FIT1047 S2 2016
Assignment 2

Submission guidelines

This is an individual assignment, **group work is not permitted** (except for parts of task 1.1 as stated below).

Deadline: October 21, 2016, 23:55pm

Submission format: PDF (one file containing both parts 1 and 2), uploaded electronically via Moodle.

Late submission:

- By submitting a special consideration form, available from `http://www.monash.edu.au/exams/special-consideration.html`
- Or, without special consideration, you lose 5% of your mark per day that you submit late (including weekends). Submissions will not be accepted more than 5 days late.

  This means that if you got x marks, only $0.95^n \times x$ will be counted where n is the number of days you submit late.

Marks: This assignment will be marked out of 70 points, and count for 17.5% of your total unit marks.

Plagiarism: It is an academic requirement that the work you submit be original.

Zero marks will be awarded for the whole assignment if there is any evidence of copying (including from online sources without proper attribution), collaboration, pasting from websites or textbooks.

The faculty's Plagiarism Policy applies to all assessment:

`http://intranet.monash.edu.au/infotech/resources/students/assignments/policies.html`

Further Note: When you are asked to use internet resources to answer a question, this **does not mean copy-pasting text** from websites. Write answers in your own words such that your understanding of the answer is evident. Acknowledge any sources by citing them.

1 Wireless networks

For this task, you will perform an analysis of a real large-scale wireless network. Your task is to collect data about WLAN access points and discuss several features of the network that you observe.

1.1 Use a WLAN analysis tool on your laptop to record WLAN access points at a **large shopping centre**. State the centre in your report. Visit the shopping centre with your laptop, and record the details of the available wireless networks in **three different locations**. Include screenshots of your WLAN tool that show **at least 10–15 access points** for each location, with **at least 5 different SSIDs**, and include their technical characteristics like channel number, RSSI, 802.11 standard, security, supported data rate, etc.

Note: This activity can be completed by a group of 2-4 students. Give the full names and student IDs of all team members. The report must be written individually (but can obviously use the same screenshots for each student in the group).

Tools: You can use e.g. Acrylic Wifi (`https://www.acrylicwifi.com/en/`) or inSSIDer-2 (`http://bit.ly/1KcqkN2`) for Windows, or NetSpot (`http://www.netspotapp.com`) for Mac OS and Windows.

If your laptop WLAN NIC does not support the 5 GHz band, you may want to team up with someone who has a laptop that does – the results you find will be more interesting if you can scan on both 2.4 GHz and 5 GHz. You can find out if your laptop supports 5 GHz by using the WLAN analysis tool while you're on the Monash campus (if you can't see any 5 GHz networks, then your laptop doesn't support it).

(10 marks)

1.2 Write a report (word limit 800) on your observations analysing the data collected in the previous step. For each point below, briefly describe the *general concept* in your own words, then analyse the *data you gathered* with respect to the concept.

Your analysis should investigate into the following aspects:

- Usage of different WLAN channels. Briefly explain how WLAN channels should be allocated, then describe channel usage in the data you gathered (which channels are very "crowded", which are free, taking signal strength into account). (5 marks)
- Interference from neighbouring access points and its effects. Briefly describe under which circumstances access points interfere with each other, and analyse if you see potentially interfering access points in your data. (5 marks)

- Dual band WiFi. Briefly explain the advantages and technical consequences of using both 2.4 GHz and 5 GHz at the same time. Analyse whether any access points in your data are likely offering both 2.4 GHz and 5 GHz access (e.g. if their MAC addresses and signal strengths are very similar). (5 marks)
- The security situation. Name the different options for providing secure WLAN access, and analyse which security options have been implemented in the networks you recorded as well as the implications for users. (5 marks)
- Support for roaming between access points. Briefly explain the concept of roaming, and analyse which access points in your data offer roaming. (5 marks)
- One other aspect of your own choice. E.g. which hardware vendors for access points you can observe, whether you found special networks for certain applications, whether you detected any "personal hotspots" (mobile phones used as WiFi access points), how the shopping centre might be using its WiFi to track shoppers, or any other observation you find interesting. Describe the observation, including the technology behind it. (5 marks)

Your report needs to be your individual work (no group work is permitted). 30 marks are allocated to the technical content, while another 10 marks will be based on the presentation and language of the report. You do not need to follow a strict template for technical reports, but it should be well structured, readable, and use adequate language. All information from external sources must be properly referenced. **If you copy text from web sites, it needs to be referenced and quoted!** See resources on Moodle for more information about referencing.

(40 marks)

2 Cyber Security

The security expert and author *Bruce Schneier* also runs a security blog. His Cryptogram Newsletter (`https://www.schneier.com/crypto-gram/`) provides a monthly digest of posts of this blog. All Cryptogram Newsletters consist of several longer articles and news on Bruce Schneier and there is always one item simply called *News*.

The task is to pick an item in one of the 3 last Cryptogram Newsletters, read the news item, look up the referenced sources and read them and finally write a brief report on the findings.

1. Read through the *News* item in the three most recent Cryptogram Newsletters (`https://www.schneier.com/crypto-gram/` and choose a reported issue that either covers a weakness in a software or a hardware product, or covers a particular attack. Make sure that you take one of the short items in the News section.

2. Look up and read the articles and information referenced in the news item.
3. Write a short summary of the news item in your own words (between 30 and 50 words).
4. Identify which software, hardware or system is affected (max 20 words). The identification should be as precise as possible.
5. Describe how the problem was discovered and how it was initially published (between 30 and 50 words). Try to find this information in the referenced articles. The problem might have been found by researchers at a university, by a professional security company, by some hacker, published in a scientific conference/journal, in a newspaper on a blog, etc.
6. Estimate how serious the issue/weakness/attack is, what the consequences might be, and what reactions you think are necessary/useful on a technical level, in terms of human behaviour, and on a policy level (between 150 and 250 words).

Your report needs to be your individual work (no group work is permitted). You should structure the report in accordance with the items in the task description. However, there is no need to follow a strict template for technical reports, but it should be well structured, readable, and use adequate language. All information from external sources must be properly referenced (see resources on Moodle about referencing). References do not count for the word count.

You should stick to the word count. Write at least as many words as required, but not more than the maximum. A maximum of 20 percent above the maximum word count is acceptable. Additional text will be ignored in the marking. You should first think about the main statements you want to make and then write a concise text.

(20 marks)