JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY UNDERGRADUATE EXAMINATIONS

1ST YEAR 1ST SEMESTER 2016/2017 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3113

COURSE TITLE: PC SECURITY AND PRIVACY

EXAM VENUE:	**STREAM: BIS**
DATE:	**EXAM SESSION:**
TIME: 2.00 HOURS	

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE [30 MARKS]

a) Differentiate using examples between a flaw, a fault and a failure in computer security (6 marks)

b) Why is it so critical to secure our computers (3 marks)

c) You **control** a **vulnerability** to prevent an **attack** and block a **threat**. Explain the statement (6 marks)

d) List five general methods of defenses used to secure our computers (5 marks)

e) What do you understand by the terms least privileged and defense in-depth? (2 marks)

f) What's the difference between an intrusion detection and intrusion prevention system (2marks)

g) Underscore the rationale of the following thoughts in baking security

i. **Principle of Easiest Penetration** (3 marks)

ii. **Principle of Adequate Protection** (3 marks)

QUESTION TWO [20 MARKS]

a) Briefly explain how the following malicious codes manifest themselves (6 marks)

i. Back doors
ii. Salami attacks
iii. Rootkits
iv. Interface illusions
v. Keystroke logging
vi. Man-in-the-middle attacks

b) The Krigler report identified that one way of sanitizing our electoral process was to automate the authentication step. What are some of the administrative and physical control measures would you advice the IEBC to put in place to secure this vital process (8 marks)

c) Under what circumstances do TOCTOU errors occur (6 Marks)

QUESTION THREE [20 MARKS]

a) *You're surfing the Web and you see a button on the Web site saying, "Click here to see the beneficiaries of the Kshs. 200 billion scandal." And you click on the Web site and then this window comes up saying, "Warning: this is an untrusted Java applet. It might damage your system. Do you want to continue? Yes/No."* . Will you go ahead reveal the identity of the looters or you will take the precaution. What kind of manifestation is this condition and how do you prevent it from happening (8 marks)

b) Describe at least six types of vulnerabilities, corresponding threat can exploit within a computer. (12 marks)

QUESTION FOUR [20 MARKS]

a. At which stage should security controls be considered within the software development lifecycle? (2 marks)

b. Some key concepts have to be adopted and incorporated in the design of programs so that they're less likely to have security flaws? Discuss these concepts listed below
   i. Modularity
   ii. Encapsulation
   iii. Information hiding
   iv. Mutual suspicion
   v. Confinement (10 marks)

c. Outline the four classes of authentication classes (4 marks)

d. A corporation is considering a best authentication method for access control within their computers, which method has the best authentication strength explain you answer? (4 marks)

QUESTION FIVE [20 MARKS]

a. Briefly explain five best practices for limiting access to computer systems which can help secure systems and their data. (10 marks)

b. Passwords are one of the mechanisms of computer systems access control it is advised that they shouldn’t be the sole mechanism employed. Give reasons to justify the advice (7 marks)

c. For a user to access a secure computer, explain the conditions that should be met? (3 marks)