University of Glasgow

Wednesday 12 December 2018
1.00 pm – 2.30 pm
(Duration: 1 hours 30 minutes)

DEGREES of MSci, MEng, BEng, BSc, MA and MA (Social Sciences)

Networks and Operating Systems Essentials 2

Answer All Questions

This examination paper is worth a total of 60 marks

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS

Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

1. *(Bookwork + Reflection) An implementation that closely follows the layered model will likely be easier to validate for correctness against that model, and easier to debug [**2 marks**]. On the other hand, there may be optimisations that can be performed by combining layers or exposing details across layer boundaries, potentially leading to improved performance [**2 marks**]. There is clearly no single correct answer, and the trade-off depends on the performance and correctness requirements of the system [**2 marks**]. An additional [**2 marks**] are available for high quality written argument, irrespective of the technical points made.*

[8 marks]

2. *(Bookwork for the knowledge of the DV protocol + Problem solving)*

		Time: 0				
		Distance/Next hop to node				
		A	B	C	D	E
Information stored at node	A	0/-	2/B	1/C	∞/-	∞/-
	B	2/A	0/-	2/C	5/D	∞/-
	C	1/A	2/B	0/-	2/D	∞/-
	D	∞/-	5/B	2/C	0/-	2/E
	E	∞/-	∞/-	∞/-	2/D	0/-

*[**2 marks** for filling in the 1-hop neighbours]*

		Time: 1				
		Distance/Next hop to node				
		A	B	C	D	E
Information stored at node	A	0/-	2/B	1/C	3/C	∞/-
	B	2/A	0/-	2/C	4/C	6/C
	C	1/A	2/B	0/-	2/D	4/D
	D	3/C	4/C	2/C	0/-	2/E
	E	∞/-	7/D	4/D	2/D	0/-

*[**8 marks**, one per update vs t0]*

		Time: 2				
		Distance/Next hop to node				
		A	B	C	D	E
Information stored at node	A	0/-	2/B	1/C	3/C	5/C
	B	2/A	0/-	2/C	4/C	6/C
	C	1/A	2/B	0/-	2/D	4/D
	D	3/C	4/C	2/C	0/-	2/E
	E	5/D	6/D	4/D	2/D	0/-

*[**2 marks**, one per update vs t1]*

[12 marks]

3. *(Bookwork) In this context, a reliable connection is one that doesn't suffer from the issues caused by the best-effort nature of the network layer: dropped, reordered, duplicated, delayed and corrupted messages. [**2 marks**]*

*Alleviating delays is very difficult and the best thing the transport layer can do is try to alleviate congestion [**1 mark**]. For the remaining cases: the transport layer protocol (e.g., TCP) can include in its header a checksum to detect corrupted messages [**1 mark**] and sequence numbers to detect duplicates and drop them **[1 mark**] (this requires that the receiver keeps track of the sequence numbers of* *received messages [**1 mark**]), or out-of-order delivery of messages and reorder them [**1 mark**] (this requires that the receiver stores out-of-order messages until missing messages are received [**1 mark**]). Furthermore, each message that is correctly received by its destination, will be acknowledged to its sender [**1 mark**], with messages not acknowledged within a certain amount of time being retransmitted [**1 mark**]. If an ACK is lost in transit, then the sender will assume the original message was lost and will retransmit it [**1 mark**].*

[11 marks]

4. *(Bookwork) TLS uses a mix of public key and symmetric cryptography. Before the exchange even begins, the server has created a public-private key pair, usually signed by a trusted third party whose signing (public) key(s) are widely available and/or distributed with the TLS client libraries [**1 mark**]. Initially the two sides (client/server) exchange random numbers and agree on a cipher to use [**1 mark**]. The client retrieves the server's public key/certificate from the server [**1 mark**], uses it to encrypt a new random number (pre-master secret) and sends it to the server [**1 mark**]. This encryption task is fast as the pre-master secret is small in size [**1 mark**]. Both sides then compute a common master key (session key/keys) based on the exchanged random numbers and pre-master secret [**1 mark**]. All further data transfers are encrypted using symmetric cryptography keyed by the session key(s), which is considerably faster than public key cryptography [**1 mark**].*

[7 marks]

5. *(Bookwork for the knowledge of the algorithms + Problem solving):*

*LRU (assuming leftmost position is most recently accessed) [**4 marks**]:*

A -> [A, -, -] (miss)

B -> [B, A, -] (miss)

C -> [C, B, A] (miss)

A -> [A, C, B]

B -> [B, A, C]

B -> [B, A, C]

B -> [B, A, C]

A -> [A, B, C]

C -> [C, A, B]

D -> [D, C, A] (miss)

B -> [B, D, C] (miss)

*LFU [**4 marks**]:*

A -> [A (1), -, -] (miss)

B -> [A (1), B (1), -] (miss)

C -> [A (1), B (1), C (1)] (miss)

A -> [B (1), C (1), A (2)]

B -> [C (1), A (2), B (2)]

B -> [C (1), A (2), B (3)]

B -> [C (1), A (2), B (4)]

A -> [C (1), A (3), B (4)]

C -> [C (2), A (3), B (4)]

D -> [D (1), A (3), B (4)] (miss)

B -> [D (1), A (3), B (5)]

[8 marks]

6. *(Bookwork for the knowledge of the algorithms + Problem solving)*

*The scheduling order for the algorithms will be [**6 marks**: 1 for each of FCFS/SJF/Priority, 3 for RR):*

FCFS	*P1 (0-10), P2 (10-11), P3 (11-15), P4 (15-22), P5 (22-24)*
SJF	*P2 (0-1), P5 (1-3), P3 (3-7), P4 (7-14), P1 (14-24)*
Priority	*P2 (0-1), P5 (1-3), P1 (3-13), P4 (13-20), P3 (20-24)*
RR	*P1 (0-3), P2 (3-4), P3 (4-7), P4 (7-10), P5 (10-12), P1 (12-15), P3 (15-16), P4 (16-19), P1 (19-22), P4 (22-23), P1 (23-24)*

*Turnaround time [**4 marks**, 1 per algorithm]:*

	P1	*P2*	*P3*	*P4*	*P5*
FCFS	*10*	*11*	*15*	*22*	*24*
SJF	*24*	*1*	*7*	*14*	*3*
Priority	*13*	*1*	*24*	*20*	*3*
RR	*24*	*4*	*16*	*23*	*12*

*Average waiting time [**4 marks**, 1 per algorithm]:*

FCFS	*(0 + 10 + 11 + 15 + 22)/5 = 11.6*
SJF	*(14 + 0 + 3 + 7 + 1)/5 = 5*
Priority	*(3 + 0 + 20 + 13 + 1)/5 = 7.4*
RR	*((0 + 9 + 4 + 1) + (3) + (4 + 8) + (7 + 6 + 3) + (10))/5 = 11*

[14 marks]