2008 Paper 4 Question 7

Introduction to Security

(a) The following files are shown by an `ls -l` command on a typical Unix system:

```
-r-xr-sr-x  1 charlie acct      70483 2008-01-04 22:53 accounting
-r--rw----  1 alice   acct     139008 2008-05-13 14:53 accounts
-rwxr-xr-x  1 system  system   230482 1997-04-27 22:53 editor
-rw-r--r--  1 alice   users      7072 2008-06-01 22:53 cv.txt
-r--r-----  1 bob     gurus     19341 2008-06-03 13:29 exam
-r--r-----  1 alice   gurus      6316 2008-06-03 16:25 solutions
```

Unix users `alice` and `bob` are both members of only the group `users`, while `charlie` is a member of only the group `gurus`. Application `editor` allows users to read and write files of arbitrary name and change their permissions, whereas application `accounting` only allows users to append data records to the file `accounts`. Draw up an access control matrix with subjects {alice, bob, charlie} and objects {accounts, cv.txt, exam, solutions} that shows for each combination of subject and object whether the subject will, in principle, be able to read (R), (over)write (W), or at least append records (A) to the respective object. [9 marks]

(b) A C program uses the line

$$buf = (char *) malloc((n+7) >> 3);$$

in order to allocate an $\lceil \frac{n}{8} \rceil$-bytes long memory buffer, large enough to receive `n` bits of data, where `n` is an unsigned integer type.

(i) How could this line represent a security vulnerability? [2 marks]

(ii) Modify the expression that forms the argument of the `malloc()` call to avoid this vulnerability without changing its normal behaviour. [3 marks]

(c) Name *three* types of covert channels that could be used to circumvent a mandatory access control mechanism in an operating system that labels files with confidentiality levels and give a brief example for each. [6 marks]