MASENO UNIVERSITY

UNIVERSITY EXAMINATIONS 2016/2017

THIRD YEAR SECOND SEMESTER EXAMINATIONS FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

CITY CAMPUS

CIT 310: INFORMATION ASSURANCE AND SECURITY II

Date: 23rd June, 2017 Time: 5.30 - 8.30 pm

INSTRUCTIONS:

- Answer ALL question in SECTION A and any other TWO from SECTION B
- Write your registration number on all sheets of the answer book used.
- Use a NEW PAGE FOR EVERY QUESTION attempted, and indicate number on the space provided on the page of the answer sheet.
- Fasten together all loose answer sheets used.
- No mobile phones in the examination room.

ANSWER QUESTION 1 AND ANY OTHER TWO QUESTIONS

Question 1 [30 marks]

a) A software house incorporates a time-lock which causes their product to stop working if it is not supplied with a suitable password every 6 months. What risks are they running?

[4 marks]

b) A hospital de-identifies patient records by removing names and addresses, leaving only the patient's postcode and date of birth as an identifier. These records are then sold to researchers and drug companies. What risk is the hospital running? **[4 marks]**

c) Explain what covert channels are, and how they can limit the usefulness of multilevel secure systems.

[4 marks]

d) Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z.

i. Write a set of access control lists for this situation. Which list is associated with which file? **[4 marks]**

ii. Write a set of capability lists for this situation. What is each list associated with? **[5 marks]**

e) Describe three of the problems from which classical multilevel-secure systems suffer.

[9 marks]

Question 2 [20 marks]

a) Describe the Bell–LaPadula security policy model. **[6 marks]**

b) Discuss how one might implement a system enforcing the Bell–LaPadula model. **[6 marks]**

c) Explain what covert channels are, and how they can limit the usefulness of multilevel secure systems.

[4 marks]

d) You have been employed in a reputable data forensics firm and your first assignment is to lead a team of members assigned to carry out a forensic audit to the Kisumu

county offices. You have a limited time to carry out the exercise and thus time is of essence. Describe the steps you will use in order to accomplish the exercise.

[4 marks]

Question 3 [20 marks]

e) Describe the Clark–Wilson security policy model, and discuss how it might typically be applied. **[12 marks]**

f) It is suggested that, in order to control the spread of computer viruses, a company implement a Clark–Wilson policy in which the constrained data items are all the executable files on its computers. In what ways might this be inadequate and how, if at all, might these inadequacies be remedied? **[8 marks]**

Question 4 [20 marks]

a) What is meant by Mandatory Access Control? Give an example. **[5 marks]**

b) How might you use mandatory access control to protect the safety-critical systems in a car (engine control unit, ABS, stability control, etc.) from user programmable systems (telephone, entertainment, navigation, etc.)? **[5 marks]**

c) What problems would you anticipate in keeping the implementation clean as these systems evolve? **[5 marks]**

d) What architecture might you therefore propose a car maker adopt for its next generation networking? **[5 marks]**

Question 5 [20 marks]

a) Describe briefly security policy models that might be suitable for protecting

i. Medical records; **[4 marks]**

ii. Police intelligence data; **[4 marks]**

iii. School records. **[4 marks]**

f) The Children Act 2004 empowers the Government to establish child protection databases for Kenya which will, it is hoped, identify cases of child abuse at an early stage. These databases will be fed with medical and school records, police intelligence data, and social work assessments. Social workers, doctors, nurses, teachers and police officers will be able to query them. Sketch a possible security policy for such a database, and discuss the most likely implementation problems. **[8 marks]**