TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS – 2014

TRIMESTER 2

NWEN 243

Network Applications

Time allowed: THREE HOURS

Instructions: Closed Book

Answer all questions

All answers

There are 6 questions, each question is worth 30 marks.

All questions are to be answered directly in this booklet. No separate answer sheets will be provided.

Question 1: Cryptography and Security Layers
Question 2: Physical and Datalink Layers
Question 3: Network/Routing/IP Layer
Question 4: Transport Layer
Question 5: HTTP/Email/FTP/DNS
Question 6: XML/Web Service/Android Application Development/Media Streaming

Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this examination.

Paper foreign language dictionaries are allowed.

No other materials are permitted.

THIS PAGE IS INTENTIONALLY LEFT BLANK FOR WORKING

Question 1: Cryptography and Security [30 Marks]

a) [2 Marks] State Kerckhoffs's Principle.

"All algorithms must be public; only the keys are secret"

b) [4 Marks] Is a KDC trusted or trustworthy? Justify your answer.

A KDC is trusted, but not guaranteed to be trustworthy.

As it generates the session key, it can potentially intercept the communications without the knowledge of either party. Therefore while it needs to be trusted, we cannot prove it is trustworthy.

c) Briefly define the following security threats:

i. [2 Mark] Snooping

(passive) wiretapping

ii. [2 Mark] Spoofing

Impersonation with intent to deceive

iii. [2 Mark] Repudiation of Origin

A false denial that an entity sent something

iv. [2 Mark] Denial of Service

A long term inhibition of a service

d) [4 Marks] What are homophones and why were they used?

Each of the plaintext vowels has several possible equivalents. This attempts to 'even out' all the vowel frequencies in the cypher text to counter frequency analysis.

e) [4 Marks] What is a trapdoor function and why is it essential in modern cryptographic algorithms?

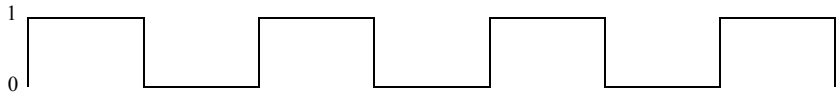
The result of a trapdoor function does not assist in recovering the original. This is why (for example) with digital signatures - we must repeat the hash, rather than reversing the hash (which is not possible). This makes the search space very large and essentially non-tractable. Similar examples from RSA and DHM.

f) [8 Marks] Outline DHM key exchange, either algorithmically or by using an analogy.

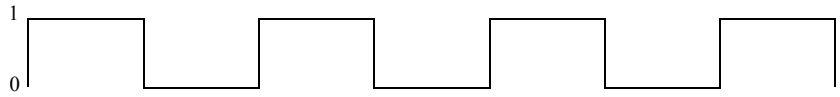
Question 2: Physical and Data Link Layers [30 MARKS]

a)

i. [2 Marks] Annotate the following square wave signal showing a typical result of attenuation.



ii. [3 Marks] Annotate the following square wave signal showing a typical result of limited bandwidth.



b)

i. [5 Marks] What is a token ring network? Answer this question by drawing a diagram in the box below. Be sure to indicate the role of the token on your diagram.

ii. [5 Marks] What is a star network? Answer this question by drawing a diagram in the box below. Be sure to indicate the name and role of each entity in your diagram.

c) Outline what happens when an Ethernet frame arrives at a (self-learning) **switch** that is:

i. [3 Marks] addressed **to** a previously unknown host from a known host.

As the switch does not have an entry for the destination in its switch table it will send the packet out on all links (excluding the source link – 2 marks). (not part of the answer) If multiple hosts are connected to the source link – then they must be connected via another switch or hub and therefore will have already flooded – so no additional is needed.

ii. [6 Marks] **from** a previously unknown host and addressed to a known host.

First the switch table is consulted and as the source is unknown it will be added to the table. In addition to the address and link, a TTL parameter will be included so the entry can be later garbage collected. It is possible if the switch table is full that the new entry will overwrite an older entry (as above). The frame is then sent out only on the link indicated from the known address in the switch table.

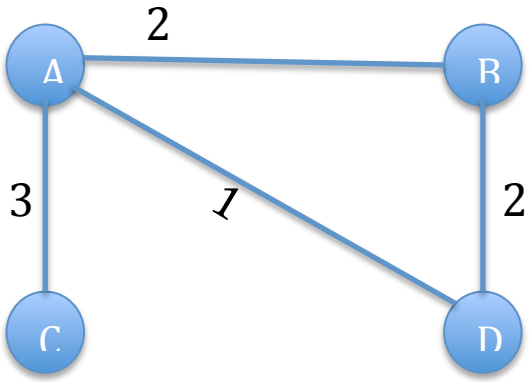
d) [6 Marks] What are three pieces of meta information we might typically in the header of an Ethernet frame.

We need an address.
We may also need a sender's address.
We usually also need some bits to check that the data has not been corrupted.

YOU MAY USE THE REST OF THIS PAGE FOR WORKING

Question 3: Network/Routing/IP Layer [30 MARKS]

a) Consider the following network using the Distance Vector algorithm (without poisoned reverse or split horizon):



i. [8 Marks] Complete all four routing tables (below) after the network has stabilised:

$D^A()$			
B			
C			
D			

$D^B()$		
A		
C		
D		

$D^C()$	
A	
B	
D	

$D^D()$		
A		
B		
C		

ii. [6 Marks] Now break the link between A and B. Show all four routing tables (below) after the network has been re-stabilised:

$D^A()$			
B			
C			
D			

$D^B()$		
A		
C		
D		

$D^C()$	
A	
B	
D	

$D^D()$		
A		
B		
C		

b) You have been given the IPv4 range 192.168.128.0/26. You need to split this into 4 equal subnets.

i. [12 Marks] Complete the following IP address details:

Give your answer for the network addresses in the format x.x.x.x/x

Subnet 1

Network Address: 192.168.128.0/28
First Host: 192.168.128.1
Last Host: 192.168.128.14

Subnet 2

Network Address: 192.168.128.16/28
First Host: 192.168.128.17
Last Host: 192.168.128.30

Subnet 3

Network Address: 192.168.128.32/28
First Host: 192.168.128.33
Last Host: 192.168.128.46

Subnet 4

Network Address: 192.168.128.48/28
First Host: 192.168.128.49
Last Host: 192.168.128.62

ii. [2 Marks] What is the broadcast address for subnet 2.

Broadcast Address: 192.168.128.31

iii. [2 Marks] How many valid host IP addresses are available within this network?

56

YOU MAY USE THE REST OF THIS PAGE FOR WORKING

Question 4: Transport Layer [30 MARKS]

a) [2 Marks] What function does the Transport Layer provide?

Application to application delivery of data.

b) Answer the following questions related to UDP:

i. [3 Marks] Explain why UDP is sometimes referred to as Unreliable Datagram Protocol.

UDP provides no guarantees to the upper layer protocol for message delivery and the UDP protocol layer retains no state of UDP message once sent.

ii. [3 Marks] Explain why the source port field in the header of a UDP datagram is optional.

This is because UDP only supports unidirectional communication. If no reply is expected, the source port can be omitted.

c) Answer the following question related to RTP:

i. [3 Marks] RTP does not ensure real-time delivery. So why is it called a real-time protocol?

No end-to-end protocol, including RTP, can ensure in-time delivery. This always requires the support of lower layers that actually have control over resources in switches and routers. RTP provides functionality suited for carrying real-time content, e.g., a timestamp and control mechanisms for synchronizing different streams with timing properties.

d) Answer the following questions relate to TCP:

i. [3 Marks] What is the TCP windowing concept?

TCP windowing concept is primarily used to avoid congestion in the traffic. It controls the amount of unacknowledged data a sender can send before it gets an acknowledgement back from the receiver that it has received it.

ii. [3 Marks] What are the THREE segments exchanged between two hosts when they want to establish a TCP connection?

SYN – (Synchronizing Packet)
SYN ACK – (Synchronizing Acknowledgement Packet)
ACK– (Acknowledgement Packet)

iii. [4 Marks] Distinguish between flow and congestion control.

Flow control advised the sender of the recievers buffer limits, so as not to send more data than the receiver can handle.

Congestion control limits the rate at which data can be sent in to the network. When segments are lost (assumed due to congestion) the rate is reduced and then begins to increase again. Over time this should tend to a fair share of network capacity.

e) [6 Marks] With the help of a diagram, describe how a sender can reliably send three consecutive messages (m1, m2, and m3) to a receiver by using the Go-Back-N protocol. Assume that message m2 was lost in transmission and needs to be re-transmitted.

(diagram here)

The receiver process keeps track of the sequence number of the next frame it expects to receive, and sends that number with every ACK it sends. The receiver will discard any frame that does not have the exact sequence number it expects (either a duplicate frame it already acknowledged, or an out-of-order frame it expects to receive later) and will resend an ACK for the last correct in-order frame. Once the sender has sent all of the frames in its window, it will detect that all of the frames since the first lost frame are outstanding, and will go back to sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.

f) [3 Marks] Explain why the Selective Repeat protocol is more complicated than the Go-Back-N protocol.

For the selective repeat protocol, the sender's window control is much the same as with go-back-n, but now the receiver must implement a complementary window control of equal sophistication.

Question 5: HTTP/Email/FTP/DNS [30 MARKS]

a) Answer the following questions related to HTTP:

i. [2 Marks] What is the typical port number used by an HTTP server for communicating with its clients?

80

ii. [6 Marks] Identify at least THREE situations when a proxy server will not cache a Web object.

If the HTTP response header tell the cache not to keep it, it won't.

If no validator (e.g. Last-Modified header is absent) in the HTTP response, it will be considered uncacheable.

If the HTTP is encrypted, it won't be cached.

b) Answer the following questions related to the email service in the Internet:

i. [2 Marks] What is the store-and-forward model in an email system?

Store-and-forward model: email servers accept, forward, deliver, and store messages.

Neither the users nor their computers are required to be online simultaneously. Decoupled communication both in time and in space.

ii. [6 Marks] Identify and briefly explain THREE protocols that are often used in practice to retrieve emails from mail servers.

POP3: Post Office Protocol 3 [RFC 1939]
Although most POP clients have an option to leave message on the server after downloading a copy, most of the time after retrieving a message, it is deleted from the server

IMAP: Internet Mail Access Protocol [RFC 1730]
More complete and complex remote access to mailbox
Usually mail is saved on a mail server

HTTP: Hotmail , Google Mail, etc.

c) Answer the following questions related to FTP:

i. [6 Marks] List THREE data transfer modes supported by the File Transfer Protocol (FTP). Which data transfer mode is the most frequently used?

Data transfer mode

- Stream mode: data is sent as a continuous stream
- Block mode: break data into block
- Compressed mode: data is compressed

Of the three methods, stream mode is the one that is by far the most widely used in real FTP implementations. There are likely three reasons for this. First, it is the default and also the simplest method, so it is the easiest to implement and one that is required for compatibility. Second, it is the most general, because it treats all files as simple streams of byte without paying attention to their content. Third, it is the most efficient method because no bytes are wasted on "overhead" such as headers.

ii. [2 Marks] Explain why the FTP passive mode is generally preferred when a firewall is involved in handling FTP traffics.

As described in the FTP Protocol Overview, FTP uses multiple TCP/IP connections; one for sending the commands on, the rest for transferring data. Problems can arise when a filewall is introduced. Since the main connection is outgoing the NAT firewall allows this connection to be made, but when the server tries to connect back to the client it is blocked by the firewall.

The technique called "passive mode" or PASV was introduced to reduce this problem. In this scheme connections are always made from the client to the server and not vice-versa.

d) Answer the following questions related to DNS:

i. [2 Marks] Who is responsible for managing the top-level domain name space?

The Internet Corporation for Assigned Names and Numbers -- ICANN

ii. [4 Marks] Does each local area network (LAN) need to have its own DNS server? Justify your answer.

No need to have a DNS server for each LAN.

You can configure a host to access a DNS server located in a different network. Router can provide the necessary relay service for any DNS query.

Question 6: XML/Web Service/Android Development/Media Streaming [30 MARKS]

a) Answer the following questions related to XML:

i. [3 Marks] Identify THREE major benefits of using XML for representing domain knowledge.

It facilitates the sharing of structured text and non-text information across the Internet.

Languages based on XML are themselves described in a formal way, allowing programs to modify and validate documents in these languages without prior knowledge of their form.

Inherently supports internationalization (Unicode) and platform independence.

ii. [4 Marks] Identify at least FOUR building blocks of an XML document.

- Elements
  - The pairing of a start tag and an end tag.
- Attributes
  - A name-value pair that is part of a starting tag of an Element.
- Processing instructions
  - Special directives to the application that will process the XML document.
- Comments
  - Messages helping a human reader understand the source code.
- Character Data
  - Characters (in a specific encoding)
  - Entities
  - Escapes

b) Answer the following questions related to Web Service:

i. [3 Marks] In a WSDL document, which element is used to specify the network address of the endpoint hosting the Web Service?

The port element, which associates a single protocol-specific address to an individual binding element.

ii. [3 Marks] When should a message element be used in a WSDL document?

A WSDL document can contain zero or more message elements. Each message element can be used as an input, output or fault message within an operation.

iii. [4 Marks] List and briefly explain FOUR main technologies that are commonly used in Web Services.

XML: eXtensible Markup Language is a uniform data representation and exchange mechanism.

SOAP: Simple Object Access Protocol, SOAP is a standard way of using XML vocabulary to enable programs on separate computers to interact across any network and describing messages between applications.

UDDI: Universal Description, Discovery, and Integration specification, UDDI is a mechanism to register and located WS based application.

WSDL: Web Services Description Language, this is a standard meta language to describe the services offered. Specifically, WSDL states what a request message much contain and what the response will look like in a clear notation. WSDL also defines where the service is available and what communications protocol is used to talk to that service.

c) Answer the following questions for Android application development:

i. [3 Marks] Identify at least THREE different types of resources that can be externalized in an Android application.

Android supports the externalization of resources, ranging from simple values such as strings and colors to more complex resources such as images (Drawables), animations, themes, and menus. Perhaps the most powerful externalizable resources are layouts.

ii. [3 Marks] What are the benefits of externalizing resources in an Android application?

By externalizing resources, you make them **easier to maintain, update, and manage**. This also lets you easily define alternative resource values for internationalization and to include different resources to support variations in hardware — particularly, screen size and resolution.

d) Answer the following questions for Media Streaming:

i. [4 Marks] Outline the forward error correction scheme that can be used by multimedia protocols to hide the effect of packet loss.

See page 20 and page 21 of the lecture notes on "Media Streaming".

ii. [3 Marks] State the THREE main problems to be solved in order to allow a best-effort multimedia service to be implemented at the application-level.

Limited bandwidth

Random network delays

Packet loss

YOU MAY USE THE REST OF THIS PAGE FOR WORKING