University of Glasgow

Wednesday, 30 April 2014
9.30 am - 11.00 am
(1 hour 30 minutes)

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

NETWORKED SYSTEMS 3

Answer all 3 questions

This examination paper is worth a total of 60 marks.

The use of calculators is not permitted in this examination.

For examinations of less than 2 hours duration, no candidate will be permitted to exit during the 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. **(a)** To ensure the confidentiality of data sent across a network, it is important to encrypt that data before transmission. Encryption can be performed using either symmetric cryptography or public-key cryptography.

(i) Outline the differences in the number of keys, and how the keys are used, between these two approaches [4]

(ii) Explain what important problem is solved by public-key cryptography that is not solved by symmetric cryptography. Briefly explain why public-key cryptography solves this problem. [3]

(b) The Transport Layer Security (TLS) protocol, which is used to secure HTTP connections, uses a mixture of both symmetric and public-key cryptography. Explain why this is done, and how it ensures both security and good performance. [5]

(c) To subvert encrypted communication, an eavesdropper might perform a man-in-the-middle attack on a connection, to try to fool the sender into thinking they are the legitimate receiver. Man-in-the-middle attacks can be detected by sending a digital signature along with the data, provided the receiver checks the signature. Explain the basic steps that are involved in generating and checking a digital signature, and how the receiver can use the digital signature to detect a man-in-the-middle attack. [8]

2. **(a)** TCP congestion control relies on "ACK clocking" to determine when the sender can transmit new packets.

(i) Describe what information is contained in TCP ACKs. [2]

(ii) Explain what is ACK clocking, and how it helps prevent network congestion. [4]

(b) TCP congestion control uses a sliding window to determine how many packets can be sent. During the congestion avoidance phase of a TCP connection, two possible events can cause the window to be reduced. These are an ACK timeout, or receipt of a triple duplicate ACK. Outline what network conditions cause these two congestion signals to be generated. [4]

(c) A TCP sender uses the receipt of a triple duplicate ACK as a congestion signal.

(i) State why a triple duplicate ACK is used as a congestion signal, rather than a single or double duplicate ACK. [1]

(ii) Explain under what circumstances would a single duplicate ACK be a sufficient congestion signal. [2]

(iii) Discuss why a triple duplicate ACK is a more appropriate congestion signal than a double duplicate ACK. [4]

(d) Why does TCP congestion control perform poorly on many wireless networks? [3]

3. **(a)** Many applications use the Domain Name System (DNS) to map between host names and IP addresses. Imagine some catastrophic failure happened, so that the DNS root name servers all failed simultaneously, and stopped answering queries.

(i) Discuss how the effects of such a total DNS failure would manifest themselves, and how quickly they would become visible. [5]

(ii) Explain what effects this failure would have on applications using the Internet. [3]

(b) Traditionally, top-level DNS names have been limited to chose ending in two-level country code domains (e.g., ".uk" or ".sg") or a small number of generic top-level domains (e.g., ".com", ".org"). More recently, many more domains have been introduced, including a mixture of internationalised domain names (i.e., using non-ASCII characters), and large numbers of new generic top-level domains (e.g., ".clothing", ".coffee"). Discuss whether you think this expansion is a good idea from a social and business perspective, justifying your answer. [6]

(c) Consider the technical impact of the changes outlined in part (b) of this question, and describe how they will affect the operation of the DNS, and the load on various the servers that make up the DNS infrastructure. [6]

END OF QUESTION PAPER