Wi-Fi Network Vulnerability Analysis and Risk Assessment in Lebanon

Elie Nasr¹, Mohammad Jalloul¹, Joseph Bachalaany¹, and Roy Maalouly¹

¹Information and Communications Technology Department, American University of Science and Technology, Beirut, Lebanon

Abstract— The aim of this paper is to analyze the Wi-Fi network vulnerabilities and risk assessment in Lebanon in order to raise awareness to the Lebanese public by informing them of threats that occur on the network and their impact. The analysis is done by first performing a wardrive; this involves capturing the network access points in several Lebanese regions with the use of two programs: Acrylic Wi-Fi Professional™, and Kismet™, as well as connecting an Alfa Network Antenna to the device in order to increase the range of capture. The data collected are stored in a database where they are processed in order to generate a statistics report of the security and risk level of the network in selected cities. Moreover, a custom survey of the basic knowledge of networking and security is publicly distributed.

1 Introduction

According to Sys-con, there will be more than 7 billion new Wi-Fi enabled devices in the next 3 years. That means that more than 7 billion new Wi-Fi devices might be vulnerable to Wi-Fi attacks. A Wi-Fi attack on an open network can take less than 2 seconds, according to Extreme Networks. Based on a research done by Gigaom, it is predicted that by 2020, 24 billion devices will be connected to the internet and the vast majority will use some form of wireless for access. In a recent survey it was reported that 90 percent of all businesses suffered some sort of computer hack over the past 12 months and 77 percent of these companies felt that they were successfully attacked several times over the same period of time.

In this study, an in-depth analysis was performed on wireless networks located in various Lebanese commercial and residential districts and regions. Based on the analysis performed on the acquired data, statistical results will be generated which will be used to raise awareness for people regarding the Wi-Fi attacks issue. The main contributions of this paper are raising awareness to the Lebanese citizens by: (a) Emphasizing on the severity of Wi-Fi network attacks. (b) Analyzing the weaknesses and vulnerabilities of existing Wi-Fi networks. (c) Offering guidance on how to improve Wi-Fi security measures.

2 Methodology

The main issue is to address the overwhelming deficiency in awareness and knowledge in cyber–security topics that the Lebanese society has. This research is exploratory in nature and uses quantitative research methodology in order to answer the research questions listed in subsection 2.1. Throughout the process of conducting this research, a wardrive was performed and a survey containing a list of questions related to cyber-security awareness was distributed all for the purpose of risk assessment. The table below illustrates the five different types of Wi-Fi attacks, examples on each type and the threat which each type of attack rises to the victim [1,6].

Table 1. Wi-Fi vulnerability risk assessment

Type of attack	Short Description	Example
(1) Access Control	Evades WLAN access control measures.	MAC Spoofing. Rogue Access Points.
(2) Confidentiality	Private information interception	Eavesdropping. Man in the Middle attacks.
(3) Integrity	Misleading recipient by manipulating the data	Frame Injection.
(4) Authentication	Identity theft and credentials stealing.	Login Theft.
(5) Availability	Prevent users from accessing WLAN resources.	AP Thefts. Queensland DoS.

2.1 Research questions

Do people living in certain Lebanese regions know less about Wi-Fi password encryption types than people living in other regions? (1) Is the person's interest to learn more about Wi-Fi security related to the person's educational level? (2) Are people who have never attended a conference related to security awareness more likely to be interested in learning how to secure their Wi-Fi? (3) Are people who acknowledge the severity of a Wi-Fi attack generally more concerned with their own privacy? (4)

2.2 War-driving

Wardriving is the process of cruising around in a moving vehicle while passively using computer hardware and software in order to scan different areas for Wi-Fi networks and access points. Through wardriving, we were able to capture publicly available data about each scanned Wi-Fi access point. Data includes: security protocol (WEP, WPA, WPA2 or OPN), channel being used, router manufacturer, SSID and BSSID [2,5]. The route we took throughout our wardrive spans from Beirut to Kaslik as shown in figure 1. This route was chosen since Beirut is the capital of Lebanon and it hosts a significant population density. The road from Beirut to Kaslik constitutes mainly of urban areas where residents are assumed to be quite educated and technologically literate. However, the wardrive can be extended across the entire country and this sample was selected to narrow down results and findings.

2.3 Survey

The purpose of the survey was to get a glimpse of the level of cyber-security knowledge and awareness which a sample of people have [3,4]. The type of the survey used is a questionnaire since the questions tend to be closed-ended, which are naturally followed by response options. For the sake of data simplicity, the survey was distributed online to a number of university students of the BS level from different departments and majors. This sample was chosen assuming that university students of the BS level should have the basic knowledge of Wi-Fi attacks and their consequences. Subsection 3.1 illustrates the results generated from the survey.

3 Results and findings

Results generated from the survey and the warddrive helped in answering several research questions and to estimate the severity of the issue at hand.

3.1 Wardrive results

The Wardrive [9] performed for the purpose of this research generated data for over 10,000 Wi-Fi access points. It was discovered that approximately 11.1% of Wi-Fi access points located in the various regions in Lebanon still rely on WEP security which is the easiest to crack, while 4.9% use WPA and 84.1% use WPA2. In addition to that, 797 access point have the SSID “Blink” followed by an alphanumeric set of characters which could imply that this access point is using default credentials which makes it vulnerable to brute force attacks [7,8].

3.2 Survey results

(1) 35.3% do not know how to change their Wi-Fi password; (2) 37.9% do not know, 50.9% WPA2, 7.8% WPA, 2.6% WEP and 0.9% none; (3) 50% do not know what the brand of their modem/router is; (4) 54.3% do not know how to check who is connected to their Wi-Fi network; (5) 30.2% do not know what a firewall is; (6) 65.5% do not know what MAC filtering is; (7) 36.2% do not acknowledge the severity of a Wi-Fi attack; (8) 45.7% are concerned, 44.8% are somewhat concerned and 9.5% are not concerned; (9) 20.7% have attended conferences related to security awareness; (10) 73.3% are interested in learning how to secure their Wi-Fi;

3.3 Answering the research questions

By using the SPSS™ software and applying the Chi-square χ^2 test of independence, the following was found:

Do people living in certain Lebanese regions know less about Wi-Fi password encryption types than people living in other regions?

To check whether the location where a person lives is related to the person’s knowledge regarding what their Wi-Fi password encryption is, the following hypothesis is set:
H0: The location of a person’s accommodation and their knowledge of their Wi-Fi password encryption type are independent.
H1: The location of a person’s accommodation and their knowledge of their Wi-Fi password encryption type are dependent.
For testing this hypothesis using the chi-square χ^2 test on independence, SPSS™ tool is used to create the cross tabulation.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.042 ^a	16	.741
Likelihood Ratio	13.937	16	.603
N of Valid Cases	116		

Fig. 2. Chi-Square Test #1 showing the relationship between a person’s accommodation location and their knowledge of their Wi-Fi password encryption type.

From the top row of the table, Pearson Chi-Square statistic, $\chi^2=12.042^a$, and $p=0.741=74.1\%$; i.e., a very high probability of the observed data lies under the null hypothesis of no relationship. The null hypothesis is accepted, since $p>0.05$.

Conclusion: A person’s accommodation location doesn’t seem to be related to their knowledge of their Wi-Fi password encryption type. This implies people living in different Lebanese regions lack security awareness and that the issue is not just present in one location only.

Is the person's interest to learn more about Wi-Fi security related to the person's educational level?

To check whether people of specific educational levels should be addressed and targeted to give security awareness seminars and workshops to, the relationship between the person’s educational level and their interest in learning more about Wi-Fi security was tested.
H0: “Educational level” and “Interest in learning more about Wi-Fi security” are independent.
H1: “Educational level” and “Interest in learning more about Wi-Fi security” are dependent.
For testing this hypothesis using the chi-square χ^2 test on independence, SPSS™ tool is used to create the cross tabulation.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.429 ^a	3	.330
Likelihood Ratio	3.359	3	.340
N of Valid Cases	116		

Fig. 3. Chi-Square Test #2 showing the relationship between a person’s educational level and their interest in learning more about Wi-Fi security.

From the top row of the table, Pearson Chi-Square statistic, $\chi^2=3.429^a$, and $p=0.330$; i.e., a high probability of the observed data under the null hypothesis of no relationship. The null hypothesis is accepted, since $p>0.05$.

Conclusion: A person’s educational level doesn’t seem to be related to their interest in learning about securing their Wi-Fi networks. This implies that people of different educational levels are interested in learning more about this toping and this interest isn’t limited or exclusive to people from the same educational level. 65.2% of school students are interested in learning more about securing their Wi-Fi, as well as 79% of university undergraduates, in addition to 80% of university graduates and 61.9% of people who completed their university studies.

Are people who have never attended a conference related to security awareness more likely to be interested in learning how to secure their Wi-Fi?

To check if people’s interested in learning more about Wi-Fi security is related to whether they previously attended a conference related to security awareness or not, the following hypothesis is set:

H0: “Attended a Security Awareness Conference Before” and “Interest in learning more about Wi-Fi security” are independent.

H1: “Attended a Security Awareness Conference Before” and “Interest in learning more about Wi-Fi security” are dependent.

For testing this hypothesis using the chi-square χ^2 test on independence, SPSS™ tool is used to create the cross tabulation.

Chi-Square Tests					
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5.643 ^a	1	.018		
Continuity Correction ^b	4.480	1	.034		
Likelihood Ratio	5.231	1	.022		
Fisher's Exact Test				.036	.020
N of Valid Cases	116				

Fig. 4. Chi-Square Test #3 showing the relationship between a person’s interest in learning more about Wi-Fi security and whether or not they have attended a security awareness conference before.

From the top row of the table, Pearson Chi-Square statistic, $\chi^2=5.643^a$, and $p=0.18$; i.e., a very small probability of the observed data under the null hypothesis of no relationship. The null hypothesis is rejected and the alternative hypothesis is accepted, since $p<0.05$.

Conclusion: A person’s interest in learning more about securing their Wi-Fi networks seems to be related to whether or not they previously attended a conference related to security awareness. People who have never attended a conference related to security awareness (92/116 respondents) seem to be more interested in learning about securing their Wi-Fi networks (72 respondents).
Are people who acknowledge the severity of a Wi-Fi attack generally more concerned with their own privacy?

To check if there is a direct relationship between people who acknowledge the severity of a Wi-Fi attack and the level of concern they have towards their own privacy, the following hypothesis is set:
H0: “Wi-Fi Attack Severity Acknowledgement” and “Privacy Concern” are independent.
H1: “Wi-Fi Attack Severity Acknowledgement” and “Privacy Concern” are dependent.
For testing this hypothesis using the chi-square χ^2 test on independence, SPSS™ tool is used to create the cross tabulation.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.874 ^a	2	.007
Likelihood Ratio	9.772	2	.008
N of Valid Cases	116		

Fig. 5. Chi-Square Test #4 showing the relationship between a person’s privacy concern level and whether or not they acknowledge the severity of Wi-Fi attacks.
From the top row of the table, Pearson Chi-Square statistic, $\chi^2=9.874^a$, and $p=0.007$; i.e., a very small probability of the observed data under the null hypothesis of no relationship. The null hypothesis is rejected and the alternative hypothesis is accepted, since $p<0.05$.

Conclusion: People who acknowledge the severity of a Wi-Fi attack are generally more concerned with their own privacy. 54.1% of people who acknowledge the severity of a Wi-Fi attack are “very concerned” with their own privacy, 41.9% who acknowledge the severity of a Wi-Fi network attack are “somewhat concerned” with their own privacy leaving only 4% of people who acknowledge the severity but are not concerned with their own privacy.

4 Discussion

Conducting the wardrive and distributing the survey helped in gathering information to answer the research questions. However, one question remains: how much are we at risk?
A common formula used to calculate the risk would be:

$$Risk = Vulnerability * Threat \tag{1} [10]$$

The threat is the attacker who exploits a certain vulnerability in order to perform all sorts of attacks listed in Table 1. For example, the survey showed that 54.3% of participants do not know how to check who is connected to their Wi-Fi network; this helps the attacker in performing confidentiality (2) and integrity (3) attacks and intercept the network without people knowing. The survey results also showed that 30.2% of participants do not know what

a firewall is; this helps the attacker in performing authentication (4) attacks and steal a user's login credentials on a network that isn't protected with a firewall. There are countless vulnerabilities that are published and anyone can exploit them with enough technical skill so it's essential to raise awareness for people regarding such issues to mitigate the risk as much as possible.

4.1 Recommendations

The Wi-Fi security protocol WPA3 is now available however most of our current devices do not support that security protocol yet. WPA3 mitigates against brute force attacks for it limits the number of connection attempts (guessing passwords) however one should always use a strong password for their Wi-Fi network. Since WPA3 is still new and most of our current devices do not support it, it is advised to use WPA2 Wi-Fi security protocol and to keep installing the latest updates and patches to it.

4.2 Legality issues

According to Carnegie Mellon University's (CMU) [11] "Wardriving: Legal or Illegal" article, it is stated that war driving is not an illegal issue, it is in fact perfectly legal since it is the process of just passively collecting publicly available data from wireless routers similar to how any user's PC does. As of 2019, Lebanon has not yet adopted any cyber-laws against performing wardrives. We conducted the wardrive as ethical penetration testers and all the information gathered stays confidential and is used only for research and educational purposes and will not be shared with anyone among the public.

5 Conclusion

The analysis performed on the results generated from the wardrive and the survey clearly showed that an alarming number of Lebanese people are unaware of the Wi-Fi attacks and threats they're susceptible to. More precisely, the wardrive helped in identifying vulnerable Wi-Fi networks which are using outdated security protocols while the survey helped in identifying the lack of security awareness for individuals; all of which lead to an increasing risk of being a victim to Wi-Fi attacks. Conducting security awareness campaigns, conferences and workshops would help in educating many people on the different Wi-Fi attacks, their severity, the threats they form and how to mitigate against such attacks and keep yourself safe.

References

1. C. Teyou and P. Zhang, "Solving Downgrade and DoS Attack Due to the Four Ways Handshake Vulnerabilities (WIFI)", *International Journal of Engineering and Management Research*, vol. **8**, no. 4, (2018). Available: 10.31033/ijemr.8.4.1.
2. A. Makki, A. Siddig, M. Saad and C. Bleakley, "Survey of WiFi positioning using time-based techniques", *Computer Networks*, vol. **88**, pp. 218-233, (2015). Available: 10.1016/j.comnet.2015.06.015.
3. S. Li, H. Li and L. Sun, "Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization", *EURASIP Journal on Wireless Communications and Networking*, vol. **2016**, no. 1, (2016). Available: 10.1186/s13638-016-0624-2.
4. S. Yousefi, H. Narui, S. Dayal, S. Ermon and S. Valaee, "A Survey on Behavior Recognition Using WiFi Channel State Information", *IEEE Communications Magazine*, vol. **55**, no. 10, pp. 98-104, (2017). Available: 10.1109/mcom.2017.1700082.
5. S. Li, H. Li and L. Sun, "Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization", *EURASIP Journal on Wireless Communications and Networking*, vol. **2016**, no. 1, (2016). Available: 10.1186/s13638-016-0624-2.
6. K. ., "PROTECTION AGAINST INFORMATION LEAKAGE AND MALWARE WITH RISK FREE PUBLIC WIFI USAGE", *International Journal of Research in Engineering and Technology*, vol. **06**, no. 04, pp. 64-66, (2017). Available: 10.15623/ijret.2017.0604015.
7. Parsons, J. (2018). *Hackers crack Wi-Fi security – 'almost all' devices at risk say security experts*. Available at: <https://www.mirror.co.uk/tech/wifi-crack-security-hack-wpa2-11349768>
8. *How to Hack Wi-Fi: Cracking WEP Passwords with Aircrack-ng*. Available at: <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/>
9. Tools.kali.org. (2018). *Kismet | Penetration Testing Tools*. Available at: <https://tools.kali.org/wireless-attacks/kismet>
10. E. Cole, "Cyber Defense | Insider Threat Risk Formula: Survivability, Risk, and Threat | SANS Institute", *Cyber-defense.sans.org*, (2012). [Online]. Available: <https://cyber-defense.sans.org/blog/2012/10/23/insider-threat-risk-formula-survivability-risk-and-threat>.
11. "Wardriving: Legal or Illegal?", cmu95752. [Online]. Available: <https://cmu95752.wordpress.com/2011/12/12/wardriving-legal-or-illegal/>.