The University of Western Australia

1st SEMESTER EXAMINATIONS
JUNE 2016

SCHOOL OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

NETWORKS AND SECURITY (CITS3002)

This Paper Contains 5 Pages and 4 Questions
You are required to attempt THREE (3) of the FOUR (4) questions.

Time Allowed: 2 Hours
Reading Time: 10 Minutes

Do not write verbose answers to any question.
As a guide, a question worth EIGHT (8) marks should be answered on at most a single page of your answer booklet.

PLEASE NOTE

Examination candidates may only bring authorised materials into the examination room. If a supervisor finds, during the examination, that you have unauthorised material, in whatever form, in the vicinity of your desk or on your person, whether in the examination room or the toilets or en route to/from the toilets, the matter will be reported to the head of school and disciplinary action will normally be taken against you. This action may result in your being deprived of any credit for this examination or even, in some cases, for the whole unit. This will apply regardless of whether the material has been used at the time it is found.

Therefore, any candidate who has brought any unauthorised material whatsoever into the examination room should declare it to the supervisor immediately. Candidates who are uncertain whether any material is authorised should ask the supervisor for clarification.

THIS PAGE INTENTIONALLY LEFT BLANK

1a) Using pseudo-code similar to either Java or C, develop a small set of methods or functions to simulate network stations communicating using a slotted ALOHA protocol.

With reference to your simulation's implementation, explain how the maximum observed channel utilization may be calculated.

(Don't be overwhelmed by this problem. You are not being asked to develop a protocol using the *cnet* framework. A correct solution requires only about 25 lines of pseudo-code).

(10)

1b) Consider the delivery of messages in an internetworked environment in which the source and destination nodes are many hops apart. Large messages must be fragmented and reassembled using one of two possible approaches.

The first approach involves fragmenting each message at the source node, and then reassembling them at the destination node.

The second approach involves fragmenting each message at the source node, reassembling and re-fragmenting them at intermediate nodes, and final reassembly at the destination node.

With reference to two distinct examples, describe circumstances where each of the methods would be preferred over the other.

(10)

2a) The Internet Protocol (IPv4) addressing scheme has, for over 15 years, been described as *running out of addresses*.

In April 2011, the Asia Pacific Network Information Centre allocated the world's last block of IPv4 addresses. However, since then, the wider Internet has not ground to a halt, and tens of millions of new hosts have been added.

Describe two distinct mechanisms that are currently being employed to extend the lifespan of IPv4.

Will it be possible for these mechanisms to extend the lifespan of IPv4 almost indefinitely? Explain your answer.

(10)

2b) With reference to two examples, explain the relationship between the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP).

(5)

2c) Both UDP and TCP employ port numbers to identify the destination entity when delivering a message.

Give two distinct reasons why these protocols introduced a new abstract identification value (the port number), instead of using process-identifiers (PIDs), which already existed when these protocols were designed.

(5)

---

3) The problem with supporting mobile devices on the Internet is that the Internet is designed to route packets hierarchically. The Mobile IPv4 protocol was created to address this challenge.

The most widely accepted standard for Mobile IPv4, permits a mobile device to communicate via the Internet in a relatively transparent manner. For example, a laptop computer from UWA that uses IP address 130.95.1.100 when physically located at UWA, may still be contacted, while it is in Sydney, with the IP address 130.95.1.100.

A mobile device's IP address must change as it moves from network to network. At the same time, applications require a constant IP address. The apparent conflict is resolved by maintaining two separate addresses for each device.

The first is the *home address*. This is the natural address for the device, the one that resides in the address space of the home network. The home address is assigned by the home network itself and stays with the device long-term. With regard to applications, this is always the IP address of the device.

The second address is referred to as the *care-of address*. This address can potentially change from minute to minute as a device travels through several foreign networks. To the routing protocols of the Internet, this is the destination address of the device.

Any packets that are destined for the mobile device will be first routed to the home network, since that is the network defined in the home address of the device.

Additional software, termed the *home agent*, will be present in a mobile IP-enabled network. The home agent is responsible for intercepting any packets addressed to mobile devices that are not currently ''at home,'' and then forwarding those packets to the current care-of address for the device. It does this by encapsulating the packet inside another packet destined for the care-of address. This packet is then sent via the Internet, where standard routing protocols ensure that it arrives at the foreign network temporarily hosting the device.

A *foreign agent* unwraps the packet and sends it to the mobile device via its home address, which it has associated with a hardware destination address for the device. When the packet arrives at the device, it is accepted as being appropriately addressed; it then travels up the TCP/IP stack to the relevant application software.

i) Draw one or more diagrams showing how a computer, that is neither in the home network nor in the foreign network, can communicate with web server software running on the mobile laptop.

On your diagram(s) draw a number of relevant IP packets, and clearly show all IP addresses (included any addresses in encapsulated packets).

(5)

ii) With reference to your diagram(s), outline the potential security challenges associated with Mobile IPv4.

(5)

iii) Propose and discuss a mechanism to address these potential security challenges.

(10)

4a) The Address Resolution Protocol (ARP) associates hardware addresses with IP addresses. This association may change over time. Each node in the network maintains an ARP cache mapping corresponding IP and hardware addresses. A node trying to find the hardware address for an IP address that is not in its cache, broadcasts an ARP request that also contains its own IP and hardware addresses. The node with the requested IP address replies with its hardware address.

What are the possible vulnerabilities for spoofing in the ARP protocol?

What defences can be used against ARP spoofing?

(10)

4b) The File Transfer Protocol (FTP) was first defined in 1980 and revised in 1985. Since then, there have been no modifications to the structure nor the number of FTP messages types.

However, we continue to see a number of new, often graphical, FTP clients and Web browsers that are able to communicate with established FTP servers running the 1985 FTP protocol. These new FTP clients appear to provide a greatly increased set of features.

With reference to two distinct examples, explain how this is possible.

(10)

END OF PAPER