Name……..….ID……..……..Section…….……Seat No……..….

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination: Semester 2/2007

Course Title : ITS 413 – Internet Technologies and Applications

Instructor : Dr Steven Gordon

Date/Time : Thursday 10 January 2008, 13:30 – 16:30

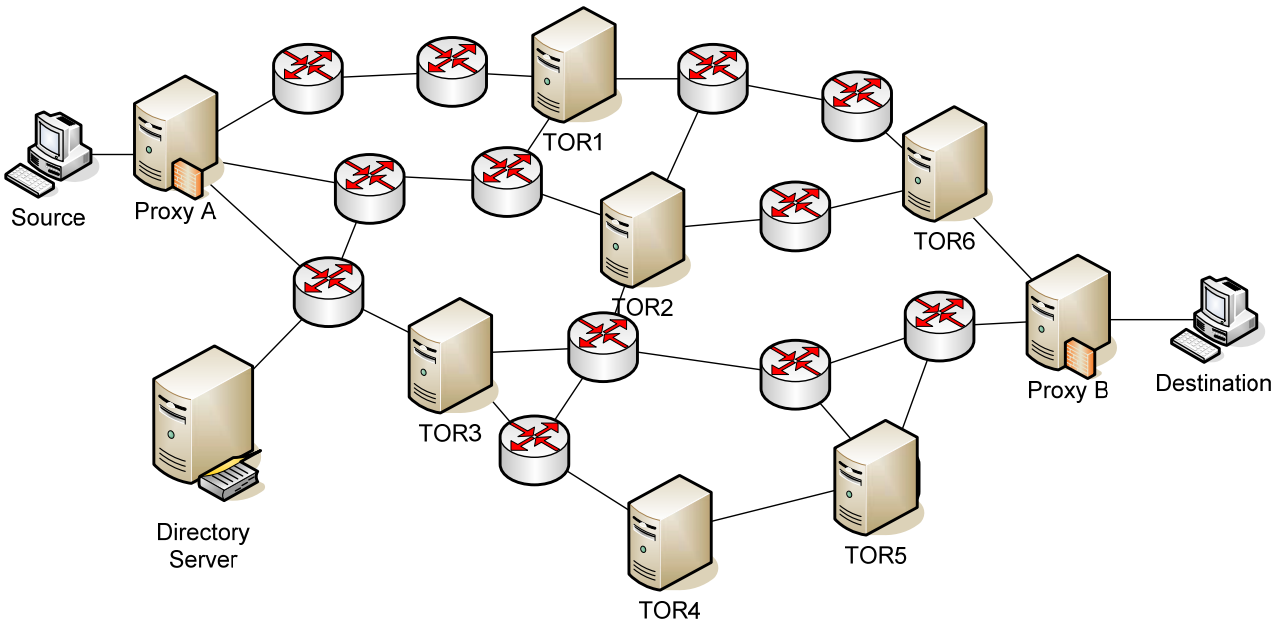
Instructions:

- This examination paper has 17 pages (including this page).
- Condition of Examination
  Closed book (No dictionary, **Non-programmable calculator allowed**)
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.
- The space on the back of each page can be used if necessary.

General Questions [100 marks]

Question 1 [13 marks]

The following diagram shows a TOR network.



a) What is the purpose of the Directory Server? [2 marks]

Assume Proxy A selects a path to Proxy B via TOR3, TOR4 and then TOR5.

b) After connection setup is complete, what keys do the following nodes have [2.5 marks]:
   i. Proxy A
   ii. TOR3
   iii. TOR4
   iv. TOR5
   v. Proxy B

c) In what order is a packet from Source to Destination encrypted. [2.5 marks]

d) Explain how the encryption order in part (c) provides anonymity in TOR. [3 marks]

e) Explain why using IPsec in tunneling mode (e.g. between proxy A and proxy B) does not provide similar level of anonymity as TOR. [3 marks]

Question 2 [12 marks]

Describe the following four methods of data delivery/routing, and for each method give an example application where the method would be beneficial (and explain why it is beneficial).

a) Unicast [3 marks]

b) Broadcast [3 marks]

c) Multicast [3 marks]

d) Anycast [3 marks]

Question 3 [14 marks]

a) Using the lines below, draw a diagram that illustrates the normal operation of IEEE 802.11 DCF in Basic Access mode when one station (A) transmits to another (B). Make sure you *clearly* label each component. [5 marks]

A _____

B _____

b) Explain a reason why the random backoff is used in DCF. [1 mark]

c) Explain what we mean by a "collision" in DCF. [1 mark]

d) Why do we want to avoid collisions in DCF? [1 mark]

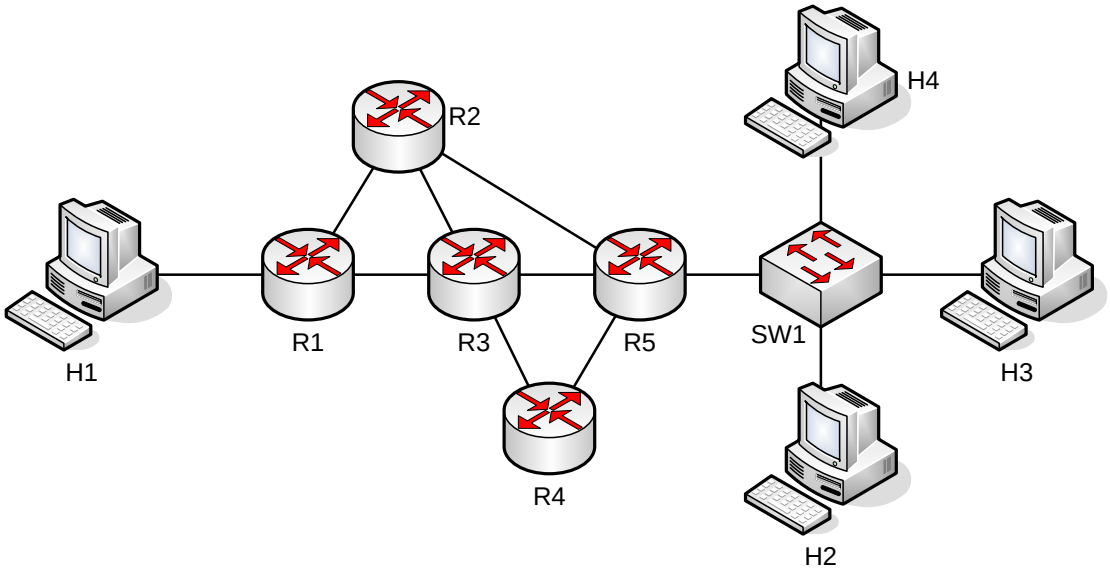
e) Explain two ways in which a collision can occur in DCF. [2 marks]

f) Describe the hidden terminal problem in wireless LANs, including how the presence of hidden terminals can significantly reduce throughput. [2 marks]

g) Explain how RTS/CTS can reduce the impact of hidden terminals [2 marks]

Question 4 [16 marks]

The figure below shows an internet with several Hosts, Routers and a Switch.



Below is the structure of the packet that host H1 has to send:

IP	TCP	Data

a) If using IPsec in Transport Mode to provide confidentiality and authentication between H1 and H3, answer the following:

   i. What type of IPsec must be used? [1 mark] (circle one answer)

      ESP or AH

   ii. Can an attacker at an intermediate node (e.g. R3) determine the application being used between H1 and H3? (Explain your answer) [2 marks]

   iii. Can an attacker at an intermediate node (e.g. R3) identify that H1 and H3 are communicating with each other? (Explain your answer) [2 marks]

b) If using IPsec in Tunneling Mode to provide confidentiality and authentication between H1 and any of hosts H2, H3, H4, answer the following:

i. What type of IPsec must be used? [1 mark] (circle one answer)

ESP or AH

ii. What are *two* suitable options for the tunnel end points? [2 marks]

iii. Can an attacker at an intermediate node (e.g. R3) determine the application being used between H1 and H3? (Explain your answer) [2 marks]

iv. Can an attacker at an intermediate node (e.g. R3) identify that H1 and H3 are communicating with each other? (Explain your answer) [2 marks]

c) Explain an *advantage* of using IPsec in Transport Mode instead of Tunneling Mode in this network. [2 marks]

d) Explain a *disadvantage* of using IPsec in Transport Mode instead of Tunneling Mode in this network. [2 marks]

Question 5 [18 marks]

a) Mobility in the Internet involves an IP host moving from one IP network to another IP network. Before Mobile IP was developed, explain the two options for handling IP mobility, and for each option, explain the disadvantage of the option. [4 marks]

b) Draw an example network that illustrate the components of Mobile IP. The network should include at least 1 foreign network, as well as a correspondent node. Make sure you clearly label the nodes in the network. [4 marks]

c) A Mobile IP host is turned on in a foreign network. Explain two methods for the host to discover it is in a Mobile IP foreign network? [3 marks]

d) Draw a diagram to illustrate the steps for a Mobile IP host to register once it discovers it is in a Mobile IP foreign network. Make sure you clearly label the nodes involved and the types of messages sent [3 marks]

e) If a correspondent node sends a packet to a Mobile IP host in a foreign network, then draw a diagram that illustrates the path of the message. [2 marks]

f) Explain when and why tunneling is used in Mobile IP. [2 marks]

Question 6 [9 marks]

NEMO supports network mobility as opposed to host mobility supported by Mobile IP. However, Mobile IP could be used to provide the same service as NEMO.

a) Explain how Mobile IP could be used to support network mobility. [2 marks]

b) Explain two advantages of using NEMO (as opposed to Mobile IP) for network mobility. [4 marks]

c) NEMO uses tunneling in both directions of data transfer (CN to MN and MN to CN), as opposed to Mobile IP. Explain why tunneling is needed when transferring data from Mobile Node to Correspondent Node. [3 marks]

Question 7 [8 marks]

Two key characteristics of Mobile Ad Hoc Networks are *infrastructure-less* and *dynamic topology*. Explain what each means, and for each characteristic describe an advantage and disadvantage. (For example, the advantage should indicate why this characteristic is beneficial in MANETs, and the disadvantage should indicate how this characteristic makes tasks difficult in MANETs).

Infrastructure-less

Dynamic Topology

Question 8 [10 marks]

a) Describe the difference between an active attack and a passive attack in network security. [2 marks]

b) Data confidentiality is one security service. List and explain 3 *other* security services [3 marks]

c) In providing data confidentiality, explain the keys used in the following encryption methods (your explanation should include: what keys are used, who's keys are they, who has access to the keys, and any other characteristics of the keys):

i. Symmetric key encryption [2 marks]

ii. Public key encryption [3 marks]