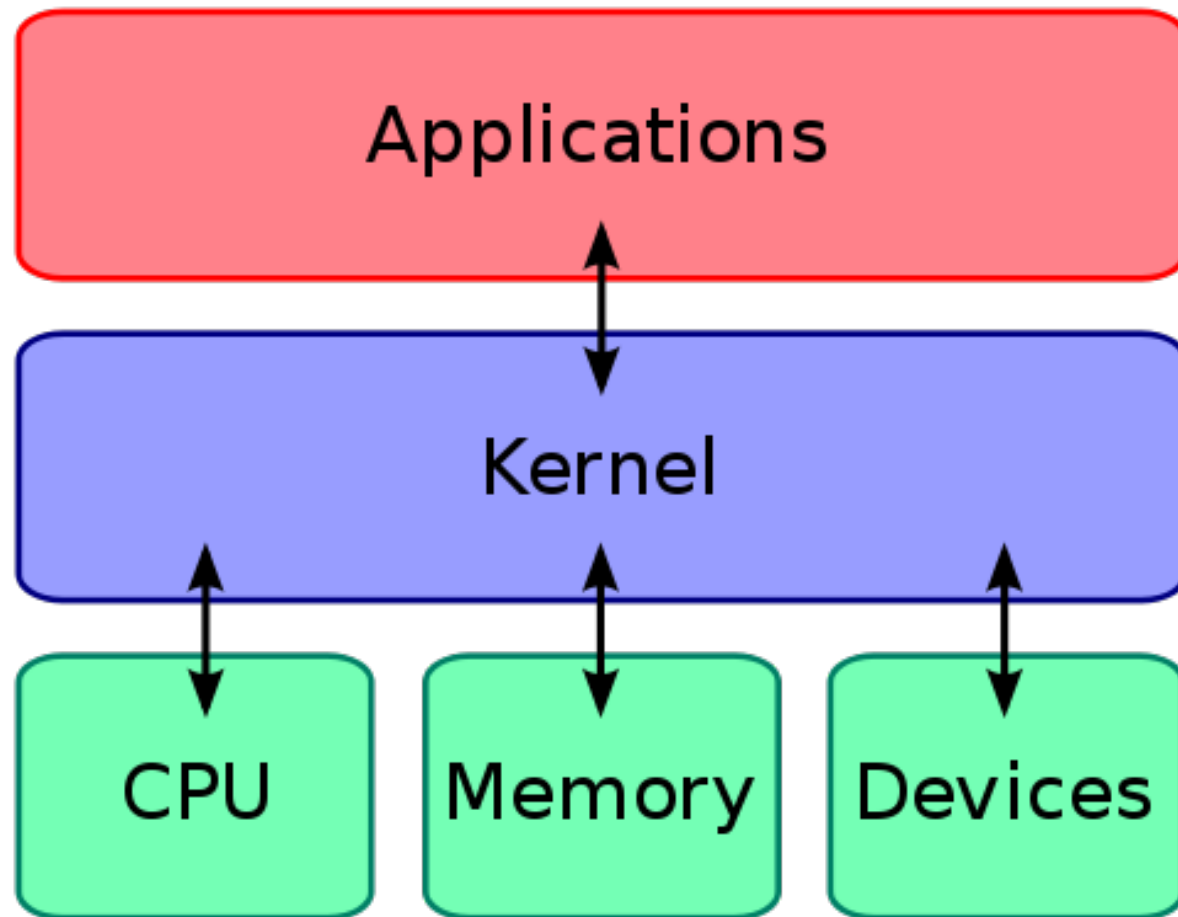


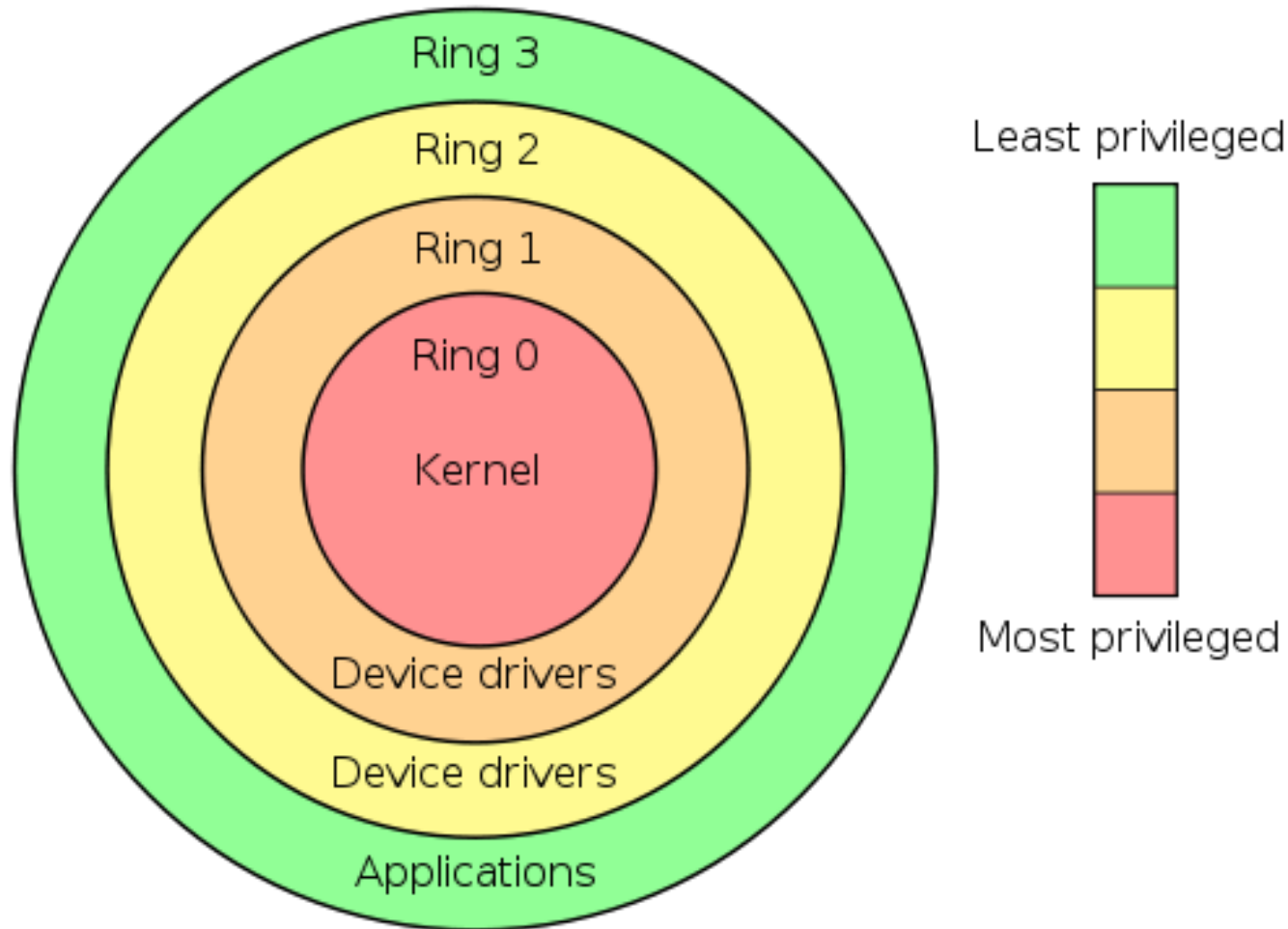
Bartłomiej Świercz

System calls

Operating system



Go to kernel ...



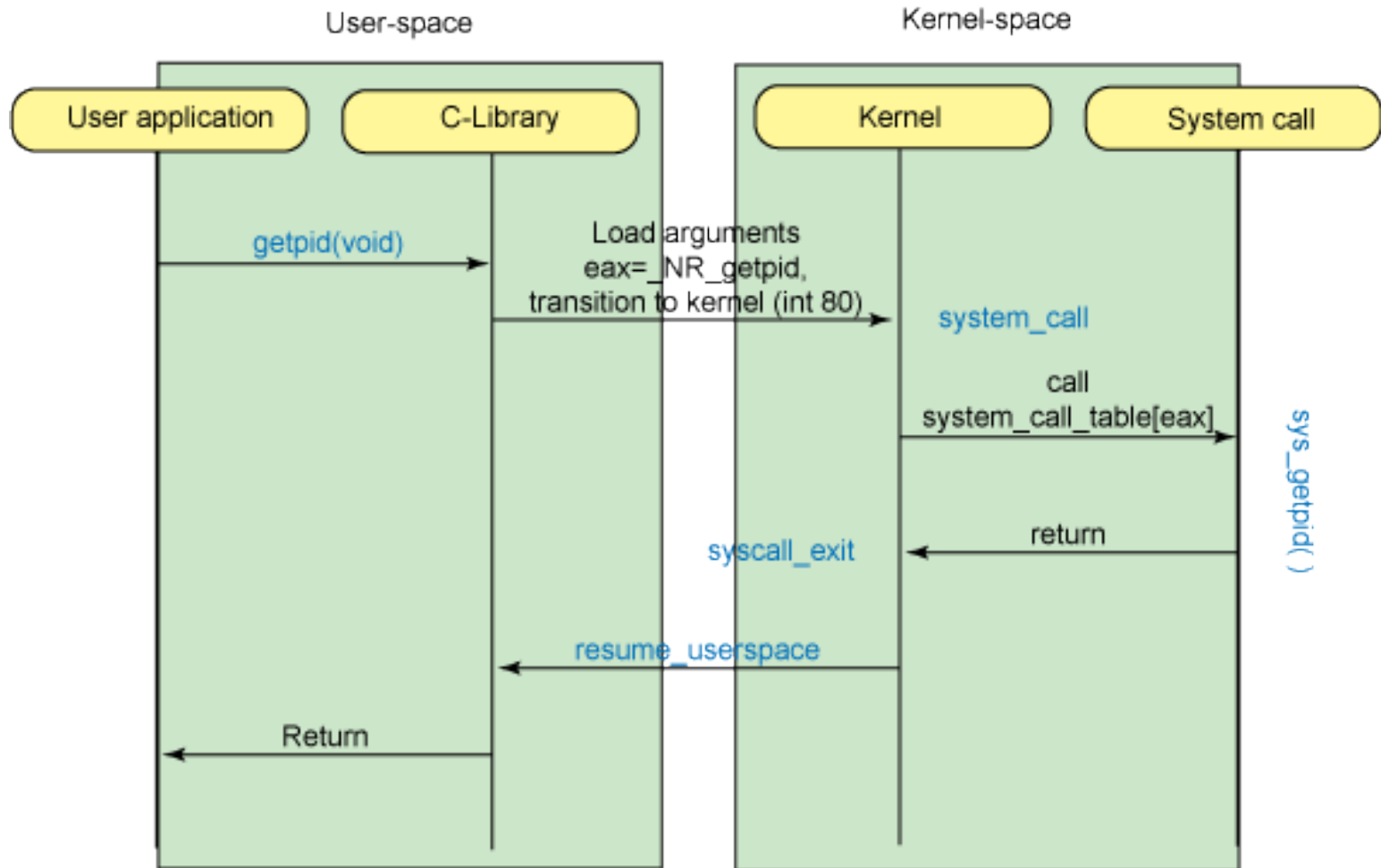
Interrupts

- Hardware interrupts
- Software interrupts
 - System calls
- Slim top half
- Fat bottom half
 - Softirq
 - Tasklets
 - Task queue

System call

- Mechanism to request operation with increased privileges
- System call is provided by OS
 - Kernel code snippet run by user process
- The mechanism is wrapped by library
 - Transmission is hidden
 - Context switching

Syscall path



Syscall table

et	Symbol	sys_call_table	System call location
	__NR_restart_syscall	.long sys_restart_syscall	--> ./linux/kernel/signal.c
	__NR-exit	.long sys_exit	--> ./linux/kernel/exit.c
	__NR_exit	.long sys_fork	--> ./linux/arch/386/kernel/proce
2	__NR_getcpu	.long sys_getcpu	--> ./linux/kernel/sys.c
6	__NR_epoll_pwait	.long sys_epoll_pwait	--> ./linux/kernel/sys_ni.c
	__NR_syscalls	-----	
	./linux/include/asm/unistd.h	↑	
		↑	
		./linux/arch/386/kernel/syscall_table.S	

How to enter to kernel space?

- `int 0x80`
 - Syscall number read from `%eax`
- `SYSCALL/SYSEENTER`
- `SYSRET/SYSEXIT`
- <http://lkml.org/lkml/2002/12/9/13>