

Constraints to the Security and Effectiveness of Bluetooth Technology in File Transfer among Postgraduate Students in South Eastern University by

Uzoegwu, R. A., Onah, B. I., Eze, B.N. & Agbo, L. N.

Department of Computer and Robotics Education

University of Nigeria, Nsukka

Corresponding Author: ifeoma.onah@unn.edu.ng

Abstract

Bluetooth technology has become an integral part of this modern world. It provides a short distance wireless communication between devices and other network with low cost and low power, making it convenient for the users. However, as the Bluetooth technology becomes widespread, vulnerabilities in its security protocols are increasing which can be potentially dangerous to the privacy of a user's personal information. The study aimed to determine the Constraints to the Security and Effectiveness of Bluetooth Technology in file transfer among Postgraduate Students in Universities in South East, Nigeria. Three specific purposes were used for the study while three research questions guided the study and one null hypothesis was formulated and tested at 0.05 level of significance. The research design used for the study was descriptive survey design. The study was carried out in the five federal Universities in South east Nigeria. The population for the study comprises of 930 respondents which include master's students in the study area. Multistage sampling technique was used for the study. Therefore, the sample size is 93 postgraduate students. Questionnaire was used to collect relevant data from the respondents. The instrument was validated by five experts in the department of computer and related discipline. Internal consistency of the instrument was determined using Cronbach Alpha reliability coefficient. A reliability coefficient of 0.774 was obtained. The data collected were analyzed using mean and standard deviation to answer the research questions and t-test statistics for testing the hypothesis. The study found out the constraints to the security and effectiveness of Bluetooth technology in file transfer to include but not limited to Bluetooth range, transmission rate of the Bluetooth, and vulnerabilities in Bluetooth technology. Based on the findings of the study, it was recommended that Bluetooth security experts should include awareness-based education to support user's understanding and knowledge of Bluetooth security among others.

Keywords: Constraints, File transfer, Effectiveness, Security and Bluetooth technology

Introduction

The increasing popularity of wireless technologies and the continuing advancements in portable computing are flowing together in a raising demand for wireless networks such as Bluetooth Technology. This Technology has become a smart technology for efficient and flexible wireless communication system. Bluetooth Technology was designed as a cable replacement technology. Bluetooth is defined as a wireless alternative to data cables by which data is interchanged using radio transmission (Muhammed, Mosharani, Muthapriya, Mufthas, Malikberdi, & Dhishan, 2016). It is also a short radio link designed to connect portable and/or

fixed electronic devices (Vikethozo, 2014). In view of Purvish, Akash, Nisarg and Clinton (2015), Bluetooth Technology is a short-range data transmission technology that is used primarily to build wireless personal area networks. The authors further explained that Bluetooth Technology has been linked up with many kinds of devices, including cell phones, laptops, automobiles, and many hand-held devices supporting this technology.

However, this is in line with the Gypsy, (2014), view that Bluetooth Technology is a combination of software and hardware technology. The author further explained that the hardware is riding on a radio chip and the

main control and security protocols have been implemented in the software. Bluetooth Technology allows your device to establish ad hoc (temporary) networks which allow easy connection between devices in the same physical area with no need of any infrastructure devices (Purvish et al, 2015). The authors further explained that in Bluetooth Technology, the master gadget manages and builds the network, which also include defining the network's frequency hopping scheme. In the same vein, the authors said that the topology also gets changes once the device moves away or towards the master device, along with the relationships of the devices in the immediate network. Hence, in the context of this study, Bluetooth Technology is the technology that will allow the postgraduate student to share educational resources through file transfer.

Bluetooth is a great way to wirelessly transfer of files like Educational resources among postgraduate students. Bluetooth file transfer is a simple way to send files to another nearby device without the need for a separate app (Goodner, 2018). The author further explained that one needs to know how to pair a Bluetooth headset to a smart phone and equally capable of transferring files over Bluetooth. In view of Stanley, (2019), pairing in Bluetooth, is considered as a trusted relationship between two devices and it is formed by exchanging shared secret codes referred to as PINs. This is in line with the view of Muhammed et al (2016), who stated that A 'master' device has the option of pairing with up to seven 'slave' devices establishing a network called a piconet and two or more piconets together forms a scatternet, which can be used to eliminate Bluetooth range restrictions. The author further explained that a scatternet is formed when the devices act as 'master' or 'slave' devices in multiple piconets at the same time. In support of this, (Purvish et al, 2015), buttressed that a master is the device which initiates communication with other devices and governs the communications link and traffic between itself and the slave devices associated with it. The authors explained that a slave device is the device that responds to the master device and are required to synchronize the transmit/receive timing with that of the

masters. In addition, Purvishet all further explained that transmissions by slave devices are governed by the master device (i.e., the master device dictates when a slave device may transmit).

Bluetooth file transfer offers an efficient way of exchanging files from one Android device to another and contents of Bluetooth enabled devices (Unuth, 2018). Similarly, the author buttressed that Bluetooth users can easily select a file from their devices and send it to a device of their choice, or find the specific file on another device and download it. The ease of use and great user interface make this a phenomenal application (Andrea, 2014). The author further stressed that the Bluetooth file transfer is a mere 2.9MB, making it an incredibly light and quick application that downloads within seconds. On startup, users are greeted by a friendly user interface featuring a modern dark background with sharp white text that is easy to read (Muhammed et al, 2016). In support of Vikethozo, (2014), who stated that on the first tab, users can browse their own file structure and select files that they wish to share; while on the second tab, users can manage their Bluetooth connections and browse the file structure of selected devices. The author further discussed that this app also adds another level of security to Bluetooth connections by requiring authentication on all incoming connections. Favorite and trusted connections can be saved for faster file transfer in the future Goodner (2018). However, for the effectiveness of this Bluetooth file transfer among postgraduate students, there is need to consider the constraint to the use of the technology.

Constraint is something that imposes a limit or restriction or that prevents the effectiveness of Bluetooth file transfer of educational resources among the postgraduate students. According to Pasquale, Jan and Marco (2012), Bluetooth file transfer constraint is the limitation to the sharing of files among users. The author further explained that the constraints will restrict the users for efficient way of exchanging files from one Android device to another. In view of Unuth, (2018), the constraint may limit users from easily selecting

a file from their devices and send it to a device of their choice, or find the specific file on another device and download. Moreover, according to Gypsy, (2014), Bluetooth file transfer constraints include Bluetooth range, transmission rate of the Bluetooth and Security vulnerability in Bluetooth technology.

Bluetooth Technology is a short-range wireless network technology that can be used to share educational resources among postgraduate students. According to Gypsy, (2014), Bluetooth range is a short-range wireless technology that enables wireless data communication between digital devices, such as a computer and digital camera. The author further explained that the Bluetooth wireless technology operates within a range of about 10m (30 feet). In view of Goodner, (2018) that because of the short-range of Bluetooth, the devices and Wi-Fi use the same frequency, microwave interference may occur and resulting in communication speed deterioration, noise, or invalid connection. Unuth (2018), also noted that the limited range is dependent on the specific class of radio it uses. The author further explained that the enabled devices can only establish and maintain wireless communication as long as the devices are within the range limit. For the fact that the Bluetooth covers a short range, the transmission rate will equally short.

Transmission data rate of the Bluetooth is the process of wireless signals transmission that cover a short distance up to 10m. In addition, Colak, Oral, Caglayan and Kazanci (2015), explained that the transmission allows both data and voice connections, with a nominal maximum data of 723kbps. This is in line with Andrea (2014), who stated that data transmission rate in Bluetooth sends data relatively slowly. The author further explained that the data transmission in Bluetooth is not a substitute for faster technologies. This is because data can be transmitted only over short distances, network overloading may occur, if one path is busy then the other will wait till the part is cleared. On the other hand, Muhammed et al (2016) pointed out that the data transmission rate in Bluetooth is related to its low power. The authors further explained that

the low power devices limit the rate of transmission to 10meters. The authors buttressed that even with the low power, Bluetooth do not require line of sight between communicating devices.

Security vulnerability in Bluetooth technology is a weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system. Bluetooth offers several security modes, and device manufacturers determine which mode to include in a Bluetooth-enabled gadget (Carol, 2015). The author explains more that in almost all cases, Bluetooth users can establish "trusted devices" that can exchange data without asking permission. When any other device tries to establish a connection to the user's gadget, the user has to decide to allow it. According to Pravin, (2015), security methods include authorization and identification procedures that limit the use of Bluetooth services to the registered user and require that users make a conscious decision to open a file or accept a data transfer. The author buttressed more than as long as these measures are enabled on the user's phone or other device, unauthorized access is unlikely. Nateq and Mohammed (2012), supported the view that a user can also simply switch Bluetooth mode to "non-discoverable" and avoid connecting with other Bluetooth devices entirely. The authors further buttressed that if a user makes use of the Bluetooth network primarily for synching devices at home, this might be a good way to avoid any chance of a security breach while in public. Still, early cell-phone virus writers have taken advantage of Bluetooth's automated connection process to send out infected files Marcus and Erik (2014). However, since most cell phones use a secure Bluetooth connection that requires authorization and authentication before accepting data from an unknown device, the infected file typically does not get very far (John, John, Mayank, Marcel, Rhonda, Lily and Karen (2017). When the virus arrives in the user's cell phone, the user has to agree to open it and then agree to install it. This has, so far, stopped most cell-phone viruses from doing much damage.

Although the Bluetooth technology is a key component of wireless communication and is undoubtedly considered a very popular technology, it provides a low-energy and low-cost solution for short-range radio transmissions. It has also some security 'loop-holes' that make it vulnerable. The postgraduate student in the universities in Southeast Nigeria make use of the Bluetooth technology, but preliminary investigation by the researchers shows that it is not used effectively. Therefore, there is need to determine the constraints to the effectiveness of the Bluetooth technology among the postgraduate students.

Statement of the Problem

Bluetooth technology has been considered as a cheap, reliable and power efficient replacement of cables for connecting electronic devices. It permits to connect various electronic devices wirelessly to a system for the transferring of data. Bluetooth technique offers numerous advantages such as the use of it to transfer data, verbal communication as well as in exchanging multimedia data such as songs, videos, pictures among others. Bluetooth power consumption is low and it is cheap. It can be used anywhere because no wire is required for its connection and it is easy to use because of the interactive interface it offers. It offers some security methods which include authorization and identification procedures that limit the use of Bluetooth services to the registered users and require that users make a conscious decision to open a file or accept a data transfer.

Despite these advantages that Bluetooth technology offer, and the security features that it has, students are still not very able to transfer file/data through Bluetooth effectively and there are still some security loopholes in Bluetooth technology. A preliminary investigation by the researches revealed that postgraduate students in Southeast Nigeria is still making use of flash drive, Compact disk, external hard disk among others to share educational resources. This will increase the spread of computer virus, piracy and plagiarism among students.

Based on this backdrop, the researchers decided to conduct a research on the Constraints

to the Security and Effectiveness of Bluetooth Technology in file transfer among Postgraduate Students in South East University to bridge the gap.

Purpose of the Study

The purpose of this study is to find out the Constraints to the Security and Effectiveness of Bluetooth Technology in file transfer among Postgraduate Students in South East University. Specifically, the study seeks to identify;

1. factors affecting Bluetooth range.
2. factors affecting the transmission rate of the Bluetooth.
3. security vulnerabilities/threats in Bluetooth technology.

Research Questions

The following research questions guided the study;

1. What are the factor affecting Bluetooth range?
2. What are factors affecting the transmission rate of the Bluetooth?
3. What are the security vulnerabilities/threats in Bluetooth technology?

Hypothesis

The following null hypotheses were formulated and tested at 0.05 level of significance.

H₀₁: There is no significant difference in the mean ratings of the respondents on the Constraints to the Security and Effectiveness of Bluetooth Technology in file transfer among Postgraduate Students in South East University

Methodology

This study adopted descriptive survey research design. Carol (2015) stated that, descriptive survey design attempts to describe and explain conditions of the present by using many subjects and questionnaires to fully describe a phenomenon. Descriptive survey is therefore appropriate for this study since questionnaires were developed and utilized for data collection. The study was carried out in the five federal Universities in the South east

Nigeria. These include University of Nigeria, Nsukka, Nnamdi Azikiwe University, NdufuAleke University, Micheal Okpara University and Federal University of Technology Owerri. The choice of the area is based on their peculiarity in the use of Bluetooth Technology among postgraduate students. The population for the study comprised of 930 respondents which include master's students in the study area. Multistage sampling technique was used for the study; stage one, Purposive sampling technique was used to select the five federal Universities out from the state and private Universities. Stage 2 stratification sampling techniques was use to select 10% of the student from the entire population. Therefore, the sample size is 93 postgraduate students. Questionnaire was used to collect relevant data from the respondents. A structured questionnaire consisting of 23 items, divided into three sections was used to collect information from the respondents. The questionnaire items were generated from literature review to reflect the research questions.

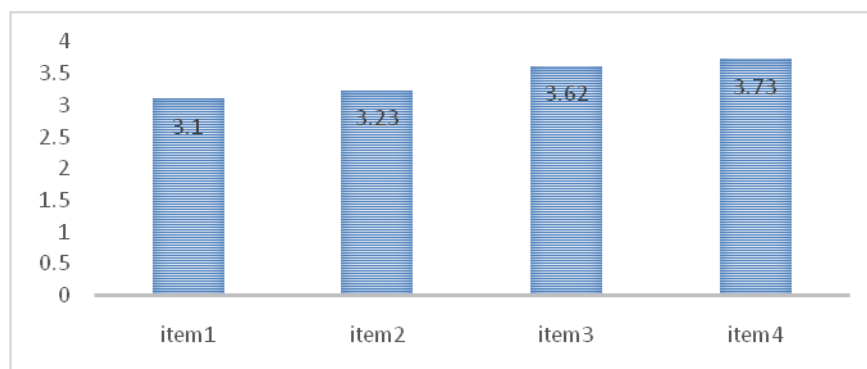
Results

Table 1

Mean Responses and Standard Deviation of the Postgraduate Students on the Factors Affecting Bluetooth Range

S/N	ITEMS	$\bar{X}$	SD	DECISION
1	The output power of the transmitter	3.10	0.55	Agree
2	The sensitivity of the receiver	3.23	0.53	Agree
3	Physical obstacles in the transmission path	3.62	0.71	Agree
4	The antennas	3.73	0.59	Agree

Note: SD: Standard Deviation; $\bar{X}$: Mean



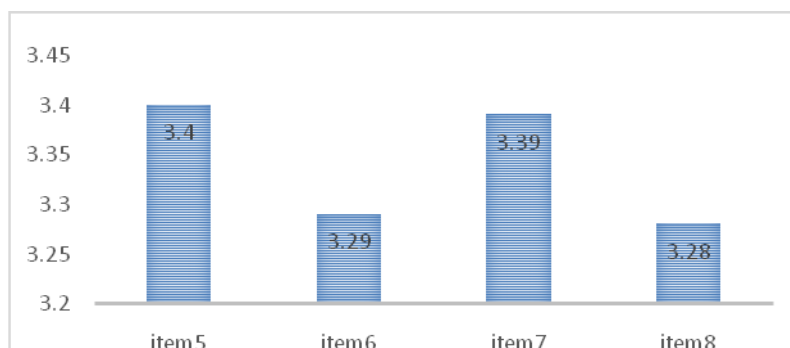
The data presented in table 1 above indicated that 2 out of 4 items (item 3 and 4) on the factors affecting Bluetooth range, had their mean scores ranging from 3.62 to 3.73 which indicates that they fall within the response of Strongly Agree. Furthermore, the table shows that items 1 and 2 had a mean score of 3.10 and 3.23 respectively, which fall within the response

statement of Agree. This implies that the four items are the factors affecting Bluetooth range. The table also showed that the standard deviations of the items were within the range of 0.53 to 0.71; this indicated that the respondents were not far from the mean and one another in their responses.

Table 2: Mean Responses and Standard Deviation of the Postgraduate Students on the Factors affecting the Transmission Rate of Bluetooth

S/N	Items	$\bar{X}$	SD	DECISION
5	Network congestion	3.40	0.98	Agree
6	Network latency	3.29	0.52	Agree
7	Health of the client and server	3.39	0.86	Agree
8	Infrastructure parameter	3.28	0.61	Agree

SD: Standard Deviation; X: Mean



Data in table 2 revealed that all the four items had their mean values ranged from 3.28 – 3.40. This indicates that the four items are the factors affecting the transmission rate of Bluetooth. The table also showed that the

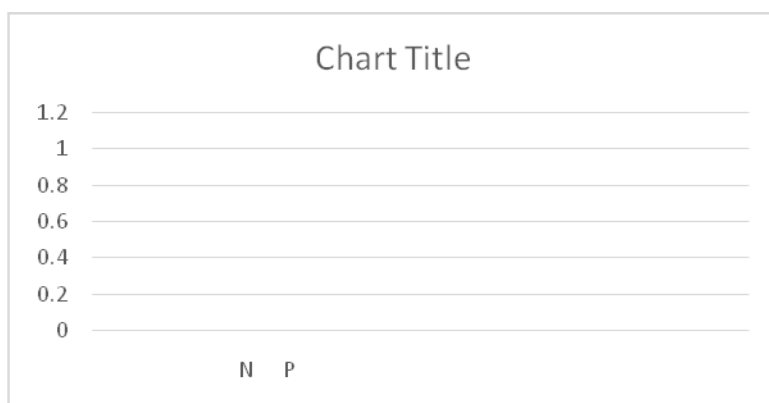
standard deviations of the items were within the range of 0.61 to 0.98; this indicated that the respondents were not far from the mean and one another in their responses.

Table 3: Mean Responses and Standard Deviation of the Postgraduate Students on the Security Vulnerabilities/Threats in Bluetooth Technology

S/N	Items	$\bar{X}$	SD	DECISION
9	Sensitive information that is not encrypted(or that is encrypted with poor cryptographic technique) and that is transmitted between two wireless devices may be intercepted and disclosed	3.30	0.72	Agree
10	Denial of service attack may be directed at Bluetooth connections or devices	3.31	0.71	Agree
11	Malicious entities may steal the identity of legitimate users and masquerade as them on internal	3.29	0.74	Agree

	or external networks			
12	Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external networks	3.40	0.68	Agree
13	Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements	3.32	0.72	Agree
14	Malicious entities may deploy unauthorized equipment to surreptitiously gain access to sensitive information	3.29	0.63	Agree
15	Handheld devices are easily stolen and can reveal sensitive information	3.54	0.63	Agree
16	Data may be extracted without detection from improperly configured devices	3.33	0.78	Agree
17	Viruses or other malicious code may corrupt data on a Bluetooth device and subsequently be introduced on a wired network connection	3.43	0.79	Agree
18	Malicious entities may, through Bluetooth connections, connect to other agencies or organizations for the purpose of launching attack and concealing their activities.	3.28	0.79	Agree
19	Interlopers, from inside or outside may be able to gain connectivity to Bluetooth management controls and thereby disable or disrupt operations	3.34	0.78	Agree
20	Internal attack may be possible via ad hoc transmission	3.40	0.65	Agree
21	The deliberate alteration of information in an attempt to mislead the recipient	3.20	0.88	Agree
22	Information can leak from the target system to an eavesdropper that is not authorized to access the information	3.39	0.82	Agree
23	The user can be blocked to get connected to a service by making it unavailable or severely limiting its availability to an authorized user	3.35	0.83	Agree

SD: Standard Deviation; X: Mean



Data in the table above shows that one item out of 15 items had a mean score of 3.54 which indicates that it falls within the response of Strongly Agree. This implies that the respondents strongly agreed that item 15 is one of the security vulnerabilities in Bluetooth

technology. Furthermore, the table shows that item 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22 and 23 had their mean score ranging from 3.20 to 3.43 which falls within the response of Agree. This implies that items 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, and 23 are also

seen by the respondents as the security vulnerabilities in Bluetooth technology.

Table 4: Summary of test of Significance between the Male and Female Post Graduate Students on Constraints to the Security and Effectiveness of Bluetooth Technology in File Transfer among Postgraduate Students in South East University

Among Postgraduate Students in South East University								
Respondents	N	X	SD	DF	Sig value	F	Decision	
Male	40		3.56	0.75	91	.342	22.01	N/S
Female	53	3.93	0.91					

Note: SD: Standard Deviation; DF: Degree of Freedom; X:Mean

Table 4 shows that F-calculated value for the groups are 22.01 with a significance of 0.34 which is greater than 0.05. Hence, the null hypothesis was therefore accepted at 0.05 level of significance. With this result, it indicated that there was no significant difference in the mean responses of male and female on the Constraints to the Security and Effectiveness of Bluetooth Technology in file transfer among Postgraduate Students in South East University

Discussion of the Findings

The findings of the study in research question 1 which deals with the factors affecting Bluetooth range revealed that the factors are: the output power of the transmitter, the sensitivity of the receiver, the physical obstacle in the transmission path and the antennas. This finding is in line with Jon Gunnar, (2018) who stated that radio performance and antennas are pretty static for Bluetooth devices. In the same vein, John et al (2017), explained that obstacles like concrete walls will attenuate the radio signal and the effective range will be drastically reduced. Therefore, Nateq and Mohammed (2012), further outlined the procedures in developing a Bluetooth device to include; give device a better range by selecting the Bluetooth chip with the best receiver and output power, and making use of a good antenna.

The finding of the study in research question 2 which deals with the factors affecting the transmission rate of Bluetooth, showed that the factors are: network congestion, network latency, health of the client and server and the infrastructure parameters. This finding is in agreement with what The Annese Team,

(2017) stated, that because wireless signals travel through the atmosphere, they are susceptible to different types of interference. Interference weakens wireless signals and therefore is an important consideration when working with wireless networking. Interference is unfortunately inevitable, but the trick is to minimize the levels of interference. This finding is also in line with the view of Muhammed et al (2016), that each and every wireless technology has its own set of constraints and limitations. However, regardless of the specific wireless technology in use, all the communication methods have a minimum channel capacity, which is determined by the same underlying principles (Carol, 2015). In other words, Unuth, (2018), stated that to ensure maximum throughput, it is necessary to avoid any noise and interference as well as ensure that the receiving and sending device is possible. The convenience of wireless communication does not have its costs. This is in line with John et al (2017), who stated that measuring wireless performance is a tricky business in that a small change on the order of a few inches, in the receiver can easily double throughput, and a few instants later, the throughput could be halved again because another receiver has just woken up and is now competing for access to the radio channel.

The findings of the study in research question 3 which deals with security vulnerabilities/threat in Bluetooth technology showed that the security vulnerabilities in Bluetooth technology are that: sensitive information that is not encrypted (or that is encrypted with poor cryptographic technique) and that is transmitted between two wireless

devices may be intercepted and disclosed, denial of service attack may be directed at Bluetooth connections or devices, malicious entities may steal the identity of legitimate users and masquerade as them on internal or external networks, sensitive data may be corrupted during improper synchronization, malicious entities may be able to violate the privacy of legitimate users and be able to track their movements, malicious entities may deploy unauthorized equipment to surreptitiously gain access to sensitive information, handheld devices are easily stolen and can reveal sensitive information, data may be extracted without detection from improperly configured devices, viruses or other malicious code may corrupt data on a Bluetooth device and subsequently be introduced on a wired network connection, malicious entities may, through Bluetooth connections, connect to other agencies or organizations for the purpose of launching attack and concealing their activities, interlopers, from inside or outside may be able to gain connectivity to Bluetooth management controls and thereby disable or disrupt operations, internal attack may be possible via ad hoc transmissions. The results of this study were in agreement with those of Joseph Steinberg (2014) who stated that software in Bluetooth devices especially those using the newer Bluetooth versions will not be perfect. According to the author, it's unheard of to find software that has zero security vulnerabilities.

According to the findings of the security vulnerability/ threats in Bluetooth technology revealed that the security threats in Bluetooth technology are: the deliberate alteration of information in an attempt to mislead the recipient, information can leak from the target system to an eavesdropper that is not authorized to access the information, the user can be blocked to get connected to a service by making it unavailable or severely limiting its availability to an authorized user. The finding is in line with what NateqBe and Mohammed (2012) found out, that like any other wireless communication system, Bluetooth transmission can be deliberately jammed or intercepted. According to them, false or modified

information could be passed to devices by the cyber criminals.

Conclusion

This paper presented an overview of the major limitations, security vulnerabilities/ threats that Bluetooth has faced over the years. Some safety tips for the users have also been provided to instantly create awareness among them to be more cautious. Bluetooth security specialists need to provide automatic updates to its security protocols and user privacy protection methods for every new security breach so that protection of the device user's personal information becomes the primary objective.

Recommendations

Based on the findings of the study, the following recommendations were made among others that the.

1. Use notification and writes without response, Use LE 2m physical layer.
2. The Bluetooth security experts should include awareness-based education to support user's understanding and knowledge of Bluetooth security.
3. Bluetooth security specialists need to provide automatic updates to its security protocols and user privacy protection methods for every new security breach.

References

- Carol, S. (2015). *Types of research designs you can use for your dissertations*. <http://computer.org/internet>
- Colak, O., Oral, O, Caglayan, N. and Kazanci, H.O. (2015). Wireless tool vibration monitoring for milling. *International Journal of Scientific and Research Publications*, 6(4), 11-20
- Gypsy, N. (2014). Bluetooth Technology: Security Issues and its Prevention. *International Journal of Computer Technology and Applications*, .5(5).

- Hua, J., Lin, X., Xu, L and Ouyang, M. (2009), Bluetooth wireless monitoring, diagnosis and calibration interface for control system of fuel cell bus in Olympic demonstration. *Journal of Power Sources*, 3(5)
- John, P., John, B., Mayank, N., Marcel, H., Rhonda, S., Lily, C., & Karen, S., (2017). *Guide to Bluetooth Security*. <https://doi.org/10.6028/NIST.SP.800-121r2>
- Keijo H. (2009). Bluetooth threats and countermeasures in Bluetooth-Enabled Systems. Kuopio University Publication H. Business and Information Technology 13.2009.187p
- Lo'ai, H. (2016). Bluetooth Technology/Security. New York Institute of Technology (NYIT) Jordan's campus.
- Marcus, C. & Erik.H. (2014). File Transfer Using Bluetooth.
- Muhammed, U.L., Mosharani, S., Muthapriya, S.A., Mufthas, M.M., Malikberdi, H., & Dhishan, D. (2016). Bluetooth Security Analysis and Solution. *International Journal of Scientific and Research Publications*, 6(4), 11-20
- Nadeem, U. (2018). Bluetooth File Transfer Essentials. *Journal of Computer Science Education*. Nadeem publications, 10.
- Nardagi, A.V., Aparva, D., Sonali, J., & Gajondra, S.S. (2015). Study of securing computer folders with Bluetooth. *International Advanced Research Journal in Science, Engineering and Technology* 2(2)
- Nateq, B.M. and Mohammed T. (2012). Bluetooth Security Threats and Solutions: A Survey. *International Journal of Distributed and Parallel Systems (IJDPS)* 3(1)
- Pravin, B. (2015). Bluetooth: Technology for Short-Range Wireless Apps.
- Purvish, P., Akash, M., Nisarg, T., & Clinton, T. (2015). Bluetooth security issues. *International Journal of Computer Science and Information Technologies*, 6(6), 2015, 5292-5299.
- Sanjay, H. & Arvind, S. (2016). Introduction to Bluetooth. EV3 lessons. Last edit 7/19/2016
- Stanley, G. (2017). Swap music and files between phones Using Bluetooth File Transfer <https://www.lifewire.com/bluetooth-file-transfer-4147725>.
- Niem, T.U. (2012). Bluetooth and it's inherent security issues. SAN GIAC Security Essential Certification (GSEC) V1. 46 11/04/2003 www.dissertationstatistics.com/eseachdesi gns.html
- Vikethozo, T. (2014). Bluetooth Technology: Security Issues and its Prevention. *International Journal of Computer Technology and Applications*, 5(5)