JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE IN COMPUTER SECURITY AND FORENSICS

4TH YEAR 1ST SEMESTER 2021/2022 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1405

COURSE TITLE: OPERATING SYSTEMS SECURITY

GROUP: CSF

DATE: EXAM SESSION:

TIME: 2 HRS

INSTRUCTIONS

Answer question **one** and any other **two** questions

QUESTION ONE 30 MARKS

a) How does the reference monitor interface ensure that all security sensitive operations are mediated correctly in Multics systems?
(4 marks)

b) What is *information flow in* secure operating systems? (6 marks)

c) Does the reference monitor interface mediate security-sensitive operations on all system resources?
(4 marks)

d) Identify the two information flow secrecy models. (4 marks)

e) What is a virtual machine? (4 marks)

f) Distinguish between multi- programming operating systems and single user operating systems. (2 marks)

g) Consider the access matrix shown in below . It defines the set of operations that the subjects S1, S2, and S3 can perform on objects O1 and O2. Note that some operations, such as append, getattr, and ioctl have to be mapped to their resultant information flows, write, read, and both, respectively. Draw the corresponding information flow graph . (6 marks)

Access Matrix

	O1	O2
S1	read append	read getattr
S2		read ioctl
S3	read write	append

QUESTION TWO 20 MARKS

a) How do we verify that the reference monitor interface provides complete mediation? (4 marks)

b) For information flow secrecy, we want to ensure that no matter which programs a user runs, she cannot leak information to an unauthorized subject. The classical problem is that the user may be coerced into running a program that contains malware that actively wants to leak her information.
For example, a *Trojan horse* is a type of malware that masquerades as a legitimate program, but contains a malicious component that tries to leak data to the attacker.

1. Explain why the access control models of UNIX and Windows cannot prevent such an attack. (6 marks)

2. Explain how security policy models used in mandatory protection systems aim to solve these problems. (6 marks)

c) Identify any two information flow integrity models. (4 marks)

QUESTION THREE 20 MARKS

a) How does the system protect the reference monitor, including its protection system, from modification? (4 marks)

b) The secure operating systems that followed the Multics system focused on the key limitations of Multics: performance and verifiability. Discuss how the idea of a *security kernel* was used to overcome these two limitations. (6 marks)

c) How does the reference monitor interface in Linux ensure that all security sensitive operations are mediated without creating security problems, such as TOCTTOU? (6 marks)

d) Does the system's protection system protect the trusted computing base programs? (4 marks)

QUESTION FOUR 20 MARKS

a) What is basis for the correctness of the system's trusted computing base? (4 marks)

b) Does the protection system enforce the system's security goals? (8 marks)

c) A problem in building a new, secure operating system is that existing applications may not run on the new system. Operating systems define an application programmer interface (API) consisting of a set of system calls it supports. New operating systems often define new APIs, resulting in the need to port applications and/or write new applications. This has been a major problem in gaining acceptance for secure operating systems based on emerging kernels, such as Trusted Mach and Flask , and the reason for so much focus on securing commercial systems.
Discuss how virtual machine can be used as alternative to encounter the above problem. (8 marks)

QUESTION FIVE 20 MARKS

a) Using a diagram, discuss how kernel provides security of jobs being executed in the main memory in a multiprogramming environment. (8 marks)

b) Define the following: (12 marks)

1) Virus
2) Worm
3) Trojan horse
4) Trapdoor
5) Logic bomb
6) Rootkit