Assessing Wireless Security Implementation in Government and Private Sector Companies in Malacca – A Case Study

Mohd Fairuz Iskandar Othman, Nazrulazhar Bahaman, Zulkiflee Muslim, Haniza Nahar, and Mohd Najwan Md Khambari
Department of Computer Systems and Communication
Universiti Teknikal Malaysia Melaka
Locked Bag 1200, Ayer Keroh, Malacca, Malaysia
mohdfairuz@utem.edu.my, nazrulazhar@utem.edu.my, zulkiflee@utem.edu.my, haniza@utem.edu.my, mohdnajwan@gmail.com

Abstract—**Wireless local area networks (WLAN) have become a common technology in our everyday life. The use of WLAN can be seen among home users who use it to access the Internet and play games to business users who conduct daily business activities over the WLAN. The main objective of this case study was to ascertain the level of security with regards to wireless implementation in government and private sector companies in Malacca. To gauge the level of security being implemented, we conduct war driving sessions where we use certain hardware and software to map these wireless networks and then analyze their level of security in terms of whether they use encryption techniques such as WEP or WPA for data confidentiality. Simulation was done to show that some of these techniques are not secure. Then, comparisons are made between the use of open source software against vendor based software to collect and analyze the wireless networks before making several conclusions. The most alarming conclusion was that the level of awareness of wireless security among users in Malacca was still relatively low, especially in government sectors. Finally, we propose several steps that can be taken to minimize and counter problems faced when using wireless technology.**

***Keywords*—security awareness; war driving; wireless LANs**

I. INTRODUCTION

Since its introduction in the late 1990's, wireless networks have become one of the most prevalent technologies in use today due to its ease of use, mobility and portability and low cost and maintenance. Often, these wireless network infrastructures are deployed and operated without any regards to security. As wireless signals are broadcast in nature, significant security issues exist as these signals might be detectable and thus vulnerable to attacks from unauthorized users outside the operator's perimeter or boundary. In this paper, we describe a case study that was done to ascertain the level of security with regards to wireless implementation in government and private sector companies in three areas in Malacca. The purpose was to scan for wireless networks to determine qualitatively and quantitatively how secure these networks before determining the more secured sector.

Our research was motivated by the emergence of new and always improving software and programs readily made available on the internet which expose the vulnerabilities of encryption algorithms used on wireless networks, namely Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). The lack of user awareness was also a key factor whereby we feel a lot more can be done to educate users and the best way was to show them the statistical data collected and simulation of attacks on these networks.

This paper discusses the details of our research project, compares the findings between government and private sector companies as well as the use of open source against vendor based software during data collection sessions. This paper concludes by suggesting possible steps that can be taken to minimize and counter problems faced when using this technology.

Section II describes the basics of 802.11 wireless network including vulnerabilities associated with them. Section III deals with the approach taken to capture, map and analyze wireless networks including the tools used. Our findings and simulation are explained in detail in Section IV. Section V concludes this paper with recommendations and best practices.

II. 802.11 BASICS

A. What is a wireless local area network (WLAN)

A wireless local area network (WLAN) can be thought of as two or more unwired computers using the airwaves for typical computing purposes, between stations or with the help of an access point (AP). A WLAN that does not make use of an AP is called an ad-hoc network, often referred to as an Independent Basic Service Set (IBSS), as shown in Figure 1. In this mode, communication is formed on the fly where stations communicate directly with each other when within proximity. On the other hand, a wireless network that uses an AP is called an infrastructure mode, or often referred to as a

cell or Basic Service Set (BSS), as shown in Figure 2. Often, installations will be formed by several cells, where the APs are connected through a backbone called a distribution system (DS) which typically is an Ethernet. Meanwhile, an Extended Service Set (ESS) is an interconnected wireless LAN that includes the different cells, their respective APs and the distribution system (DS) as shown in Figure 3.

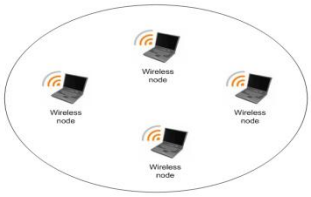

Figure 1. Independent Basic Service Set (IBBS)

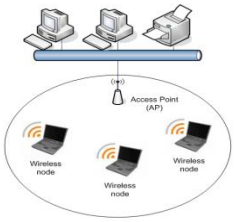

Figure 2. Basic Service Set (BSS)

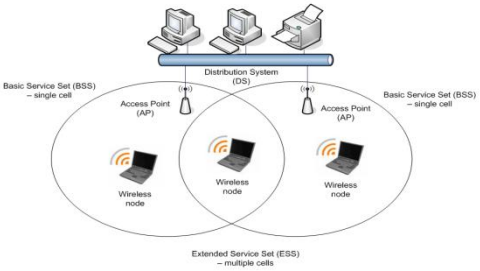

Figure 3. Extended Service Set (ESS)

B. Why wireless?

The growth of wireless can be attributed to a number of factors. People realized that using wireless technology is beneficial whether in home or business environments which include [1], [2] scalability, ease of installation, access to accurate information, mobility and increased productivity which is described below.

Wireless network provides the scalability where upgrading the wireless network is often easy as you only need to configure your AP and installation is a breeze as no wires will have to be laid and no walls will have to be drilled into. Configuration can often be made by using simple step by step wizard or guide.

In terms of accessing accurate information, wireless network provides the "anytime, anywhere" aspect of wireless communications that allows increased access to accurate information when it is needed most. This can often be seen in health care department and facilities especially in life or death situation.

Besides that, being unwired and mobile, people able to travel anywhere and use their laptops without the need to connect to a wired network. Among the most significant results revealed by recent end user surveys is that using wireless LANs allows users to stay connected to their network for approximately one and three quarter more hours each day. A user with a laptop and a wireless connection can roam their office building without losing their connection, or having to log in again on a new machine in a different location. This translates to a very real increase in productivity, as much as 22% for the average user [1].

Being easy to access information anytime and anywhere, unwired and mobile, productivity are enhanced as connectivity is increased, accuracy is acquired and time is saved.

C. Wireless Association Process

In order for a station to join an existing BSS, it will need to get synchronization information from the AP or from the other stations, if in ad-hoc mode. There are 2 methods a station can use which are *active scanning* and *passive scanning*. *Active scanning* is where the station tries to find an AP by transmitting probe request frame, and will wait for a probe response from the AP. Meanwhile, *passive scanning* is where the station just waits to receive a beacon frame from the AP (the beacon frame is a periodic frame sent by the AP with synchronization information).

After successfully finding an AP, the next step is to go to the process of authentication and then association [3]. Authentication process is where the station and the AP will exchange information to prove authenticity by proving their knowledge of a shared password. If the authentication process is successful, then the station will start to associate with the AP. This process involves the exchange of information about the station and BSS capabilities. Only after the association process is successful that the station and AP will begin to transmit and receive data frames.

D. Wireless network vulnerabilities

Wireless network is prone to attacks compared to wired network. This is because radio signals do not remain within the confines of a building, and their signals may propagate far enough to be detected externally in a neighboring area such as another building or a car park. Because of their broadcast nature, wireless LANs require the addition of user authentication methods that can be accomplished using open and shared keys, Service Set Identifier (SSID) and Media Access Control (MAC) address. WLANs also require data privacy methods in the form of WEP, WPA or WPA2 encryption. All these authentication and privacy methods have been found to be insecure, for example the encryption algorithm WEP was found to be flawed [4]. WPA algorithm meanwhile is still not enough as research has shown that using

short passphrases of less than 21 characters will make WPA-PSK vulnerable to dictionary attacks [5].

III. APPROACH

A. Method used

Wireless security presence and security information regarding APs was collected from 3 areas that represent a high concentration of government and private sector companies. To cover each area, cars were used with external antennas. To accomplish this task, 3 groups were formed where each group focused on one area. Results were then compiled. Each wireless AP Medium Access Control (MAC) address was counted only once to prevent duplicate data points. We decided to collect all data during normal business hours, which is between 9am to 5pm. As cars were used and attached with external power adapters, battery power on the laptops was not an issue. The length of the data acquisitions was limited to 2 hours for every sample. 8 samples were taken from each area for data analysis. 3 different software were used to compare and contrast their level of effectiveness in detecting wireless networks which are Kismet, Netstumbler and Omnipeek. Based on comparison done, Kismet was found to have the most balanced features in terms of ease of use and effectiveness in detecting wireless networks. Output data from Kismet was then imported into a program called Ksngem [6] where important information like level of encryption and Global Positioning Systems (GPS) coordinates was able to be generated. The output was in .kml format which enabled us to view it in Google Earth. This mapping enabled us to show in general comparison which area had the most concentration of vulnerable networks. After relevant and valuable data had been collected, a detailed analysis was able to be done. To analyze the data, an assumption of what constitutes a government sector network and a private sector network was made. The area in which the network resides also helped to determine which group that network will be put into. We assumed that public schools, public higher institution of higher learning, government link companies, state and federal agencies constitute the government sector. Meanwhile, the private sector will consist of private organizations, companies, factories and small medium enterprises.

B. Equipment used

Specific hardware was used to ensure that data collected was valid. This includes a Proxim Orinoco Gold wireless card with an external 7dbi omnidirectional antenna and a Garmin Etrex Legend GPS receiver [7] due to its portability, ease of use and proven capability in detecting hidden or cloaked wireless networks. The wireless card was chosen as it has the ability to be attached to an external antenna to boost signal strength. For software tools, we decided to use Backtrack Live CD that consists of a number of well known penetration testing software like Kismet and the Aircrack-ng suite [8]. Using an all-in-one distribution enabled us to save the time and hassle of downloading and installing the software tools separately. Other than that, we had also used Netstumbler and Omnipeek for packet capture and mapping of the wireless networks. Aircrack-ng suite was used in the later stages of attack simulation.

IV. FINDINGS

A. Analysis

Our findings were focused on the security issues that arise from improper configuration and setup of the wireless networks. This includes the use of default configuration settings, the use of organizational names as SSIDs and whether these networks employ any type of encryption. Fig. 4 shows a comparison between the government and private sector in terms of usage of default configuration settings in their networks. The graph clearly shows that while the number of APs that use default configuration settings in both the government and private sectors are significantly low, there are still organizations that use out of the box settings which is an easy target for attackers. Fig. 5 meanwhile shows a comparison between the government and private sector in terms of using the organization's name as its SSID. Using the organization's name as its SSID enables a malicious hacker to pinpoint locations and target attacks to a specific wireless network of an organization. Fig. 6 shows a comparison between the government and private sector companies on whether they employ any encryption techniques in their networks. Our findings show that only 18% of all networks combined implement some method of encryption. Although some do implement WEP or WPA, we show that these encryption algorithms are susceptible to attacks.

B. Simulation of attacks

To show that encryption techniques especially WEP which suffer from vulnerabilities, we ran a simulation of a wireless network that used WEP and Wi-Fi Protected Access-Pre Shared Key (WPA-PSK) as a method of encryption with varying key sizes. As noted before, the Aircrack-ng suite was used to initiate the attack. Fig. 7 shows that for a 10 bit hex key size used for WEP, only 2 minutes 26 seconds was needed to retrieve the key while a 26 bit hex key required just 22 minutes and 54 seconds. These figures were obtained by using the Pyshkin-Tews-Weinmann (PTW) method [9] which significantly reduced the time taken to crack the key while needing fewer packets. We also showed that WPA-PSK using simple words that can be found in a dictionary, like "baseball" can be cracked just as easily. With faster and more efficient processors coming into the market and made available to normal everyday consumers, it is not hard to imagine WPA-PSK's inept ability in safeguarding our wireless networks.

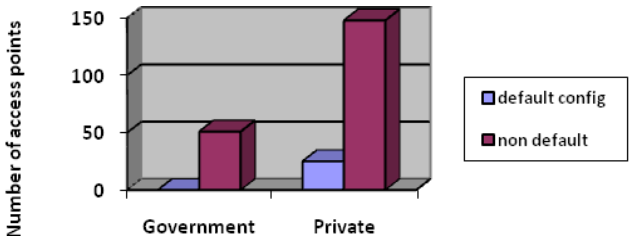

Figure 4. Use of default configuration settings

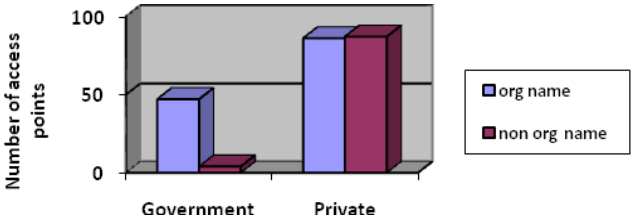

Figure 5. Use of organization name as SSID

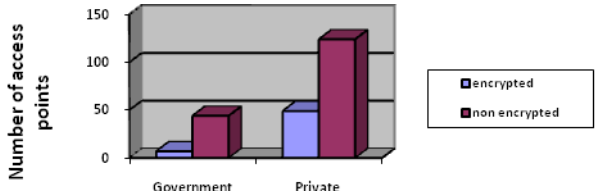

Figure 6. Use of encryption techniques

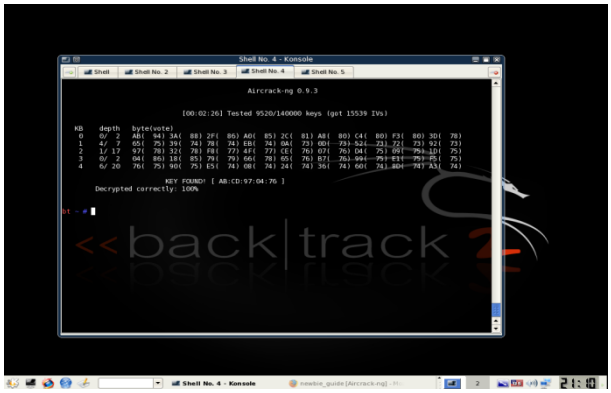

Figure 7. 10 bit hex key cracked using Aircrack suite

V. RECOMMENDATION AND CONCLUSION

Based on the outcome of the research, we describe several recommendations and best practices that can be used as a guide when implementing a wireless network infrastructure. Among them include:

1. Change default SSID and wireless AP settings.
2. Implement stronger and more secure encryption algorithms like WPA and WPA2.
3. Use long and strong keys.
4. Implement and enforce wireless LAN security policy.
5. User awareness and training sessions on a periodic basis.
6. Ensure wireless signal does not propagate outside organization parameter.
7. Ensure proper planning before wireless network roll-out.

As a conclusion, this paper presents the findings of a case study done to assess the wireless security implementation in government and private sector companies in Malacca and compared the level of awareness between the two sectors. It has exposed the urgent need for both government and private sector companies in Malacca to put enough emphasis on securing their wireless network communications. The study also confirms that while certain positive steps have been taken, most users especially in the government sector are still unaware of the potential threats and vulnerabilities posed by unsecured wireless networks. It is our hope that our study will shed light and increase users awareness of risks that must be taken into account when deploying wireless networks and what methods that can be applied to mitigate these problems.

REFERENCES

[1] S. Williams, "New Study Points to Substantial Financial Returns from Broad-Based Wireless LAN Deployments," 2003.
[2] T. Bradley, Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security: Syngress Publishing, Inc., 2006.
[3] P. Brenner, "A Technical Tutorial on the IEEE 802.11 Standard," BreezeCom, 1997.
[4] R. F. Scott, M. Itsik, and S. Adi, "Weaknesses in the Key Scheduling Algorithm of RC4," in Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography: Springer-Verlag, 2001.
[5] R. Moskowitz, "Weakness in Passphrase Choice in WPA Interface," 2003.
[6] JB580, "KNSGEM wifi mapping," 2007.
[7] A. A. Vladimirov, K. V. Gavrilenko, and A. A. Mikhailovsky, Wi-Foo : The Secrets of Wireless Hacking: Addison Wesley, 2004.
[8] C. Hurley, *WarDriving and Wireless Penetration Testing*: Syngress Publishing, Inc, 2007.
[9] E. Tews, R.-P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," Cryptology ePrint Archive, Report 2007/120, 2007.