An Analysis Of Wi-Fi Security Vulnerabilities In Malaysia: A Survey In Golden Triangle Kuala Lumpur

M. S. Sajat*, S. Hassan and S.C. Chit
Department of Computer Sciences, Faculty of Information Technology
Universiti Utara Malaysia
06010, Sintok, Kedah, Malaysia
Email : {mohdsamsu@yahoo.com}*, {suhaidi, chareen}@uum.edu.my

Abstract - The widespread use of Wi-Fi in the US and Europe has brought a new security concern among Wi-Fi owners and developers. However this concern and awareness are still low in Malaysia. A survey using the NetStumbler and a GPS receiver to locate the coordinates of detected Wi-Fi APs was carried out in the Golden Triangle area of Kuala Lumpur, Malaysia. This paper will describe how far the owners and administrators in Malaysia secure their Wi-Fi networks and subsequently create security awareness among Wi-Fi owners and administrators.

1. INTRODUCTION

The rapid development of wireless network and communication has resulted in the emergence of new technologies such as WiFi, GPRS, 3G, Bluetooth, and WiMAX. Blouetooth is a wireless technology for the Personal Area Network (PAN). It is usually used for short range, ad hoc communication between devices and computers. A PAN may also be used to enable connectivity to a larger local area network (LAN), wide area network (WAN), or the Internet. GPRS and 3G are two technologies for voice and data communication for mobile devices. GPRS is widely used in Malaysia whereas 3G is still in its early implementation by two companies that have been given the license to run the service. WiMAX, a newly introduced wireless technology is a Wireless Metropolitan Area Network (WMAN). WiFi is a popular wireless LAN technology widely used in most Cybercafés, hotels, airports, and institutions of higher learning . PCs, notebooks and PDAs that are equipped with wireless adapter can access the LAN through a base station or access point. One important issue needs to be addressed in using WiFi is its security. This paper will describe out how far is Wi-Fi in Malaysia vulnerable to intruders.

1.1 Motivation

The intrusion and virus attack of a wireless network brings a lot of problems to wireless network administrators. The Incident Statistics 2005 (Fig. 1) reported by NISER (2005) shows that intrusion is the highest incident in Malaysia. Utusan Malaysia (2003) reported that virus threat is now spreading to Wi-Fi networks. Therefore this paper seeks to provide a statistical analysis of the many access points which are currently deployed in the Golden Triangle Kuala Lumpur, and to map the location of the unsecured access points on the wardriven area.

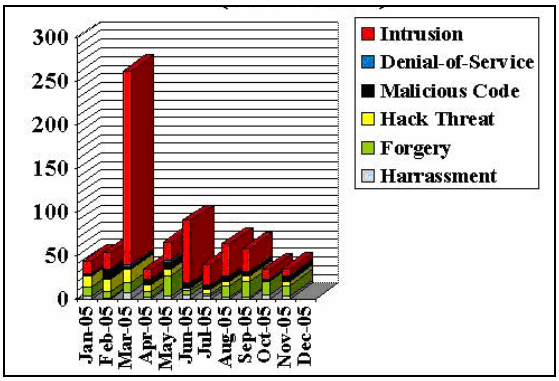

Figure 1: Incident Statistic November 2005 (MyCERT/NISER, 2005)

The remainder of this paper is organized as follows. The next section gives a brief overview of the Wi-Fi technology, Section III gives an overview of Wi-Fi Security, Section IV describes the experiment settings, Section V presents and discusses the results, and concluding remarks follow in Section VI.

2. Wi-Fi TECHNOLOGY

Wi-Fi is the short form for ***Wi**reless **Fi**delity* and is meant to be used generically when referring of any type of 802.11 network,

1-4244-0220-4/06/$20.00©2006 IEEE

whether 802.11b, 802.11a, dual-band, etc.

Any products tested and approved as "Wi-Fi Certified" by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. Typically any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 11g, 5GHz for 802.11a) will work with any other, even if not "Wi-Fi Certified."

Many experts predict that the current mass of Wi-Fi installations in the U.S. and elsewhere could quickly expand to millions of access points representing even more millions of potential users. For instance, the Canadian wireless industry observers predicted that wireless access points will double every two years. According to a report by Pyramid Research, the number of individuals using Wi-Fi by 2008 will go up to 707 million from 12 million in 2003 (news.com, 2003).

Wi-Fi's impact in Malaysia and Singapore will be multiplicative, that of creating bigger broadband networking opportunities for all participants even though it cannot replace wired or mobile network. It will be synergic and not competitive to existing telecommunications technology (Resource4Business, 2005).

3. Wi-Fi SECURITY

Wireless networks are vulnerable to attackers and not only it harms the owner of Wi-Fi networks, it will also bring threat to the security of the country as a whole. According to a report by Wired News (2005), the US Department of Homeland Security labels Wi-Fi as a terrorist threat. The US government warns companies and individual of Wi-Fi owners to secure their Wi-Fi or else the US government will regulate the Wi-Fi.

There are many ways to secure the Wi-Fi networks. Some of them are discussed here including SSID, WEP, WPA, WPA2, EAP, 802.1x, RADIUS, and MAC address filtering.

3.1 SSID

Short for ***S**ervice **S**et **Id**entifier*, a 32-character unique identifier attached to the header of packets sent over a Wi-Fi that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one Wi-Fi from another, so all access points and all devices attempting to connect to a specific Wi-Fi must use the same SSID. A device will not be permitted to join the Basic Service Set(BSS) unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. For a minimum Wi-Fi security, SSID broadcast should be disabled to hide the AP from the public.

3.2 WEP

The **W**ired **E**quival ent **P**rivacy - WEP is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

3.3 WPA

Wi-Fi Protected Access - WPA is a powerful, standards-based, interoperable security technology for Wi-Fi networks. It provides strong data protection by using encryption as well as strong access controls and user authentication. WPA can be enabled in two versions — WPA - Personal and WPA - Enterprise. WPA - Personal protects unauthorized network access by utilizing a set-up password. WPA-Enterprise verifies network users through a server by utilizing a 128-bit encryption keys and dynamic session keys to ensure wireless network's privacy and enterprise security

3.4 WPA2

The Wi-Fi Protected Access 2 (WPA2) provides network administrators with a high level of assurance that only authorized users can access the network. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm.

WPA2 can be enabled in two versions — WPA2 - Personal and WPA2 - Enterprise. WPA2 -Personal protects unauthorized network access by utilizing a set-up password. WPA2 - Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

1-4244-0220-4/06/$20.00©2006 IEEE

3.5 EAP

Extended Extensible Authentication Protocol (EAP) is an addition to the Wi-Fi Protected Access-(WPA™) and WPA2™-Enterprise certification programs, which further ensures the interoperability of secure Wi-Fi networking products for enterprise and government users

3.6 802.1x

The Wi-Fi Alliance, the IEEE 802.11 standards committee and many Wi-Fi members are working to develop new security standards such as 802.11i and 802.1x . These new security standards will use advanced encryption technologies such as AES and TKIP, as well as secure key- distribution methods. Hackers can break encryption codes by intercepting and analyzing large amounts of data, but breaking codes takes time. By automatically "changing" the encryption keys every five minutes or so, the Wi-Fi network is already using a new code by the time a hacker has managed to intercept and crack the old one. Most enterprise-level Wi- Fi networks already enable IT managers to change the codes manually, but 802.1x makes the process automatic

3.7 RADIUS

Remote Access Dial-Up User Service - RADIUS is another standard technology that is already in use by many major corporations to protect access to wireless networks. RADIUS is a user name and password scheme that enables only approved users to access the network; it does not affect or encrypt data. The first time a user wants access to the network, secure files or internet locations, he or she must input his or her name and password and submit it over the network to the RADIUS server. The server then verifies that the individual has an account and, if so, ensures that the person uses the correct password before she or he can get on the network.

3.8 MAC Address Filtering

As part of the 802.11b standard, every Wi-Fi radio has its unique Media Access Control (MAC) number allocated by the manufacturer. The MAC control works like "call blocking" on a telephone: if a computer with an unknown MAC address tries to connect, the access is denied.

However it is possible for a dedicated hacker to "spoof" a MAC address, by intercepting valid MAC addresses and then programming his or her computer to broadcast using one of those. Despite that, for small network installations, using a MAC filtering technique can a be very effective method to prevent unauthorized access.

4 EXPERIMENT SETTINGS

The research is done using the wardriving technique. The area to be covered in this research is in the golden triangle area of Kuala Lumpur, Malaysia. It specifically focuses on Wi-Fi located along Jalan Sultan Ismail, Jalan Bukit Bintang, Jalan Pudu, Jalan Tun Perak, Jalan Tuanku Abdul Rahman and Jalan Ampang (Fig. 2).

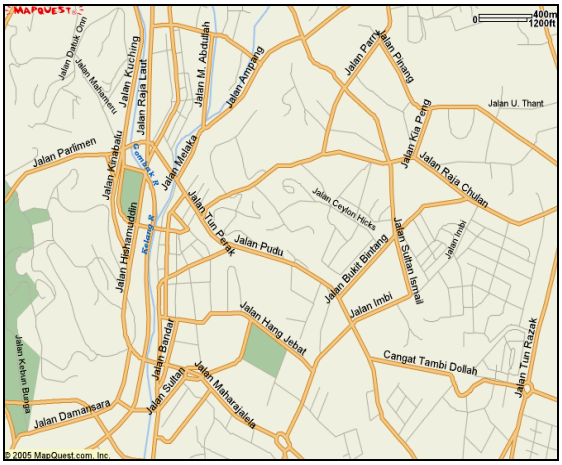

Figure 2: Golden Triangle, Kuala Lumpur (MapQuest 2005).

These locations are chosen since many large corporations are housed here. The survey is conducted for one week from 11.00 am to 5.00 p.m.. The NetStumbler is used to detect Wi-Fi and create a log file to record the findings. This time period is chosen since it is the working hours in Kuala Lumpur. Most offices and shops are open within that period.

The wardriving activities are conducted daily between 23 January 2006 until 29 January 2006 covering all targeted areas. A GPS receiver is used to locate the longitude and latitude of the Wi-Fi detected by the NetStumbler. The *Garmin GPS 18 PC* is used along the NetStumbler and is connected via the RS-232 serial port of the laptop. The setup of equipment used in this

1-4244-0220-4/06/$20.00©2006 IEEE

research is shown in Figure 3.

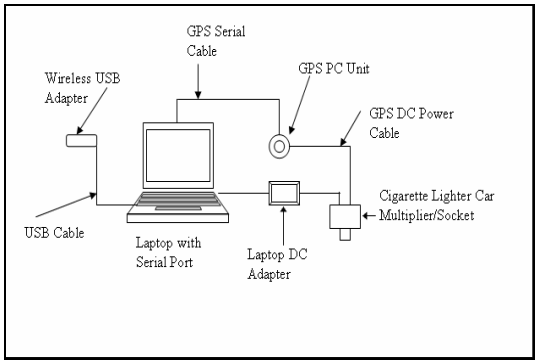

Figure 3 : Wardriving equipment setup

4.1 The Process Flow

The process flow of this research is shown in Figure 4 which begins with scanning the AP, followed by logging and saving the collected data, extracting the data, analyzing it and lastly mapping the location of the detected Wi-Fi.

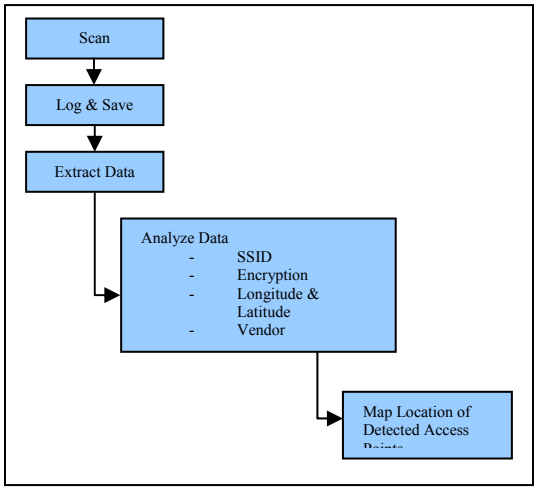

Figure 4 : Process of Scanning, Locating and Mapping Access Points

In this research, a summary was extracted from the NetStumbler. This data was then exported to Microsoft Excel that was used as raw data for analysis purposes.

5 FINDINGS & DISCUSSIONS

The collected data has been analyzed and the overall result shows that Wi-Fis in Malaysia are still vulnerable to intrusions as securty level is considerably low. This findings however does not consider the security measures taken by some of the Hotspot providers such as the usage of RADIUS server which redirects users to login page and requires users to login before being able to access the network or the Internet. The total number of detected Wi-Fi is 251 of which 8 are adhoc Wi-Fi or peer networks.

5.1 Encryption

The encryption method shown by NetStumbler is only the WEP even though the actual encryption method used could be other than WEP such as WPA and WPA2.

Table 1: WiFi Encryption Status

Encryption status	Frequency	Percentage
On	140	55.78
Off	111	44.22

The result in Table 1 shows that more than 40% or nearly half of the scanned Wi-Fi AP are not protected by any encryption method. This percentage is still considered quite high even though other wardriving results in USA are reaching 50%.

5.2 SSID

The SSID is also one of the factors that contribute to the vulnerability of Wi-Fi in Malaysia. More than 80% of SSIDs were broadcasted. Only 12% of the SSIDs were not broadcasted.

Table 2: SSID Status

SSID		Frequency	Percentage
Broadcasted	Default	31	12.3
	Non-default	190	75.7
Not broadcasted		30	12

5.3 Security Vulnerabilities

Based on the analysis of SSID and WEP above, a Security Level of Wi-Fi in Malaysia has been made. Level 1 is the lowest and the most vulnerable to intruders. It consists of 21 Wi-Fi APs or 8.4%. This number is considered small. Level 2 which composed of 34.3% is also considered very vulnerable because today's Wi-Fi clients can easily connect to the AP even though the default SSID has been changed. Level

1-4244-0220-4/06/$20.00©2006 IEEE

3 is considered secured from ordinary users because it needs sniffer softwares to capture the SSID. Only crackers equipped with sniffer like Ethereal or CommView can capture the SSID and eventually connect to the APs. Level 4 and 5 which composed 51.4% of the total detected Wi-Fi are less vulnerable compared to Level 3 and below. It is because the encryption key is difficult to break and often consumes a much longer time.

From the 251 Wi-Fis detected, only 26 or 10.3% of them are categorized at Level 6 which is considerd the least vulnerable to intruders. Without SSID being broadcasted and the encryption is on, it will be very difficult for any intruder to get into the network.

Table 3: Wi -Fi Security Measures categorized into Six Levels

Level	Security measures	Frequency	Percentage
1	Broadcast SSID, Default SSID, Encryption Off	21	8.4
2	Broadcast SSID, Non-Default SSID, Encryption Off	86	34.3
3	Not Broadcast SSID, Encryption Off	4	1.6
4	Broadcast SSID, Default SSID, Encryption On	10	4
5	Broadcast SSID, Non-Default SSID, Encryption On	104	41.4
6	Not Broadcast SSID, Encryption On	26	10.3

5.4 Channel

There are 11 channels (channel 1 to 11) detected being used by APs in Kuala Lumpur. Channel 1, 6 and 11 are the most used channels. Only 1 AP is detected using channel 2. From this finding it can be concluded that, most Wi-Fi owners and administrators are using channel 1, 6 and 11 which are the default channels used by most vendors in 2.4 GHz spectrum.

Table 4: Channels used by APs

Channel	Frequency	Percentage
1	38	15.1
2	1	0.4
3	6	2.4
4	7	2.8
5	5	2.0
6	85	33.9
7	8	3.2
8	8	3.2
9	9	3.6
10	7	2.8
11	77	30.7

5.5 WiFi Locations

The mapping of Wi-Fi locations is done with the help of GPSVisualizer.com. Figure 5 shows the location of Wi-Fi detected in Golden Triangle Kuala Lumpur. The red pins are the encrypted Wi-Fis whereas the greens are the open Wi-Fis. Most Wi-Fis are located around KLCC and Bukit Bintang area. The closed or encrypted Wi-Fi are mostly found around the KLCC area. Internet surfers can zoom onto the desired location using the zoom button on the website. Apart from that, the surfers can also navigate on the map using the navigation button.

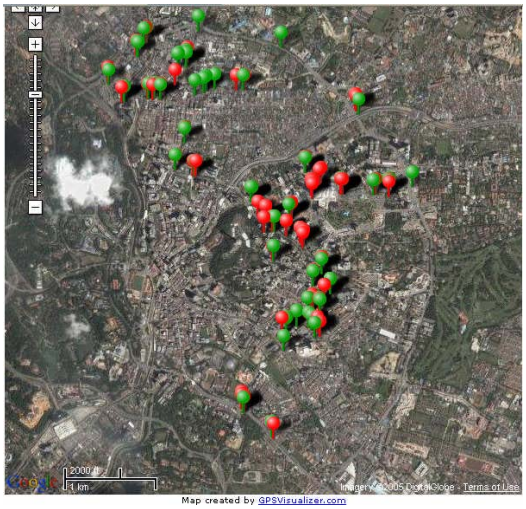

Figure 5: Locations of Wi-Fi APs in the Golden Triangle Kuala Lumpur, Malaysia

6.0 CONCLUSION

In conclusion, this study was carried out to make companies and Wi-Fi owners aware of their own security lapses. The objective of this research to provide statistical analysis of Wi-Fi in Malaysia particularly the Golden triangle Kuala Lumpur has been achieved together with two other objectives which are mapping the unsecured

1-4244-0220-4/06/$20.00©2006 IEEE

Wi-Fis and publishing the findings on the Internet. The scope and research methodology discussed above have been able to achieve the stated objectives. This research or study could be enhanced and cover a bigger area in the future so that the unawareness among Wi-Fi owners of their Wi-Fi security could be reduced and hence could make wireless network safer and convenient to use.

REFERENCES

[1] Carter, B. & Shumway, R(2002). Wireless Security: End to End**.** New York: John Wiley & Sons.

[2] Coffer.com(2006). *Vendor/Ethernet MAC Address Lookup and Search*. Retreived from http://www.coffer.com/mac_find/?string=00%3A13%3A19

[3] Fifield, Tom (2006) *Wireless Default settings* Retreived from http://www.gummay.net/kbase.php?category=Wireless

[4] Howard, David (2002). It's a Wi-FiWorld :Wireless broadband may finally be ready for prime time, *ACM Computer*, Jul. 2002.

[5] Intel (2006), *Wireless Universal Serial Bus(WUSB)*. Retrieved from http://www.intel.com/technology/comms/wusb/index.htm

[6] Jpatokal(2005). Kuala Lumpur. Retrieved from http://wikitravel.org/en/Kuala_Lumpur

[7] MapQuest (2005), *Map of Kuala Lumpur*. Retrieved from http://www.mapquest.com/maps/map.adp?city=Kuala%20Lumpur&state=&address=&zip=59100&country=MY&zoom=5

[8] Mohd Ridzwan Md. Iman (2003,May). Ancaman virus ...kini menular ke rangkaian WiFi. *Utusan Malaysia*. Retrieved from http://www.utusan.com.my/utusan/content.asp?y=2003&dt=0528&pub=Utusan_Malaysia&sec=Megabait&pg=me_01.htm

[9] MyCERT/NISER (2005). Incident Report. Retreived from http://www.mycert.org.my

[10] Netstumbler.org (2006)*Step-by-step guide for making DiGLE/JiGLE compatible mappacks, via GPSVisualizer.com.* Retrieved from http://www.netstumbler.org/showthread.php?t=10935

[11] NOP World Technology(2001) .*Wireless LAN Benefit Study*. New York: Cisco. Pahlavan, K., & Levesque, A (1995). *Wireless Information Networks*. New York: J. Wiley & Sons, Inc.

[12] Rappaport T. (2000). *Wireless Communications: Principles & Practice*. New Jersey: Prentice Hall.

[13] Resource4Business (2005).*Future of Broadband Wireless Access Technology :Wi- Fi, Malaysia & Singapore 2006-12, Nov. 1, 2005*

[14] Reynolds, J.(2003). *Going Wi-Fi: A Practical Guide to Planning and Building an 802.11 Network.* New York:CMP Books.

[15] Rittinghouse, J. & Ransome, J.(2004). *Wireless Operational Security* New York: Digital Press**.**

[16] Schneider, Adam (2006) *Draw a map from a WiFi log file.* Retreived from http://www.gpsvisualizer.com/map?form=wifi

[17] Shipley, Pete(2005). Retrieved from http://www.dis.org/ Shipley

[18] S.J. Vaughan-Nichols(2003), The challenge of Wi-Fi Roaming, *ACM Computer*, Jul. 2003.

[19] Visant Strategies study (2003). 3G and 3G Alternatives: 3G vs. Wi-Fi vs. 4G.

[20] Wall, D., Kanclirz, Jan Jr., Jing, Y., Faircloth, J. and Barrett, J. (2004) *Managing and Securing a Cisco Structured Wireless-Aware Network (SWAN)* New York:Syngress Publishing.

[21] Wi-Fi Alliance (2005). *Learn About Wi-Fi.* Retrieved from http://www.wi-fi.org/OpenSection/index.asp

[22] Wireless LAN Security: 802.11(2006). *Wardriving & Warchalking***.** Retrieved from http://www.wardrive.net/wardriving/tools

[23] Yee, J. & Pezeshki-Esfahani, H.(2002). Understanding Wireless LAN Performance Trade-Offs. *Communication Systems Design* (November 2002)

1-4244-0220-4/06/$20.00©2006 IEEE