Question 2
A networked server hosts a Kerberos Authentication Service and an Apache web-server that uses a MySQL back-end database server.

b) On discovery of the injection attack, a full application code review was ordered and another web-form was discovered that passes data to the following C program.

```
void main1(int argc, char* argv[]){
        char buff[6];
        strcpy(buffer,argv[0]);
        .....
}/*main1*/
```

Describe how a buffer-overflow attack on this application could enable an attacker to gain control of the host. (15 marks)

- Answered in Summer 2011

c) In light of the above attacks, it has been decided to replace the existing server host by a high-assurance system that enforces mandatory Multilevel security (MLS). Describe the (Bell LaPadula) access-rules for MLS and give a suitable compartmentalization policy for the server host that would provide better system protection. Discuss any limitations of this approach. (15 marks)

- Answered in Mac Exercises

Question 5
a) Describe the access-control mechanism that is used in unix, paying particular attention to the file system access controls. (15 marks)

- Answered in Summer 2011

b) An order processing system is implemented in terms of programs prop and appr, which are executed when proposing a new order and order approval, respectively. Both programs are permitted access to the order file. Clerk Clare is permitted to propose orders, which may be approved by Manager Mike. The data in the order file is periodically checked for entries that don't match the company's goods-received log.

i. Outline how security of the application system should be represented and interpreted in terms of the Clark-Wilson model. (7 marks)

ii. Sketch how the Unix protection mechanism can be used to support the Clark-Wilson model of this application. (8 marks)

c) Develop suitable Java security policy grant entries for the following requirements.

i. Any code signed by the public key simon may have read and write access to files under /usr/home/simon/. (5 marks)

ii. Any jar files or classes from source http://cs.ucc.ie may have read access to any file in the directory /usr/home/simon/cs. (5 marks)

iii. The principal simon, authenticated in Kerberos domain CSDOMAIN, may read and write files in /tmp/. (5 marks)