MASENO UNIVERSITY

UNIVERSITY EXAMINATIONS 2016/2017

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

MAIN CAMPUS

CIT 310: INFORMATION ASSURANCE AND SECURITY II

Date: 16th June, 2017 Time: 8.30 - 11.30 am

INSTRUCTIONS:

- Answer ALL questions in SECTION A and any other TWO from SECTION B
- 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.
- Mobile phones and PDAs are NOT allowed in the examination room.

ANSWER QUESTION ONE AND ANY OTHER TWO QUESTIONS

Question 1 [30 marks]

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

i. medical records; **[2 marks]**

ii. police intelligence data; **[2 marks]**

iii. School records. **[2 marks]**

b) 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]**

c) You are developing a multi-user computer game, and wish to make it harder for players to cheat. Discuss the possible benefits of using

i. encryption/authentication **[3 marks]**

ii. virus detection technology **[3 marks]**

iii. intrusion detection techniques **[2 marks]**

d) What might be the advantages and disadvantages of issuing players with a smartcard and reader? **[8 marks]**

QUESTION 2 [20 marks]

a) Windows implements static inheritance for the access-control lists of NTFS files and folders.

i. What does static inheritance mean here and how does it differ from dynamic inheritance? **[4 marks]**

ii. Five flag bits (ci,oi,np,io,I) in each NTFS access-control entry (ACE) manage how it is inherited. Briefly describe the purpose of each bit. **[5 marks]**

iii. User mike gives his folder project the following access-control list:

Project
AllowAccess mike: full-access (oi,ci)
AllowAccess alice: read-execute (ci,np)
AllowAccess bob: read-only (oi)

It contains one folder and two text files, none of which have any non-inherited access-control entries:

project\doc.txt
project\src
project\src\main.c

For each of these three objects, list all inherited access-control entries, showing in parentheses the inheritance-control flag bits that are set (using the same notation as above). **[5 marks]**

b) Describe the purpose and four typical functions of a ***root kit.*** **[6 marks]**

Question 3 [20 marks]

You are consulting for a large online services company which stores personal information on millions of customers. Your client's directors are alarmed by the Wikileaks saga and are concerned about damage to their company's reputation should a disaffected member of staff steal and publish personal information on a large number of customers.

Discuss the security policy options available to your client to minimise the damage that a member of staff could do. **[20 marks]**

Question 4 [20 marks]

a) Formally state the two rules of the Bell-LaPadula (BLP) security policy model and then re-state them informally in terms of a single rule about the direction of information flow. **[2 marks]**

b) Consider a distributed system in which A is a TOP SECRET process running on machine Alice and B is a CONFIDENTIAL object residing on machine Bob.

i. Explain and justify whether A is allowed to read and/or write from B according to the BLP policy. **[2 marks]**

ii. Discuss the claim made by some researchers that this scenario highlights a fundamental problem with the BLP policy. **[4 marks]**

c) Consider the following description of Brewer and Nash's Chinese Wall security policy model.

• *Simple rule*: Read or write access to object O_2 by subject S is granted if and only if, for all objects O_1 to which S has had access, we have: (class(company(o1)) ≠class(company(O_2)) or (company(O_1) =company(O_2)).

• ***-rule**: Write access to object O_2 by subject s is granted if and only if access is granted by the simple rule and there does not exist any unsanitized object O_1, readable by s, for which company(O_1) ≠company(2).

i. Explain the context and goal of the Chinese Wall security policy model. Then explain what each of the two rules is intended to enforce or prevent. **[4 marks]**

ii. Some researchers have claimed that the formal rules of Chinese Wall do not match the policy that Brewer and Nash intended to enforce, to the extent that the resulting policy is unusable in practice. Explain precisely why the policy would be unusable and give a clear proof of this claim. **[8 marks]**

Question 5 [20 marks]

a) Clearly explain the Clark-Wilson security policy model and what it tries to achieve, defining technical terms such as CDI, UDI, CW triples, IVP, TP and auditing. **[6 marks]**

b) Under security considerations

a. What is a master key system? What is its purpose? How can we turn a normal pin-tumbler lock into one supporting a master key? **[5 marks]**

b. Describe in detail the Blaze Privilege Escalation attack on master key systems. What resources does an attacker need and what can be achieved? Compare the effort required to that of a brute-force attack. **[5 marks]**

c) Discuss the security, privacy and economic aspects of the iPhone's "App Store" model, as opposed to the traditional desktop software model. **[4 marks]**