FIT1047 Introduction to computer systems, networks and security - S1 2022

Assignment 3 – Networks

Purpose	In Part 1 of this assignment, students will record data from a real-world wireless network and demonstrate that they can analyse it, identify its properties and potential issues. In Part 2, students analyse Internet traffic and identify servers, clients and protocols used. The assignment is related to Unit Learning Outcomes 5 and 6.
Your task	You need to submit a report with your findings regarding the analysis tasks for Part 1. The instructions below contain concrete questions you should answer in your report. Part 2 is submitted via a Moodle quiz.
Value	**30**% of your total marks for the unit The assignment is marked out of 60 marks.
Word Limit	600 words for Task 1.2, no word limits for the remaining tasks
Due Date	**11:55 pm Friday 20 May 2022**
Submission	● Via Moodle assignment submission (Part 1) ● Turnitin will be used for similarity checking of all submissions. ● Via Moodle quiz submission (Part 2)
Assessment Criteria	See rubric
Late Penalties	● 10% deduction per calendar day or part thereof for up to one week ● Submissions more than 7 calendar days after the due date will receive a mark of zero (0) and no assessment feedback will be provided.
Support Resources	See Moodle Assessment page
Feedback	Feedback will be provided on student work via: ● general cohort performance ● specific student feedback ten working days post submission

INSTRUCTIONS
This assignment has two parts. Make sure you read the instructions carefully.

Part 1: WLAN Network Design and Security

For this part of the assignment, you will perform a real-world WLAN site survey. Your task is to produce a map of (part of) a building that gives an overview of the wireless networks that are available, as well as an analysis of the network.

What you will need: a WiFi-enabled laptop (some smartphones also work, see below), and a place to scan. For example, you can perform a survey of your home, of an office space, of parts of the Monash campus. If you don't own a suitable device that you could use for this activity, try to borrow one from a friend, or contact us to figure out an alternative.

You have to complete two tasks (a survey and a report).

Task 1.1: Survey (15 marks)

Create a map of the place you want to survey. A simple floorplan will be sufficient, it doesn't have to be perfectly to scale. See the appendix for an example. The map needs to include distances and needs to be labelled with all relevant information (e.g. wall material, if used for the discussion). Your survey should cover an area of at least 60 square metres (e.g. 6x10 metres, or 4x15, or two storeys of 6x5 each). Be creative – the survey can include hallways or outside areas. Be sure to take the analysis in Task 1.2 into account, by designing your survey to include walls, doors etc. it will be easier to write something interesting in Task 1.2. Furthermore, your survey must include at least three WiFi access points. These can be your own, but can also include your neighbours' APs or the ones at Monash, for example. If you are scanning in a commercial area or on campus, you should be able to see enough APs. If you want, you can create an additional AP with a phone (using "Personal hotspot" or "Tethering" features).

For the survey, use a WLAN sniffing tool (see below) in at least eight different locations on your map. For each location, record the technical characteristics of all visible APs. Depending on the scanning tool you use, you can record features such as the network name, MAC address, signal strength, signal to noise ratio (SNR), 802.11 version(s) supported, band (2.4 or 5 GHz) and channel(s) used.

Add the data gathered from the survey into the map of the covered area. On the map you should indicate the location of the access points and the locations where you took measurements.
For the access points, use the actual location if you know it, or an approximation based on the observed signal strength (e.g. if it's your neighbour's access point and you don't know exactly where it is).
For each measurement point, you can either add the characteristics directly into the map, or create a separate table with the details. You can submit several maps if you choose to enter data directly into the maps, or a single map if you use additional tables. Create the map

yourself, do not use the mapping features available in some commercial (i.e., paid) WLAN sniffing tools.

Task 1.2: Report (20 marks)

Write a report (word limit 600) on your observations analysing the data collected in the previous step (Task 1.1). Your analysis should investigate the following aspects:

- Channel occupancy: Are different access points competing on the same channels? Are they configured to use overlapping channels? Could the configuration be improved?
  (5 marks)
- Interference from walls, doors etc.: How do different materials affect signal strength and/or noise? Can you notice a difference in attenuation for different APs?
  (5 marks)
- Coverage: Do the access points sufficiently cover the desired area? Could the placement or configuration be improved?
  (5 marks)
- Any other aspect of your own choice. Here are a few suggestions:
  - measure the attenuation caused by your own body
  - measure the download and upload speeds in different locations
  - determine the overlap that has been implemented to enable roaming
  - describe how you interpolated the locations of access points from the signal strengths

  Describe your findings and explain them with some technical detail (i.e., not only say what you found, but also how you performed the analysis or why you think the network is behaving that way).
  (5 marks)

Tools: You can use e.g. Acrylic Wifi (https://www.acrylicwifi.com/en/) for Windows, NetSpot (http://www.netspotapp.com) for macOS and Windows, and LinSSID or wavemon for Linux. If you have an Android smartphone, apps like Wifi Analyzer can also be used. On iOS, WiFi scanning apps do not provide enough detail, so iPhones won't be suitable for this task.
For drawing the site maps, any drawing tool should work, for example LucidChart, or even presentation tools such as PowerPoint, Keynote or Google Slides. Scans of hand-drawn maps are acceptable if they are neat and easily readable.

Part 2: Internet Traffic Analysis (25 marks)

This part of the assignment requires you to download a PCAP file, open it in Wireshark and answer a few questions about the captured frames. The PCAP files are individualised, so make sure that you download the correct file while you are logged into Moodle.
You can access your individual PCAP file through the Assignment 3 Part B quiz link on Moodle. All of your answers have to be submitted via that Moodle quiz. You have two hours to complete the quiz after starting the attempt.
Here are a few tips on how to approach these tasks.

MAC addresses:
These are the addresses of individual devices at the Data Link Layer. Each frame contains a sender and receiver MAC address. For each frame, think about which device would be the sender and which the receiver.

IP addresses:
These are the Network Layer addresses. Remember that we use the DNS protocol to map a human-readable address (such as www.monash.edu) to an IP address (such as 202.9.95.188). So in order to find out the IP address for some of the devices, you may have to try to find DNS requests and responses in the PCAP file.

TCP connections:
Remember that each TCP connection starts with a three-way handshake. This was covered in the lectures, so you may have to go back to the videos if you're not sure what those frames look like.

Appendix: Sample map