23

(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2021/2022 ACADEMIC YEAR

SPECIAL/SUPPLIMENTARY EXAMINATIONS
YEAR three SEMESTER two

FOR THE DEGREE IN
(Computer science)

COURSE CODE : **CSC 321**

COURSE TITLE : **COMPUTER SYSTEM SECURTY**

DATE: 22/11/22 **TIME: 11.00 A.M – 01.00 P.M**

INSTRUCTIONS TO CANDIDATES

ANSWER **QUESTIONS ONE** AND **ANY OTHER TWO**.

QUESTION ONE (COMPULSORY) [30 MARKS]

a) Briefly explain the following terms, and for each give one example of a technique that implements it:

i) Secure commitment (2 marks)

ii) Mandatory access control policy (2 marks)

iii) Perfect secrecy (2 marks)

iv) Message authentication code (2 marks)

b) You have been hired by kRONA Ltd to secure the web interface to a legacy system. This system is complex, its source code has been lost, and you have been asked to write input validation procedures, that will identify values which are suspected to be malicious, and flag them for later manual inspection. For each of these input fields, explain one validation procedure you could perform, and justify why it is appropriate:

i) The name of a file in a particular directory on the server (3 marks)

ii) A parameter that you believe will be used on a command-line (3 marks)

iii) A string that will be loaded into memory and parsed (3 marks)

c) For one of the validation procedures you gave in part (b), discuss how a sophisticated attacker could circumvent detection. (3 marks)

d) Identify and discuss the fundamental goals of system security (10 marks]

QUESTION TWO [20 MARKS]

a) Anti-virus software is commonly used to detect and prevent potential harmful attacks on a computer. With respect to the detection element of an anti-virus program, how does the antivirus program work and how do virus writers try to exploit the way these programs typically work in order to avoid detection? (3 marks)

b) Viruses are often viewed as a combination of three elements: propagation, payload and activation. Two methods to propagate a virus are either as a Trojan or a 'worm'. Describe each of these two methods of propagation and assess which is able to spread fastest and why. (6 marks)

c) A colleague has recommended switching your company's account verification process to a pure biometric approach. You are not convinced this is an ideal method.

i) What is biometric authentication and which authentication factor does it address? (2 marks)

ii) Discuss the problems of biometric authentication and why it requires a difficult balancing act. (5 marks)

iii) Ideally, what form of authentication process should you use for:

- A public discussion forum that enables moderated comments to be added to published articles

- A web base online banking system

Justify each of your answers and describe the advantages and disadvantages of your chosen approaches. (4 marks)

QUESTION THREE [20MARKS]

a) You have been asked by a company to provide a security review for code that will control a new web based shopping site.

   i) One test that you have decided to perform is to check boundary conditions. What is meant by checking boundary conditions with respect to code testing and what sort of coding failures does it try to identify? (3 marks)

   ii) Describe three further security related tests that you would undertake to ensure that the code is fit for the purpose. For each test, provide an example of the sort of actual test you would make and how it would pick up an error if it was present. (5 marks)

   iii) As part of your tests, you have discovered that the company has switched off client side debugging output from PHP scripts. This is making it difficult for you to understand what is happening when faults are found with your tests. You have asked the system administrators to turn the debugging output back on but they are reluctant to do this. Why do you think they might be reluctant to turn on client side PHP debugging output, are their objections valid and what alternative approach could you take if they refuse to turn it on? (5 marks)

b) As part of your security review, you have found a form on a user interface that asks a user to enter their name and date of birth. This form appeared to work normally until you provided a name exceeding 16 characters in length, at which point the date of birth recorded in the internal database did not match the one you entered and in many cases, the recorded date of birth was invalid. Rather oddly, the date of birth changed depending on which long name you typed in.

   i) What is the common name given to the error that you have found and what type of coding fault produces this error? (3 marks)

   ii) With the aid of a diagram and pseudo-code, describe how the date of birth could have become corrupted and explain how a hacker could use this fault to inject code into a program (4 marks)

QUESTION FOUR [20 MARKS]

a) Make the following statements correct by changing one word or number. (Negating the sentence is not sufficient)

i) The Advanced Encryption Standard defines a 16-round Feistel cipher (1 mark)

ii) Files encrypted with Cipher Block Chaining start with a zero initial vector (1 mark)

iii) Each user on a Unix system is identified by a unique prime number (1 mark)

iv) The "read' bits associated with a Unix directory affect whether the files in its subdirectory "foo" can be accessed. (1 mark)

v) The "real user ID" associated with a Unix process determines its access rights. (1 mark)

b) Name five examples of actions for which a Unix application will need to be invoked with root privileges. (5 marks)

c) Explain the attack on Double DES that motivates the use of Triple DES (6 marks)

d) Under which conditions is the Vigin'ere cipher unconditionally secure? (4 marks)

20

QUESTION FIVE [20 MARKS]

a) Your colleague wants to use a secure one-way hash function h in order to store h(password) as pass-verification information in a user database for which confidentiality might become compromised. For h, she suggests using an existing

CBC-MAC routine based on AES with all bits of the initial vector and the 128-bit AES key set to zero. Is this construct a suitable one-way hash function for this

application? Explain why (8 marks)

b) Explain how, and under which circumstances, overlong UTF-8 sequences could be used to bypass restrictions regarding which files an HTTP server serves. (8 marks)

c) Name four techniques that can be used to make buffer-overflow attacks more difficult.

(4 marks)