UNIVERSITY OF SOUTHAMPTON COMP6236W1

SEMESTER 1 EXAMINATIONS 2015/16

Software Engineering and Cyber Security

Duration: 2 hours

This paper contains 5 questions

Answer **BOTH** questions in **Section A** and **only ONE** question in **Section B.**

Section A carries 50% of the total marks for the exam paper.

Section B carries 50% of the total marks for the exam paper.

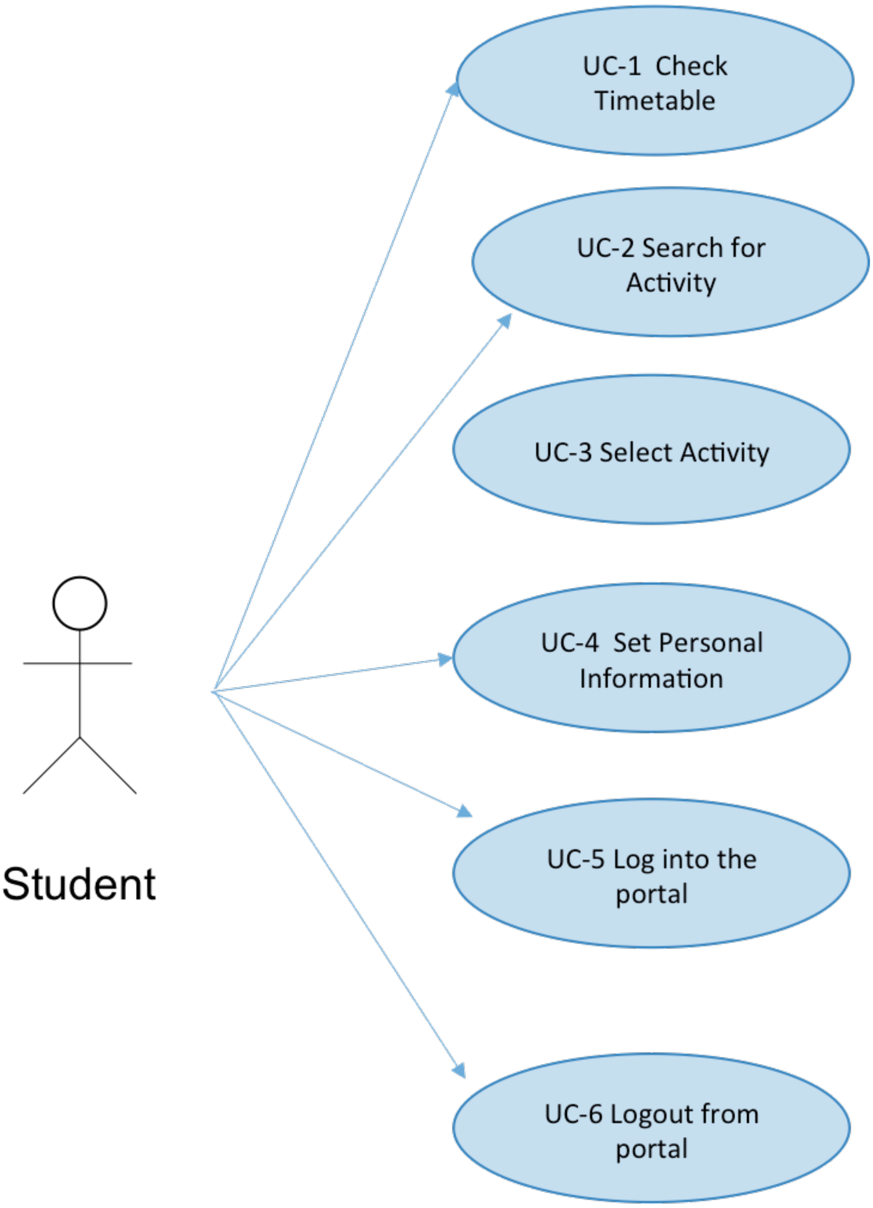
Only University approved calculators may be used.

A foreign language dictionary is permitted ONLY IF it is a paper version of a direct ‘Word to Word’ translation dictionary AND it contains no notes, additions or annotations.

SECTION A

Answer ALL questions

Question A1



The use case above represents a student portal application. It consists of six use cases described as follows:

Question continues on following page

UC-1 – **Check timetable**: First the user's appointments for the rest of the day are shown. Time, place and name of the appointment shall be shown in bold writing. From the calendar window, the user can also choose to see weekly and monthly overviews, which can be stepped forward and backward. By clicking into the weekly and monthly overviews, the user can also see the calendar for other dates than the current one.
UC-2 – **Search for activity**: The user can select between various types of activities from a menu, for instance courses, lectures, lab exercises, and other academic and social activities. Alternatively, the user can select an activity, which should be added to the calendar (UC-3).
UC-3 – **Select activity**: The user can select one of the activities displayed to be added to the calendar. If the activity demands registration, the system can automatically take care of this based on personal information already stored in the portal. If such personal information has not been entered, the system asks the user to enter it (UC-4).
UC-4 – Set personal information: This function begins with a window where the user may enter or edit personal information such as name, address, phone number and email address.
UC-5 – Log in to the portal: The user supplies their user name and password.
UC-6 – Log out from the portal: The user quits using the portal. If the user does not log out but is idle for 5 min, s/he is logged out by automatic time-out.

(a) For at least three of the use cases above identify a misuse case. Add the misuse cases to the model and link them to the use case.

[10 marks]

(b) For one of the misuse cases draw the corresponding attack tree.

[10 marks]

Question continues on following page

TURN OVER

(c) For each of the identified misuse cases, add to the model a security use case that mitigates the misuse case.

[13 marks]

Question A2

(a) Explain what Microsoft STRIDE is.

[13 marks]

(b) Explain what LINDDUN is.

[13 marks]

(c) Compare Microsoft STRIDE and LINDDUN. List the key difference(s) between the two.

[7 marks]

SECTION B

Answer *ONE* out of *THREE* questions

Question B1

```
#include <stdio.h>
#include <string.h>

int main(void)
{
    char buff[15];
    int pass = 0;

    printf("\n Enter the password : \n");
    gets(buff);

    if(strcmp(buff, "thegeekstuff"))
    {
        printf ("\n Wrong Password \n");
    }
    else
    {
        printf ("\n Correct Password \n");
        pass = 1;
    }

    if(pass)
    {
       /* Now Give root or admin rights to user*/
        printf ("\n Root privileges given to the user
          \n");
    }

    return 0;
}
```

Question continues on following page

TURN OVER

The C program above contains a vulnerability that can be exploited.

(a) Explain what the program does.

[5 marks]

(b) Explain the vulnerability.

[10 marks]

(c) Explain how the vulnerability can be exploited.

[10 marks]

(d) Provide an example of input to the program that allows exploitation of the vulnerability.

[8 marks]

Question B2

a) What is “*software penetration testing*”? Describe a modern approach to it.

[10 marks]

b) What tools are typically used in “*software penetration testing*”?

[10 marks]

c) What is “*risk-based security testing*”? In what ways it is similar to penetration testing, and how does it differ?

[13 marks]

Question B3

(a) Explain what model checking is. Contrast design and code verification listing their respective advantages and disadvantages. Illustrate your answer with a diagram, if relevant. [10 marks]

(b) Describe the two main approaches to model checking: "*enumerative"* and "*symbolic*." List and describe at least three existing model checking tools.

[10 marks]

(c) List and describe at least three applications of model checking to cyber security problems.

[13 marks]

END OF PAPER