Exam 3 Cheatsheet DRAFT

Syscall

rax	System Call	rdi	rsi	rdx
0	read	file descriptor	buffer	number of bytes
1	write	file descriptor	buffer	number of bytes
60	exit	exit code	—	—

Calling C library functions

- Parameters are stored in registers in the following order: rdi, rsi, rdx, rcx, r8, r9. (If there are more parameters, they are pushed onto the stack)
- Most C functions return an integer or a pointer (which is just an integer). The return value is placed in the rax register
- The called functions may use or destroy the content of the following registers: rax, rcx, rdx, rsi, rdi, r8, r9, r10, r11, r15
- Other registers may be used, but the called function is responsible for saving them.

General Purpose Registers

64-bit	32-bit	16-bit	8-bit low	8-bit high	Calling Convention	”Owned” by caller	”Owned” by callee
rax	eax	ax	al	ah	Return Val/Accum		Yes
rbx	ebx	bx	bl	bh	—	Yes	
rcx	ecx	cx	cl	ch	4th argument		Yes
rdx	edx	dx	dl	dh	3rd argument		Yes
rsi	esi	si	sil	–	2nd argument		Yes
rdi	edi	di	dil	–	1st argument		Yes
r8	r8d	r8w	r8b	–	5th argument		Yes
r9	r9d	r9w	r9b	–	—		Yes
r10	r10d	r10w	r10b	–	—		Yes
r11	r11d	r11w	r11b	–	—		Yes
r12	r12d	r12w	r12b	–	—	Yes	
r13	r13d	r13w	r14b	–	—	Yes	
r14	r14d	r14w	r14b	–	—	Yes	
r15	r15d	r15w	r15b	–	—	Yes	

Special Purpose Registers

Register	64-bit	32-bit	16-bit	8-bit low	”Owned” by caller	”Owned” by callee
Stack Pointer	rsp	esp	sp	spl		Yes
Base Pointer	rbp	ebp	bp	bpl	Yes	
Instruction Pointer	rip	eip	ip	–		Yes
Flags and Conditions	rflags	eflags	flags	–		Yes