UNIVERSITY OF LONDON

BSc EXAMINATION 2023

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. State which of the following statements are **TRUE** and which are **FALSE**, making sure that in each case you provide a brief justification for your answer (no marks will be awarded for answers that are not justified).

   (a) The diagram of the Ware report (see Figure 1 on the next page) is no longer applicable to modern IT security. Justify your answer with an example. [3 marks]

   (b) Data stored in a process' memory is always accompanied by type information. [2 marks]

   (c) The TCP handshake prevents man-in-the-middle attacks. [2 marks]

   (d) DNS by itself provides strong integrity guarantees. [2 marks]

   (e) Assume that some script is running in a browser window under the origin `https://london.ac.uk`. If this script sends a request (e.g., an XMLHttpRequest) to the origin `https://royalholloway.ac.uk`, then the cookies for `london.ac.uk` will be included in that request. [2 marks]

   (f) Reflected cross-site scripting attacks are based on a vulnerability of the database system used by the web application. [2 marks]

   (g) Process gates are a technique to prevent reference monitors. [2 marks]

   (h) Unprivileged processes can modify the UNIX system clock. [2 marks]

   (i) UNIX user groups always have the same ID number as the user's UID. [2 marks]

   (j) SYN cookies can have the secure flag and are then not sent in plain. [2 marks]

   (k) MULTICS inspired fundamental concepts of modern operating system access control. [2 marks]

   (l) PCs in the 1980s came with strong security controls. [2 marks]

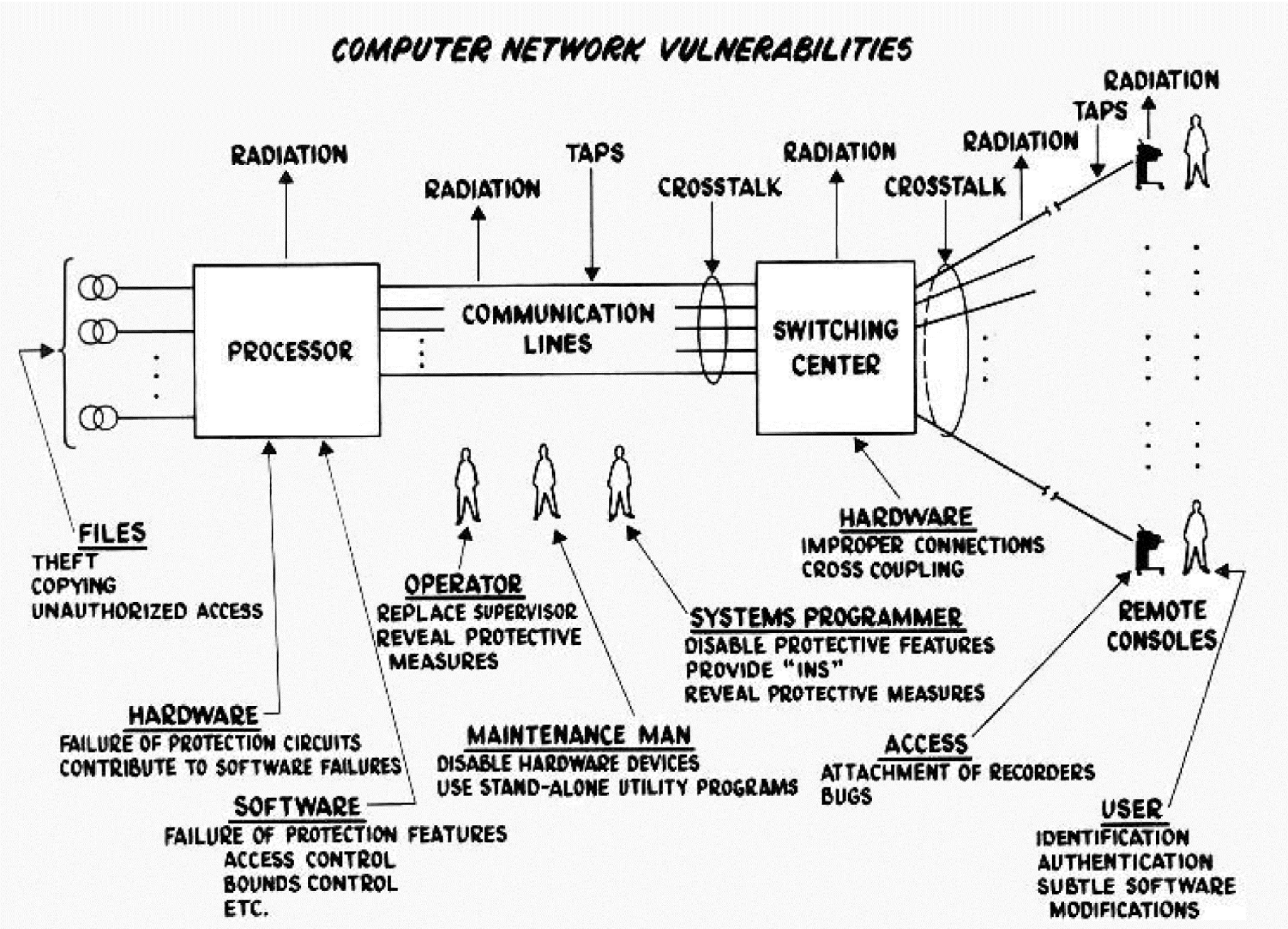

Figure 1: Computer Network Vulnerabilies (Ware Report, 1967.)

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? [3 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

This question concerns a Linux machine on which you are the administrator (with `sudo` rights). The system has 5 normal users `user1, user2, user3, user4, user5` (with their respective home directories in `/home`: `/home/user1`, and so on). In addition to the default user groups, there are 3 additional groups:

- `prime = {user2, user3, user5}`
- `odd = {user1, user3, user5}`
- `even = {user2, user4}`

(a) You have been asked to create a folder in the root directory called `IncidentsReports`. This folder should be owned by `user2` and `even` but only `user2` should allowed to delete other users' files; write access is to be granted to the group `prime`, no other users get any access. Write down the commands, in order, that you would execute to create a folder matching this description. [6 marks]

(b) Consider that the folder `/IncidentsReports` has the files `IR1, IR2, IR3, IR4`.

i. Give the Access Control List for read rights to the *files*. [4 marks]

ii. Give the Access Control List for the write rights to the *directory*. [2 marks]

(c) Consider another folder in the root directory called `ProjectLonghorn`. This directory is owned by `user2` and by the group `prime`. Both owner and group have full read, write and execute access. `user2` executes the following commands

```
ln /IncidentsReports/IR3 v512IR
touch v512update
echo "Delays to v512 due to incident." > v512update
```

Does this cause a security violation? Provide details of the cause and effect of any security violations. [8 marks]

(d) 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. [6 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. [5 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]

END