eISSN:2600-7920
INTI JOURNAL
Vol.1, 2018 (9)

Study on Wireless Network and Restrictive Approaches to Enhance the Data Security

[1]Kannan Ponkoodalingam, [1]Nitashine a/p Baskaran, [1]Deshinta Arrova Dewi

[1]Faculty of Information Technology and Sciences, INTI International University, Nilai, Negeri Sembilan, Malaysia.

Correspondence author: pon.kannan@newinti.edu.my, Deshinta.ad@newinti.edu.my

Abstract

Many organizations nowadays use wireless networks or Wi-Fi (Wireless Fidelity) networks. This is because of the resilience and flexibility, simplicity in installing, and lower costs when compared to fixing wired cables all over an organization's infrastructure. The Wi-Fi technology are not only installed on private wireless networks, it is installed speedily on the public wireless network via hotspots. For example, hotels, airports, restaurants and more. Wi-Fi is certain type of WLAN (Wireless Local Area Network) whereby the WLAN technology is the quickest growing technology besides the Internet. In response with the growing of the security hazards on WLAN's data security and unauthorized corporate is what the network administrators and information security managers must give an extra attention to. Hence, the scope of this research focuses on the wireless network security in terms of threats and restrictive approaches whereby multi-factor authentication technology is proposed as one of the ways to mitigate the threats. Five hypothesis are included to support this study and they are analyzed using quantitative and qualitative software i.e. SPSS and QDA Miner. The result shows that multi-factor authentication should be implemented as additional security feature on the wireless network.

Keywords

Wireless Network, Restrictive Approach, Data Security

Introduction

The wireless technologies have turned out to be progressively prominent in the ordinary business and individual's life. Individual advanced collaborators enable people to get to logbooks, email, address and telephone number records, and the Internet (Tom Karygiannis and Les Owens, 2002). A few advances even offer worldwide situating framework (GPS) capacities that can pinpoint the area of the gadget anyplace on the planet. Wireless technologies guarantee to offer even more highlights and capacities in the following couple of years.

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet) (Tom Karygiannis and Les Owens, 2002). Wireless networks are numerous and different in any case, are as often as possible arranged into three gatherings considering their scope go: Wireless Wide Area Systems (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). An expanding number of government organizations, organizations, and home clients are utilizing, or considering utilizing, remote advancements in their surroundings. Offices ought to know about the security dangers related to wireless technologies.

Wireless customers would associate with each other through at least one access focuses that are associated with a wired LAN. Framework mode is more typical to execute on a bigger scale arrange condition, for example, inside a company. Unauthorized users can slow your connection down to a crawl, access your private data, or even use the network to perform shady activities that can be traced back to you (Brandon Widder, 2013).

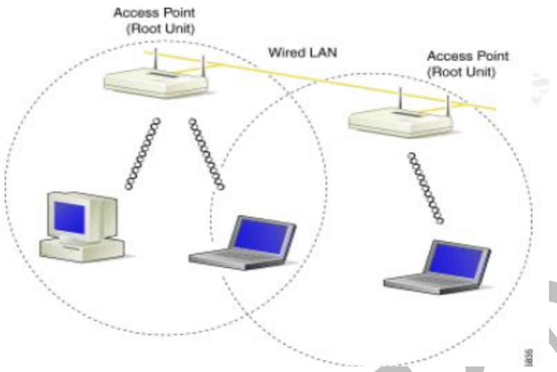


Figure 1: Wireless Infrastructure with Workstations Accessing a Wired LAN

Unfortunately, the number of threats and attacks occurring in a wireless network are also increasing drastically. By implementing wireless technology without understanding its associated risks, organizations are prone to hackers' attacks and/or unauthorized access to internal networks carrying confidential data (Danny Neoh, 2003). Utilizing wireless has numerous focal points because of its adaptability and simplicity of usage. Frequently arrange overseers neglect the significance of security. The real security for a wireless network comes from the selection of a proven security technique, there have been many different security techniques deployed that have been broken. As of this writing, the most secure technique is IEEE 802.11i which is also known as WPA2 (Sean Wilkinds, 2011)**.**

Due to the increase in crimes that occurs in the network, many companies or enterprises data loss and difficulties. Some companies in the current state are not really exposed to proper approaches in restricting more attacks from occurring in the network. This situation makes customers don't feel secured to give out or save their sensitive data in the system. In response to the above situation, this paper carried out quantitative and qualitative research to study the existing security issues and the preventive approaches. The study aims to prevent threats and provide utmost security for the data present in the network.

Many proper approaches have been proposed by previous study but one of them becoming very popular nowadays i.e. multifactor authentications. This happens because since single-factor authentication is no longer adequate for high-risk transactions that reveal customer information especially ones that involving the movement of funds to other parties (Tiwari et.al, 2011).

The idea of multifactor authentication is adding an extra layer of protection on top of username and password. For example, after users sign in to a website, they will be prompted for username and password (first factor) and the website will provide an authentication code for the user (second factor). Hence, the multifactor authentication techniques are including extra hardware and software or biometrics or Trusted Internet Connection (TIC) or SMS confirmation, etc. TIC authentication is a technique which is used to verify both the user and the ongoing transaction. A TIC code will certify that the current transaction has been initiated by the right person and that it is a valid user who is trying to access his/her account. After the TIC code identification is completed, the user will get an SMS from the website authentication server to confirm his/her transaction. Altogether, these multiple factors increase the security of users and their personal data.

The research questions that are related to this study is presented as follows:

- RQ1: What are the possible threats that can be found if the wireless network is not well secured?
- RQ2: What are the restrictive approaches in a wireless network?
- RQ3: What are the mitigation ways of avoiding the network from getting attacked by any threats or risks?
- RQ4: What are the actions that can be taken in an enterprise or company when faced with any security issues?

Classifying the various actions are important to meet the risks of security, like identifying the actions to be taken in an enterprise or company when there are security issues arise. As a starting point for further investigations, the hypothesis has been derived based on literature review and consultation with experts in the field. The following list of the hypothesis is outlined:

- H1: The ease of use of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.
- H2: The suitability of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.
- H3: The security & privacy of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.
- H4: The level of knowledge in IT will affect their agreement towards usage of multi-factor authentication as the restrictive approach.
- H5: The performance of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.

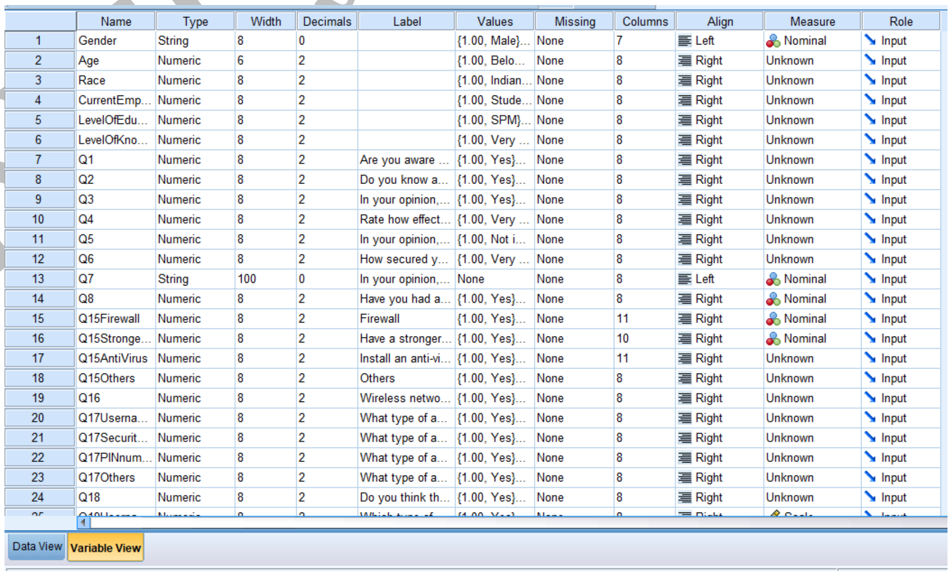
Methodology

Designing relevant instruments for data gathering is the important step in this study whereby the range is limited within Malaysia only. The characteristic of the samples involved is presented in Table 1 below.

Variables		Frequency	Percentage (%)
Gender	Male Female	83 59	58.5% 41.5%
Age	Below 18 years old 18 - 29 years old 30 - 39 years old 40 - 49 years old 50 – 59 years old 60 years old and above	11 97 15 9 4 6	7.7% 68.3% 10.6% 6.3% 2.8% 4.2%
Race	Indian Malay Chinese Others	88 18 29 7	62% 12.7% 20.4% 4.9%
Current employment status	Student Self-employed Employment for wages Retired Others	98 10 26 7 1	69% 7% 18.3% 4.9% 0.7%
Education Level	SPM Foundation Diploma Degree Master PhD	13 23 35 68 3 0	9.2% 16.2% 24.6% 47.9% 2.1% 0%
Level of knowledge in IT	Very weak Weak Neutral Strong Very strong	2 12 80 34 14	1.4% 8.5% 56.3% 23.9% 9.9%

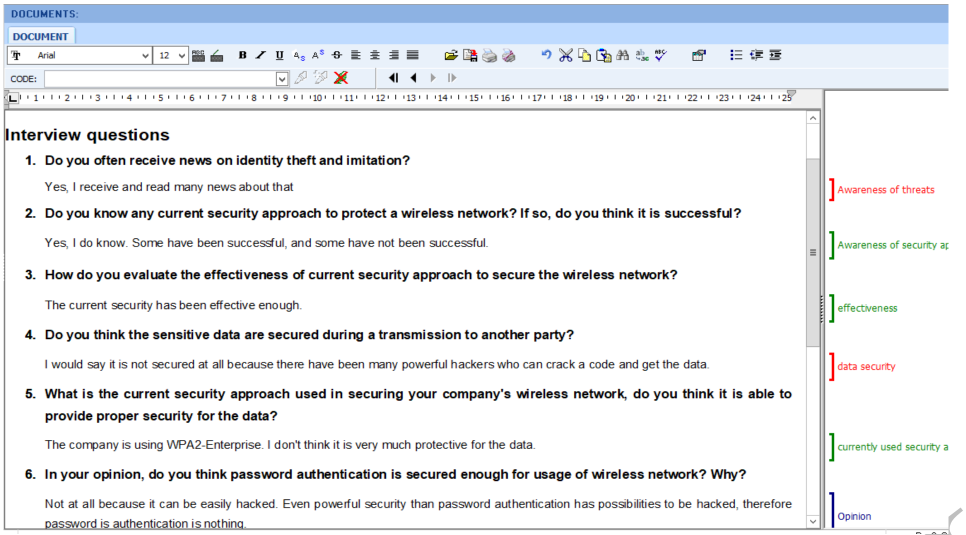
Table 1. Characteristic of samples in this paper

The next step is conducting data collections and using the software as a data analysis tool. The quantitative data is analyzed using SPSS software (Statistical Package for the Social Sciences) and qualitative data is analyzed using QDA miner software. The QDA miner is an open source software for qualitative data analysis with the ability of code, annotate, retrieve and analyze small to large data collections. It can be used to analyze the interview session, focus group, legal documents, etc. This tool is selected in this research to provide valid analysis. The samples of how the data is being analyzed are presented in Figure 1 and 2.



	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	Gender	String	8	0		{1.00, Male}...	None	7	Left	Nominal	Input
2	Age	Numeric	6	2		{1.00, Belo...	None	8	Right	Unknown	Input
3	Race	Numeric	8	2		{1.00, Indian...	None	8	Right	Unknown	Input
4	CurrentEmp...	Numeric	8	2		{1.00, Stude...	None	8	Right	Unknown	Input
5	LevelOfEdu...	Numeric	8	2		{1.00, SPM}...	None	8	Right	Unknown	Input
6	LevelOfKno...	Numeric	8	2		{1.00, Very ...	None	8	Right	Unknown	Input
7	Q1	Numeric	8	2	Are you aware ...	{1.00, Yes}...	None	8	Right	Unknown	Input
8	Q2	Numeric	8	2	Do you know a...	{1.00, Yes}...	None	8	Right	Unknown	Input
9	Q3	Numeric	8	2	In your opinion,...	{1.00, Yes}...	None	8	Right	Unknown	Input
10	Q4	Numeric	8	2	Rate how effect...	{1.00, Very ...	None	8	Right	Unknown	Input
11	Q5	Numeric	8	2	In your opinion,...	{1.00, Not i...	None	8	Right	Unknown	Input
12	Q6	Numeric	8	2	How secured y...	{1.00, Very ...	None	8	Right	Unknown	Input
13	Q7	String	100	0	In your opinion,...	None	None	8	Left	Nominal	Input
14	Q8	Numeric	8	2	Have you had a...	{1.00, Yes}...	None	8	Right	Nominal	Input
15	Q15Firewall	Numeric	8	2	Firewall	{1.00, Yes}...	None	11	Right	Nominal	Input
16	Q15Stronge...	Numeric	8	2	Have a stronger...	{1.00, Yes}...	None	10	Right	Nominal	Input
17	Q15AntiVirus	Numeric	8	2	Install an anti-vi...	{1.00, Yes}...	None	11	Right	Unknown	Input
18	Q15Others	Numeric	8	2	Others	{1.00, Yes}...	None	8	Right	Unknown	Input
19	Q16	Numeric	8	2	Wireless netwo...	{1.00, Yes}...	None	8	Right	Unknown	Input
20	Q17Userna...	Numeric	8	2	What type of a...	{1.00, Yes}...	None	8	Right	Unknown	Input
21	Q17Securit...	Numeric	8	2	What type of a...	{1.00, Yes}...	None	8	Right	Unknown	Input
22	Q17PINnum...	Numeric	8	2	What type of a...	{1.00, Yes}...	None	8	Right	Unknown	Input
23	Q17Others	Numeric	8	2	What type of a...	{1.00, Yes}...	None	8	Right	Unknown	Input
24	Q18	Numeric	8	2	Do you think th...	{1.00, Yes}...	None	8	Right	Unknown	Input
25	Q19Userna...	Numeric	8	2	Which type of ...	{1.00, Yes}...	None	8	Right	Scale	Input

Figure 1. SPSS analysis for quantitative data



Interview questions

1. **Do you often receive news on identity theft and imitation?**

   Yes, I receive and read many news about that

2. **Do you know any current security approach to protect a wireless network? If so, do you think it is successful?**

   Yes, I do know. Some have been successful, and some have not been successful.

3. **How do you evaluate the effectiveness of current security approach to secure the wireless network?**

   The current security has been effective enough.

4. **Do you think the sensitive data are secured during a transmission to another party?**

   I would say it is not secured at all because there have been many powerful hackers who can crack a code and get the data.

5. **What is the current security approach used in securing your company's wireless network, do you think it is able to provide proper security for the data?**

   The company is using WPA2-Enterprise. I don't think it is very much protective for the data.

6. **In your opinion, do you think password authentication is secured enough for usage of wireless network? Why?**

   Not at all because it can be easily hacked. Even powerful security than password authentication has possibilities to be hacked, therefore password is authentication is nothing.

Figure 2. QDA miner software to analyze qualitative data

Results and Discussion

In this section, the hypothesis testing is described. The Chi-square test to know whether there is an association between variables is used. The chi-square test for independence additionally called Pearson's chi-square test or the chi-square test of association, is utilized to find if there is a connection between two categorical variables (Laerd Statistics, 2013). It is additionally called a "goodness of fit" measurement since it measures how well the observed distribution of data fits with the distribution that is normal if the variables are independent. The value that should be taken in the count is the *p*-value. The *p*-value is compared with the alpha value which is a 5% level of significance. If the *p*-value is lesser compared with the *alpha* value, the result is statistically *significant*. By the end of this test, the state whether there are an association between the categorical variables can be found.

Hypothesis	Test statistic	df	p-value (Sig)
H1: **The ease of use** of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.	0.517	2	0.049
H2: **The suitability** of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.	9.659	2	0.008
H3: **The security & privacy** of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.	10.690	4	0.030
H4: **The level of knowledge** in IT will affect their agreement towards usage of multi-factor authentication as the restrictive approach.	32.641	8	0.000

H5: **The performance** of multi-factor authentication technologies will affect their agreement towards usage of multi-factor authentication as the restrictive approach.	11.791	2	0.003

Table 1. Results of Hypothesis testing

- **Ease of use:** Based on the findings, the ease of use has a positive impact on users' agreement towards usage of multi-factor authentication as the restrictive approach. Hence, it is important to implement multi-factor authentication that does not affect or amend any of the processes of security of the wireless network. Multi-factor authentication technologies do not have to be the same as the previous or other technologies that have existed to protect the network in order for users to know how it works and get their hands on multi-factor technologies easily.

- **Suitability:** Based on the findings, the suitability influences the users' agreement towards usage of multi-factor authentication as the restrictive approach. This shows users give priority to the comfort and cost of using the multi-factor authentication technology.

- **Security and Privacy:** There has been found that the security and privacy will affect the users' agreement towards usage of multi-factor authentication as the restrictive approach. The security provided by the multi-factor authentication should be excellent for it to be accepted by people and companies to implement it.

- **Level of knowledge in IT:** Based on the findings, the level of knowledge in IT has a positive impact on users' agreement towards usage of multi-factor authentication as the restrictive approach. It is essential to implement multi-factor authentication technology that is concise and effective yet clear for users who uses it without bringing down the data security.

- **Performance:** This finding shows that the factor has an influence towards users' agreement towards usage of multi-factor authentication as the restrictive approach. It is important to provide the performance without damaging the existing performance of the network.

Conclusions

Through the wide number of results collected from the questionnaires and also the result from the interview sessions, it can be concluded that multi-factor authentication technology should be implemented as multi-factor authentication acts an additional security feature by itself. All the hypothesis were accepted which shows both the factors and users' agreement towards multi-factor authentication as the restrictive approach.

References

1. Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S. J., & Sanyal, S. (2011). A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. *arXiv preprint arXiv:1111.3010*.
2. Karygiannis, T., & Owens, L. (2002). Wireless network security: 802.11, Bluetooth and handheld devices. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.
3. Neoh, D. (2003). Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate them. SANS Institute.
4. Widder, B. (2013, July 25). How to secure a wireless network. Retrieved from https://www.digitaltrends.com/computing/how-to-secure-a-wireless-network/
5. Wilkins, S. (2011). Wireless Security Considerations: Common Security Threats to Wireless Networks. Retrieved from https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats.