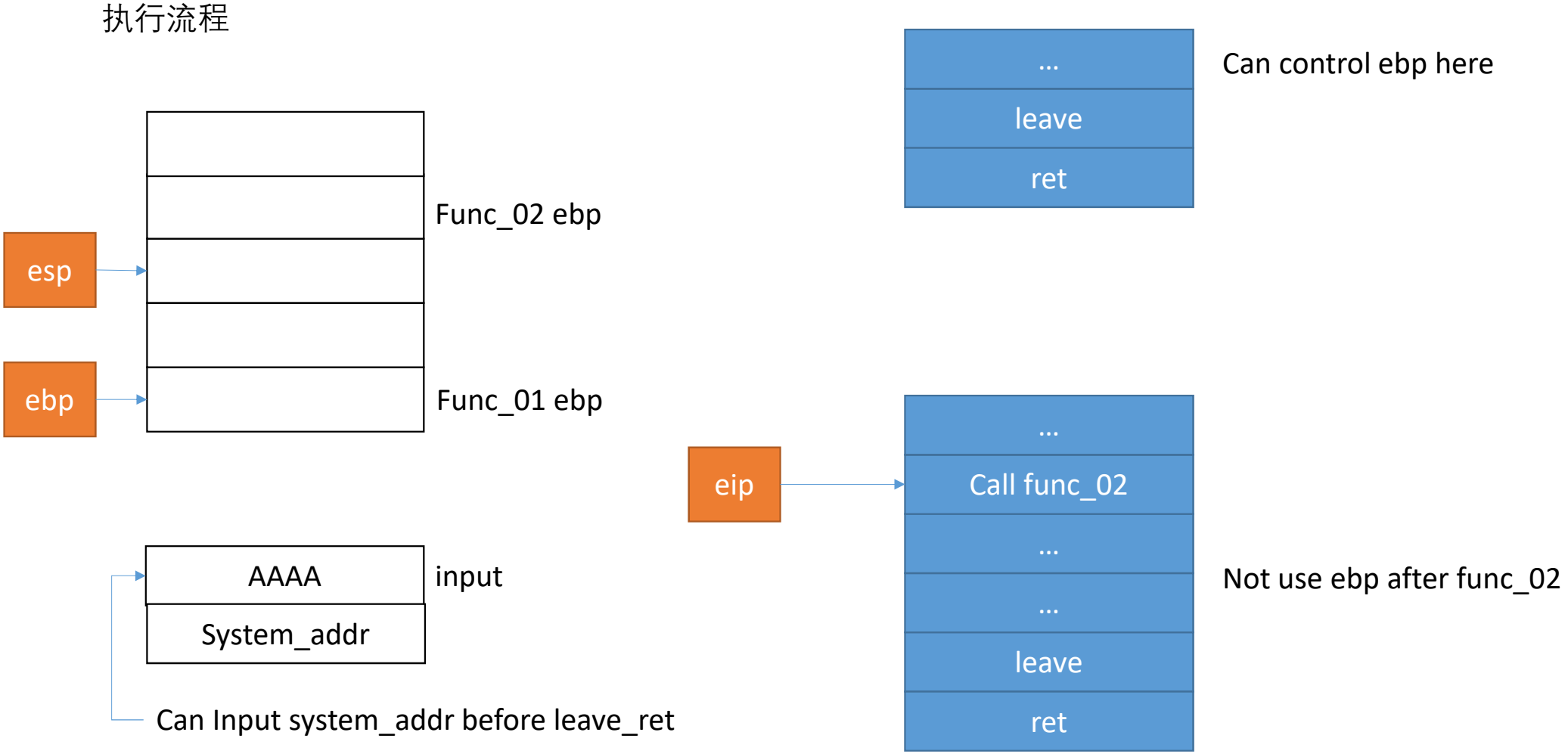
Control ebp, control the world

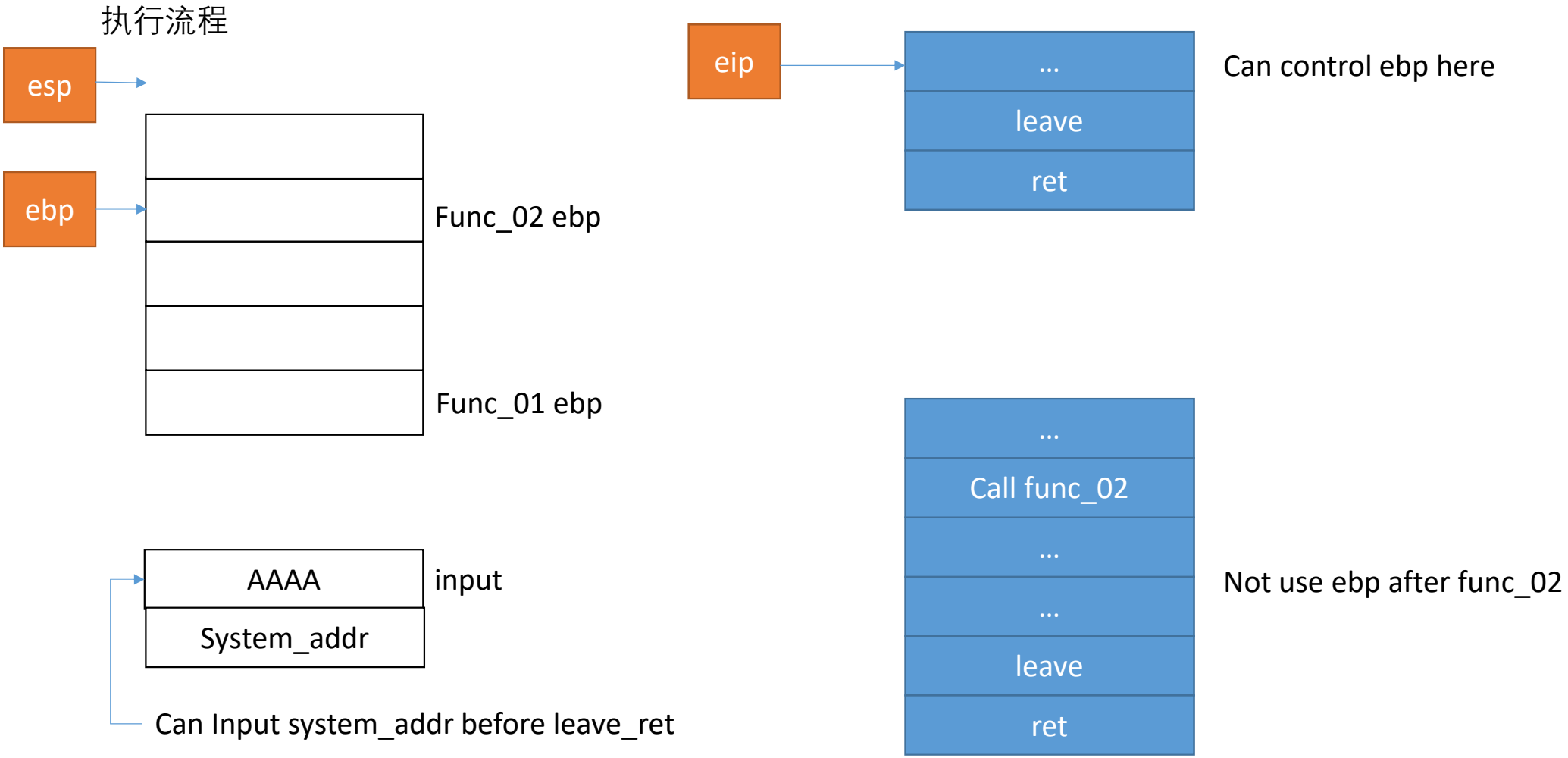
条件

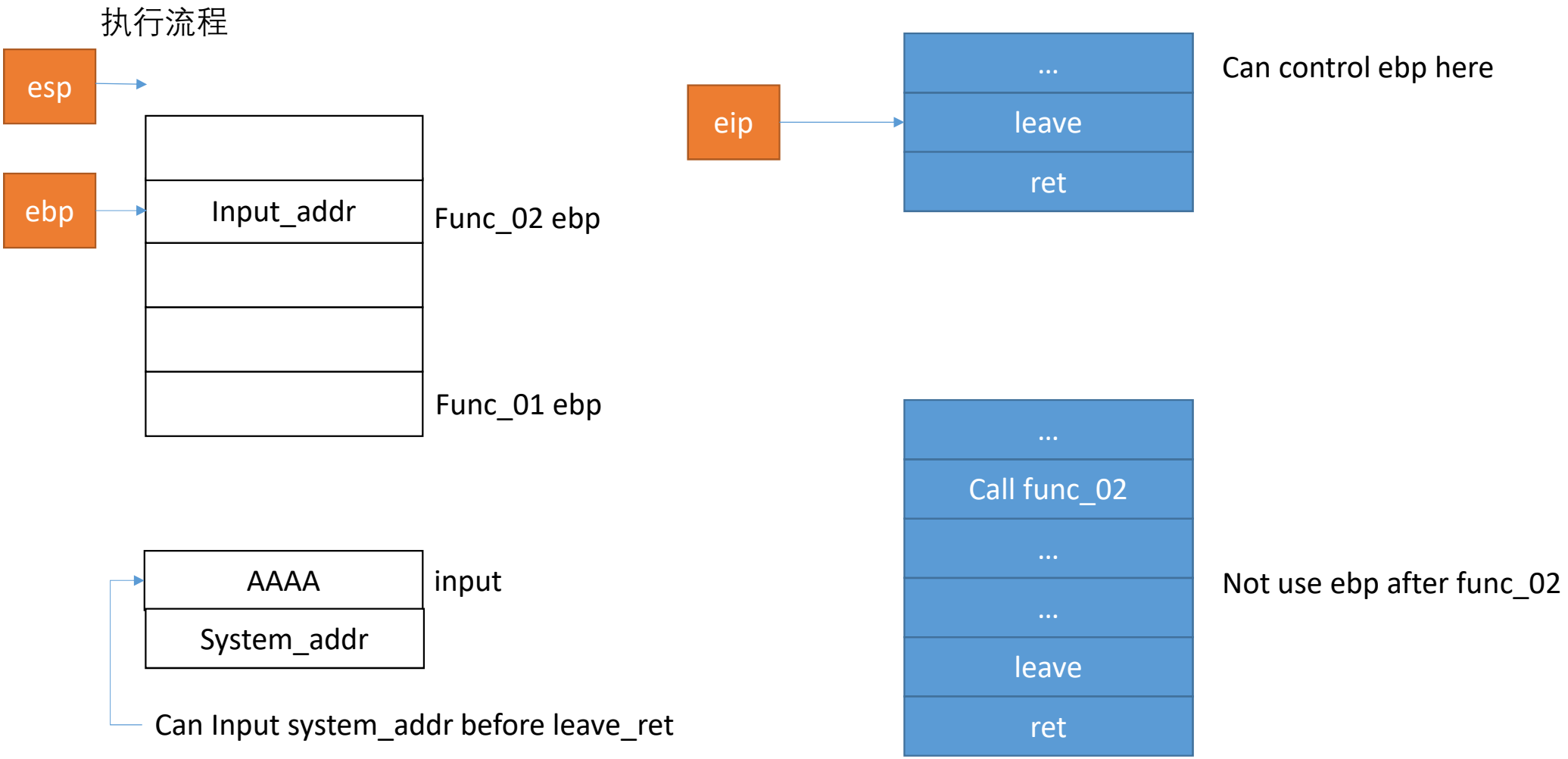
- 可以执行连续两次(leave ， ret)
- 有一段已知地址的输入
- 可以控制ebp



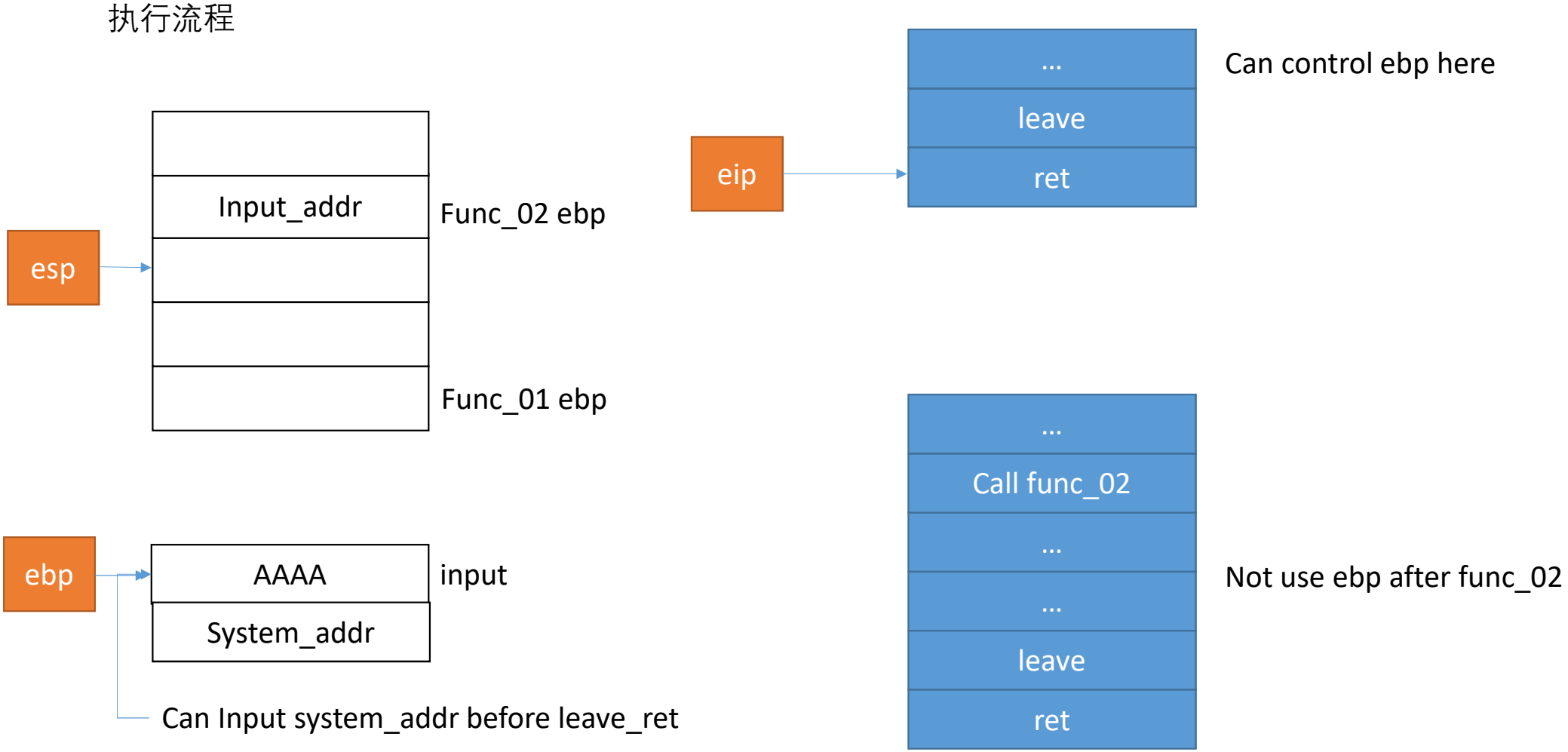
执行流程


esp
ebp
Func_02 ebp
Func_01 ebp
AAAA
System_addr
input
Can Input system_addr before leave_ret
eip
...
Call func_02
...
...
leave
ret
...
leave
ret
Can control ebp here
Not use ebp after func_02

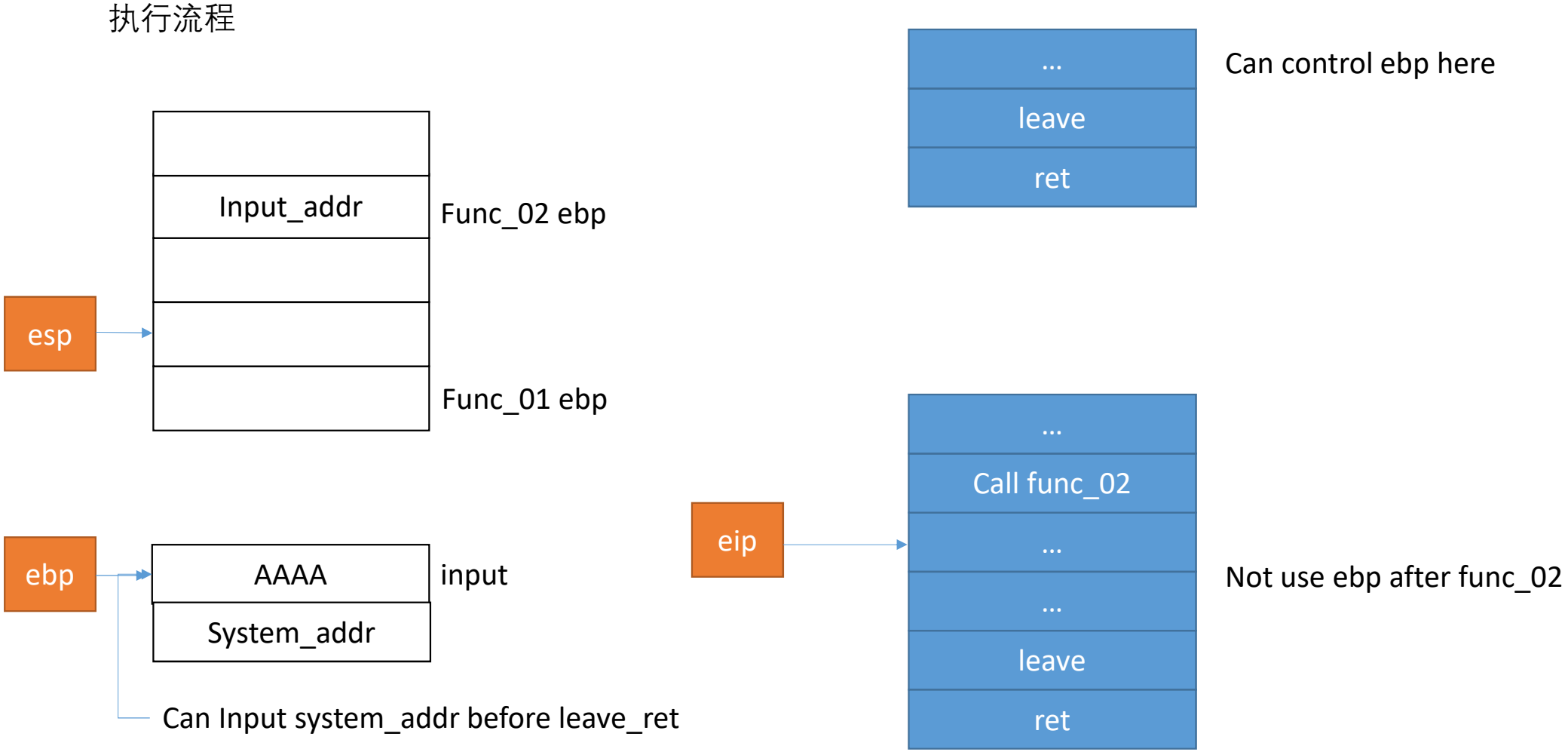

执行流程
esp
ebp
Func_02 ebp
Func_01 ebp
AAAA
System_addr
input
Can Input system_addr before leave_ret
eip
...
leave
ret
Can control ebp here
...
Call func_02
...
...
leave
ret
Not use ebp after func_02


执行流程
esp
ebp
Input_addr
Func_02 ebp
Func_01 ebp
AAAA
System_addr
input
Can Input system_addr before leave_ret
eip
...
leave
ret
Can control ebp here
...
Call func_02
...
...
leave
ret
Not use ebp after func_02

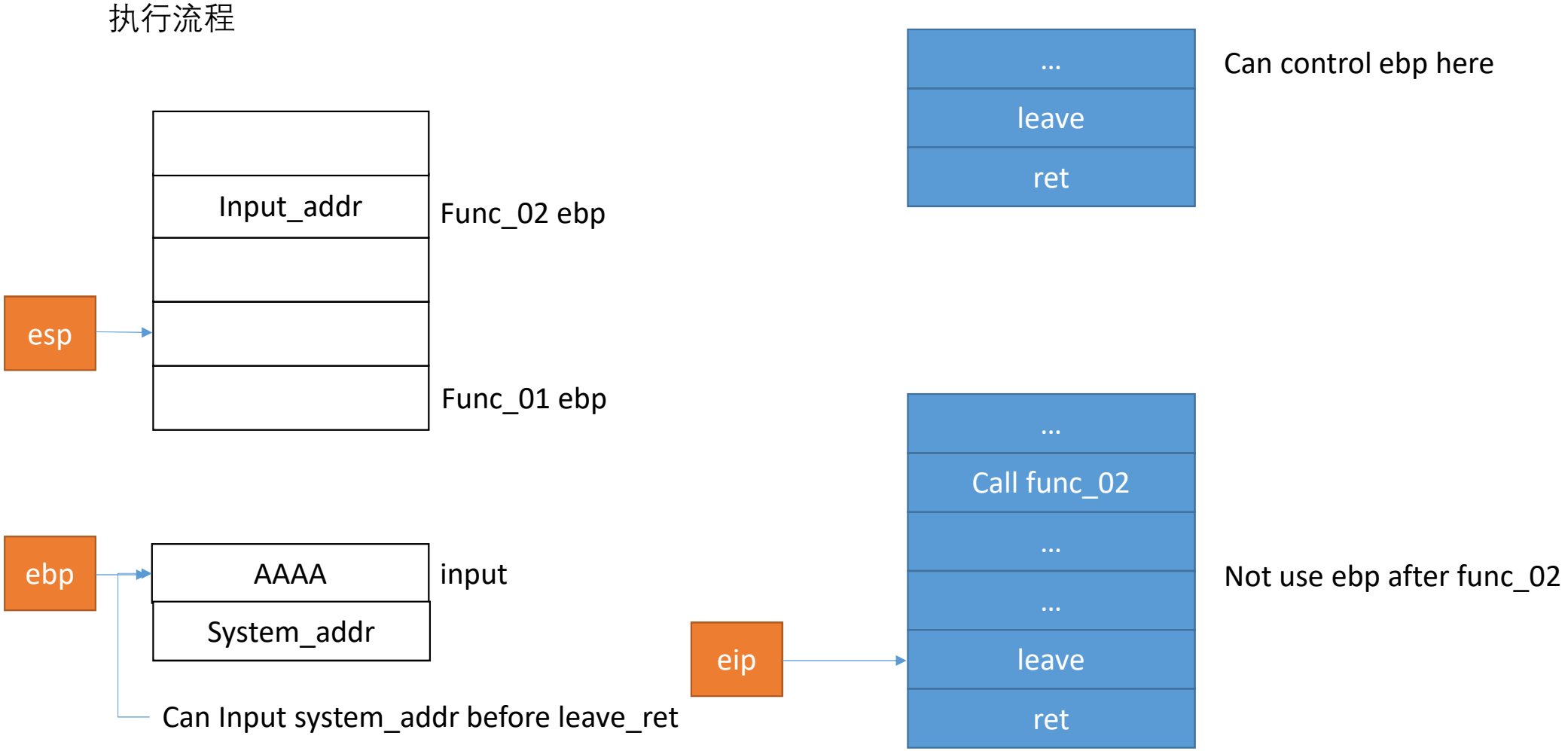
执行流程


esp
Input_addr
Func_02 ebp
Func_01 ebp
ebp
AAAA
System_addr
input
Can Input system_addr before leave_ret
eip
...
leave
ret
Can control ebp here
...
Call func_02
...
...
leave
ret
Not use ebp after func_02

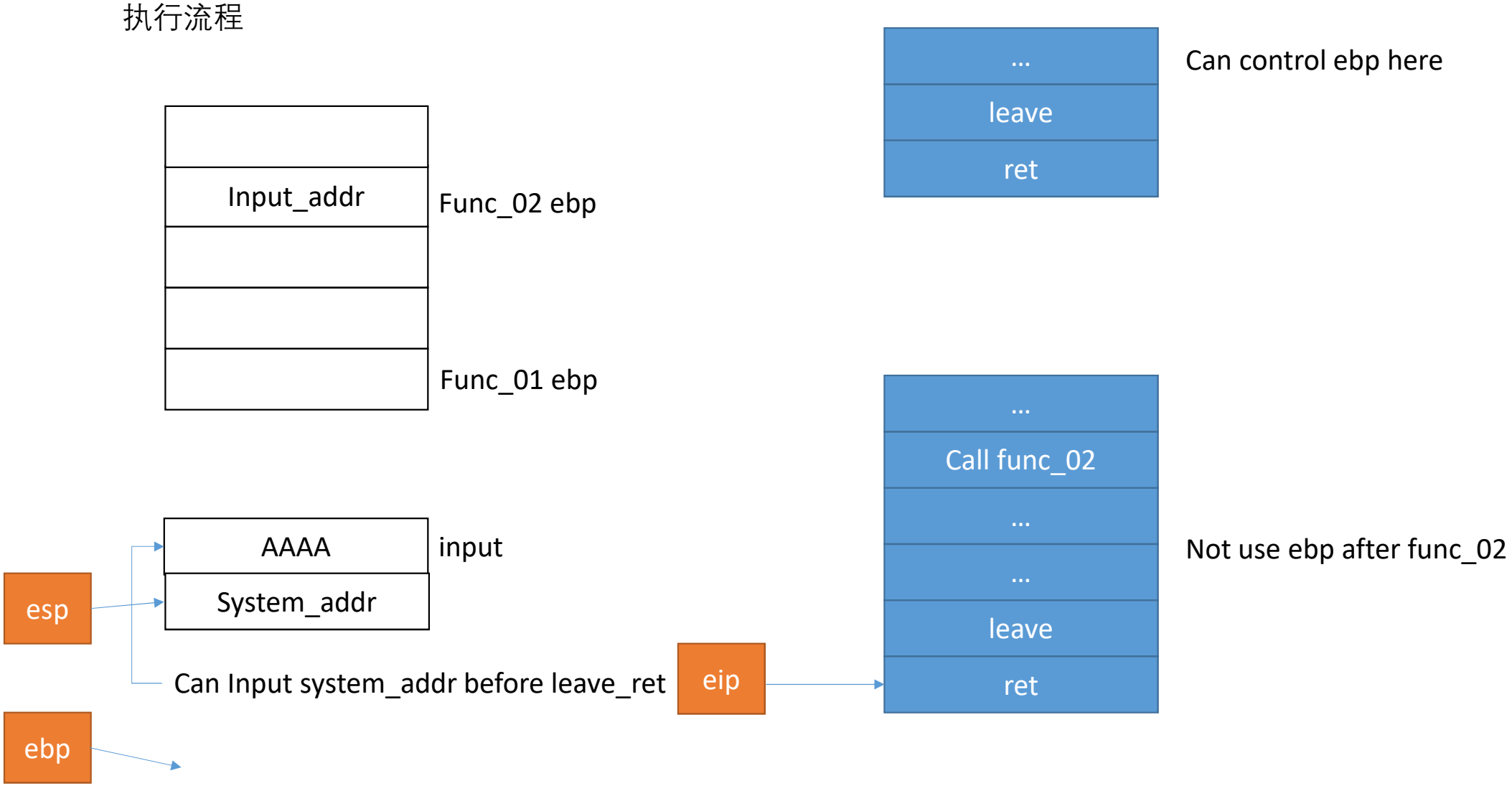
执行流程


...
leave
ret
Can control ebp here
Input_addr
Func_02 ebp
esp
Func_01 ebp
...
Call func_02
eip
...
Not use ebp after func_02
ebp
AAAA
input
...
System_addr
leave
ret
Can Input system_addr before leave_ret

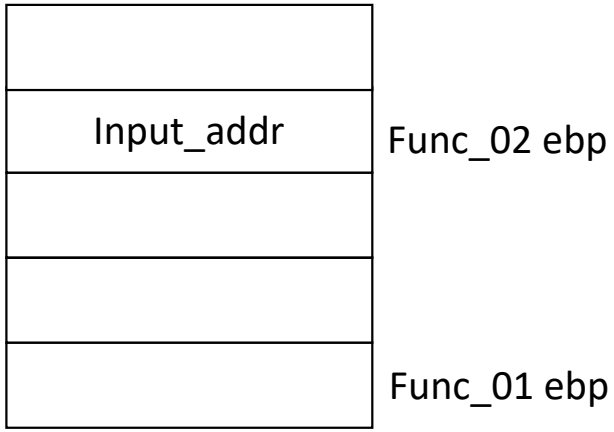
执行流程

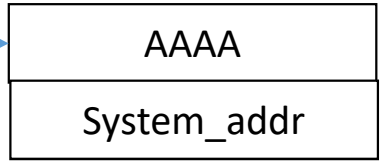

...
leave
ret
Can control ebp here
Input_addr
Func_02 ebp
esp
Func_01 ebp
...
Call func_02
...
...
leave
ret
Not use ebp after func_02
ebp
AAAA
input
System_addr
eip
Can Input system_addr before leave_ret

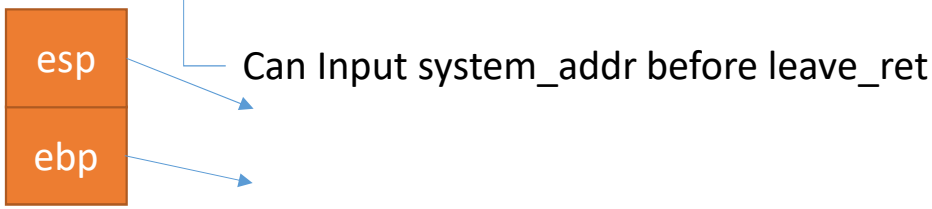
执行流程


...
leave
ret
Can control ebp here
Input_addr
Func_02 ebp
Func_01 ebp
...
Call func_02
...
...
leave
ret
Not use ebp after func_02
AAAA
System_addr
input
esp
Can Input system_addr before leave_ret
eip
ebp

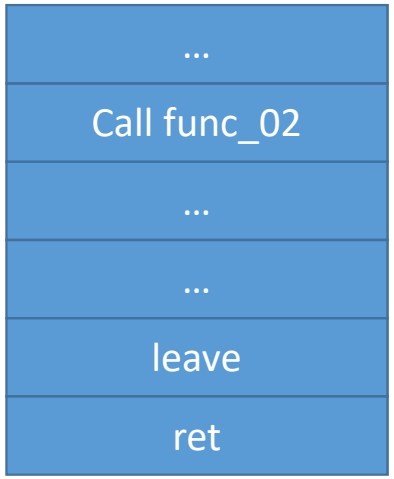
执行流程


Input_addr
Func_02 ebp
Func_01 ebp


AAAA
System_addr
input


esp
ebp
Can Input system_addr before leave_ret


...
leave
ret
Can control ebp here


...
Call func_02
...
...
leave
ret
Not use ebp after func_02


Eip = system_addr

OK