7 Security (mgk25)

(a) In a Linux shell session, you can see the following information:

```
$ ls -la
drwxr-xr-x 25 root root 4096 Jun  3 13:29 ..
-rwxr-xr-x  1 root root  4675 Jun  3 13:29 script.pl
```

Consider how you need to change the file access-control information shown above in order to achieve the following additional goals:

- Only members of the group staff who are not also members of the group interns can execute script.pl.
- When script.pl is called, it should be able to switch between using the access privileges of the caller and those of the user primary.
- All members of group staff should be able to read the contents of script.pl.

What would “ls -la” output after you have applied these changes? [6 marks]

(b) Sending a password over a network connection is vulnerable to replay attacks by eavesdroppers. Briefly describe three other forms of unilateral (or one-pass) authentication suitable for human keyboard entry that reduce that risk with the help of a hardware token, and name one advantage of each. [6 marks]

(c) The Windows NT operating-system family offers two variants of many API functions that receive a string: one for strings using ASCII (or one of its 8-bit “code page” extensions) and one for 16-bit Unicode strings. Linux and many Internet protocols instead use an ASCII-compatible encoding of Unicode called UTF-8.

(i) Briefly explain how UTF-8 is decoded. [4 marks]

(ii) What particular security risk can emerge when UTF-8 is used in a system along with another Unicode encoding, such as the 16-bit wide characters on Windows, and how can this be avoided? [4 marks]