MCD4700 – Introduction to computer systems, networks and security

Assignment 2 – Trimester 3, 2018

Submission guidelines

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

Deadline: 18 January 2019, 11:55pm

Submission format: A single Word (doc, docx) file, uploaded electronically via Moodle.

Late submission:

- By submitting a Special Consideration Form or visit this link: https://goo.gl/xtk6n2
- 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 20% 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. Monash Colleges policies on plagiarism, collusion, and cheating are available here or see this link: https://goo.gl/bs1ndF

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 don't 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.

Tools: You can use one of the following

- NetSpot (http://www.netspotapp.com) for Mac OS and Windows
- Acrylic Wifi (https://www.acrylicwifi.com/en/) for Windows
- LinSSID or wavemon for Linux
- Wifi Analyzer for Android (only if you do not have a laptop)

This activity has two sub-tasks:

a) **Survey (20 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. Your survey should cover an area of **at least 90 square meters** (e.g. 9x10 meters, or 6x15, or two storeys of 9x5 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 **least eight different locations** on your map. For each location, record the technical characteristics of all visible APs. In particular, you should record *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*. Some of these parameters may not be available with depending on the concrete tools you use, in that case collect as much data as possible. In your report, include screenshots of the WiFi scanning software. There should be at least one screenshot for each data recording location.

Create maps, based on your floorplan, that *visualize* the information you have gathered. **Do not use automatically generated "heatmaps" as produced by professional versions of the apps mentioned above.** Simple maps that show the values of the different characteristics in different locations are sufficient. You can submit one or two maps, showing different aspects of your scan. The maps need to include area dimensions, data recording locations, access point names and locations (as far as you can determine them, or an approximation of the location based on the observed signal strength). For HD marks, you will need to indicate on the map, some technical characteristics of access points, materials of walls/doors/windows and some visualization of coverage area for each access point.

For drawing the site maps, any drawing tool should work, for example

- LucidChart
- Google Drawings
- Scans of hand-drawn maps are acceptable only if they are neat and easily readable. Use a scanner instead of taking a photo.

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)**
- Attenuation 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.**(5 Marks)** 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

Important: Describe your findings and then **analyze and explain** them with some technical detail (i.e., not only say what you found, but also why you think the network is behaving that way or what are the consequences of observed behaviour).

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.wired.com/story/foreshadow-intel-secure-enclave-vulnerability/
- https://www.wired.com/story/fax-machine-vulnerabilities/
- https://www.zdnet.com/article/instagram-hack-is-locking-hundreds-of-users-out-of-their-accounts/
- https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/
- https://krebsonsecurity.com/2018/07/lifelock-bug-exposed-millions-of-customer-email-addresses/
- https://www.darkreading.com/endpoint/privacy/stealth-mango-proves-malware-success-doesnt-require-advanced-tech/d/d-id/1332408
- https://www.schneier.com/blog/archives/2018/08/hacking_police_.html
- https://www.securityweek.com/critical-flaws-found-netcomm-industrial-routers
- https://www.securityweek.com/smart-irrigation-systems-expose-water-utilities-attacks
- https://blog.checkpoint.com/2018/08/08/whatsapp-group-chat-fake-news-vulnerability/
- https://blog.talosintelligence.com/2018/07/samsung-smartthings-vulns.html

1. Chose one of the 11 news items above, read the text. Mention the chosen article clearly in your report.
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 when and where 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).

(20 Marks)

Report Structure

For task 1 and task 2, you should stick to the word count. A maximum of 10 percent above orbelow the limits 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. The word limit doesn't include the title page, the contents page, summary, references, labels and the description of the figures.

Your report must be your individual work, as no group work is permitted. Your report should be well structured in accordance with the items in the task description. It should be presented **professionally**, which includes use of adequate language and proper formatting. All information from external sources must be properly cited (see resources on Moodle about referencing). **Use either APA or IEEE style of referencing.**

A suggested structure of the report is given below

- Title page (including Title, your name, student ID, lecturer Name, tutor name, tutorial day/time)
- Summary (max 100 words)
- Table of Contents (auto generated)
- Introduction (optional if Summary is provided)
- 1. WLAN Network Design

  1.1 WiFi Survey (includes map and screenshots)

  1.2 Analysis (create 4 subheadings for each discussion point)
- 2. Cybersecurity

  - Summary

  - Affected systems

  - Problem discovery

  - Analysis
- Conclusion
- References

You will be marked on the structure and presentation of your report. It includes (but is not limited to) overall structure, presentation, formatting, grammar, punctuation, spellings, appropriate use of figures and tables, references and in text citations. **(10 Marks)**

File to be submitted

One file only named "FirstName-YourLastName-StudentID".docx or doc containing the report as described above.