Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 4, 2020

Review Article

WIRELESS SECURITY IN MALAYSIA: A SURVEY PAPER

Haitham Ameen Noman[1], Sinan Ameen Noman[2], Qusay Al-Maatouk[3]

[1]Prince Sumaya University, Jordan. h.ani@psut.edu.jo
[2]University of Alabama, United States of America.sanoman@crimson.ua.edu
[3]Asia Pacific University of technology and innovation, Malaysia. qusay@staffemail.apu.edu.my

Received: 25.12.2019 *Revised: 16.01.2020* *Accepted: 11.02.2020*

Abstract
This paper evaluates the wireless 802.11 (WLAN) security of residents in a major city in Malaysia by collecting and analyzing passively data traffic of coffee shops and companies using particular tools on Kali Linux operating system in order to drag people attention to use more secured wireless environment. The paper evidently shows the lack of security awareness among people which may expose their privacy to threats.

Keywords: Wireless, Security, Survey.

DOI: http://dx.doi.org/10.31838/jcr.07.04.57

INTRODUCTION

With the advent of online social networking and the evident evolution of mobile devices there has been an obvious trend and need among people to access those web services very frequently from different places due to many reasons like smart devices operating systems usability, friendly GUI also the reliable services provided by them not to mention the instinct need for people to be always connected with their friends and loved once in simple way [1]. As a consequence, most of the popular social networking websites started to transform into mobile domain by providing varies types of applications and games designed exclusively for their devices. Gradually in a short time these smart phones devices transformed into mini fully functionalized computers that allow the user to store personal data like passwords, personal notes, photos, calendar events and even bank account details which naturally turn out to be precious bounties and attractive target to malicious hackers [2].

On the other hand the wireless 802.11 networking standard, also known as, "Wireless Ethernet", Wi-Fi, and Wireless LAN has become very popular and essential component in our life, despite of its effectiveness in carrying large amount of data and the layers of security that has been added recently to secure this technology yet it still has many vulnerabilities and flaws in its design making it a target for malicious advanced knowledgeable computer users [3].

People have been deploying 802.11 wireless access points in their houses, coffee shops and everywhere, however they kept neglecting security factor of this technology, meanwhile, a new activity has taken form they call it Wardriving whereas participants of this activity assemble their equipment of hardware and software (The rig) intending to cruse streets to find open or weakly secured wireless access points in order to steal or alter every single packet that goes en route to the targeted AP [4].

The risk of this activity occurred in the sensitive data that might be eavesdropped or altered like credit cards private personal information or even governmental secret information.

Wardriving can be used for good purposes as well as it can monitor the signal strength, policy, encryption, access point activities and the channel of the access point. In fact people are always doing wardriving intentionally or not, as long as they use their smart phones or notebooks to search for available Wi-Fi signals in a certain place [5].

Many procedures have been proposed to reduce wireless attacks chances such as hiding SSID, updating the router firmware, avoid using WEP encryption, etc. However, few residents and companies enforce these security measures [6].
This paper surveys the security of wireless networks in some populated parts of Kuala Lumpur city. The survey results reveal a large number of unsecured wireless networks and a great demand for better wireless security awareness among the public.

BACKGROUND

WLAN is a term stands for Wireless Local Area Network, also known generally as Wi-Fi. WLAN is a Wireless version of the Ethernet (The wired network) where the data transferred between nodes through radio waves. The covered area by WLAN is called the Basic Service Set (BSS), which is recognized by the Service Set Identifier (SSID). The standard used in WLAN is IEEE 802.11 (ABGN).

The following components are used in establishing the WLAN:

- **Access Points (AP)**: Is a device that acts as a base station to communicate wireless devices via radio frequencies.
- **Clients**: Are devices like laptops, PDA's, Mobile devices... etc. that connect to access point via WLAN service.
- **Channel**: Is a radio frequency allocated by the access point.
- **BSSID**: Is the MAC address (physical address) of the access point. Wi-FI connection can be set to "open" or "closed". In the first scenario, the access point broadcasts its SSID name meanwhile on the other side; client's devices connect to strongest transmitted signal. In the second scenario, also known as "hidden", wireless access point doesn't broadcast its SSID name. The client manually inserts the SSID in order to establish a connection. Once the client does so, the wireless card requests a connection through all channels; the access point then receives the request and establish the connection [7].

Different encryption algorithms have been proposed to provide authentication and data integrity in the wireless network, basically there are two main used encryption WEP and WPA2, WEP principally uses frequently changing digits known as “Initialize Vector”, “IV” this IV combines with the chosen passphrase “The Encryption key” to encrypt data en route yet unfortunately WEP proved to be broken and can be cracked within average of ten minutes due to a security flaw in its design[8].

In the new routers firmware, a new feature was added to simplify the security configuration to the regular users, this feature called WPS (Wireless Protected Settings). WPS consisted of eight digits and can be found on the back of the router alongside a recognizable small button.

The user only needs to connect his/her device to the router and click on the button then a friendly GUI will be displayed to let the user go through few steps to choose whether to generate WPA passphrase automatically or manually or even to choose the default eight digits.

The early version of WPS is unfortunately vulnerable to Brute Force attack as it can be broken within maximum of seven hours, however the eight digits once cracked the WPA2 password will be shown. The good news is this flow was patched in the new WPS version [9].

WIRELESS 802.11 SECURITY RISKS

Data confidentiality: Data transmitted between the access point and connected clients can be intercepted or modified while en route this data may contains sensitive information like bank account credentials thus encryption need to be applied to encrypt the data and make it understandable for any unauthorized entity, WEP and WPA2 are an example for encryption however, as mentioned before WEP is easy to be broken [10].

Network Availability: Wireless Network is susceptible to Denial of Service Attack “DOS Attack” by means the attacker can use a spoofed de-authentication command to force the access point to re authenticate the connected clients unfortunately this kind of attacks considered unstoppable till this day [11].

Many security procedures have been suggested to secure wireless networks. Such measures like using hidden SSID, Updating the access point firmware, implementing strong encryption like WPA2 Enterprise and avoid using WEP encryption method. Also Changing default login credentials for Access point configurations is highly recommended alongside using MAC filtering to ensure the accessibly for solely desirable clients.

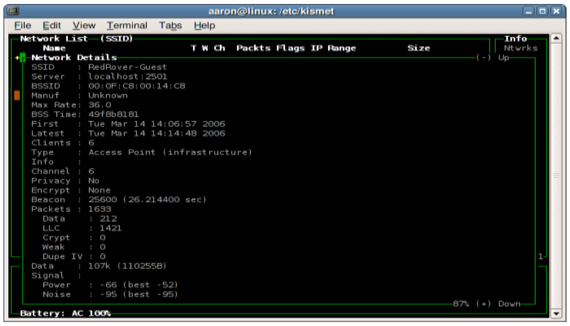
EVALUATION METHODOLOGY

The methodology this paper considers in collecting and analyzing the data is benign wardriving and in order to perform and achieve the evaluation meticulously, the following hardware and software were used in the survey:

1. Packard bell EasyNote TJ75 Laptop.
2. External Alfa Long Ranged Wireless Adapter - 5DB
3. Linux – Kali Operating System.
4. Aircrack-ng Software package.
5. Kismet Software Package.
6. Reaver tool for WPS Security Assessment.
7. Google Maps.

By taking the advantages of Linux operating system, the wireless network card set to be on monitor mode to monitor all traffic received from the wireless networks.

Moreover, Kismet tool was used to store the data into a log file and to classify it according to the encryption type each access point implements. The log file contains other information like SSID, Channel used. The following figure shows the data the log file contains.



```
Network List (SSID)                                                    Info
   Name                          T W Ch  Packts Flags IP Range     Size   Ntwrks
+ Network Details                                                   (-) Up
  SSID     : RedRover-Guest
  Server   : localhost:2501
  BSSID    : 00:0F:C8:00:14:C8
  Manuf    : Unknown
  Max Rate : 36.0
  BSS Time : 49f8b8181
  First    : Tue Mar 14 14:06:57 2006
  Latest   : Tue Mar 14 14:14:48 2006
  Clients  : 6
  Type     : Access Point (infrastructure)
  Info     :
  Channel  : 6
  Privacy  : No
  Encrypt  : None
  Beacon   : 25600 (26.214400 sec)
  Packets  : 1633
    Data     : 212
    LLC      : 1421
    Crypt    : 0
    Weak     : 0
    Dupe IV  : 0                                                         1
  Data     : 107k (110255B)
  Signal   :
    Power    : -66 (best -52)
    Noise    : -95 (best -95)
                                                               87% (+) Down
Battery: AC 100%
```

Figure 1: Kismet Log File

DATA COLLECTION

While cursing in major city in Malaysia, we decided to choose vital and crowded business places in the city center. The region has mostly residential flats, offices and hotels as well. We so far were able to scan and identify 1282 access points using a car and Alfa long ranged wireless adapter on Linux – Kali operating system.

The wireless set into monitor mode and used kismet tool to log the scanned wireless access points. The log file contains the following valuable information:

- Access Point SSID.
- Access Point BSSID.
- Encryption type.
- Channel.
- IP range (in case the access point was without encryption)

Also we used Revear tool to check whether the scanned access points are vulnerable to WPS Brute force or not. The following figure represents wireless scanned area during the wardriving.

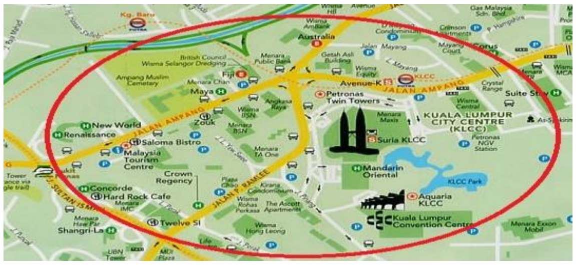


Figure 2: The scanned area

DATA ANALYSIS

Off all the scanned access points (1282 AP) only nine found to disable broadcasting their SSID.

The survey also found that among the scanned access points only 19.73% (253 AP) do not use encryption and leaving their wireless open. Meanwhile 16.77% (215 AP) from those scanned access points implement the weak encryption (WEP). The rest 63.7% (814 AP) represent networks that fortunately use WPA/WPA2 encryption. The following chart indicates the percentage use of wireless security in Malaysia.

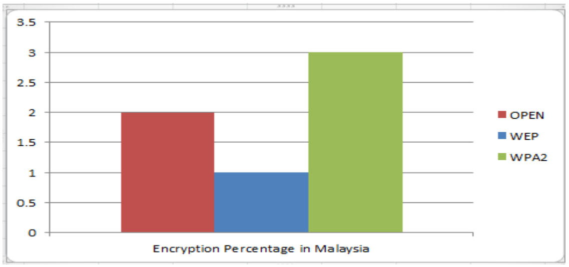


Figure 3: Encryption types in Malaysia

The survey also found that among the scanned networks that implement WPA2 (814 AP) there are 44 AP vulnerable to Brute force attack which forms 5.4%. By combining the three percentages will get 41.6 % of access points that symbolize a live example on weak encryption and a potential target for malicious wardrivers.

The following chart represents the overall percentages of the secured and unsecured wireless however; this paper categorized the unsecured wireless networks into three categories (Open, WEP and vulnerable WPA2).

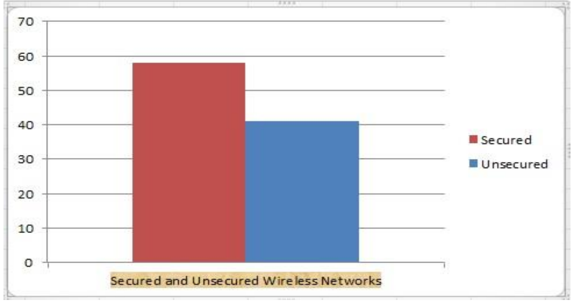


Figure 4: The overall secured and unsecured wireless networks.

Another noticeable issue showed by the survey, some SSID names revealed private information and the identity related to the company or home user which might be potential and useful information for the burglars and hackers to monitor the access point activity and to exploit this information in a dangerous way.

CONCLUSION

In this paper, security issues of WLAN in a Malaysian major city has been surveyed and analyzed. Overall, 1282 access points were identified.

Results show a significant number of unsecured wireless networks in a major city in Malaysia, the lack of timely response raises a very important question about who is responsible for raising the awareness among the people and applying strict policies against the established wireless networks.

The majority of people who use Wi-Fi have no idea about the consequences of using unencrypted wireless network as such kind of networks definitely exposes their data to several confidentiality and integrity types of attacks, many people do not mind to access their bank accounts via their smart phones in unencrypted wireless network, this ignorance encouraged the hackers to develop more powerful tools to exploit this medium.

Wireless security awareness must be considered very seriously by government authorities to provide more secured wireless environment and to ensure the safety of people privacy, however there are many ways to achieve such goal.

Enforcing strict regulations on public places that use wireless access points is such a good solution, also Youtube ads can play a major role in increasing the awareness among the people by showing the significant importance and the need for powerful encryption.

REFERENCES

1. H. Berghel, “Wireless Infidelity I: War Driving,” Communications of ACM on Digital Village, 47(9).
2. MAC Layer DoS Attacks in IEEE 802.11 Networks - Taimur Farooq, David Llewellyn-Jones, Madjid Merabti Liverpool John Moores University, UK
3. Mohamed Saleem TS, Jain A, Tarani P, Ravi V, Gauthaman K. "Aliskiren: A Novel, Orally Active Renin Inhibitor." *Systematic Reviews in Pharmacy* 1.1 (2010), 93-98. Print. doi:10.4103/0975-8453.59518
4. Backtrack WIFU book Mati Aharoni – Thomas d’Otrepp
5. Wireless Security in UAE - A Survey Paper by Omar Alomar, Mohammad Hajipour, Amir Kalbasi
6. Wardriving, a Target Rich Tool - Paul E Manning
7. SANS Institute InfoSec white paper - A Guide to Wardriving and Detecting Wardrivers.
8. Using Wireless Technology Securely – US Cert
9. Collaborative approach to mitigating ARP poisoning based Man-in-the-Middle attacks Seung Yeob Nama, Sirojiddin Djuraev a, Minho Park
10. Wardriving - Building A Yagi Pringles Antenna Spyridon Antakis Mark van Cuijk Jo¨el Stemmer 13 October 2008
11. WarDriving Funchal António Franco MEI student Universidade da Madeira
12. The Dangers of Deauthentication Attacks in an Increasingly Wireless World David Cossa, CprE 537, Iowa State University
13. Denial of Service Attack Techniques: Analysis, Implementation and Comparison Khaled M. Elleithy. Drazen Blagovic, Wang Cheng, and Paul Sideleau Computer Science Department, Sacred Heart University Fairfield, CT 06825, USA.
14. Gupta, R.K., Gupta, R., Chaudhary, S., Bhatheja, H., Pathak, P.Assessment of asymptomatic coronary heart disease in type 2 diabetics with treadmill test and framingham 10-Year CHD risk scoring system(2015) Journal of Cardiovascular Disease Research, 6 (3), pp. 131-137. DOI: 10.5530/jcdr.2015.3.4