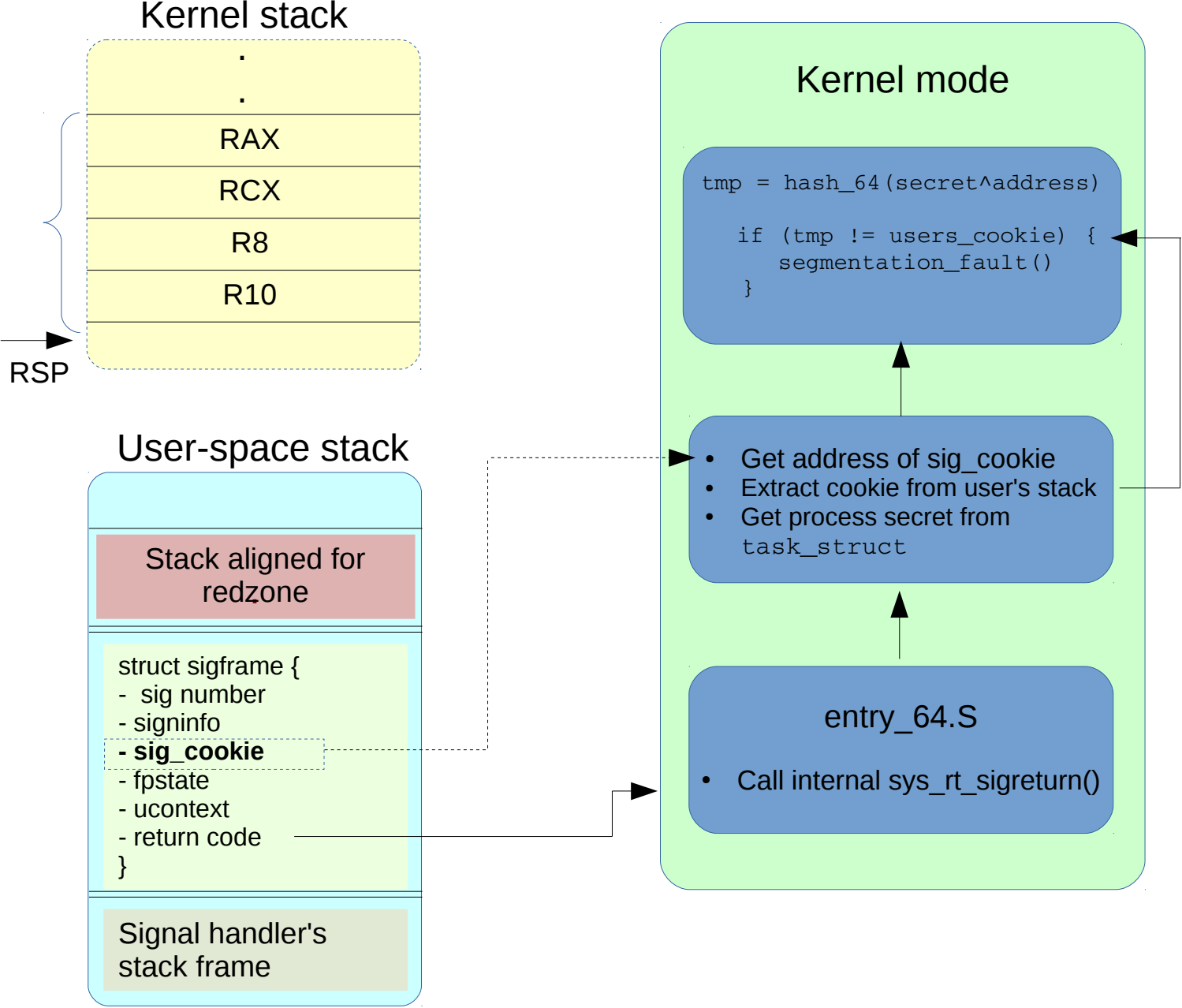
Kernel stack
.
.
RAX
RCX
R8
R10
RSP
User-space stack
Stack aligned for redzone
struct sigframe {
- sig number
- signinfo
- sig_cookie
- fpstate
- ucontext
- return code
}
Signal handler's stack frame
Kernel mode
tmp = hash_64(secret^address)
if (tmp != users_cookie) {
segmentation_fault()
}
• Get address of sig_cookie
• Extract cookie from user's stack
• Get process secret from task_struct
entry_64.S
• Call internal sys_rt_sigreturn()