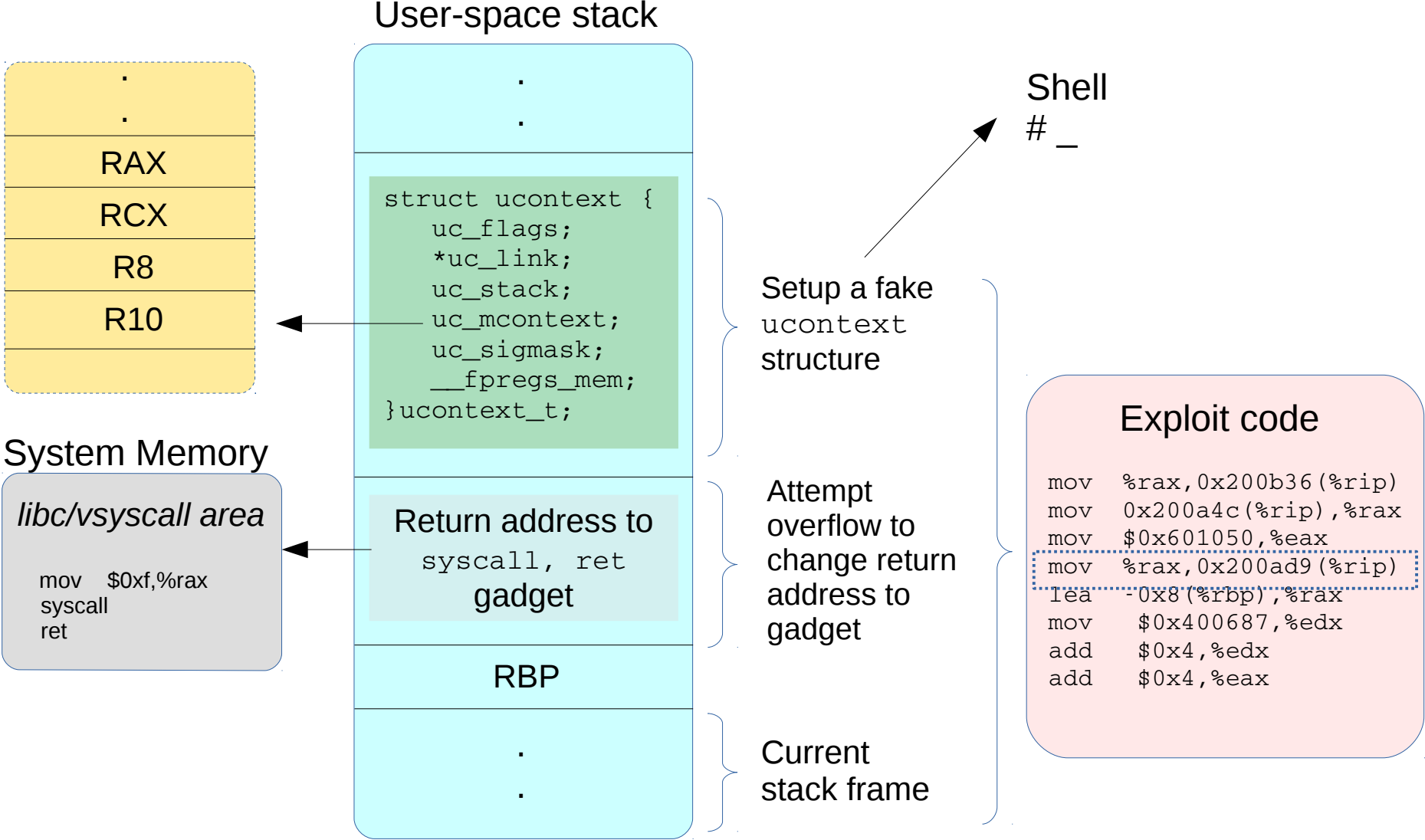
User-space stack
.
.
RAX
RCX
R8
R10
struct ucontext {
uc_flags;
*uc_link;
uc_stack;
uc_mcontext;
uc_sigmask;
__fpregs_mem;
}ucontext_t;
Shell
_
Setup a fake ucontext structure
System Memory
libc/vsyscall area
mov $0xf,%rax
syscall
ret
Return address to syscall, ret gadget
Attempt overflow to change return address to gadget
RBP
Current stack frame
Exploit code
mov %rax,0x200b36(%rip)
mov 0x200a4c(%rip),%rax
mov $0x601050,%eax
mov %rax,0x200ad9(%rip)
lea -0x8(%rbp),%rax
mov $0x400687,%edx
add $0x4,%edx
add $0x4,%eax