



The University of Fiji

School of Science and Technology

Department of Computer Science/ Information Technology



ITC403

Network Security

Semester II, 2014

FINAL EXAMINATION QUESTION PAPER

Time Allowed: 3 Hours [10 Minutes Extra Allowed For Reading the Paper]
Weighting: 50%
Total Marks: 100 marks.

Section A - Open-Ended Questions

<i>Symmetric Encryption & Message Confidentiality</i>	8
<i>Public Key Cryptography and Message</i>	8
<i>Key Distribution and User Authentication</i>	10
<i>Transport Level Security</i>	8
<i>Wireless Network Security</i>	10
<i>Electronic Mail Security</i>	7
<i>IP Security</i>	7
<i>Intruders</i>	7
<i>Malicious Software</i>	8
<i>Firewalls</i>	7

Section B – Long Answer

Total	100 marks
-------	-----------

Instructions

- There are 4 pages in this exam paper.
- All questions are compulsory.
- Write all your answers in the Answer Book provided.
- FX-82 calculator is allowed.
- Show your answers clearly in each question to gain maximum marks.
- You may ask for extra sheets from the supervisors if the need arises.
- Do not forget to write your name and ID number on all the extra sheet(s) attached.

Section A - Open-Ended Questions [10 marks]

Symmetric Encryption & Message Confidentiality [10 marks]

1. What are the essential ingredients of a symmetric cipher? [2 marks]
2. What is the difference between a block cipher and a stream cipher? [2 marks]
3. What are the two general approaches to attacking a cipher? [2 marks]
4. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? [2 marks]

Public Key Cryptography and Message Authentication [10 marks]

5. List three approaches to message authentication. [1.5 marks]
6. In the context of a hash function, what is a compression function? [2 marks]
7. What are the principal ingredients of a public-key cryptosystem? [2.5 marks]
8. What is the difference between a private key and a secret key? [2 marks]

Key Distribution and User Authentication [10 marks]

9. List ways in which secret keys can be distributed to two communicating parties. [4 marks]
10. In the context of Kerberos, what is a realm? [2 marks]
11. What are two different uses of public-key cryptography related to key distribution? [2 marks]
12. What is the purpose of the X.509 standard? [2 marks]

Transport Level Security [7 marks]

13. What steps are involved in the SSL Record Protocol transmission? [2 marks]
14. List and briefly explain the SSH protocols. [3 marks]

15. What are the advantages of each of the three approaches (Network level, Transport level, and Application level) shown in Figure 1? [3 marks]

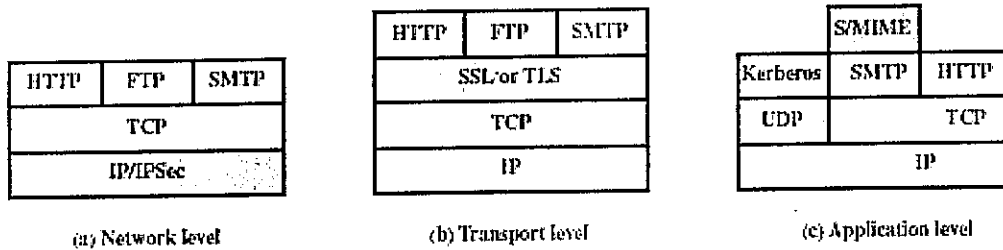


Figure 1: Relative Location of Security Facilities in the TCP/IP Protocol Stack

Wireless Network Security [10 marks]

16. List and briefly define three IEEE 802.11 services. [3 marks]
17. What is the difference between TKIP and CCMP? [2 marks]
18. What is the difference between an HTML filter and a WAP proxy? [2 marks]
19. Briefly explain three keys used in WTLS. [3 marks]

Electronic Mail Security [7 marks]

20. What are the five principal services provided by PGP? [2.5 marks]
21. What is the utility of a detached signature? [2 marks]
22. Why is R64 conversion useful for an e-mail application? [2.5 marks]

Chap 8 – IP Security [7 marks]

23. What services are provided by IPsec? [3 marks]
24. What is the difference between transport mode and tunnel mode? [2 marks]
25. What is a replay attack? [2 marks]

Chap 9 – Intruders [7 marks]

26. What are three benefits that can be provided by an intrusion detection system? [3 marks]
27. List and briefly define four techniques used to avoid guessable passwords. [4 marks]

Malicious Software [8 marks]

28. What is the role of compression in the operation of a virus? [2 mark]
29. What is a digital immune system? [3 marks]
30. Describe three worm countermeasures. [3 marks]

Firewalls [7 marks]

31. State three design goals for a firewall. [3 marks]
32. State two weaknesses of a packet filtering firewall? [2 marks]
33. Why is it useful to have host-based firewalls? [2 marks]

Section B – Long Answer Question [20 marks]

34. In this section, you have to write a program using programming language of your choice (preferably C++, Java, C# or Visual Basic) that tests and advises the user in real time the security strength of a login password as it is being entered.

Marks are allocated as follows:

- Declare all variables [2 marks]
- Data Input [2 marks]
- Process Algorithm [14 marks]
- Output Section [2 marks]

THE END