Wireless Security in UAE: A Survey Paper

Amir Kalbasi, Omar Alomar, Mohammad Hajipour, Fadi Aloul

Department of Computer Engineering, American University of Sharjah (AUS), UAE
{b0009395, b00011362, b00013727, faloul}@aus.edu

***Abstract* — The paper evaluates the security status of Wireless Local Area Networks (WLAN) used by residents and companies in two major cities of the United Arab Emirates (UAE). The goal is to study the security vulnerabilities that lie beneath the usage of WLAN by the public in UAE. Data will be collected from various populated sites and will be analyzed to better understand the wireless security awareness among the public.**

***Index Terms* — Wireless Security, Wireless LAN, SSID, WEP.**

I. Introduction

Wireless networks are one of the most growing segments of information technology. Because of the flexibility of wireless networks, businesses, educational establishments and households are adapting this technology which makes it an integral part of modern life. The introduction of new technologies always comes with a byproduct, which is the abuse of the technology. For that reason, the secure usage of wireless networks has become a major field of study.

War Driving is the "art" of sniffing 802.11 wireless traffic using a network card set to monitor (RFMON) mode. The first officially recognized War Driving was performed by Peter Shipley in 1999, who presented his work to the hacker community at DEFCON 9 in July, 2001 [1]. Laptops with WLAN cards can use special software to perform War Driving. Some software, such as AirMagnet, SnifferPDA, and Fluke WaveRunner, require expert protocol users. Other software, such as Wireless Security Auditor (WSA), can be easily used by normal users. WSA does a complete wireless network analysis and auditing. It also assists in discovering all possible security threats and vulnerabilities [2]. Today, PDAs and mobile devices can also be used to sniff wireless data by running special purpose software.

In general, depending on the war driver's goal, war driving can be used for either *monitoring* or *hacking*. In the first case, War Driving is performed on wireless networks to verify the signal strength, encryption policy, wireless network name, and the used channel. In the second case, hackers may use War Driving to gain unauthorized access to wireless networks. That includes free use of the internet, collecting plain text data and stealing valuable information, breaking encrypted messages, launching attacks on other hosts, and preventing legitimate users from accessing the wireless network by running a denial-of-service (DOS) attack.

Several security measures have been proposed to reduce the possibility of wireless attacks such as disabling SSID broadcasting, changing the default SSID name, enabling WEP encryption, etc. However, few residents and companies enforce these security measures. In this paper, we evaluate the wireless security awareness in UAE. Specifically, we survey the security of wireless networks in 3 populated parts of the cities of Dubai and Sharjah. Results reveal a large number of unsecured wireless networks and the need for better wireless security awareness among the public.

The paper is organized as follows. In Section II, we provide an overview of wireless LANs, its security risks, and methods used to secure it. In Section III, we describe the procedure used to study the wireless security in UAE. Sections IV and V, evaluates the wireless security in Sharjah and Dubai, respectively. Section VI, compares the enforced wireless security measures in Dubai and Sharjah. The paper is concluded in Section VII.

II. Background

A. How WLAN Works?

WLAN Stands for Wireless Local Area Network, which is also known as Wi-Fi. WLAN is a Wireless version of the Ethernet network where the data is transferred between nodes through radio waves. The area covered by a single WLAN is called the Basic Service Set (BSS), which is identified by the Service Set Identifier (SSID). The standard used in WLAN is IEEE 802.11(ABG) [3].

The wireless medium of a wireless network is established through the usage of the following components [3]:

- **Basic service set (BSS)**: is the medium of communication and consists of all the components that construct a wireless network. The BSS can be independent and contain no access points; in this case, it is called an Ad-Hoc network. Ad-Hoc networks are equivalent to Peer to Peer wired networks.

- **Access Points (AP)**: are the base stations and the means of communication between the clients and the rest of the network through radio frequencies. The access point may enforce data encryption using WEP and WPA to improve security. Every access point has a unique MAC address.
- **Clients**: are devices that use the services of the WLAN. They can include laptops, PDA's, mobile devices, and printers. In general, a station is a device that is connected to the WLAN through a wireless network interface card (WNIC). Every WNIC has a unique MAC address.
- **Service Set IDentifier (SSID)**: is the name of the BSS and consists of 32 bytes. A single access point can serve more than one BSS thus can have more than one SSID.
- **Channel**: is the radio frequency used by the AP to transmit the data to the clients. There are 11 different channels ranging from 1 to 11. Having adjacent networks using the same channel can cause interference and reduce the quality and speed of communication.

Wireless APs can be "open" or "closed" [4]. In the first case, the wireless AP broadcasts its SSID name. Wireless cards on the client's machines identify the strongest SSID signal and connect to the corresponding AP. In the second case, also known as "hidden", the AP doesn't broadcast the SSID name. The client has to manually insert the SSID name in order to establish a wireless network connection. Once the client enters the SSID name, the wireless card requests a connection through all channels; the AP receives the request and approves the connection.

In order to avoid the unauthorized use of wireless networks, different encryption protocols have been proposed such as WEP and WPA-PSK. In WEP a frequently changing sequence of digits, known as the Initialization Vector (IV), is combined with the secret encryption key and the combination is used to encrypt data. The IV is used to avoid getting similar encrypted code for similar data. Unfortunately, recent studies have shown that WEP encryption algorithm can be broken [7]. Nevertheless, the use of WEP encryption will turn away script kiddies (un-experienced hackers).

B. WLAN Security Risks

Data confidentiality: because the data exchanged between the access point and the clients is transmitted through clear air, unauthorized people can listen and read the data. The data security risk can have severe impact on the user if the transmitted data contains personal information or vital passwords like the ones used in bank accounts. The data security risk still holds if the user enabled a weak encryption algorithm such as WEP, since WEP encrypted networks can be cracked today in an average of 10 minutes [7].

Unauthorized internet access: can be obtained by any user if the AP is broadcasting its SSID name and doesn't filter legitimate clients. Hackers may use the internet access to initiate attacks on other hosts and hide their identity [6].

User privacy: because users of WLAN have the freedom of choosing the SSID name, some of them include personal or business information which can be used as a hint for hackers (or thieves) to direct their attacks. In many cases, the default SSID name represents the AP brand. If the user doesn't change the SSID name, hackers can identify the AP brand, obtain an exploit for the AP, and break into it [6].

C. Securing WLAN

Several measures have been proposed to secure wireless networks. Such measures include:

- Disabling SSID broadcasting
- Changing default SSID name
- Using strong encryption methods like WPA-PSK and avoid using the weak WEP encryption method
- Changing default username and password used for the AP configurations
- Using *MAC filtering*, to grant access for only known clients [7].

III. EVALUATION PROCEDURE

In order to perform the evaluation, the following set of hardware was used:

- Toshiba A100-709 laptop equipped with Intel pro wireless 3945 ABG card
- Sony VGN-S18GP laptop equipped with Intel pro wireless 2200 BG card
- Wireless pre-N notebook network card model no. F5D8010 from Belkin
- Garmin GPS 5

The wireless network cards in both laptops were set to *monitor* mode. The Belkin wireless network card has a larger antenna and therefore can detect APs at wider ranges than the default wireless cards installed in the laptops. The Belkin card was used with the Sony laptop.

In order to collect the wireless data, two software were used:

- Network Stumbler for Windows.
- Kismet for Linux.

Network Stumbler was used as a sniffer to detect the APs in Dubai and Sharjah. Kismet was used for the purpose of detecting networks that don't broadcast their SSID names. In such cases, Kismet looks for exchanged packets between the clients and the hidden APs in order

to reveal the SSID name. Note that this requires the use of the wireless network while scanning for the APs.

In the next two sections, we present results of the wireless security statistics in Dubai and Sharjah. The locations that were covered are Sheikh Zayed road and Internet city in Dubai and the Buhaira area in Sharjah. Overall 3890 APs were detected of which 1858 were in Dubai and 2032 were in Sharjah.

IV. Wireless Network Security in Sharjah

During the survey in the Buhaira area in Sharjah, the team was able to identify 2032 access points (APs). During the data collection, a path longer than 25 Km was traveled to make sure the area is covered properly and accurate information is collected. The yellow shaded area in the Figure 1 shows the surveyed region around Buhaira in Sharjah. The area has mostly residential apartments, some offices, and a few hotels.

Fig. 1. The surveyed Buhaira area in Sharjah, UAE.

Collected data shows that several APs broadcast their default SSID name and mostly without encryption. During the survey, which took almost 8 hours in Sharjah, only two APs were found to disable their SSID broadcasting. Table 1 shows the identified APs with their corresponding SSID names and WEP encryption status.

982 of the APs used the default SSID name and only 187 (i.e. 19%) of the 982 APs enabled WEP encryption. In terms of APs with non-default SSID names, 683 (i.e. 65%) of the 1050 APs enabled WEP encryption. The high number of completely unsecured wireless networks, i.e. using default SSID names and no WEP encryption, shows the public's limited awareness of the security problems in wireless networks.

TABLE I
Access points with their SSID names and their encryption status in the Buhaira area.

SSID	Number of APs	WEP enabled (%)
speedstream	700	90 (13%)
Linksys	152	50 (33%)
DLINK_WIRELESS	30	10 (33%)
USR9108	26	17 (65%)
Default	25	2 (8%)
3Com	9	6 (67%)
USR9106	6	1 (17%)
(Others AP brands)	34	11 (32%)
non-default name	1050	683 (65%)

V. Wireless Network Security in Dubai

We decided to survey Sheikh Zayed road and the Internet city in Dubai. Both locations have a high number of offices, hotels, and residential buildings. During the survey, the team identified 1587 and 271 APs in Sheikh Zayed road and Internet city, respectively. To provide complete coverage of the areas, all service streets were visited. The turquoise shaded area in the Figure 2 shows the surveyed region in Sheikh Zayed road. The area has multi-national and local offices, residential apartments, hotels, and cafes.

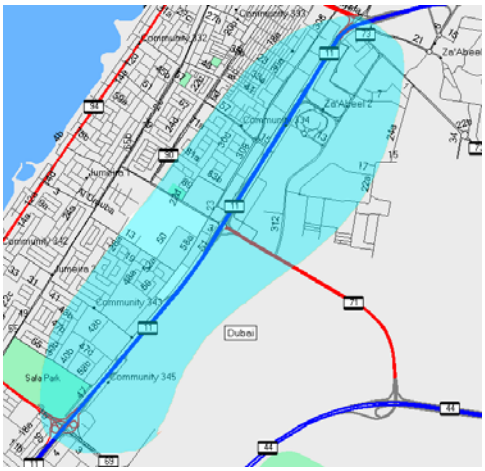

Fig. 2. The surveyed area of Sheikh Zayed road in Dubai.

During the survey, no hidden APs, i.e. with disabled SSID broadcasting, were found. Table 2 shows the identified APs with their corresponding SSID names and WEP encryption status. 468 of the APs used the default SSID name and only 105 (i.e. 22%) of the 468 APs enabled WEP encryption. In terms of APs with non-default SSID names, 806 (i.e. 58%) of the 1390 APs enabled WEP encryption. Again, the high number of completely unsecured wireless networks, i.e. using default SSID names and no WEP encryption, shows the public's limited awareness of the security problems in wireless networks.

TABLE II
ACCESS POINTS WITH THEIR SSID NAMES AND THEIR ENCRYPTION STATUS IN DUBAI.

SSID	Number of APs	WEP enabled (%)
Sheikh Zayed road		
linksys	141	39 (28%)
speedstream	133	21 (16%)
default	40	7 (18%)
belkin54g	23	6 (26%)
USR9106	22	3 (14%)
3Com	14	3 (21%)
USR9108	12	4 (33%)
DLINK_WIRELESS	11	2 (18%)
(Others AP brands)	22	5 (23%)
non-default	1169	684 (59%)
Dubai Internet City		
linksys	14	5 (36%)
speedstream	12	2 (17%)
3Com	6	3 (50%)
USR9106	5	0 (0%)
default	4	2 (50%)
(Others AP brands)	9	3 (33%)
non-default	221	122 (55%)

VI. COMPARISON BETWEEN WIRELESS NETWORK SECURITY IN SHARJAH AND DUBAI

According to Tables I and II, WEP encrypted wireless networks count for 46% of the networks found in Dubai and Sharjah. Specifically, 43% and 49% of the wireless networks are secured with WEP encryption in Sharjah and Dubai, respectively. Furthermore, 64% of the wireless networks used non-default SSID name, of those 52% and 75% were in Sharjah and Dubai, respectively (see Table III). The higher security in Dubai can be explained by the fact that more offices are found in the Sheikh Zayed road and Internet city.

Channel usage was unbalanced in both Sharjah and Dubai. Overall, 74% of the APs in Dubai and Sharjah were operating using channel 11. Table IV shows the channel distribution in the two cities.

TABLE III
WIRELESS NETWORK STATISTICS IN SHARJAH AND DUBAI.

City	Number of APs	WEP Enabled (%)	Non-Default SSID
Sharjah	2032	870 (43%)	1050 (52%)
Dubai	1858	911 (49%)	1390 (75%)

TABLE IV
USED CHANNEL NUMBERS IN WIRELESS NETWORKS IN SHARJAH AND DUBAI.

City	Channel			
	11	*6*	*1*	*Other*
Sharjah	79%	10.6%	2.0%	8.4%
Dubai	68%	17.3%	5.6%	9.1%

A. SSID Revealing Private Information

One of parameters used by hackers to target wireless networks is the SSID name. When the network administrator selects an SSID name that reveals information about his/her identity, the wireless network can become vulnerable to attacks.

Analyzing the list of SSID names identified in Dubai and Sharjah showed that 10% of the SSID names reveal some private information related to home users or business offices. Out of these SSID names, 52% and 69% enabled WEP encryption in Dubai and Sharjah, respectively.

In some cases, the SSID names corresponded to company names, building names, apartment numbers, owner name, and telephone numbers. Such SSID names may attract hackers and burglars to monitor the AP activity and break into the company or residential apartments.

B. Default SSID Names

As Tables I and II show, many APs had the default SSID name which reveals the AP brand. Such name can be used by hackers to break into the AP by running known exploits or using default passwords for the targeted AP [8].

In Sharjah, 34% and 7.5% of the identified wireless networks had the default SSID names “speedstream” and “linksys”, respectively. In Dubai, 7.8% and 8.3% of the identified wireless networks had the default SSID names “speedstream” and “linksys”, respectively. Of these SSID names, only 18% used WEP encryption.

Since most of these APs are distributed by the local ISP and given the high number of un-secure wireless networks, the ISP can better advice the public on how to secure their wireless networks.

VIII. CONCLUSIONS

In this paper, security issues of wireless local area networks in Sharjah and Dubai were surveyed and analyzed. Overall, 3890 access points were identified. Results show a significant number of un-secure wireless networks in Dubai and Sharjah. Specifically, a large number of wireless networks broadcast their SSID name, don’t change the AP default settings and administrative password, keep the default SSID name, and fail to use any data encryption algorithms such as WEP.

In general, security awareness among the public was higher in Dubai than Sharjah. This can be justified to the larger number of business offices and hotels in Dubai which are more concerned with wireless security.

REFERENCES

[1] H. Berghel, "Wireless Infidelity I: War Driving," *Communications of ACM on Digital Village*, 47(9), pp. 21-27, September 2004.

[2] IBM Corporation, "Security Research: Wireless Security Auditor (WSA)," 2007. Available: *http://www.research.ibm.com/gsal/wsa*.

[3] IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," in IEEE Standard 802.11g, 2003.

[4] H. Berghel, "Wireless Infidelity II: Air Jacking," *Communications of ACM on Digital Village*, 47(12), pp. 15-21, December 2004.

[5] N. Cam-Winget, T. Moore, D. Stanley, J. Walker, "IEEE 802.11i Overview," in *NIST 802.11 Wireless LAN Security Workshop*, December 2002.

[6] AirMagnet Inc., "Managing WLAN Risks with Vulnerability Assessment: A Technical Whitepaper," October 2005.

[7] W. Conklin, D. Williams, G. White, R. Davis, and C. Cothern, "Principles of Computer Security," *McGraw Hill Technology Education*, 2004.

[8] "Default Password List," February 2007. Available at: *http://www.phenoelit.de/dpl/dpl.html*.