UNIVERSITY OF LONDON

BSc EXAMINATION 2022

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

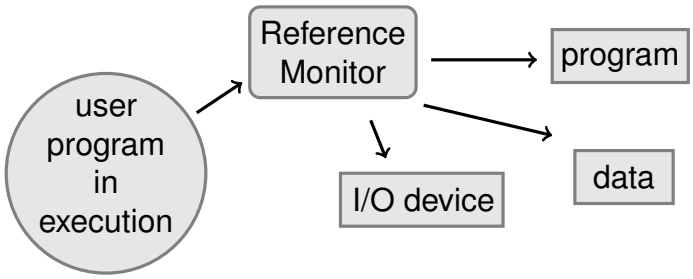
IY2840: Computer and Network Security
IY2840R: Computer and Network Security – for
FIRSTSIT/RESIT CANDIDATES

Time Allowed: **TWO hours**

Please answer **ALL** questions

1. ANDERSON REPORT

The following figure is a reproduction from the Anderson Report from 1972.



(a) In the figure, which parts symbolize a **subject** and which symbolize an **object**?

[4 marks]

(b) In Unix what are the Principals, Subjects, and Objects? [6 marks]

(c) Describe what is meant by the concept of a **Reference Monitor**.

[6 marks]

(d) List three properties that a Reference Monitor must have. [3 marks]

(e) State three places in a computer system where you might find a Reference Monitor, and give an example of each. [6 marks]

2. DNS

An adversary has gained root access to an old Linux system. They now wish to access other systems on the network and think about poisoning the local name server's DNS cache.

(a) To do this, the attacker needs to understand how DNS works. Explain the steps involved when a client uses DNS to find the IP address of a particular domain. You may use a diagram if this helps. [10 marks]

(b) How does a DNS resolver authenticate replies from authoritative name servers, and how does this help the attacker with their attack? [4 marks]

(c) Assuming the local name server has a short TTL for local cache entries, how might the adversary poison its DNS cache to set the IP address of a local server to one of his choosing? [12 marks]

3. **SYSTEM SECURITY**

Consider the following C code fragment, which is vulnerable to a memory corruption attack:

```
int
main(int argc, char **argv)
{
  char lbuf[512];

  if (argc > 1)
    strcpy(lbuf, argv[1]);

  return(0);
}
```

Explain why the above code is exploitable on x86-32 architecture. Is it possible to execute arbitrary code, such as spawning a shell? Explain how you would exploit it (high-level steps). [5 marks]

4. **WEB SECURITY**

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

i. State the main vulnerability that leads to XSS attacks. [2 marks]

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

iii. Describe the difference between a Stored XSS attack and a Reflected XSS attack. [8 marks]

(b) SQL injection is an example of a Web Application exploit.

i. Give a brief description (at most three sentences) of this attack and explain why it can succeed.

[4 marks]

ii. An online shopping site takes an email address as input to `$EMAIL` and constructs an SQL query as follows:

```
$query = "SELECT * FROM members WHERE email='$EMAIL'";
```

What would a malicious user enter as their `email` address in order to get the database to delete all entries from table `foo` (assuming the table exists)? (No need to explain the answer.)

[4 marks]

(c) While HTTP is a stateless protocol, sometimes Web Applications need to maintain state.

i. List 3 reasons why some Web Applications might need to store state information. [3 marks]

ii. Cookies are often used to store state information. Explain how the cookie mechanism works, and what policies are used to secure access to cookies. [6 marks]

iii. Session cookies are used to maintain state.

A. Explain how session cookies and session IDs are used by client and server to maintain state. [6 marks]

B. An attacker may try to steal or modify a session cookie.
Briefly describe 3 things that could be done with the cookie to defeat such an attack. [3 marks]

END