JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

UNIVERSITY EXAMINATION 2012/2013

1ST YEAR 1ST SEMESTER EXAMINATION FOR THE DEGREE OF MSC IN IT SECURITY AND AUDIT

KISUMU LEARNING CENTRE

COURSE CODE: IIT 5112

TITLE: Advanced Information Systems Security

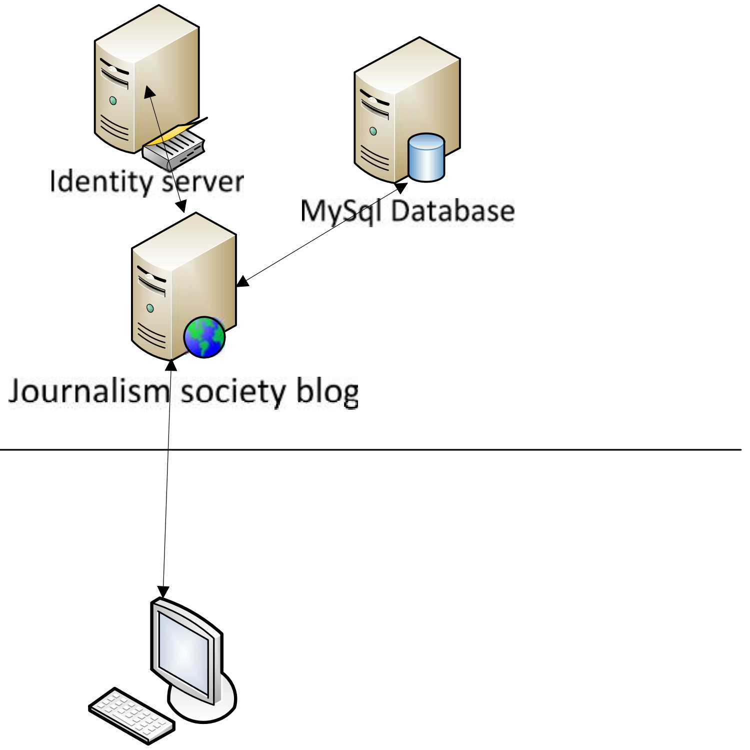
DATE: 15/4/2013 **TIME: 9.00-12.00 NOON**

DURATION: 3 HOURS

INSTRUCTIONS

1. **This paper contains FIVE (5) questions**
2. **Answer question 1 (Compulsory) and ANY other 2 Questions**
3. **Write all answers in the booklet provided**

Section-A (Compulsory)



i) Given the diagram above, what core areas of security guarantees would you consider? Give a brief explanation for each (4mks).

ii) Explain what security policy and security mechanisms are (2mks).

iii) On the assumption that you own and administer the topology above:-

  a. Name three (3) categories of potential threats that you would consider. Give a brief explanation (3mks).

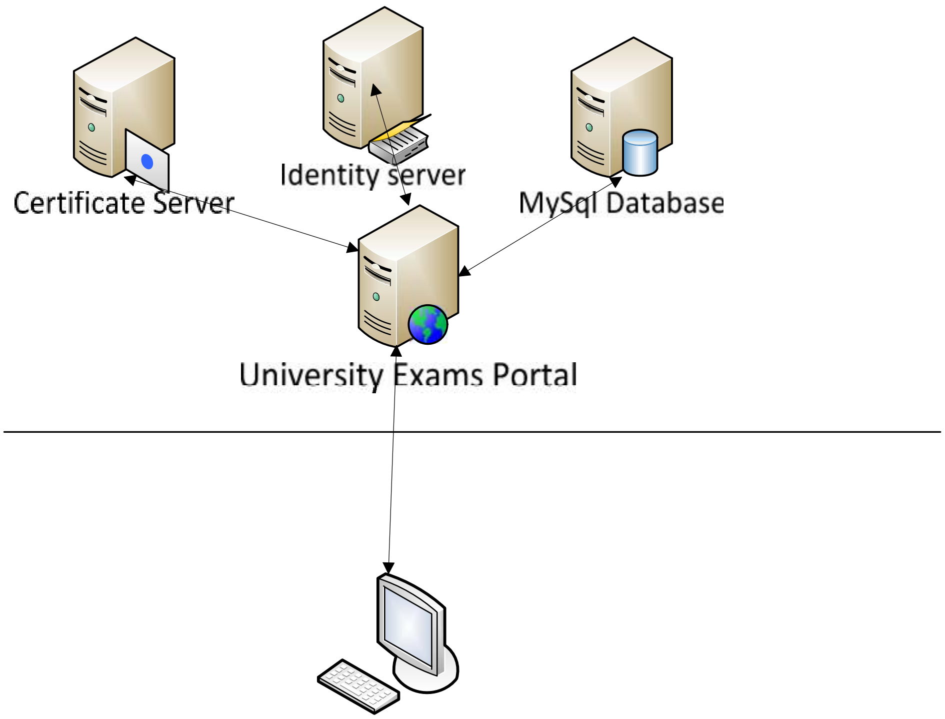
  b. Name four (4) security policies that you would put in place (4mks).

  c. Name four (4) security mechanisms that you would implement with respect to (b) above (4mks).

  d. Mention three (3) difficulties in implementing security policies in (b). (3mks)

Section-B (Answer any two questions)

<u>Question1. 20marks</u>



What is a Threat model? (2mks)

i) Using STRIDE(Spoofing identity, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges):-
   a. Identify potential threats in the diagram above, (8mks)
   b. Severity of the threats (Sev1 – Sev4 with Sev1 being the most severe and Sev4 being the least severe) (4mks)
   c. Possible mitigations you would recommend for each of the threats. (6mks)

<u>Question2 20marks.</u>

i) Mention and explain four (4) issues that affect security policies and mechanisms in an organization (4mks)
ii) Mention and explain four (4) organizational problems that a security manager is likely to encounter (4mks).
iii) Mention and explain four (4) people problems in as far as I.T security within an organization is concerned (4mks).
iv) Mention and explain four (4) broad categories of threats (4mks)

v) Spoofing/Masquerading falls under what categories of threats? Explain (2mks)

vi) Mention and explain two (2) types of integrity (2mks).

__Question3. 20marks__

i) What properties should a “secure” security model enjoy? Explain (4mks).

ii) What is:-

a. Discretionary Access Control (DAC) (1mk)

b. Mandatory Access Control (MAC) (1mk)

c. Role-based Access Control (RBAC) (1mk)

iii) Mention and explain the three (3) approaches for implementing access control in a practical way (3mks).

iv) Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it.

a. Create the corresponding access control matrix (5mks)

b. Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix (5mks).

__Question4.20marks__

i) Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.

a. The file access control mechanisms of the UNIX operating system (2mks)

b. A system in which no memorandum can be distributed without the author's consent (2mks)

c. A military facility in which only generals can enter a particular room (2mks)

d. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them (2mks)

ii) Mention four (4) and give an example (for each) of assumptions that are required to trust a security mechanism (8mks).

iii) Classify each of the following as violation of confidentiality, of integrity, of availability or a combination thereof

a. Carol changes the amount of Angelo’s check from 500 to 5000 (1mk).

b. Paul crashes Linda’s system (1mk)

c. John copies Mary’s homework (1mk)

d. Gina forges Roger’s signature on a deed (1mk).