FIT1047 – Introduction to computer systems, networks and security

Assignment 2 – Semester 1, 2017

Submission guidelines

This is an individual assignment, **group work is not permitted**.

Deadline: May 26, 2017, 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 WLAN Network Design and Security

For this task, you will perform a **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. You can perform a survey of your home, of an office space, of parts of the Monash campus, or inside a shopping centre. If you dont own a suitable device that you could use for this activity, please try to borrow one from a friend, or contact us to figure out an alternative.

This activity has two sub-tasks:

a) **Survey**

Create a map of the place you want to survey. A simple floorplan will be sufficient, it doesnt have to be perfectly to scale. Your survey should cover an area of **at least 60 square meters** (e.g. 6x10 meters, 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 part b) into account, by designing your survey to include walls, door etc. it will be easier to write something interesting in part b).

Furthermore, your survey must include **at least three WiFi access points**. These can be your own, but can also include neighbours APs. 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) at **at least eight different locations** on your map. For each location, record the technical characteristics of all visible APs. In particular, you should record *RSSI (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.*

Create maps, based on your floorplan, that visualise the information you have gathered. Professional apps can produce nice heatmaps of signal strength and SNR, but for this exercise you will need to create your own representation based on the raw data you have collected (i.e., dont use the visualisations generated by sophisticated scanning apps). You will need to submit **at least two maps** showing different aspects of your scan. The maps need to include locations of the access points (as far as you can determine them, or an approximation of the location based on the observed signal strength).

(15 marks)

b) Write a report (word limit 600) on your observations analysing the data collected in the previous step. 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? (5 marks)
- Interference from walls, doors etc.: How do different materials affect signal strength and 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 Mac OS 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 wont 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.

2 Cyber Security

Information on security problems, weaknesses and attacks can be found in many places (blogs, newsletters, experts' pages, etc.). Your task is to pick one item from the following list, read the news item, look up and read the referenced sources, and finally write a report on the findings.

- `https://www.xudongz.com/blog/2017/idn-phishing/`
- `https://www.schneier.com/blog/archives/2017/04/smart_tv_hack_v.html`
- `https://www.wired.com/2017/04/obscure-app-flaw-creates-backdoors-millions-smartphones/`

- https://threatpost.com/hundreds-of-thousands-of-vulnerable-ip-cameras-easy-target-for-botnet-researcher-says/124192/
- https://arstechnica.com/security/2017/02/high-severity-vulnerability-in-edgeie-is-third-unpatched-msft-bug-this-month/
- https://it.slashdot.org/story/17/04/05/2344257/android-devices-can-be-fatally-hacked-by-malicious-wi-fi-networks

1. Chose one of the 6 news items above, read the text.
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 50 and 200 words).
4. Identify which software, hardware or system is affected (max 50 words). The identification should be as precise as possible. Include exact product names, distribution of the product, version numbers, etc.
5. Describe how the problem was discovered and how it was initially published. 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. Was it the result of targeted research, found by chance, were any tools used, etc? (write 50-100 words)
6. Estimate how serious the issue/weakness/attack is, describe what is necessary to exploit the weakness, evaluate what the consequences might be if it is exploited, and what reactions you think are necessary/useful on (i) a technical level, (ii) in terms of human behaviour, and (iii) on a policy level (between 150 and 300 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)