FIT1047 – Assignment 2

Student Name: Gloria Siew Phing, Ooi

Student ID: 2746 7449

Tutor name: Safi Uddin

Date: 26/05/17

Part1: WLAN Network and Security

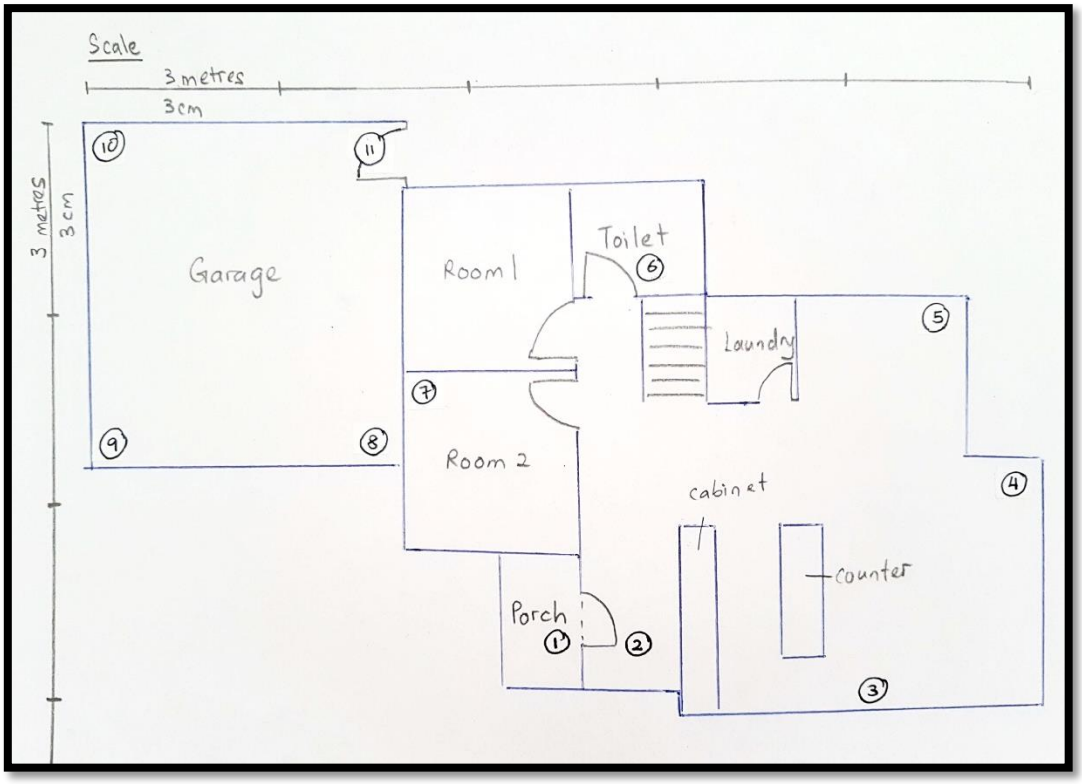

Diagram1: Floor plan of surveyed area

Diagram 1 shows the floor plan of the surveyed area with 11 locations numbered accordingly. With the help of Netspot, data from all 11 locations in the map were collected and analysed for 3 access points (AP).

Diagram 3 & 4 shows snapshots of Netspot and how data was collected. To help with understanding, a simple heat map has been created for each AP with the scale of *'Green'* being *weak* signal strength & signal-to-noise(SNR) ratio to *'Red'* being *strong* signal strength and SNR. (Refer below)

SNR is the difference in decibels between the received signal and background noise level. As noise level in normal environments are very low except during usage of microwaves, codeless phones etc, the SNR levels found is ***in proportion*** to Signal strength.

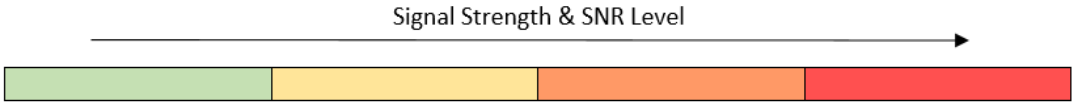

Diagram2: Signal strength and SNR Lvl indicator

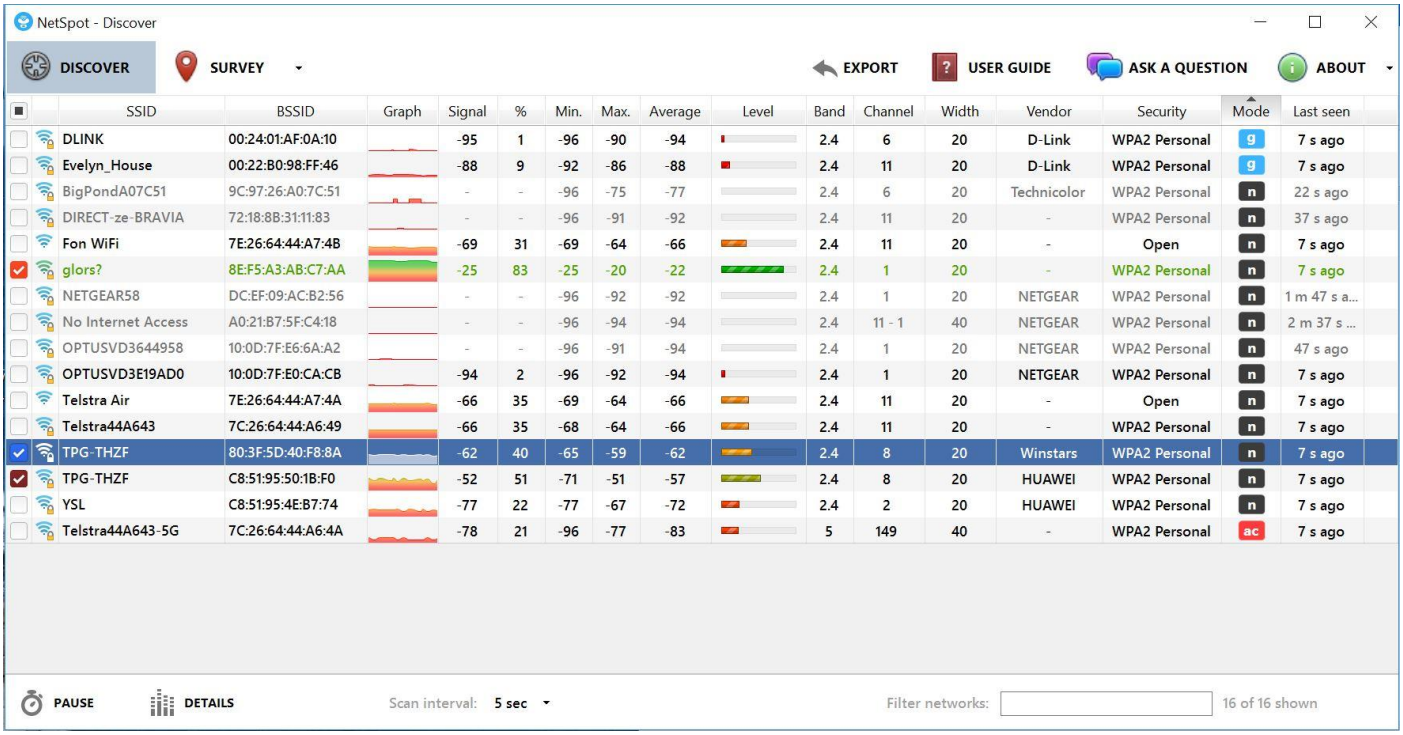

Diagram3: Screenshot of Netspot in 1 of the locations

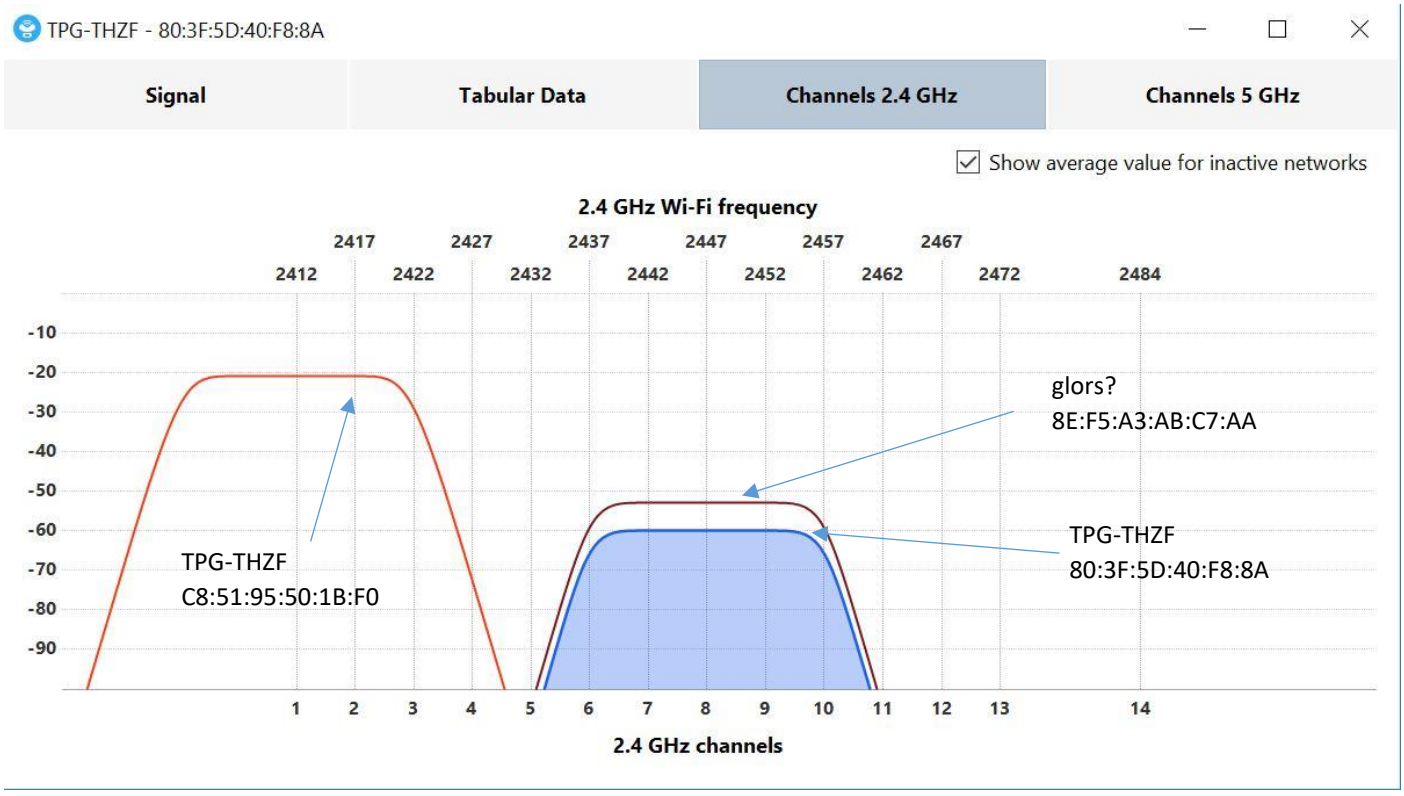

Diagram4: Available APs with channels of 2.4GHz

AP1

SSID: glors?
MAC Address: 8E:F5:A3:AB:C7:AA
802.11: n
Band: 2.4GHz
Channel: 1

Location No.	Signal Strength (dBm)	SNR
1	-95	
2	-74	
3	-55	
4	-56	
5	-60	
6	-77	
7	-78	
8	-89	
9	-90	
10	-89	
11	-81	

Table 1: Signal Strength and SNR Level for AP1

Diagram 5: Heatmap reflecting signal strength and SNR level for AP1

AP2

SSID: TPG-THZF
MAC Address: C8:51:95:50:1B:F0
802.11: n
Band: 2.4GHz
Channel: 8

Location No.	Signal Strength (dBm)	SNR
1	-61	
2	-56	
3	-70	
4	-78	
5	-75	
6	-66	
7	-60	
8	-71	
9	-79	
10	-81	
11	-72	

Table 2: Signal Strength and SNR Level for AP2

Diagram 6: Heatmap reflecting signal strength and SNR level for AP2

AP3

SSID: TPG-THZF
MAC Address: 80:3F:5D:40:F8:8A
802.11: n
Band: 2.4GHz
Channel: 8

Location No.	Signal Strength (dBm)	SNR
1	-74	
2	-67	
3	-44	
4	-53	
5	-50	
6	-65	
7	-67	
8	-76	
9	-78	
10	-82	
11	-72	

Table 3: Signal Strength and SNR Level for AP1

Diagram 7: Heatmap reflecting signal strength and SNR level for AP3

Analysis

1. Channel Occupancy

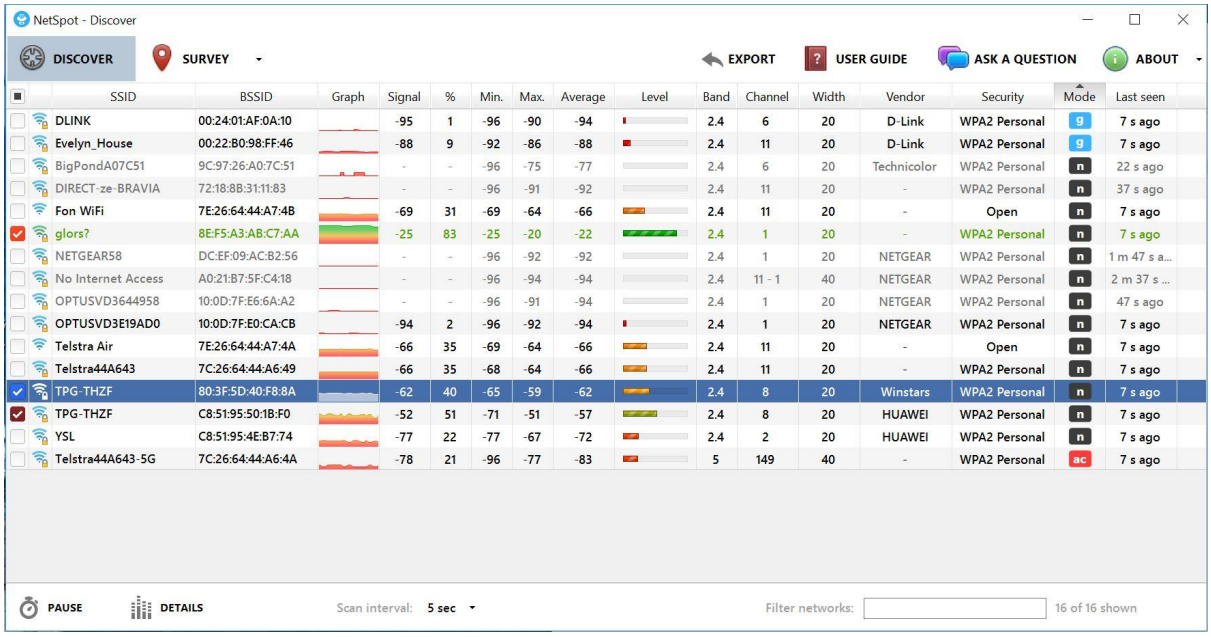

Diagram 8: Screenshot of Netspot

By analysing Diagram 8, there is co-channel interference where 2 or more devices are using the same channel. For example, both devices with SSID “TPG-THZF” are occupying Channel 8. This means that each device must compete with each other for talk time. The more devices on a channel, the longer a device must wait for its turn to talk (metageek, n.d.).

For no overlap to occur in a 2.4GHz spectrum, only Channels 1,6 and 11 are selected. However, based on the screenshot, “TPG-THZF” is occupying Channel 8. This means that there is an overlap, and adjacent channel congestion occurs. Adjacent channel congestion is not encouraged as data corruption can occur when APs transmit data at the same time over shared frequency space (Coleman, 2012).

2. Interference of Materials on Signal Strength

Based on the surveyed area, only locations 1 and 2 are separated by brick walls. As seen in the data collected for the 3 APs, there is obvious attenuation between the 2 locations (Table 4).

AP Number	Location 1 Signal Strength (dBm)	Location 2 Signal Strength(dBm)	Difference
1	-95	-74	21
2	-61	-56	5
3	-74	-67	7

Table 4: Signal strength difference between location 1 & 2

For other locations, they are separated by internal walls, which use plaster boards instead of bricks. As seen in locations 7 and 8, there is slight attenuation in signal strength compared to brick walls (Table 5).

AP Number	Location 7 Signal Strength(dBm)	Location 8 Signal Strength (dBm)	Difference
1	-78	-89	11
2	-60	-71	11
3	-67	-76	9

Table 5: Signal strength difference between location 7 & 8

However, generally the locations in the garage are weak as they are far from the APs' locations. For locations 2 and 3, they are separated by a line of kitchen cabinets. It can be seen that there is also attenuation between the 2 locations (Table 6).

AP Number	Location 2 Signal Strength (dBm)	Location 3 Signal Strength (dBm)	Difference
1	-74	-55	19
2	-56	-70	14
3	-67	-44	23

Table 6: Signal strength difference between location 2 & 3

3. Coverage

Looking at the floor plans for each AP, the signal strength and SNR in the living room is strongest. However, Room 1, Room 2 and the garage only receives medium to low signal strength.

In this case, it would be better if 1 of the APs are positioned at Room 1 or 2 (near location 7) instead of the living room. This will ensure that the signal strength across the whole floor plan can receive at least medium signal strength.

4. Attenuation Caused by Body

The signal strength of AP1 at location 3 was measured with my body facing the router. After that, I turned around so that my back was facing the router, and I measured the signal strength again.

It is found that the signal strength changed from -55dBm to -63dBm. This means that there is attenuation caused by the body as signal becomes weaker as they travel through a medium. This also explains how signal strengths reduce when passing through walls/doors etc. However, the degree of attenuation will be different as it is based on the material of the medium.

Part2: Cybersecurity

Article title: Phishing with Unicode Domains by *XuDong Zheng*

1. Write a short summary of the news item in your own words (between 50 and 200 words).

The article by Xudong Zheng talks about Internationalised Domain Name (IDN) Homograph attacks. He started off by introducing Punycode, which enables non-Latin domain names to be registered in the range of limited ASCII characters. For example, it is possible to register domains such as "xn--pple-43d.com"(Punycode), which is equivalent to "apple.com" (Zheng, 2017). However, the 'a' is Cyrillic compared to ASCII 'a'. Because of this, users unknowingly enter false websites where they may provide their credentials to the wrong people who are seeking to exploit that information. The article then carries on to describe the efforts made by mainstream web browsers such as Chrome, Firefox, Internet Explorer and Opera to provide more security to its users. Fortunately for Safari, the fonts between Latin letters and other languages are different, allowing users to identify fraudulent websites more easily (Zheng, 2017). Lastly, Zheng advises users to protect themselves by either manually typing in the website URL into browsers or navigate to websites through search engines.

2. Identify which software, hardware or system is affected (max 50 words).

Main stream web browsers such as Google, Firefox and Opera are affected. Among these, Google and Opera has released security patches to beef up security – Chrome 5 and Opera Stable 44.0.2510.1449 (Kumar, 2017). Fortunately, Safari, Internet Explorer and other less mainstream browsers are not affected (Sulleyman, 2017).

3. Describe how the problem was discovered and how it was initially published (write 50-100 words).

The problem was made known to public by a blogpost written by web developer XuDong Zheng on April 14 ,2017. A proof of concept example was demonstrated by Zheng himself to recreate awareness on IDN homograph attacks. He created a fake version of apple.com, which appears to be a genuine site but the actual URL is "xn—80ak6aa92e.com". Zheng (2017) states that the bug was reported to Chrome and Firefox on January 20, 2017.

4. 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).

The attack is very serious as users who are not up to date regarding this matter will be unaware that have entered a malicious site. Even for those who are aware, it is a hassle to ensure each site they have entered is secure by checking the registered domain name of the website.

Hackers can exploit the problem by displaying fake website domain names of legitimate services, such as Apple, Ebay, Google etc. If so, credentials of a user/organisation or other sensitive information may be stolen (Kumar, 2017) for the wrong reasons such as identity theft or financial theft.

On a technical level, browsers should implement more complex and wholesome security algorithms for detecting unusual domain names. For example, Chrome has rolled out some solutions to counter the problem, one of them being: If a site from domains like '.com' or '.net' are loaded but if its domain name contains Cyrillic characters, it will be blocked as a dangerous site (Brant, 2017). Web browsers should also provide an option for users to view their browsers in Punycode. Moreover, web browsers should always update their IDN policies so that the public is updated on the latest measures to protect themselves.

For human behaviour, users should manually enter the domain name into the browser or navigate to the desired page through a search engine (Zheng, 2017). Users should avoid randomly accessing sites found on the web such as emails or social media platforms. Moreover, users should use password managers. This is because password managers will not autofill a password from a domain that is not exactly the correct one (Google Chrome, n.d.).

On a policy level, an education campaign should be implemented to increase the awareness of cyber threats to the public. Also, more funding should be provided for cybersecurity research to boost the interest of researchers to enter this field of Information Technology. Lastly, programmes providing rewards should be given to hackers that successfully penetrate a system through safe environments.

References

Brant, T. (2017). *Chrome Blocks Crafty URL Phishing Method*. Retrieved from PC Mag: http://au.pcmag.com/antiphishing-products/47566/news/chrome-blocks-crafty-url-phishing-method

Coleman, D. (2012). *WI-FI BACK TO BASICS | 2.4 GHZ CHANNEL PLANNING*. Retrieved from Aerohive : http://boundless.aerohive.com/experts/wi-fi-back-to-basics--24-ghz-channel-planning.html

Google Chrome. (n.d.). *IDN in Google Chrome*. Retrieved from Chromium: https://www.chromium.org/developers/design-documents/idn-in-google-chrome

Kumar, M. (2017). *This Phishing Attack is Almost Impossible to Detect on Chrome, Firefox and Opera*. Retrieved from The Hacker News: http://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html

metageek. (n.d.). Retrieved from Why Channels 1, 6 and 11?: http://metageek.com/training/resources/why-channels-1-6-11-2.html?utm_expid=190328-189.BCYMV3QrTsW_lMQM0PlqcA.1&utm_referrer=https%3A%2F%2Fwww.google.com.au%2F

Sulleyman, A. (2017). *Imperceptible Internet Scam to Trick Google Chrome Users to Visit Dodgy Websites Returns*. Retrieved from Independent: http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-chrome-scam-websites-url-non-latin-characters-undetectable-a7695886.html

Zheng, X. (2017). *Phishing with Unicode Domains*. Retrieved from xudongz: https://www.xudongz.com/blog/2017/idn-phishing/