University of Glasgow

Friday, 5 May 2023
14:00-15:30 BST
Duration: 1 hour 30 minutes
Timed exam – fixed start time

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

NETWORKED SYSTEMS (H)
COMPSCI 4012

Answer all 3 questions

This examination paper is an open book, online assessment and is worth a total of 60 marks.

1. **(a)** A routing algorithm is used to find the best network layer path between two hosts that are not directly connected. Two types of routing algorithm are used: intra-domain routing and inter-domain routing. State what is the difference between these two types of routing, and describe in what environment each type of algorithm would be used. [3]

(b) The Border Gateway Protocol (BGP) is used for inter-domain routing in the Internet. A BGP router builds its routing tables based on exchange of Autonomous System (AS)-path vectors giving routes to destination IP address prefixes. The routing information exchanged is often filtered to enforce policy, with the Gao-Rexford filtering rules being widely used. Describe the Gao-Rexford rules, and explain why they are desirable. [5]

(c) BGP routing is vulnerable to prefix hijacking attacks. Explain what is a prefix hijacking attack in BGP, and discuss how the Resource Public Key Infrastructure (RPKI) can help prevent such attacks. [7]

(d) Addresses in IPv6 are divided into a network part and a local identifier part. The network part identifies the network to which the host connects, and the local identifier part identifies the host on that network. There are two options for assigning the local identifier part: it can either be derived from the link layer address of the host's network interface or it can be assigned randomly (a so-called privacy address). Discuss what are the privacy concerns with using the host's link layer address as the local identifier part of an IPv6 address, and whether they are solved by using privacy addresses. [5]

2. **(a)** The first lab exercise showed how to establish a TCP connection from a client to a server, with the client first performing a DNS lookup then iterating through the results and trying to connect to each possible IP address in turn. While this approach works, modern clients often try to establish some of the connections in parallel rather than performing them all in sequence. Explain why this is, and how they might decide what addresses to try in parallel. [4]

(b) Servers are increasing supporting QUIC as well as TCP. How does the addition of QUIC to the network affect connection establishment? [4]

(c) In the Internet, reliable data transfer is achieved by having transport protocols, such as TCP or QUIC, detect and retransmit any lost packets. This is known as end-to-end packet loss recovery. An alternative approach might be to make packet loss detection and retransmission a property of the link layer, such that loss is detected and packets are retransmitted within the network, at the link where the problem occurs. This is known as in-network packet loss recovery. Outline what are the advantages and disadvantages of end-to-end packet loss recovery compared to in-network packet loss recovery. Discuss whether you think the designers of the Internet made the right choice in selecting end-to-end recovery. [12]

3. **(a)** The Domain Name System (DNS) is a hierarchical distributed database that maps from names to IP addresses. At the top of the DNS hierarchy are the root servers. Explain what role the root servers play in the DNS, and how resolvers know how to find the root servers. [3]

(b) The root servers typically use anycast IP addresses. Briefly explain what is an anycast IP address, and they anycast is useful for the root servers. [5]

(c) There are two aspects to DNS security: transport security and record security. Briefly explain what type of threat each of these protects against, and discuss which aspect of DNS security is likely to give the biggest improvement to Internet security today. [4]

(d) Two methods of providing DNS transport security are to run DNS over TLS or to run DNS over HTTPS. Running DNS over TLS is widely accepted, while running DNS over HTTPS has proven to be controversial with operators and governments. Considering technical differences between these transports, operational differences in how they are used, any legal constraints, and business considerations of the operators, explain why DNS over HTTPS is controversial and DNS over TLS is not, and discuss whether you think the concerns about DNS over HTTPS are valid. Justify your answer. [8]

END OF QUESTION PAPER