



**TX6224: Research Topic**

**FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT  
UNIVERSITI KEBANGSAAN MALAYSIA**

Pusat Pengajian Sains Komputer  
*School of Computer Science*

<b>TX6224:</b> <b>Ethical Hacking and Penetration Testing</b>	<b>SEMESTER 2</b>	<b>SESI 2015/2016</b>
--	-------------------	-----------------------

Lecturer/Instructor:

**Mr Zamri Bin Murah**

<b>NAMA</b>	<b>NO DAFTAR</b>
1. Mahizon Aliah Binti Awang	GP04280
2. Warhamni Binti Jani @ Mokhtar	GP04294

# THE SECURITY STATE USING WIRELESS ENVIRONMENT IN PUTRAJAYA: A STUDY OF PutraWifi WIRELESS ENVIRONMENT IN PRESINT 4

Mahizon Aliah Awang<sup>1</sup>, Warhamni Jani @ Mokhtar<sup>2</sup>

<sup>1</sup>*mahizon@gmail.com*

<sup>2</sup>*warhamni@gmail.com*

**Abstract:** In recent years, the adoption of wireless networks in the corporate and public environments has increasingly deployed. This paper discusses the security state of using wireless networks and outlines the best practices for deploying wireless networks in corporate and public environments. Analysis on wireless traffic offers various resolutions for forensics as similar to wired traffic analysis however there are added signatures from the 802.11x protocol. One of the purposes of forensics study on wireless traffic is to allow investigators to identify a computer security incident. The tools that are commonly used can be commercial or open source such as Kismet and Wireshark to name a few. These tools can assist in monitoring the wireless traffic and analysing the traffic using captured data. It is important to examine the applicability of wireless networks for information processing in a corporate and public environment. Finally suggestive recommendation or best practices of security is provided as operation guidelines for organisation and users to ensure effectiveness and security while using the public wireless networks.

**Keywords:** Wireless Networking, Network Sniffing, Security, Wireshark, IEEE802.11n.

## INTRODUCTION

The rapid evolution of wireless network in last few years was believed due to the expansion of new wireless standard and cost-effective wireless hardware. It becomes a preferred adoption of the technology especially for home and small business. Mashhour, A. S., & Saleh, Z. (2013) states that with the growth of wireless networking, security is the main weakness of the whole wireless system, which results in improper uses of network resources. As wireless access increase, securities become an even more alarming issue due to its convenient functionality, portability and accessibility. However, there are pro and cons by using wireless networking which can also gave bad impact especially for negligence users.

This paper was intentionally focused on analysis of traffic sends through the PutraWifi wireless network in Presint 4, Putrajaya. Presint 4 was one of the Presint in Putrajaya that have good coverage of PutraWifi wireless networking. PutraWifi was using IEEE 802.11n standards. IEEE 802.11n is a wireless network standard that providing connectivity to multiple transmitter and receiver antennas to increase the data rate [1]. This is the most common wireless LAN implementation, and is used everywhere from corporate networks to hotspot environments and high-security government institutions. Each wireless AP is uniquely identified by the Basic Service Set Identifier (BSSID). The BSSID is found in the IEEE 802.11 header and present in every data or management frame transmitted by a wireless station or an AP to uniquely identify the wireless LAN.

We feel that this is suitable for research because we want to know the security state of using PutraWifi and its impact to user. During the analysis, Wireshark act as a tool for network sniffing and information gathering, Kali Linux as the Operating System and TP-Link as the wireless adapter. Information from wireless access points are collected anonymously without connecting directly to any network. By respect to laws and ethical standard, we have disabled our wireless network connection and focusing solely on using the wireless adapter. With the TCP-IP stack disable, a connection to this wireless network is never established.

## PUTRAWIFI TODAY

PutraWifi is a network infrastructure services provided by the Federal Government Administrative Centre of Malaysia for government agencies in Putrajaya [12]. PutraWifi provide internet and wireless secure intranet access to government application and internal application for government employee in Putrajaya. PutraWifi can also support multiple of devices in all state including smartphone. It is one of the initiatives under the NKEA programme in CCI (Content and Communication Infrastructure) sector in order to make Putrajaya a reference model for government connectivity. The PutraWifi project was started to ensure ubiquitous Wi-Fi connectivity. Each Government employee has been provided a unique ID which can now be used at 13 premises within Putrajaya [12].

As part of the Government initiative as stated above, they have divided into two main wireless networks namely PutraWifi-Staff and PutraWifi-Guest respectively. PutraWifi-Staff are provided for valid and registered user in Putrajaya while the PutraWifi-Guest is open for public with username and password given on the login page. However the PutraWifi are limited to certain webpages that not included in content filtering by MAMPU based on Pekeliling Kerajaan Pentadbiran Awam Bilangan 1 Tahun 2003. PutraWifi also provide WPA encryption

as the communication is done with the air media to provide security and awareness. Figure 1 shows the network architecture and the tabular of APs for PutraWifi [12].

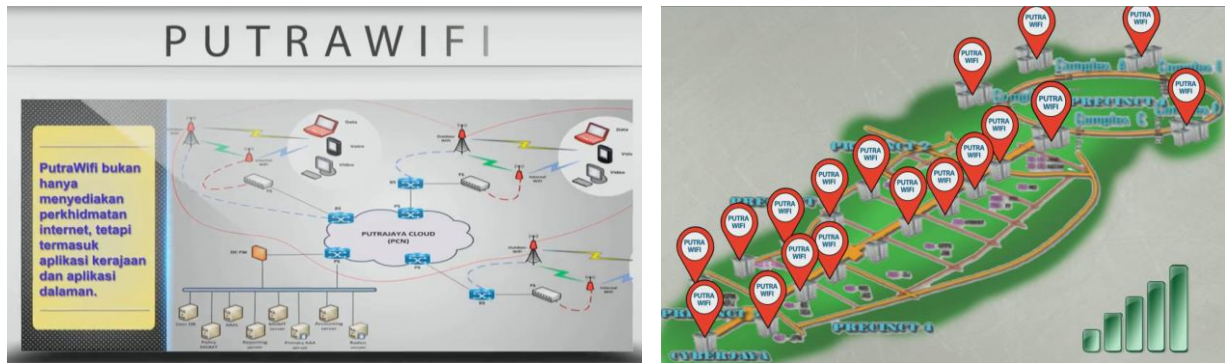


Figure 1. PutraWifi Network Architecture and Tabular [12]

## TEST SETUP AND METHODS

The goal of traffic analysis is to collect and analyse traffic information transmitted via PutraWifi for security and information gathering of wireless networks. On the other hands, traffic analyses also have potential to be exploited by attackers to threaten user privacy in wireless networks. As an example, a user's online activities may be exposed to strangers, even if the traffic is encrypted. If the hackers are determined, it is not possible for them to gather and profile the intended victim's activity.

### A. Test Setup

In order to get the sufficient wireless network information regarding PutraWifi, the network packet traffic was collected starting from 3rd to 4th May 2016 at 9.00 a.m. until 11.00 a.m. respectively [10]. It is believed to be the most effective time to capture due to most government servants are currently at working hour thus the information will be adequate for the analyse purposes. Based on the records, the packets total byte of number is 312,142 and total numbers of MAC address captured are 2,075. The packet captures will be review later.

### B. Communication Between PutraWifi and Virtual Interfaces Card

- 1) **Configuration:** Wireless card needs to be configured manually into monitor mode for sniffing and capturing purposes [5]. The process includes steps which are : (1) First of all, plug-in the wireless antenna to Kali Linux machine and bring it to the up state. (2) Next, choose the capture interface to open (wlan0) and set the interface to monitor mode. (3) Setting the network software detector (Aircrack-ng) with the interface to start (Airmo-ng wlan0) and when successfully begun the capture, test by sending some packets across the wire. (4) Monitor the traffic capture in Wireshark [6], [11]. Once sufficient number of packets captured, stop and save it for later review and investigation. Wireshark will then use to filter out the network traffic. The steps are shown in Figure 2-5 below.

```
root@kali:~# ifconfig wlan0
wlan0: flags=4096<BROADCAST,MULTICAST> mtu 1500 txqueuelen 1000 (UNSPEC)
RX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# ifconfig wlan0 up
root@kali:~# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
RX packets 1488 bytes 245042 (239.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

Figure 2. Setting the interface for monitoring other than broadcast traffic



- 2) **Traffic Monitoring:** During packet capture, Wireshark monitor and collects Wi-Fi frames. Next, Wireshark have the ability to extracts and analyses certain significant fields such as device identifications (like BSSID or MAC addresses) and received signal strengths. The MAC address or BSSID aims to detect traffic carrying Wi-Fi devices. As described earlier, a Wi-Fi-enabled device actively broadcasts probe request to search available networks. The probe request packet contains the MAC addresses of the device, which serves as an identification of the owner of the device. Wireshark can be used to analyse network data dumps and also capture the data itself.

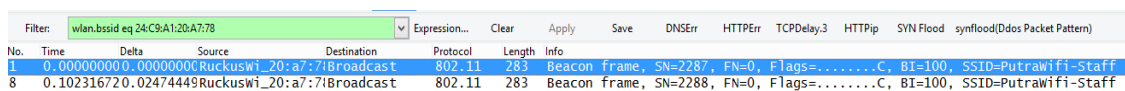
Wireshark captures the 802.11x protocol along with the Logical Link Control (LLC) protocol. The 802.11x network captures will contain the basics of arrival time and capture length [9]. LLC will contain ARP packets, IP packets and TCP segments if the traffic is unencrypted or the encryption key is known. The *current* types of information that Wireshark captures is the source and destination of the packet, transmitter address, source address, receiver address, destination address, BSSID, frame types, protected frame flag (WEP), WEP initialization vector, TKIP IV, CCMP IV, and key identifier.

## FINDINGS AND ANALYSIS

### Packet analysis strategy

There are a few steps used to get the information from the packet capture. We have detailed the steps below and some analysis based on the findings.

#### 1) Filtering the BSSID.



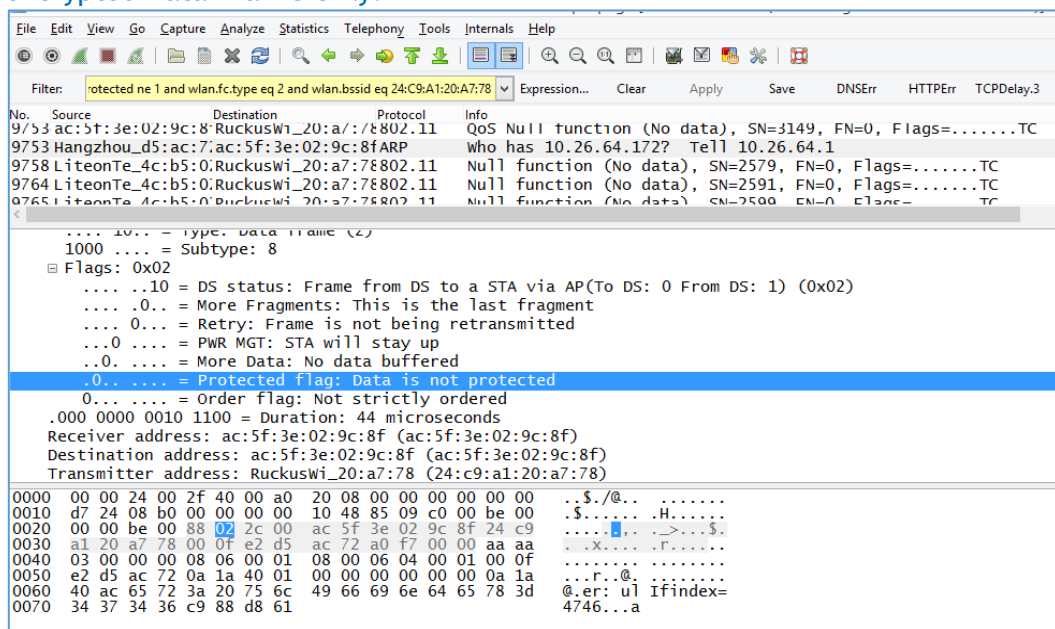
The screenshot shows the Wireshark interface with a filter applied to the BSSID field. The filter is 'wlan.bssid eq 24:C9:A1:20:A7:78'. The packet list shows two packets: a Beacon frame (No. 1) and another Beacon frame (No. 8). The packet details pane shows the structure of the Beacon frame, including the Frame Control, Duration, Address, and Data fields.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	0.000000000	0.000000000	RuckusWi_20:a7:78	Broadcast	802.11	283	Beacon frame, SN=2287, FN=0, Flags=.....C, BI=100, SSID=Putrawifi-Staff
8	0.102316720	0.02474449	RuckusWi_20:a7:78	Broadcast	802.11	283	Beacon frame, SN=2288, FN=0, Flags=.....C, BI=100, SSID=Putrawifi-Staff

Figure 6. Filter BSSID

By using a filter for BSSID we can exclude traffic from any other wireless networking so that we can get only related BSSID for our analysis. So we will then focus on either PutraWifi-Staff or PutraWifi-Guest.

#### 2) Unencrypted Data Traffic Only.



The screenshot shows the Wireshark interface with a filter applied to the Data field. The filter is 'not protected ne 1 and wlan.fc.type eq 2 and wlan.bssid eq 24:C9:A1:20:A7:78'. The packet list shows several packets, including a Data frame (No. 1000) and a Data frame (No. 1001). The packet details pane shows the structure of the Data frame, including the Frame Control, Duration, Address, and Data fields. The Data field is highlighted, showing the raw data bytes.

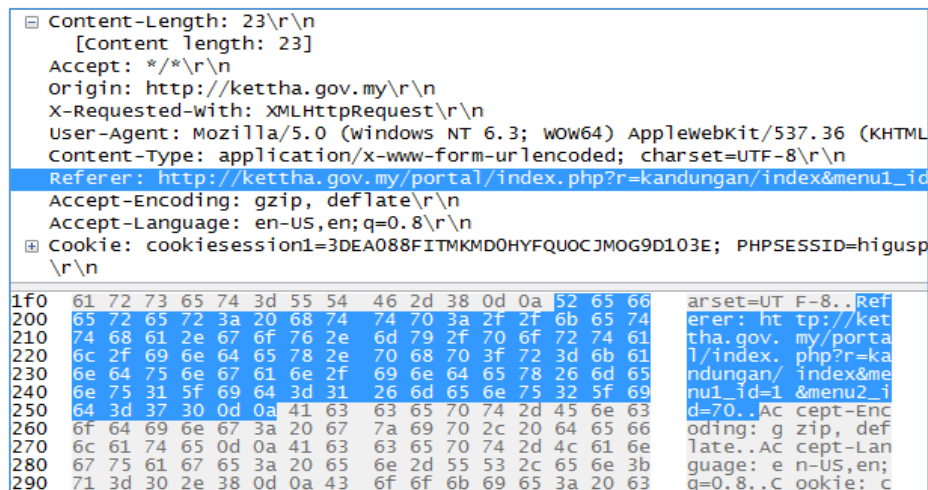
No.	Source	Destination	Protocol	Info
9753	Hangzhou_d5:ac:7f:ac:5f:3e:02:9c:8f	ARP	who has 10.26.64.172?	Tell 10.26.64.1
9758	LiteonTe_4c:b5:0:RuckusWi_20:a7:78	802.11	Null function (No data), SN=2579, FN=0, Flags=.....TC	
9764	LiteonTe_4c:b5:0:RuckusWi_20:a7:78	802.11	Null function (No data), SN=2591, FN=0, Flags=.....TC	
9765	LiteonTe_4c:b5:0:RuckusWi_20:a7:78	802.11	Null function (No data), SN=2599, FN=0, Flags=.....TC	

Figure 7. Filter Data Traffic

This command in Figure 7 above will identify wireless traffic that is not encrypted and unencrypted data frames only. As seen in above figure, flag 02 is considered as 'Data is not protected'. Hacker can use this loophole to manipulate.



### 3) User input interaction.



### Figure 8.Filter Data Traffic

The data in Figure above was easily derived from the packets, as it came from the only HTTP POST command which display the user was updating the content.

#### 4) Top website accesses by users

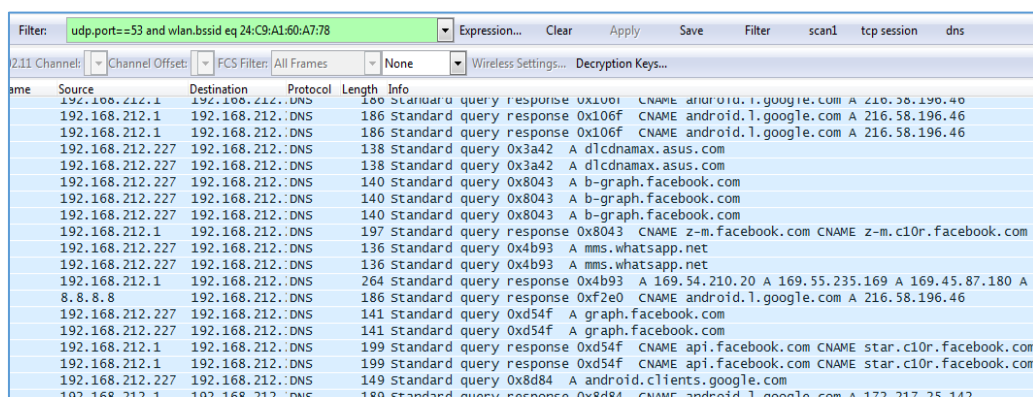


Figure 9. Example of popular site using both PutraWifi-Staff and PutraWifi-Guest

Based on the packet capture, the most popular site are Facebook, Instagram, whatsapp and gmail [2].

During the information drill from the capture packet, there is no password gather inside the packets. In order to test the security of the wireless network, we also have conducted a penetration testing to PutraWifi-Staff BSSID. The tool used is Aircrack-ng (airmon-ng and aireplay-ng) by sending deauthorization packets to reset the handshake. However, the process was unsuccessful.

## RECOMMENDATION AND BEST PRACTICES

Wireless network at any time is exposed to any network sniffing equipment once in the wrong hands. The action of sniffing is considered as a passive network attack as the unauthorized person gains access to an asset and does not modify it [3]. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping [7]. With the growth of wireless communication and wireless networks, more advanced and effective techniques were implemented to exploit the wireless communication systems of all types [4]. New security risks come with the benefits of adopting wireless networks in an organisation [8]. To tackle these risks effectively, various security best practices need to be considered. To help organisations and public understand their wireless network deployments and recommended relevant security best practice, we outline the security issues that require special attention. It is a good start for protecting wireless devices and personal information when attaching to a public wireless networks.

## 1) Operations and Maintenance Guideline for Organization

Firstly, it is important to educate the users about the risks of wireless technology as user awareness will eventually influence users to follow the policy that have been outline. Best practices or security guidelines should be developed in a way ensuring that end-users understand and follow. Next, developing the security configuration standards for access point helps simplify daily operations and attest all access points are protected with appropriate measures and simply follow the standard settings to re-configure the access point. Meanwhile, regular checking of log records must be performed, to ensure the completeness and integrity of all logs. Any irregularities spotted must be reported and organize the investigation if necessary.

## 2) Internet Surfing Via Public Wireless Network Guideline for User

Once a device such as a notebook computer or smartphone devices connected to public wireless network, there is a potential of attacks from remote attackers. Nonetheless, the following best practices listed may prevent users from falling into the traps laid by attackers.

First of all, one of the best practise is user needs to disable wireless connection when it is not in use such as Wi-Fi and Bluetooth as those devices are constantly announcing their presence if they are enabled. Next, protect your device with anti-virus software with the latest virus definitions. This can minimise the risk of infection by computer viruses or spyware. Next, removing preferred network list when using public wireless service. There are some operating systems offers a feature to build the list of preferred wireless networks. Once this list defined, our system will keep searching and try to connect to the preferred network automatically. By capturing this information sent out from our system, an attacker could set up a fake wireless access point, which meets the settings of a wireless network on our preferred network list. In doing so, our device would without doubt automatically connect to the attacker's fake wireless network. Generally, public wireless networks should be considered as insecure network. It is not advisable to transmit sensitive or personal information over a public hotspot without proper security controls to avoid loss and image tarnishing in future.

## CONCLUSION AND FUTURE WORK

In this study, we perform comprehensive analysis on 802.11n network traffic. We capture packet traces from the wireless network environment of PutraWifi. We managed to get basic information of the security state of PutraWifi. However, there is no username or password gathers from the packet capture. This may be due to limited diversity of packet capture. For future work, we suggest to set a worthy timeframe to ensure enough information gathered. In this research we have evaluate the PutraWifi wireless network environment in Putrajaya and found that high percent of it are secured, this research also provides some recommendations and best practises regarding the use of public wireless networking.

## REFERENCES

1. B. Vangie. 802.11 IEEE wireless LAN standards. [http://www.webopedia.com/TERM/8/802\\_11.html](http://www.webopedia.com/TERM/8/802_11.html)
2. Roubos S. D., Casler S., Hedigan J. & Shaw R. (2008). A Study Of Wireless Security Privacy And Forensics. Consortium for Computing Sciences in Colleges, Student Paper E-Journal. [https://works.bepress.com/david\\_costantino/3/](https://works.bepress.com/david_costantino/3/)
3. Gopalakrishnan, S. (2014). a Survey of Wireless Network Security, 3(1), 53-68.
4. Mashhour, A. S., & Saleh, Z. (2013). Wireless Networks Security in Jordan: A Field Study. *International Journal of Network Security & Its Applications*, 5(4), 43-52. <http://doi.org/10.5121/ijnsa.2013.5403>
5. Orebaugh, A., Ramirez, G., Burke, J., Pesce, L., Wright, J., & Morris, G. (2006). Chapter 6 - Wireless Sniffing with Wireshark. In *Wireshark & Ethereal Network Protocol Analyzer Toolkit* (pp. 267-370). <http://doi.org/http://dx.doi.org/10.1016/B978-159749073-3/50011-7>
6. Poddar, V. (2014). A COMPARITIVE ANALYSIS OF WIRELESS SECURITY PROTOCOLS ( WEP and WPA2 ), 4(3), 1-7.
7. Pathan, a. S. K., Lee, H.-W. L. H.-W., & Hong, C. S. H. C. S. (2006). Security in wireless sensor networks: issues and challenges. *2006 8th International Conference Advanced Communication Technology*, 2, 6 pp.-1048. <http://doi.org/10.1109/ICACT.2006.206151>
8. Rubin, A. D. (2003). Wireless Networking Security. *Association for Computing Machinery. Communications of the ACM*, 46(5), 28-30. <http://doi.org/http://dx.doi.org/10.1145/769800.769821>
9. Tietjen, K. (n.d.). Wireless Traffic Analysis. *Discovery*.
10. Yamkhin, D., & Won, Y. (2009). Modeling and Analysis of Wireless LAN Traffic. *Journal of Information Science and Engineering*, 25, 1783-1801. Retrieved from [http://www.dnclab.hanyang.ac.kr/files/publication/journals/international/200911\\_08.pdf](http://www.dnclab.hanyang.ac.kr/files/publication/journals/international/200911_08.pdf)
11. Zhang, F., He, W., & Liu, X. (2011). Defending against traffic analysis in wireless networks through traffic reshaping. In *Proceedings - International Conference on Distributed Computing Systems* (pp. 593-602). <http://doi.org/10.1109/ICDCS.2011.77>
12. Mampu JPM (2014). PutraWifi. <https://www.youtube.com/watch?v=glMyiXKxRes>