Research on Wireless Network Security Awareness of Average Users

Article *in* International Journal of Microwave and Wireless Technologies · March 2016

DOI: 10.5815/ijwmt.2016.02.03

CITATIONS
5

READS
1,855

3 authors:

Paschal A. Ochang
Federal University of Lafia
7 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Philip Irving
University of Sunderland
4 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Paulinus Okoi Ofem
Federal University of Lafia
8 PUBLICATIONS **13** CITATIONS
SEE PROFILE

I.J. Wireless and Microwave Technologies, **2016, 2, 21-29**
Published Online March 2016 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2016.02.03

***Available online at** http://www.mecs-press.net/ijwmt*

Research on Wireless Network Security Awareness of Average Users

Paschal A. Ochang[a*], Philip J. Irving[b], Paulinus O. Ofem[c]

[a]*Department of Computer Science, Federal University Lafia , Nasarawa State, Nigeria*
[b]*Department of Computing, Engineering and Technology,University of Sunderland, Sunderland, SR6 0DD, United Kingdom*
[c]*Department of Computer Science, Federal University Lafia , Nasarawa State, Nigeria*

Abstract

Network insecurity has become an increasing problem in the world of computer networks. Technical experts have tried to combat this by improving the technical awareness of the threats and technical solutions involved in Wireless Local Networks (WLAN) through technical reports and policy enforcement. The average users' knowledge and awareness of network security, how they react to the warnings and implement security measures is also very important. Current studies on users' awareness of security policies, whether it has been communicated well enough and how aware WLAN users are to the threats and issues involved are still not fully ascertained. To fill this gap it is important to find out the users basic knowledge of the security measures and policies. In this paper, statistical methods were developed and adopted in other to compare the knowledge of Information Technology (IT) related employees and that of non-technical employees on how aware they are of WLAN security threats and security measures. The techniques the paper has adopted revealed the knowledge gap between non-technical and technical users. This revelation is significant and therefore requiring more efficient methods for creating awareness on WLAN threats and countermeasures among average users.

Index Terms: WLAN, Network security, Security Policy, Employee behavior, Statistical analysis.

1. Introduction

The Literature review adopted in this paper is analyzed in two phases. First of all, possible technical solutions to wireless network attacks are discussed. Secondly, a wider discussion on policies for combating wireless network attacks and users' behavior towards the awareness and implementation of the technical solutions and adoption of the security policies are also analyzed.

* Corresponding author. Tel.: +2347032088685
E-mail address: pascosoft@gmail.com

1.1. Technical Wireless Network Challenges and Solutions

Before the advent of wireless local networks, wired networks existed with different security architectures. The transport medium of wireless networks has a higher potential of been attacked than a wired medium thereby increasing the threat to wireless networks [5]. An early study explains wireless network security as a combination of wireless channel security and network security [6]. Many challenges of the wireless network exists like the jamming of radio frequency signals using an attack called Denial of Service (DOS) which interferes with transmission over the wireless network [11]. A major reason for the success of most of this attacks has been due to the loopholes present in existing wireless network security protocols [15].

Technical solutions have been developed and made available to mitigate the threats aimed at wireless networks by the introduction of Wired Equivalent Privacy protocol (WEP) [3]. Although, [5] reiterated the claims of [3], but indicated that the Wi-Fi Protected Alliance (WPA) which was also developed to enhance wireless network security introduced a better solution through the use of Temporal Key Integrity Protocol (TKIP) to replace WEP keys for wireless user confidentiality. In spite of the fact that these solutions help so much in reducing security breach, it is also important to change the way of thinking and awareness of the users of the network. Reference [7] advocated the move of network users towards a more security-positive environment by changing their attitude and becoming part of the security solution and not part of the problem. Reference [7] went further to point out that raising awareness to change people's behavior on security concerns is a good start.

1.2. Wireless Network Users and Policies

Some prior studies have helped in their own way to change people's attitude by advocating the use of wireless security policies. In an effort to address the network security problems, many published papers have provided solutions in an organizational or technical approach [9]. Although the potential advantage of this is that the user is rescued from the technicality burdens but will face difficulties when a new challenge arises. Therefore the need to be aware that wireless network spans from an average network user to a professional has not been considered. In support of this is [2], which identified that the users of wireless internet in public hotspots are so oblivious to the dangers they are exposed to such as a hacker who doesn't need to be in the same physical location to sniff into their network, linking them to possibly that of an organization they work for. Furthermore, [14] pointed out that new technology like Near Field Communication (NFC) which is based on wireless network technologies could be compromised by a hacker through eavesdropping on the network thereby leading to stealing of payment credentials because NFC is usually used for contactless payments. A potential solution to this was [10], who pointed out that the efforts that have been made to combat unauthorized wireless access is mainly focused on outsiders thereby neglecting breaches from insiders of an organization itself and hence, adopted a policy based wireless security management solution to address organizations on how to solve the existing issues.

A more user focused empirical study by [8] which was carried out on users' behavior in a university shows that 9% of 3,331 of personal computers on campus do not have firewalls properly configured on them. In addition to this, 60% of wireless networks did not use any good form of authentication or encryption according to a survey by panda international and also vulnerability checks indicated a good number of users not having firewalls on their computers. This was attributed to negligence on the part of the users. Hence, user behavior is important in terms of network security.

Existing limitations in current literatures have somewhat not analyzed the behavior of users. They have restricted their studies to the IT professionals' behavior at work only and have not extended it to the average non-technical user who knows nothing about IT. Reference [1] emphasized that the aspect of IT professionals complying with the laid down security policies in organizations and the technical controls of securing the wireless network has mostly been the basis of literature so far neglecting the thoughts of the end user

community; however, both the professional and non-professional have still failed to comply with these rules. Reference [4], mentioned in a survey that the human aspect of insecurity is an important area to consider when listing possible threats to a wireless network. Research has also shown that there is an 80% chance of confidential information to be exposed in more than 50% of enterprises checked and this is due to the installation of ill-managed access points by careless operators.

According to [12], research in the technical aspect of security policies is far more than research in the behavioral aspect of policy making. Their theory was validated when they carried out a research into what causes security governance lapses in an organization using two different approaches, the informal approach takes into account the individual beliefs and culture of employees and the technical approach which involves applying stringent rules and constant monitoring to see if network security policies are followed. They stated that it is important to synchronize individual employee's personal values along with that of the organization.

1.3. Research Objective

The studies presented so far have indicated policy making and provided technical solutions to the engineering aspect of wireless security but currently public end users still fall victim to attacks carried out through wireless networks. The wireless network is used by virtually everyone in the world today no matter the profession but whether the IT field is sharing enough knowledge with end users who are not IT inclined in such a way that they can understand and implement is yet to be discovered. The objective of this research seeks to find out why this security problem lingers on by investigating whether the public end users who work in non IT based firms know the basic wireless network security information as much as they should. Hence we have developed a hypothesis (H1) along with a null hypothesis (H0) in case the main hypothesis is refuted.

H1: The users of the wireless networks in IT related firms have a significant knowledge of wireless security policies and measures than the average users.

H0: The users of wireless networks in IT related firms have less significant knowledge of wireless security policies and measures than the average users.

2. Research Methodology

2.1. Data Collection Procedure

In other to maximize reliability in measurement, a quantitative technique using questionnaires as the survey instrument is adopted and a sample of the questionnaire showing the questions used can be found in the appendix section of the paper. In a bid to reduce technicalities, each question has been explicitly defined using simple terms for instance (wireless security, policies awareness, wireless security attacks etc.) so that the respective respondents tend to have the same understanding and answer each question honestly. Also adopted was a 5-point Likert Scale [13] (spanning from 1-strongly disagree, 2-disagree, 3-neither agree nor disagree, 4-agree, 5-strongly agree) for each item question in the questionnaire to enable each respondent indicates his level of awareness with the statement question. The questions have been designed to find out and measure their level of awareness of wireless security policies by asking each respondent if they have heard of certain threats, attacks and solutions to wireless networks and also whether they have ever implemented it before. Each questionnaire contained Ten (20) questions and was distributed to total of 40 people comprising of 20 employees from IT firms and 20 employees in non- IT firms (average public users/employees). The main reason behind choosing respondents from these two sectors is to find out if common wireless security policies, awareness and knowledge are well known to all wireless network users and not the IT related users alone. The data gotten from the responses of the employees by summing the Likert scale grades is shown in Table 1 below. Table 1 below also depicts data gotten from both sets of respondents to the questionnaires.

Table 1. Summation of statistical data gotten from the Respondents

IT employees	80	81	89	90	78	81	90	86	81	78	86	88	90	80	75	77	93	89	86	81
Public employees	77	67	57	68	75	69	86	81	78	69	65	66	66	50	69	78	64	70	66	63

In a bid to back up the result further, a qualitative test was carried out by interviewing some of the employees. When asked if they've heard about some few published policies against using private unsecured devices on the organizational network, one of them responded thus "I have never heard of these policies" and the other employee simply said "I have heard of the policies but are too technical for my understanding". These responses confirm [7] who pointed out that people's awareness towards security is very important for a secure network

2.2. Analytical Techniques and Rationale

The use of SPSS software was implemented for the analysis, testing, measurement and validation of this model. The analytical techniques of SPSS are employed to provide descriptive statistics using histograms to graphically represent the (mean value, skewness and kurtosis) for each group of data. The mean is the average value of each set of variable based on the average users or public users and the IT related employees; the skewness is a measure of the lack of symmetry of the distribution of data on each graph and finally the kurtosis which is a measure of whether or not the scores are peaked or flat towards the mean score. A graphical representation using histograms was produced from the available data (See Fig. 1 and Fig. 2) showing the mean, skewness and kurtosis. A proof for normality of data on the graph was conducted using the Shapiro-Wilk test (See Table 3). Finally a method of comparing the means of both sets of data was also conducted for comparing the significant difference between the means of both sets of data (IT and Public).

Table 2 below is a descriptive statistic showing the mean, skewness, kurtosis and other related data. It shows that the mean of the IT employee is more than that of the Public employees. And the skewness and kurtosis are slightly close to zero which also shows approximate normality of the data distribution.

Table 2. Descriptive Statistics of Respondents

	IT employees	Public employees
Number of valid data	20	20
Mean	83.9500	69.2000
Standard error	1.18871	1.85614
Skewness	.022	-.106
Std. Error of Skewness	.512	.512
Kurtosis	-1.333	.672
Std. Error of Kurtosis	.992	.992
Standard deviation	5.31606	8.30092
Variance	28.261	68.905

3. Interpretation of Results and Suggested Findings

Table 2 above shows that the IT employees mean value (83.9500) is higher than that of the public employees (69.2000); therefore this suggests that the Public employees know little about wireless network security, laid down policies and awareness as compared to those who work in IT related firms. Furthermore, verification of the normality of the data gotten from the respondents was carried out in other to prevent the occurrence of abnormal data and also validate our findings. We used a histogram graph for both sets of data in other to get the kurtosis and skewness values.

The histogram graph of frequency against IT employees' data as shown below in Fig. 1 indicates that the data are approximately normally distributed because the skewness and kurtosis values fall in between -2 and +2. In the histogram, the pile of data to the left of the distribution shows that it is positively skewed (0.22) and the flat top near the mean indicates that it has a negative kurtosis (-1.333).

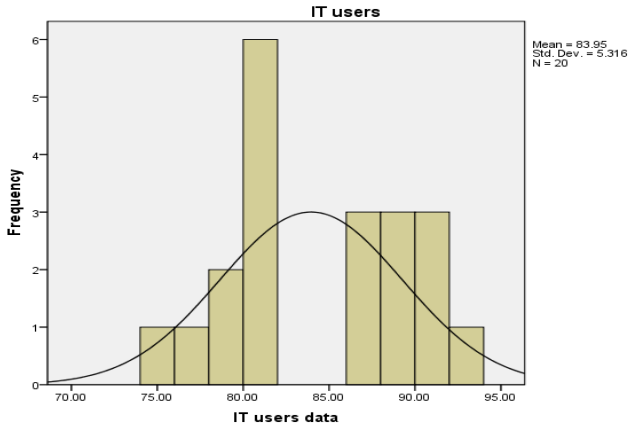

Fig.1. Histogram graph for IT employees.

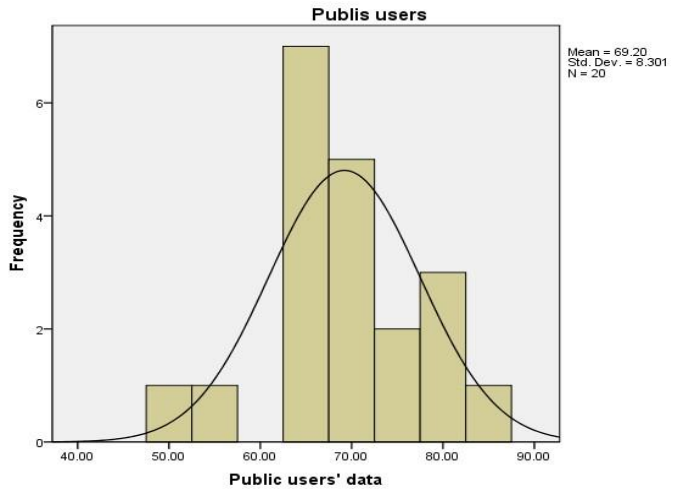

Fig.2. Histogram graph for public employees

The histogram graph of Frequency against Public employees' data as shown in Fig. 2 below indicates that the data are approximately normally distributed also because the skewness and kurtosis values fall between -2 and +2. In the histogram, the pile of data to the right of the distribution is shows it is negatively skewed (-.106) and the peaked data near the mean indicates that it has a positive kurtosis (.672).

A proof of normality of the distribution using Shapiro Wilk test was also carried out on the data. Table 3 shows both the IT and Public employees' data are normally distributed. Both significant values are greater than 0.05 (sig > 0.05) which simply means that both sets of data are normally distributed.

Table 3. Test for normality

	Shapiro-Wilk		
	Statistic	Df	Sig
IT employees	.929	20	.150
Public employees	.960	20	.551

In a further effort to compare the means and check if the difference between them is significant or not, we designed and conducted a parametric test. In this case a test for equal variance and an Independent Sample T-Test; because the groups of data are independent of each other. In the statistical procedure, both sets of data were put together as a group but differentiated by assigning zeros (0s) to IT and ones (1s) to Public employees as shown in Table 4. Table 5 below shows that irrespective of the variance being equal or not, the sig (2-tailed) value is less than 0.05 (< 0.05) which simply means that there is a significant difference between the means of both the IT and public employees.

Table 4. Grouping of data

Knowledge	N	Mean	Std. Deviation	Std. Error Mean
IT(0) and Public 0 employees(1) 1	20	83.95	5.316	1.189
	20	69.20	8.301	1.856

Table 5. Independent Sample Test Results

	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
								Lower	Upper
IT and Public employees	Equal variances assumed	.987	.327	6.692	38	.000	14.750	2.204	10.288	19.212
	Equal variances not assumed			6.692	32.341	.000	14.750	2.204	10.262	19.238

The implication of this is that the public employees are significantly low in the knowledge of wireless network security. This assists in proving the main hypothesis (**H1**) and disproving the null hypothesis (**H0**). The significant difference in the means of both sets of data and by proving the main hypothesis through our research, we have shown that average users who are not technically inclined do not know much about wireless network security especially in their respective work

4. Conclusions

Wireless networks and hotspots are now widely deployed in homes offices and public areas thereby increasing threats to security. They are already security measures embedded with most wireless network deployments. However, user's awareness towards these threats and how to mitigate these threats without the need of technical experts is still an issue. Our research and results calls for more focus to be directed towards those who are not IT inclined in other to enhance their awareness towards making their own personal in efforts in enhancing security and at the same time prevent them from being the point of entry for hackers into their organizational networks.

References

[1] Herath, T. and H. Rao, Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 2009. 47(2): p.154-165.
[2] Park, J.S. and D. Dicoi, WLAN security: current and future. IEEE Internet Computing, 2003. 7(5): p. 60-65.
[3] Miller, S.K., Facing the challenge of wireless security. Computer, 2001. 34(7): p.16-18.
[4] K. Summers, W.C. and A. DeJoie. Wireless security techniques: an overview. 2004: ACM
[5] Arbaugh, W.A., Wireless security is different. Computer, 2003. 36(8): p. 99-101.
[6] Russell, S. F. Wireless network security for users, 2001. IEEE, p. 172-177
[7] Durbin, S. (2011). Tackling converged threats: building a security-positive environment. Network Security (6): 5-8
[8] Chenoweth, T., R. Minch, and S. Tabor. User security behavior on wireless networks: An empirical study. 2007: IEEE
[9] Dourish, P., et al., Security in the wild: user strategies for managing security as an everyday, practical problem. Personal and Ubiquitous Computing, 2004. 8(6): p. 391-401
[10] Lapiotis, G., Kim, B., Das, S. & Anjum, F. A policy-based approach to wireless LAN security management, 2005. IEEE, p. 181-189
[11] Manley, M., Mcentee, C., Molet, A. & Park, J. Wireless security policy development for sensitive organizations, 2005. IEEE, p. 150-157
[12] Mishra, S. & Dhillon, G. Information systems security governance research: a behavioral perspective, 2006. p. 27-35
[13] Likert, R., A Technique for the Measurement of Attitudes. Archives of Psychology 140, 1932. p. 1–55.
[14] Nagashree R N, Vibha Rao, Aswini N,"Near Field Communication", IJWMT, vol.4, no.2, pp.20-30, 2014.DOI: 10.5815/ijwmt.2014.02.03
[15] Gu Jiantao,Fu Jinghong,Wu Tao,"Analysis of Current Wireless Network Security", IJEME, vol.2, no.10, pp.34-38, 2012.

Appendix A. Survey Questions for security awareness of average users

To what extent would you agree to the following questions/statements?

		Strongly Disagree	**Disagree**	**Neither agree Nor disagree**	**Agree**	**Strongly Agree**
	Question	**1**	**2**	**3**	**4**	**5**
1	You are very aware of the activities of your organization's information security team					
2	Wireless network security/information security is important to your daily job and activities					
3	You understand to an extent the basic wireless network security protocols and how to set up a personal hotspot					
4	No hacker would attack me or my computer. I don't have anything they would want					
5	You are very confident that you would recognize the symptoms and signs of a computer security incident. (Computer security incidents may include viruses and malware on your PC or smartphone, a hacker gaining unauthorized access to your system or an attacker tricking you into giving away sensitive information over the phone or by email)					
6	You are aware of wireless network security attacks such as denial of service, password cracking etc.					
7	If you were to suspect that your computer, smartphone or other device was involved in a wireless network security incident such as a virus, hacker attack or some other problem, you would know what to do.					
8	you worry often about the security risks of using wireless networks especially for internet access					
9	You are very familiar with the information management policies of your organization, including using your personal devices on the wireless network.					
10	you feel involved in the daily process of information security and protecting the organization's information assets					
11	you often feel it is important to keep your computers, mobile devices and programs updated and current					
12	You have set up a wireless hotspot before using either your phone, computer or mobile router					
13	You know the differences between the WEP and WPA protocols					
14	If you set up a hotspot you will know if someone else has connected to your hotspot illegaly					
15	You interact with your organization's information security team at least once a week (receiving an email, receiving security training, having an information security team member in a meeting, etc)					
16	The network security policies of your organization are to technical or difficult to understand					
17	You feel confident connecting to a wireless network or hotspot without knowing the entity that created the network					
18	You prefer using a wired network over a wireless network because you feel you are not sure of the security of the wireless network					
19	You know some of the basic tools and software used by wireless network attacks					
20	you feel you need more training on understanding basic wireless network security					

Authors' Profiles

Paschal A. Ochang: Paschal A. Ochang is an Assistant Lecturer in the Department of Computer Science, Federal University Lafia, Nigeria. He has worked in the network engineering field for over 9 years. He holds a B.Eng. in Computer Engineering and a M.Sc. in Telecommunications Engineering which was gotten from the University of Sunderland, Sunderland, United Kingdom. He is a Microsoft Certified Professional (MCP) and has worked with the largest CDMA network in Africa called Visafone Communications LTD as a Data Service Consultant. His research interests cover the areas of Voice over Internet Protocol (VoIP) networks, intelligent networks, network architecture, multicast networks and network security.

Philip J. Irving: is a Senior Lecturer in the Department of Computing, Engineering and Technology at the University of Sunderland. He has worked in the networking and operating systems field for over 20 years in both academia and industry. He holds and MSc in Ecommerce Management. He is a Cisco Certified Academy Instructor (CCAI) for Cisco Certified Network Associate (CCNA) and Cisco Certified Networking Professional (CCNP) and manages the Cisco Academy at the University of Sunderland. He teaches on a range of both undergraduate and postgraduate programmes including Telecoms and Networking. He is also research active in the area of Network Risk assessment for Systems change.

Paulinus O. Ofem: Paulinus is also an Assistant Lecturer in the Department of Computer Science, Federal University Lafia, Lafia, Nigeria. He obtained his MSc in Advanced Computer Systems Development from the University of the West Scotland, in the United Kingdom and BSc in Computer Science from the University of Calabar, Calabar, Nigeria. He began his academic and research career as a research assistant at Laurea University of Applied Sciences, Finland and the University of the West of Scotland. His research interest include empirical software engineering and software security, service oriented architecture, databases and human computer interaction.