JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SECURITY & FORENSIC

3rd YEAR 1st SEMESTER 2022/2023 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: **ICB 1309**

COURSE TITLE: **PROTOCOLS & SYSTEM FOR INTERNET AND WEB SECURITY**

EXAM VENUE: **STREAM: BSC COMPUTER SECURITY & FORENSIC**

DATE: **EXAM SESSION:**

TIME: **2.00 HOURS 85 students**

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 MKS)

a) Describe the following concepts as used in security

i) Impersonation (2 mks)

ii) Non-repudiation (2 mks)

iii) Network security policy (2 mks)

b) Discuss the various pieces of information that may be extracted from the packet header by the packet-filtering router that may then influence the decision whether the packet will pass through or be discarded. (6 mks)

c) Tunneling is used to carry traffic of one protocol over a network that does not support that protocol directly. For example, NetBIOS or IPX can be encapsulated in IP to carry it over a TCP/IP WAN link.

i) Explain requirements for tunneling (3 mks)

ii) Describe other rationale for traffic tunneling in conventional WAN links. (3 mks)

d) SSL provides an alternative to the standard TCP/IP socket API that has security implemented within it. Therefore, in theory, it is possible to run any TCP/IP application in a secure way without changing the application.

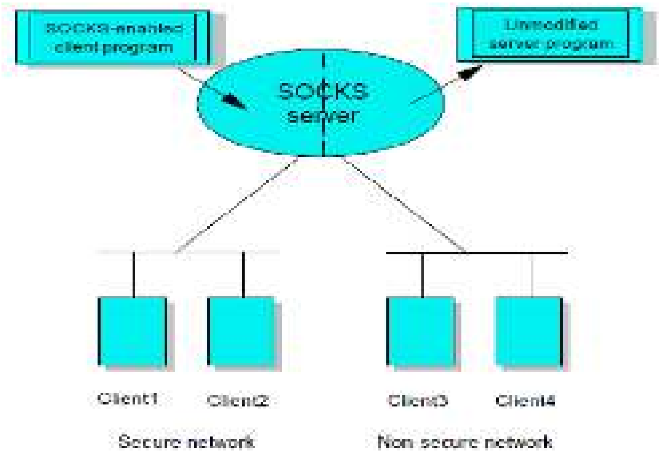
i) Discuss the TWO layers of SSL. (4 mks)

ii) Explain how an SSL session is initiated (4 mks)

e) Briefly describe the security offered by the Secure Multipurpose Internet Mail Extension (S-MIME). (4 mks)

QUESTION TWO (20 MKS)

The diagram below depicts a certain network security component. Study it carefully and use to answer the questions that follow.



a) With reason, identify the device depicted above. (4 mks)

b) Discuss the dimensions that distinguish this device from the application-level gateway

(8 mks)

c) Describe the features that you may attribute to non-secure network above. (8 mks)

QUESTION THREE (20 MKS)

a) Using relevant examples, compare and contrast IDS and IPS (8 mks)

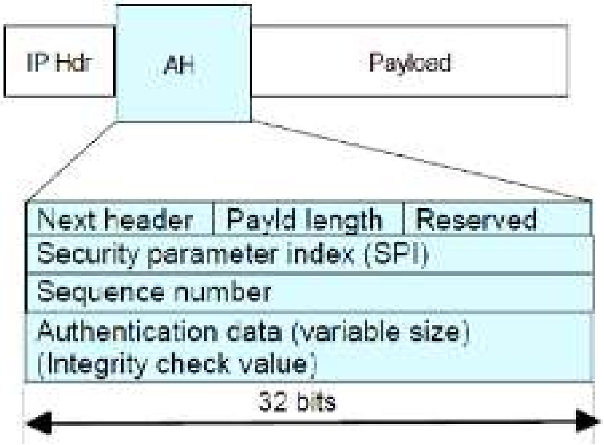
b) Justify the implementation of the following security solutions in university computerized systems and networks

i) Host based Intrusion Detection Systems (6 mks)

ii) Network based Intrusion Detection Systems (6 mks)

QUESTION FOUR (20 MKS)

The diagram below depicts a typical Authentication Header (AH). Study it carefully and use it to answer the questions that follow.



a) Explain the services provided by this IPSec component. (3 mks)

b) Describe the roles of the most critical fields in this AH architecture. (12 mks)

c) Identify and explain the two modes of using this IPSec component. (5 mks)

QUESTION FIVE (20 MKS)

The most commonly used aspect of PGP is the signing and encryption of email or files. Signing a document is a way of verifying the integrity of the original work.

i) Describe how email signing and verification is achieved using PGP. (6 mks)

ii) Discuss other services that a network administrator may want to attain through the implementation of PGP. (10 mks)

iii) Explain other algorithms that may be deployed for email signing. (4 mks)