UNIVERSITY OF LONDON

BSc EXAMINATION 2019

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

IY2840: Computer and Network Security
IY2840R: Computer and Network Security – PAPER FOR RESIT CANDIDATES

Time Allowed: **TWO hours**

Answer ALL questions

Calculators are NOT permitted

1. MECHANISMS FOR ACCESS CONTROL

(a) Anderson proposed the concept of a Reference Monitor in 1972.

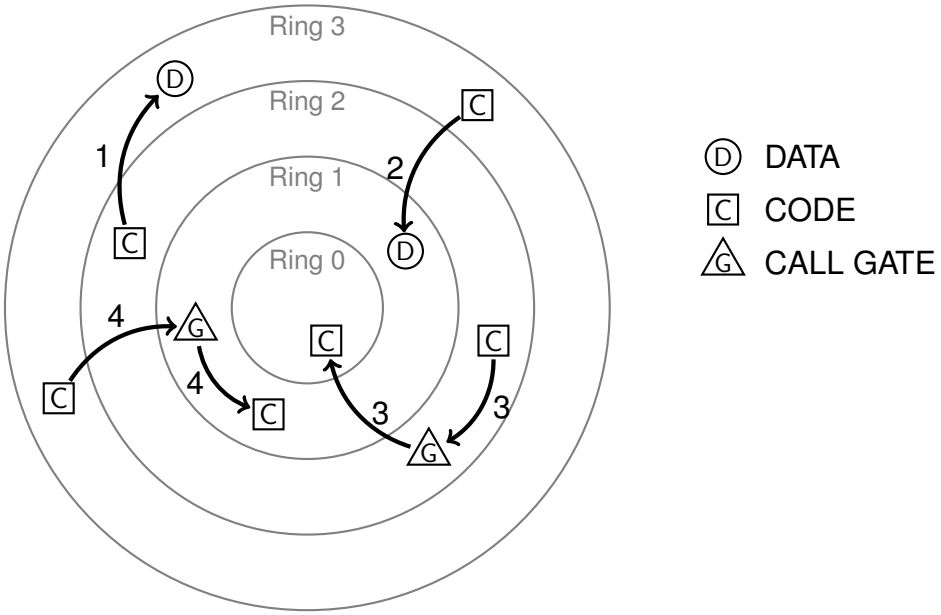
i. Describe what is meant by the concept of a Reference Monitor. [6 marks]

ii. List three properties that a Reference Monitor must have. [3 marks]

iii. For each of the three properties above, explain why the Reference Monitor would not work if it did not have this property. [6 marks]

(b) In the MULTICS hardware security architecture, the Reference Monitor was implemented by means of a protection ring architecture. What is a protection ring architecture and how does it provide access control? [6 marks]

(c) Call gates allow controlled access between protection rings. In the following diagram, arrows 1 and 2 illustrate attempts by a piece of code to access a piece of data, and arrows 3 and 4 illustrate attempts to transfer control via a call gate.



Which of the four attempts to access data or transfer control are allowed? Which ones are not allowed? (No explanation necessary.) [4 marks]

2. HARDWARE ACCESS CONTROL

The Intel 80386 architecture implements concepts from the MULTICS protection ring architecture.

NEXT PAGE

(a) This question is on the technical realization of protection rings on the 80386. Describe details **specific to the 80386** (that is, details that could be different for other CPUs) that are related to protection rings.

You can base your description on the following topics (other topics are also possible): How and where are ring numbers encoded? Which technical component makes the access control decision? Which operation is required to make such a decision? How is the controlled invocation mechanism implemented? [8 marks]

(b) Many modern CPUs offer four protection rings, but most current operating systems, including Windows and Linux, only use two. Why do you think this is the case? [4 marks]

3. **UNIX ACCESS CONTROL**

Assume Alice, Bob, and Charlie have accounts on the same UNIX system. Their usernames are `alice`, `bob` and `charlie`, respectively.

- Alice is **a member** of groups `staff` and `cdrom`.
- Alice is **not a member** of group `admin`.
- Charlie is **a member** of group `admin`.
- Charlie is **not a member** of groups `staff` and `cdrom`.

Assume a directory on the system that contains six files (`file1`–`file6`) with file mode and ownership displayed as follows:

```
$ stat --format="%a %A %U/%G %n" file[1-6]
0466 -r--rw-rw-  alice/staff  file1
0442 -r--r---w-  root/cdrom   file2
0777 -rwxrwxrwx  root/admin   file3
0044 ----r--r--  alice/staff  file4
0424 -r---w-r--  root/cdrom   file5
0204 --w----r--  root/admin   file6
```

Here, the left-most column (`%a`) lists the file mode in octal, the second column (`%A`) lists the file mode in ASCII, the third column (`%U/%G`) shows the user identifier and the group identifier of the file owner in combined form (in UID/GID format), and the right-most column shows the name of the file.

(a) List all files that . . .

i. user `alice` can open for **writing**. [2 marks]
ii. user `alice` can open for **reading**. [2 marks]
iii. user `root` (with UID = 0) can open for **reading**. [2 marks]
iv. user `charlie` can open for **writing**. [2 marks]

(b) Which of the six files has the set-user-id (SUID) bit set? [2 marks]

(c) The directory in which the six files reside has the **sticky bit** set. More precisely, the file mode is as follows:

```
$ stat --format="%a %A %U/%G %n" .
1777 drwxrwxrwt  root/root  .
```

Which two users can delete `file1`? [2 marks]

4. **SOFTWARE SECURITY and SHELLCODE**

The following assembly listing shows a *shellcode* that is functional for Linux on the Intel 80386. It is similar to the ones that were considered in the IY2840 lectures and labs.

```
1    jmp ahead
2
3    back:
4       popl %ebx
5       movl $0x0, %eax
6       movl %ebx, 0x8(%ebx)
7       leal 0x8(%ebx), %ecx
8       movb %al, 0x7(%ebx)
9       movl %eax, %edx
10      movl %eax, 0xc(%ebx)
11      movb $0xb, %al
12      int $0x80
13
14   ahead:
15      call back
16      .string "/bin/sh"
```

(a) If a shellcode is executed by the CPU (starting with the instruction in line 1), what do you expect to happen? [2 marks]

(b) What is the number of the `execve` system call in Linux? You can answer in decimal or hexadecimal, but please indicate which one you use. [2 marks]

(c) What is the effect of line 8? (That is, what is its function in the shellcode?) [2 marks]

(d) What purpose do the `call` (line 15) and `pop` (line 4) instructions serve? (That is, what is their function in the shellcode?) [4 marks]

(e) The shellcode would stop working if line 1 was replaced by `call back` (that is, a `call` to line 3). However it could be repaired by inserting an additional instruction between lines 4 and 5. Which instruction would that be, and which registers would it affect? (No need to be precise with the quantities, and no need to avoid null bytes in the opcodes.) [4 marks]

(f) A shellcode can be augmented by a so-called **NOP sled**. Explain the NOP sled concept. Explain in particular: What does it consist of, where is it placed in relation to the shellcode, what is its purpose, and how large would it optimally be. [5 marks]

5. **OPERATING SYSTEM SECURITY**

In a UNIX environment, applications might be vulnerable to one or more of the following attacks: (1) attack via environment variable, (2) attack via symlink, (3) attack by exploiting a race condition ('TOCTOU'), (4) attack by command injection.

Pick one of the four attacks (indicate which one) and give a concrete example for how it could be conducted. Likely your attack applies only in specific cases or assumes specific programming errors; say which conditions these are. Which property of the UNIX environment is relevant and exploited? Also mention what the outcome of the attack is: What did the attacker gain from conducting it? [14 marks]

6. **WEB SECURITY**

Cross-Site Scripting (XSS) is a widespread problem affecting a number of web services.

(a) State the main vulnerability that leads to XSS attacks. [2 marks]

(b) Briefly describe the *general principle* of XSS attacks. Which security policy is both evaded and exploited in such attacks. [8 marks]

(c) Describe the difference between a Stored XSS attack and a Reflected XSS attack. [8 marks]

END