主管领导审核签字

哈尔滨工业大学 2018 学年 秋 季学期

计算机系统（A）试题

题号	一	二	三	四	五	六	总分
得分							
阅卷人							

片纸鉴心 诚信不败

授课教师 密 姓名 封 学号 线 院系

一、单项选择题（每小题 1 分，共 20 分）

1（ B ） 2（ C ） 3（ A ） 4（ A ） 5（ B ）

6（ C ） 7（ D ） 8（ B ） 9（ A ） 10（ A ）

11（ C ）12（ B ）13（ B ）14（ A） 15（ C ）

16（ B ）17（ C ）18（ D ）19（ B ） 20（ A/B ）

二、填空题 (每空 1 分，共 10 分)

21 n&0x40/0x80 (== 0x40/0x80) 22 24

23 FE FF FF FF 24 gcc -S hello.c (-o hello.s)

25 text 或 代码 26 gcc p.o libx.a liby.a libx.a

27 寄存器 或 Register 28 很大

29 SIGCHLD 30 kill

三、判断对错（每小题 1 分，共 10 分，正确打 √、错误打 ×）

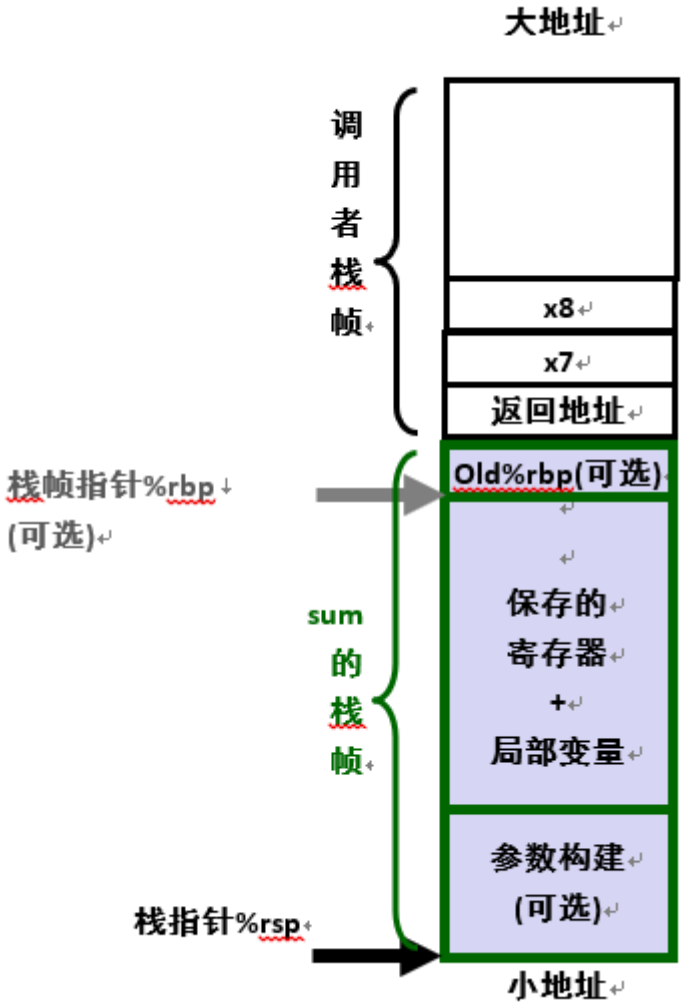
31（ × ） 32（ × ） 33（ √ ） 34（ √ ） 35（ × ）

36（ √ ） 37（ × ） 38（ √ ） 39（ √ ） 40（ √ ）

四、简答题（每小题 5 分，共 20 分）

41 题（每点 1 分，图 2 分，满分 5 分）

- 整型参数 x1~x6 分别用%rdi, %rsi, %rdx, %rcx, %r8, %r9 传递
  或：整型参数 x1~x6 分别用%edi, , %esi, %edx, %ecx, %r8d, %r9d 传递
- 参数 x7 x8 用栈传递；
- 返回值用%rax（%eax）传递
- call 指令将返回地址入栈、并将控制转移到被调用函数
- ret 指令将返回地址出栈、修改 RIP 的数值，将控制转移到调用者程序。



42 题（每个采分点 1 分，满分 5 分）

攻击原理（3 个采分点）：向程序输入缓冲区写入特定的数据，例如在 gets 读入字符串时，使位于栈中的缓冲区数据溢出，用特定的内容覆盖栈中的内容，例如函数返回地址等，使得程序在读入字符串，结束函数 gets 从栈中读取返回地址时，错误地返回到特定的位置，执行特定的代码，达到攻击的目的。

防范方法(2 个采分点,有 2 个就算对)：

1. 代码中避免溢出漏洞：例如使用限制字符串长度的库函数。
2. 随机栈偏移：程序启动后，在栈中分配随机数量的空间，将移动整个程序使用的栈空间地址。
3. 限制可执行代码的区域
4. 进行栈破坏检查——金丝雀

43 题（每个采分点 1 分，满分 5 分）

(0)Linux 系统中，Shell 是一个交互型应用级程序，代表用户运行其他程序(是命令行解释器，以用户态方式运行的终端进程)。
其基本功能是解释并运行用户的指令，重复如下处理过程：
(1)终端进程读取用户由键盘输入的命令行。
(2)分析命令行字符串，获取命令行参数，并构造传递给 execve 的 argv 向量
(3)检查第一个(首个、第 0 个）命令行参数是否是一个内置的 shell 命令
(3)如果不是内部命令，调用 fork( )创建新进程/子进程
(4)在子进程中，用步骤 2 获取的参数，调用 execve( )执行指定程序。
(5)如果用户没要求后台运行(命令末尾没有&号）否则 shell 使用 waitpid（或 wait...)等待作业终止后返回。
(6)如果用户要求后台运行(如果命令末尾有&号），则 shell 返回；

44 题

说明浮点数表示原理：以 float 为例，1 符号、8 位的阶码、23 位的尾数三部分，可以表示浮点规格化数、非规格化数、无穷大、NaN 等浮点数据（3 分）。
相等的判别描述合理即可（1-2 分）：由于浮点数的 ieee754 编码表示存在着精度、舍入、溢出、类型不匹配等问题，两个浮点数不能够直接比较大小，应计算两个浮点数的差的绝对值，当绝对值小于某个可以接受的数值（精度）时认为相等。如：

```
1 #define DBL_EPSILON          2.2204460492503131E-16
2 #define FLT_EPSILON          1.19209290E-07F
3 #define LDBL_EPSILON         1.084202172485504E-19
```

五、系统分析题（20 分）

45 题

①入栈指令，将 rbp 入栈

②传送指令，将栈顶指针 rsp 的值传送给 rbp

③传送指令，向%rbp-4 的内存位置传送数值 0（局部变量 i 赋初值 0）

④比较指令：%rbp-4 的内存数值（局部变量 i 的值）与 3 进行比较 （i<4 吗）

⑤条件跳转指令，小于等于则跳转（跳转到 4004f4 处） （i<4 则循环）

46 题

①：ae ff ff ff （反向也算正确）

②：05 0b 20 00

③：ff 0a 20 00

④：e4 05 40 00

⑤：9a fe ff ff

47 题

源操作数是内存操作数类型 或 整型

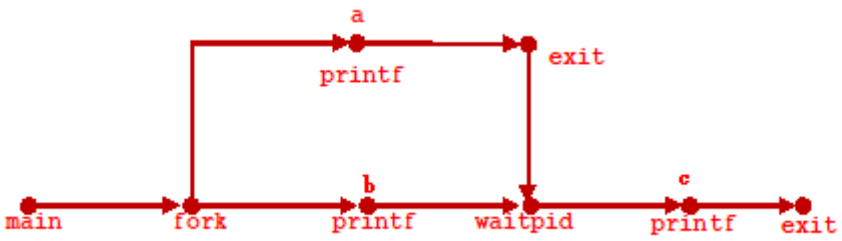
有效地址是：0x601030 + %rax*4 或 0x601030 + %rax<<2

对应 C 语言源程序中的 a[i]

rax 对应 C 语言源程序中的 i（eax 开始是有符号数 i 的值，cltq 将 eax 扩展成 8 字节值 rax）

int 类型每个元素 4 个字节，因此比例因子为 4.

48 题:48.1 进程图（3 分）



48.2 可能的输出数列（2 分）：

"abc" （1 分）

或 "bac"（1 分）

六、综合设计题（共 20 分）

49 题:

（1）取指:

icode:ifun←M1[PC]

rA:rB←M1[PC+1]

valC←M8[PC+2]

valP←PC+10

(2)译码：valB←R[rB]

(3)执行：valE←valB+valC

(4)访存：无操作（空着就行）

(5)写回：R[rB]←valE

(6)更：新 PC PC←valP

50 题

面向 CPU 的优化方式：指令级并行，可以用循环展开

面向 Cache 的优化：主要采用矩阵分块的代码优化方式

优化的说明合理可行