FIT1047 - Introduction to computer systems, networks and security
Assignment 2 – Semester 2 2020

Submission guidelines

Individual Assignment: This is an individual assignment; **group work is not permitted**.

Deadline: Week-12, Friday 4:00 PM

Submission format: PDF (***one file containing both parts 1 and 2***), uploaded electronically via Moodle. Submission name of the file. E.g. LastName_FirstName_Student_ID.pdf

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: Marked out of **100 points**, and weighs **15%** 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 on-line sources without proper attribution), collaboration, and pasting from websites or textbooks. Monash University's Academic Integrity Policy applies to all assessment:

https://www.monash.edu/students/academic/policies/academic-integrity

Important Notes:

1. Your report needs to be your individual work (no group work is permitted).
2. 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.
3. All information from external sources must be properly referenced (see resources on Moodle about referencing style followed in FIT). References do not count for the word count.
4. 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.
5. Write answers in your own words such that your understanding of the topic is evident. Acknowledge any sources by citing them. [Caution: Using Internet resources to answer a question, **does** not mean copy-pasting text from websites.]

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 Wi-Fi-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.

1.1 Survey (30 marks)

Create a map of the place you want to survey. A simple floor-plan will be sufficient, it doesn't have to be perfectly to scale (see below for an example). Your survey should cover an area of **at least 40 square meters** (e.g. 4x10 meters or two-storey buildings of 6x5 each). Be creative – the survey can include hallways or outside areas. Be sure to take the analysis in part 1.2 into account, by designing your survey to include walls, doors etc. It will be easier to write something interesting in part 1.2.

Furthermore, your survey must include **at least three Wi-Fi Access Points (WAP)**. These can be your own, but can also include neighbors' 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. Depending on the scanning tool you use, you can record (print screen) features such as the *Network Name, MAC Address, Signal Strength, Security, 802.11 Version(s) Supported, Band (2.4 or 5 GHz)* and *Channel(s) used*.

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 neighbor'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. Include the screen-shots (print screen of WLAN sniffing tool data display) in the appendix section of your report as a proof of your data source. Create the map yourself, **do not use the mapping features** available in some commercial (i.e. paid) WLAN sniffing tools.

1.2 Report (30 marks)

Write a report (word limit 600) on your observations analyzing the data collected in the previous step. The report does not have to follow any particular structure (i.e. simply answering the following questions is enough, you don't need an executive summary, table of contents etc.). 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? Is roaming available? Determine the overlap that has been implemented to enable roaming. Etc. **(6 marks)**

- **Interference:** Effect of other sources of signals (microwave oven, reflected signals from walls, doors etc.) **(6 marks)**

- **Attenuation:** How does different material affect signal strength and noise? Do you notice any difference in attenuation for different APs? How about attenuation caused by your own body? Can you measure and reflect the result? **(6 marks)**

- **Coverage**: Do the access points sufficiently cover the desired area? Could the placement or configuration be improved? **(6 marks)**
- **One more aspect** of your own choice. A few suggestions: **(6 marks)**
  —explain signal-to-noise ratio either using measured noise or by assuming that noise is slightly below the weakest signal your scanning software can detect.
  —measure the download and upload speeds in different locations.
  —describe how to extrapolate or interpolate locations of APs from signal strengths.

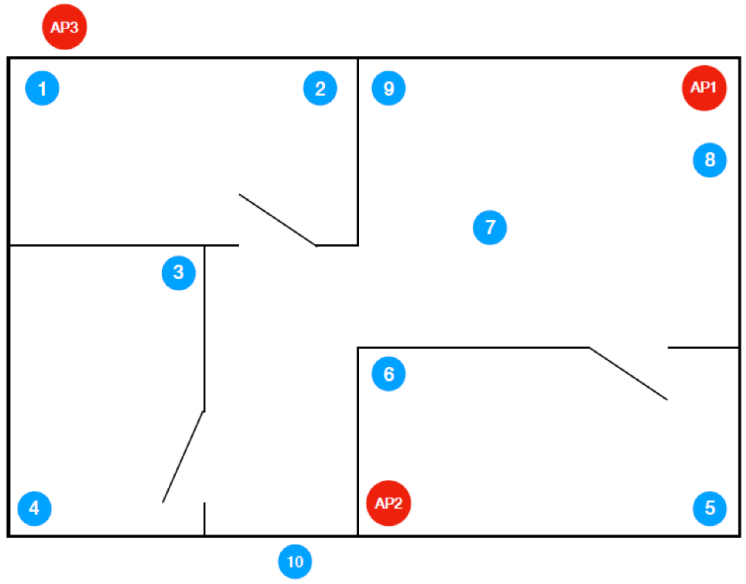
Important: Describe your findings and explain them with some technical detail accompanied by diagrams (i.e. not only say what you found, but also how you performed the analysis or why you think the network is behaving that way).

1.3 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.
- 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.
- Microsoft Visio.
- Open source Wireshark packet capture tool for analysis.
- 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.

1.4 Example Floor Plan

This is just to give you an idea of the level of detail required in the map. Your map may include either a single-story or a double-story house that you are living in. In addition to the map, your survey would have to include tables that contain details and measurements for the indicated locations.



Dimensions: 10 m (width) × 4 m (height)

Red circles: access points

Blue circles: locations of measurements **(Maximum word limit for Part-1 = 600 words)**

2 Cyber Security (40)

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.

1. Securing IPsec Virtual Private Networks. [Link]
2. Limiting Location Data Exposure. [Link]
3. Dark Basin: Uncovering a Massive Hack-For-Hire Operation. [Link]
4. Identifying Unintended Harms of Cybersecurity Countermeasures. [Link]
5. TikTok and 32 other iOS apps still snoop your sensitive clipboard data. [Link]
6. Google removes 25 Android apps caught stealing Facebook credentials. [Link]
7. New Mac Ransomware Is Even More Sinister Than It Appears. [Link]
8. Your Privilege Gives Your Privacy Away: An Analysis…….. [Link]
9. A simple telephony honeypot received 1.5 million robo-calls across 11 months. [Link]
10. Hackers Convinced Twitter Employee to Help Them Hijack Accounts. [Link]
11. 'Ghostwriter' Influence Campaign: Unknown Actors Leverage….. [Link]
12. Smart locks opened with nothing more than a MAC address. [Link]
13. U.S. Government Contractor Embedded Software in Apps to Track.... [Link]
14. The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States….. [Link]
15. Bluetooth flaw allows impersonation of trusted devices….. [Link]
16. Critical 'Sign in with Apple' Bug Could Have Let Attackers Hijack…... [Link]
17. 'I love you': How a badly-coded computer virus caused billions in damage…..[Link]
18. Top Cybersecurity Threats in 2020.. [Link]
19. Incident Of The Week: Passwords And Biometrics Info For…. [Link]
20. Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports..[Link]
21. Smart Home: Threats and Countermeasures [Link]
22. Serious flaws leave WPA3 vulnerable to hacks that steal Wi-Fi…. [Link]
23. Securing Smart Homes And Buildings: Threats and Risks to Complex[Link]
24. What Are The Biggest Cybersecurity Threats In 2019? [Link]
25. The Challenges of Security for IoT and Home Automation...[Link]
26. Risk associated with cookies. [Link]
27. Wireless Network and Wi-Fi Security Issues to Look Out For. [Link]
28. DDoS attacks in Q2 2019. [Link]/
29. Your Smart Home is Vulnerable to Cyber Attacks. [Link]
30. Hackers hijack thousands of Chromecasts to warn of the latest security bug. [Link]
31. Security Flaws in WPA3 Protocol Let Attackers Hack WiFi Password [Link]
32. CSO Provides News, Analysis And Research On Security And Risk...[Link]

Choose one or more of the related news items above, read the article(s) and any other outside related links/topics to further strengthen your research study. Look up and read the articles and information referenced in the news item.

Then write a report following the guideline given below.

2.1 Summary **(15 Marks)**

Write a short summary of the news/article item in your own words **(Maximum of 200 words)**

2.2 Identify **(5 Marks)**

Identify which software, hardware, system, or network(s) are affected with its issue. The identification should be as precise as possible. You can include exact product names, distribution of the product, version numbers, etc. **(Maximum 50 words).**

2.3 Describe The Problem **(5 Marks)**

Describe how the problem was discovered and how it was initially published. Try to find this information in the referenced articles or any related article. 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.? **(Maximum 100 words)**

2.4 Estimate the Seriousness **(15 Marks)**

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:

(a) Technical level,

(b) In terms of human behavior, and

(c) On a policy level.

(Maximum 200 to 350 words)

IMPORTANT:

Please **APPEND** your (Lab Reflective Journal Week 6 to 12) (Weight: 5%) with the ASSIGNMENT-2 at the end.

The submission is a single PDF document that contains Assignment-2 tasks & Lab Reflective Journal week 6 to 12.