Vol. 6, No. 12 December 2015 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Information Security Risks Posed by the Bluetooth Security Weaknesses to the Bluetooth-Enabled Phones

[1] Chrispus Kimingichi Wanjala, [2] Samuel Mungai Mbugua, [3] Juma Kilwake
[1,2,3] Kibabii University, Chwele - Kimilili - Kamukuywa Rd, Kenya
[1] cwanjala@kibabiiuniversity.ac.ke, [2] smbugua@kibabiiuniversity.ac.ke, [3] jkilwake@kibabiiuniversity.ac.ke

ABSTRACT
As the widespread use and acceptance of Bluetooth technology increases, concerns are being raised related to security vulnerabilities of this technology. Inadequate device resources and lack of user awareness has compounded this issue where the emphasis on design constraints, functionality and ease of use sometimes outweigh security concerns. The research determines vulnerability of Bluetooth security and the security risks these vulnerabilities poses to the users' information stored in Bluetooth-enabled phones. The research design was based on multi-case study where two cases were selected. Questionnaires and interview were used in data collection. Both qualitative and quantitative approaches were used in data analysis. Descriptive statistical method was used for data analysis. The key findings from the study were that to improve security of information stored in Bluetooth-enabled phones, application layer security should be employed to provide additional security measures not provided in the current authentication and authorization process. Secondly the E0 encryption algorithm currently used for encryption is too weak and therefore the DES and AES algorithm should be used due to their efficiency and reliability. Lastly it was found out that most users have no knowledge on how to configure these devices thus manufactures of these devices should provide users with user documentation that explains the use and device configurations.

Keywords: *Bluetooth security, bluetooth technology, bluetooth-enabled phones.*

1. INTRODUCTION
The use of Bluetooth wireless technology and functionality provides added benefits, but also brings new information security threats to user's information. When two or more Bluetooth-enabled phones connect to each other they form a piconet. Bluetooth devices are able to communicate with each other when they are in the range of ten to one hundred meters apart. Bluetooth can be used to transmit various types of data ranging from photos, videos and text. The network formed when Bluetooth connect devices connect to each other is called Personal Area Network (PAN) or piconet. This network consists of a master and seven active slaves. The devices in a piconet share the same Frequency Hopping Spread Spectrum channel, which is a transmission technology used in Local Area Wireless Network (LAWN)

This piconet just like any other network is subjected to security risks and according to [1] Bluetooth piconet employs security procedures such as authentication, authorization and optional encryption. Despite all of these defense mechanisms being in place, Bluetooth has been found to have some security risks. [2] Bluetooth devices communicating in the wild forms various sizes of ad hoc networks where varying number of devices can be entering and leaving the piconets and scatternets created by the devices at any time hence making it difficult for Bluetooth piconet to maintain good security. The research looks at the implications of using a Bluetooth-enabled handheld device in both public and private environments.

2. RELATED STUDIES
Bluetooth is a short range wireless radio technology that enables Bluetooth-enabled electrical devices to wirelessly communicate in the 2.45 GHz ISM (license free) frequency band according to [3]. The Bluetooth document also states that the communication changes the transmitting and receiving frequency 1600 times per second, using 79 different frequencies.

In a few years, Bluetooth-enabled devices will outnumber Wi-Fi devices five to one, with over seventy percent of cell-phones, sixty percent of PDAs, and sixty seven percent of notebooks having built-in Bluetooth radios [4]. Bluetooth has become a basic requirement for any mobile phone and most people will look for this feature when purchasing the mobile phone.

The introduction of Bluetooth on mobile phone has greatly affected the security of personal data stored in these mobile phones. What is even worse is that most users of mobile phones that are Bluetooth-enabled are unaware of the many threats to their privacy [5]. A large percent of mobile phone users are not aware of security issues that could put their mobile phones at risk due to the presence of Bluetooth. The users of mobile phone understand Bluetooth as a technology that will allow them to exchange data, information and pictures with friends. The communication with Bluetooth is free of charge and therefore users will prefer to communicate through Bluetooth as compared to other wireless technologies such as Wi-Fi. In addition most users do not look at the security issues associated with Bluetooth and even they do not understand settings of Bluetooth [6].

The manufactures of Bluetooth-enabled devices always takes into consideration the security issues of the devices and have implemented it in the device. The problem is that users are not aware of this security settings and how it's configured. In addition there are security weaknesses in the Bluetooth security architecture.

2.1 Information Security Weakness of Bluetooth-Enabled Phones

Information security services are the measures that are employed to prevent the unauthorized use, misuse, modification or denial of the use of assets [7].

[8] Point out some of the problems connected with Bluetooth security. The author states that: 'Bluetooth is versatile, which further increases the difficulties in finding the correct level one anticipates for the system'. This means that, because of the versatility of Bluetooth, it is hard to find a correct level of security.

Since Bluetooth development, there have been many upgrades of Bluetooth that includes security upgrades and performance but still some of the security issues are in the user's hand which means that there is still a possibility of weak security. The major problem that Bluetooth has always had is that it is based on ease of use. In order to communicate with Bluetooth, a quick network has to be formed, and the ad hoc networks that have been created are not normally in existence for long [9]. Speed and ease of use are essential for this kind of networking technology.

To further emphasis the security issues with Bluetooth, the [10] wrote an article discussing Bluetooth security recommendations and precautions, they list points about Bluetooth one of which is to 'Enable Bluetooth functionality only when necessary.' This has been always a weakness to most users of Bluetooth-enabled mobile phone since they will sometime forget to switch it off.

To improve on this, the Bluetooth should be able to switch off automatically after a few moment of not being in use. This indicates that Bluetooth does have security risks, enough that the NSA has specified a document discussing how to use Bluetooth.

2.2 User Knowledge of Bluetooth Security Threat

Bluetooth security solutions have been designed with the principles in mind that any other ordinary user should be able to configure and manage the necessary security actions needed to protect the communication links'.

Much of the emphasis is placed on the user in order to set a security level. This reveals a problem with Bluetooth security, because its users do not often consider the security implications, simply perceiving the devices as instruments by which to exchange information wirelessly.

A study by research firm called Insight Express revealed that seventy percent of mobile phone users are not aware of Bluetooth security issues that could put their data and information in mobile phones at risk.

[11] States that Phones that are Bluetooth-enabled can be tweaked to search for other handsets that will accept messages sent via Bluetooth. It simply presents a message, similar to e-mail spam. The recipient can ignore the unsolicited message, read it, respond or delete it as also expressed by [12]. A research by [13], states that People are not aware of the security risk posed by Bluetooth. The researcher also states that the figures are worrying, particularly those collected at Info Security, where you would expect people to be more security conscious if a single mobile phone had been infected, nearly all vulnerable devices would have been the security of data in mobile phones.

[14] States that the mobile phones have previously fallen victim to a range of viruses including Cabir, the most widespread virus that uses Bluetooth to replicate, so it's important that mobile users are aware of the potential threats. The author also gives three ways hackers can exploit Bluetooth to attack mobile phones as:

Social engineering – hackers can access information on a user´s phone, either by using Bluetooth to establish a ´trusted device´ connection, or by persuading the user to lower security/disable authentication for Bluetooth connections.

Protocol vulnerabilities – hackers can steal data from the phone, make calls or send messages, conduct DoS attacks on the device, use a Bluetooth earpiece to listen to calls.

Malicious code – a phone can be infected by a worm, which will then send itself to other devices, by Bluetooth or by MMS. Data on the victim phone may be corrupted, stolen, or encrypted.

Research has shown that Bluetooth technology has been attacked on a number of fronts because of failures in security and connectivity. Attackers can obtain confidential data, numbers, download contents stored in the memory chips in mobile phones and eavesdrop on all data and voice messaging [15]. The author is categorically that the device has a lot of shortcomings in terms of security.

Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and with unauthorized use of Bluetooth devices and other systems or networks to which the devices are connected [16].

2.3 Weak Encryption Algorithm

The E0 is a 128-bit symmetric stream cipher algorithm currently used by Bluetooth to transmit [17]. Several attacks and attempts at cryptanalysis of E0 and the Bluetooth protocol have shown that it may be broken into thus rendering Bluetooth unsecure due to weak encryption [18]. In addition only devices are authenticated and not the user as stated by [19]. This will make the device unsecure since the user cannot be able to know who is trying to connect the device.

2.4 Information Security Risks Posed by Bluetooth on Bluetooth-Enabled Phones

While Bluetooth connections have the advantage that they're automatic and wireless, they have the disadvantage of their data being vulnerable to interception along with any other data sent on low-power radio waves.

In addition to the risk of other people being able to receive your sensitive information, they're also able to send you files or viruses that you're absolutely not interested in. Some of the risks posed by Bluetooth are discussed below

In April 2005, Cambridge University published a paper documenting actual passive attacks by implementing off-line PIN cracking and also a paper on Bluetooth enabled phones were used to track other mobile device left inside of cars [20].

In addition, Bluetooth devices are exposed to malicious intervention during the process of pairing with another device. These weaknesses are primarily due to flaws in the link key establishment protocol, which is required for devices to pair, and the fact that the encryption of a session is optional and created at the end of the pairing process [21]. It means that the various types of attacks can be performed well before pairing is complete. Even after the pairing is complete, the attackers can still sniff the airwaves to gain enough information to steal link keys so that they can deceptively authenticate or perform Man-in-the-Middle (MITM) attacks to impersonate other devices.

Some other reported attacks on the Bluetooth security are blue jacking which is a security attack that begins with the sending of short, unsolicited and deceitful messages to mobile devices. The short messages, in the form of anonymous business cards, can grant an attacker authorized access without the victim's knowledge and can proceed to over-write information on calendar appointments, phonebook entries and mobile-residing files. Such attack tends to be location dependent, meaning it occurs in public vicinities like transportation areas, shopping malls, or restaurants [22].

Bluesnarfingis a form of information theft attack that works by connecting to a specific group of mobile devices and enables the attacker to steal and over-write sensitive data without alerting the victim. Once an unauthorized access is obtained into a particular device, residing confidential data will be at risk of information theft. The hacker retrieves the file names from the infrared mobile communications lists instead of sending vCard information such as the phonebook, calendar and other personal information. The biggest risk with this hack is that the attacker can delete crucial system files, rendering the victim's device useless [23].

Blueprinting is an attack that consists of a process of discovering the fingerprint of Bluetooth-supported devices that comprises details uniquely identifying a particular device (i.e. make, model and unique address of the equipment), just like the human fingerprint. It may not seem so deadly a threat, but such information can be used to spot promising susceptible devices and facilitate subsequent attacks [24].

Blue Smack is a form of Denial of Service attack that immediately disables any Bluetooth-compatible device.

Denial of Service consumes device resources so as to ultimately prevent the victim to rightfully use them, for instance, it exhausts the battery life that in turn affects power-intensive smart device services [25]. A nonparticipating device launches the attack that affects the piconet by throwing some devices out of the network or disrupting the master device from supporting the connection [26]. Implications of such attack leave the victim not able to use his phone when he needs it most, such as during an emergency situation. Unfortunately, the user may be led into believing that the battery is defective, thus replacing either the battery or the phone itself.

3. RESEARCH METHODOLOGY

This section discusses the methodological approach including the research design, instruments used, data collection techniques, study location, and target population.

3.1 Research Design

According to [27] research design is the plan and structure of investigation so conceived so as to obtain answers to research questions or test the research hypotheses. The plan represents the overall strategy used in collecting and analyzing data in order to answer the research questions. [28] Summarizes the essentials of research design as an activity and time based plan

The research design for this study was a multi-case study. In view of this, the researcher used quantitative and quantitative approach to carry out the study because this was a problem centered study. Combining qualitative and quantitative methods is the best way to produce a more credible quality assurance or treatment methodology-based research program [29]. The best research design is a mixed

method design that integrates qualitative and quantitative research. This type of design begins with a strong research methodology with quantitative methods that are enhanced with qualitative measures of key processes and outcomes.

The strategy of inquiry for this approach is concurrent procedures. Concurrent procedures strategy is defined as situations in which the researcher employs quantitative and qualitative data in order to provide a comprehensive analysis of the study problem [30].

3.2 Target Population

The target population for this study was university students who used Bluetooth-enabled mobile phones. This was conducted at one University College and one university in Kenya that is Kibabii University College and Maseno University.

3.3 Sampling

A formula below published by Robert, (1970) was used to determine the sample size

$$s = \frac{x^2 NP(1-P)}{d^2(N-1)} + x^2 P(1-P)$$

s = required sample size.
x^2= the table value of chi-square for 1 degree of freedom at the desired confidence level(3.841).
N = the population size.
P = the population proportion (assumed to be .50 since this would provide the maximum sample size
d = the degree of accuracy expressed as a proportion (.05).

Maseno University has an approximate of 20,000 students.
Kibabii University has an approximate of 3000 students
Using the formula to get sample population for Maseno University where N is 20000

$$s = \frac{x^2 NP(1-P)}{d^2(N-1) + x^2 P(1-P)}$$

Then
s = {3.841 *20000*0.50(1-0.5)} ÷ {0.05 ^{2}(20000-1) + 3.841*0.050(1-0.50)}

s = 377

Using the formula to get sample population for Kibabii University College where N is 3000

s = {3.841*3000*0.50(1 - 0.5)} ÷ {0.05^2(3000-1) + 3.841*0.050(1 - 0.50)}
s = 341

In summary 377 students were picked from Maseno University and 341 students were picked from Kibabii University College.

3.4 Data Collection Instruments

Data collection used mixed techniques such as questionnaires, interview and analysis of past literature on Bluetooth security (this is evident in the appendix VI and V of this thesis). [31] States that the set of concrete operations at the technique level of research entail the combined use of data collection techniques that are commonly (but not necessarily) associated with either qualitative or quantitative research, such as open-ended and un-structured interviewing and structured questionnaires, respectively.

The questionnaires were structured in such away to be able to capture the background information of the participants like gender, age, level of experience with Bluetooth and other areas that cover the main areas of the study. According to [32], questionnaires have the added advantage of being less costly and using less time as instruments of data collection. The questionnaires were administered through drop and pick-later method to the sampled population. Open and closed- ended questions were used to elicit qualitative and quantitative information respectively from the respondents.

The interviews used were face-to-face interviews with respondents. An interview guide or "schedule" with a list of questions or general topics was used to ensure good use of limited interview time. Interviews were based on two different interview styles. The first part of the interview was unstructured interview. This enabled the researcher not to miss valuable information since the interviewee were able to talk freely about the subject and were not obstructed by any pre-defined agenda as supported by [32]. The second part was a structured interview which was based on a pre-defined set of questions. Interviews are justified on the grounds that they are suited for occasions where the questionnaire is not satisfactory [33]. Interview guides are open and this characteristic was pertinent to this study because unwilling respondents were easily and flexibly convinced to answer all the questions and also for triangulation.

4. RESULT AND DISCUSSION

4.1 Response on How Often Bluetooth is Switched on

The researcher felt it necessary to establish the frequency at which respondents switch on Bluetooth for users with Bluetooth enabled phones. Figure 1 shows the study findings.

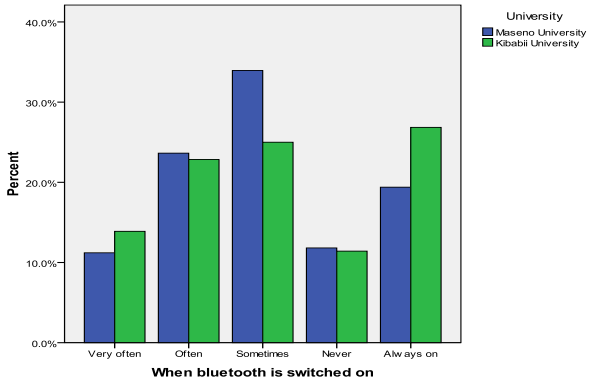

Figure 1: When bluetooth is switched on

The results from figure 1 reveal that from Maseno University 11.2% of the respondents very often switch on Bluetooth, 23% often switch on Bluetooth, 33.6% sometimes switch on, and 11.8% never switch on whereas 19.4% always switch on Bluetooth. In Kibabii University 13.9% of the respondents very often switch on Bluetooth, 22.8% often switch on Bluetooth, 24.7% sometimes switch on, and 11.4% never switch on whereas 26.9% always switch on Bluetooth. These findings clearly depict that many users of Bluetooth enabled phones often switch on Bluetooth devices.

4.2 Response on those who Leave Bluetooth on after Use

The researcher further sought to identify if the respondents left their Bluetooth on after use table 4.5 shows the findings.

Table 1: Leaves bluetooth on

		Leave Bluetooth on		
		No	Yes	Total
University	Maseno University	31.8%	68.2%	100.0%
	Kibabii University	35.5%	64.5%	100.0%
Total		33.6%	66.4%	100.0%

The study findings from table 1 reveal that 31.8% respondents from Maseno University and 35.5 from Kibabii University do not leave their Bluetooth on after use, however majority of the respondents comprising of 68% from Maseno University and 64.4% from Kibabii University agreed that they leave their Bluetooth on after use.

4.3 Response About Understanding the Effect of Leaving Bluetooth on to the Security of Your Data

The researcher sought from those who agreed that they leave their Bluetooth on to identify whether they understood the effect of leaving on their Bluetooth on to the security of their data. The findings were presented in the figure 2.

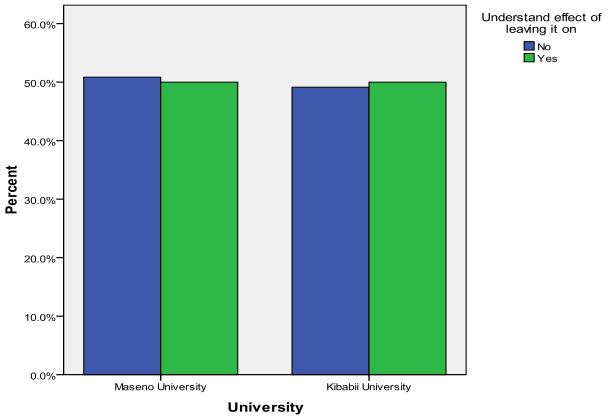

Figure 2: Understand effect of leaving bluetooth on

The results form figure 2 show that 51% from Maseno University and 49% from Kibabii University do not understand the effects of leaving Bluetooth on to the security of their data. 47% from Maseno University and 52% from Kibabii University agreed that they understood the effects of leaving Bluetooth on to the security of their data. This is a similar trend in the interview conducted by the researcher as the results were approximately the same.

4.4 Response about those who Searched for other Bluetooth Devices within the Locality

When asked to respond on whether they have ever searched for other Bluetooth devices within their locality, the following results were found:

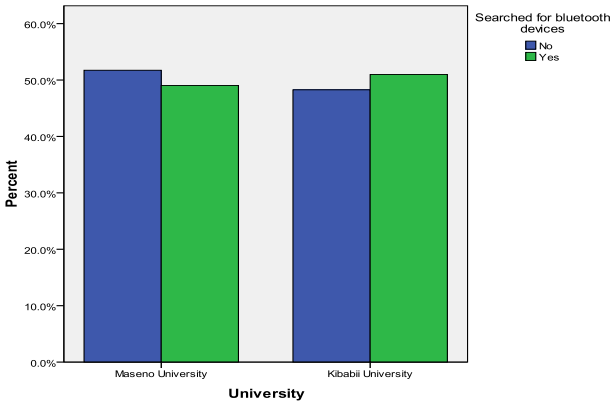

Figure 3: Searched for bluetooth devices

The findings from figure 3 reveal that 48% from Maseno University and 50% from Kibabii University searched for Bluetooth devices within their locality, While 52% from Maseno University and 50% from Kibabii University however indicated that they had not searched for Bluetooth devices within their locality. The study findings show that considerably there is a many number of users of

Bluetooth enabled phones that search for Bluetooth devices within their locality.

4.5 The Approximate Number of Devices Found on when you Searched

The researcher proceeded to get responses about the approximate number of devices found when searched by the respondents. The following data was obtained from this study.

Table 2: Average bluetooth devices found on when searched

Descriptive Statistics					
	N	Min	Max	Mean	Std. Deviation
Number of Bluetooth found on	654	0	5	1.35	1.316
Valid N	654				

The findings from table 2 indicate that an average of 1.35 which is approximately one device was found on. The study findings reveal that at least one Bluetooth device is found when searched by majority of the respondents.

4.6 Response about those who Understand the Bluetooth Security Settings

The respondents were also requested to show whether they understood Bluetooth security settings of their mobile phones. The following data was collected from this study.

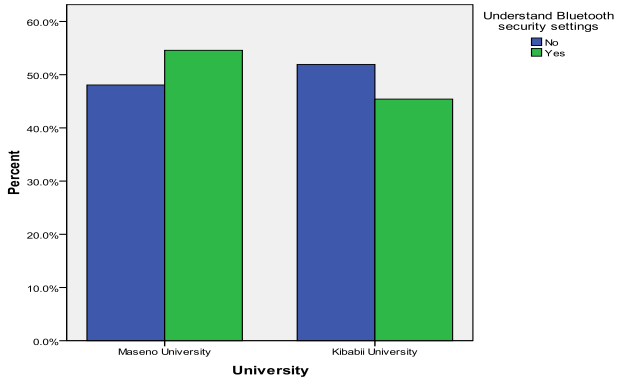

Figure 4: Understand the bluetooth security settings

The findings from figure 4.4 show that 48% of the respondents from Maseno University and 51% from Kibabii University do not understand Bluetooth security settings of their phones while 52%from Maseno University and 49% from Kibabii University understand Bluetooth security settings. In the relation to the interview carried out, it is evident that most users of Bluetooth-enabled phones are not aware of its security settings. The results therefore depict that many users of Bluetooth enabled phones do not understand Bluetooth security settings and it will be risky if the security settings is left to the user.

4.7 Reasons Why Respondent do not Understand the Settings

The researcher further sought to find out reasons for not understanding Bluetooth security settings. The results obtained from this study are graphically presented in figure 5.

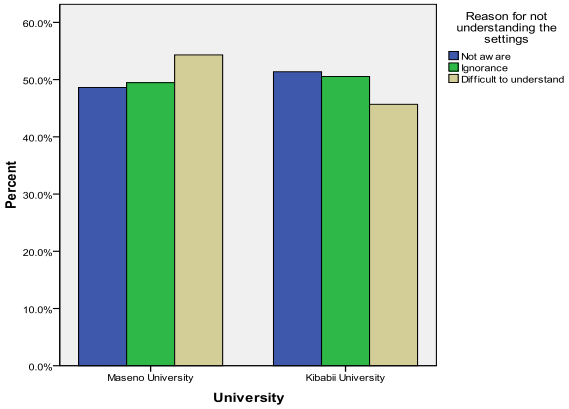

Figure 5: Reason for not understanding the bluetooth settings

The findings from figure 5 above show that 53.6% from Maseno University and 57.7% from Kibabii University are not aware, 13.9% from Maseno University and 14.5% from Kibabii University are ignorant while 32.4% from Maseno University and 27.8% from Kibabii University find it difficult to understand Bluetooth security settings for their phones. The findings shows that, there respondents who are aware of Bluetooth security settings but they ignore. In the interview carried out by the researcher, most users said that they are not aware of how to configure Bluetooth security while others said that they know how to configure but they ignore because of lack of information about the risks of Bluetooth.

5. DISCUSSION OF FINDINGS

The researcher sought to determine whether the respondents saved confidential information in their mobile phones and further asked the respondents to rate the confidentiality of information received and sent through mobile phone. The results show that majority of the respondents receive confidential information very often and store the information in the phone. The types of confidential information received and stored include; credit card number, ATM PIN number, Mpesa PIN etc. It is therefore very important to protect such kind of information from other parties. This can only be done through improving the security of Bluetooth.

The problem with Bluetooth security is that, someone can steal information from the device without the

owner noticing. This is done by use of several methods such Blue jacking and Bluesnarfingis.

Apart from saving confidential information, some respondents stated that they do not save confidential information in their phones and one of the key reason cited is information privacy. This is a good indication but on other hand the researcher is so much concerned with those who store confidential information in the phone

5.1 Bluetooth Security

The researcher established that most respondents switch on Bluetooth and leave it on unattended to. Leaving Bluetooth on is so risky because it will be subjected to attacks with intention to get the confidential information stored. In addition, it was revealed that most respondents do not even know the risks they are exposing the stored data to by leaving Bluetooth on.

The study findings show that considerably there is a high number of users of Bluetooth enabled phones that search for Bluetooth devices within their locality and an average of one device will be found on. This indicates how risky it is to leave Bluetooth on because the attackers will use Blue jacking, Bluesnarfingis and social engineering methods to gain access to the device and steal information.

The use of these methods hinders the owner to have control of the device thus the solution can be to always switch Bluetooth off which is a weakness to most users. This therefore means the security gaps in the Bluetooth security architecture as highlighted in the literature review must be improved.

In the relation to the interview carried out, it is evident that most users of Bluetooth-enabled phones are not aware of its security settings. The reason to this is due to lack of documentation or information on how to do the settings. This is so because most users were not provided with privacy statement on how to secure the information in the Bluetooth devices.

In conclusion, to properly secure data and information stored in Bluetooth-enabled phones, the weakness in the Bluetooth security architecture must be improved and also users should be made aware of their role on securing the data and information. The following recommendation will improve Bluetooth security.

5.2 Authentication and Authorization

In this regard it was established that the weakness found in Bluetooth security architecture needed to be improved. The main weaknesses were weak authentication, encryption and authorization. In authentication and authorization, only the device is authenticated and not the user.

To improve authentication and authorization, application layer security should be employed to provide additional security measures. Employing application layer security limits the Bluetooth devices to connect automatically whenever it finds devices that were previously connected. This is possible because application layer security will require a password from the user to authenticate the user in addition to using the Bluetooth device authentication. With proper authentication and authorization, data and information stored in Bluetooth-enabled devices will be secure.

5.3 Encryption

To achieve proper encryption AES and DES encryption techniques should be used to provide proper encryption and decryption. Instead of the E0 encryption currently being used, AES algorithm, known for of its higher efficiency in block encryption should be used for data transmission and DES algorithm should be used for the encryption of the AES key because it has key management advantages. The dual protection using AES and DES algorithm will make the data transmission using Bluetooth secure.

5.4 Policy

Risk mitigation can be achieved in Bluetooth systems by applying countermeasures to address specific threats and vulnerabilities. Some of these countermeasures cannot be achieved through the security features built into the Bluetooth architecture. It is therefore better to provide an adequate level of knowledge and understanding for the users of Bluetooth-enabled phones. From data analysis from the respondents, it was evident that users of Bluetooth enabled phones lack knowledge on how to configure these devices. Majority of users leave Bluetooth on after use because they are not aware of the risks they are putting the information stored in these devices. Developers of Bluetooth devices do not include user guideline and the risks of using such devices. Users should understand the security policies that address the use of Bluetooth enabled devices and their own responsibilities.

The Bluetooth security experts should provide awareness based education to support user's understanding and knowledge of Bluetooth security. The policy documents should list approved uses for Bluetooth, and the type of information that may be transferred over Bluetooth. The security policy should also specify how a password should be used. Most users do not understand how to choose strong passwords because they are not aware of the proper techniques. The mobility of Bluetooth enabled phones increases the difficulty of employing proper security measures.

Thus in order to improve on user awareness, a security policy should be provided to users who purchase Bluetooth enabled phones.

6. CONCLUSION

Despite the wide usage of Bluetooth enabled phones, there is generally low level of understanding of information security threats among the users of Bluetooth enabled phones. The lack of understanding of information security threats is evidenced by the many respondents who frequently save, receive and send confidential information such as Credit card numbers , ATM numbers among others through their mobile unaware of the information security threats that they are exposed to especially by leaving Bluetooth on. There are also weaknesses of the current Bluetooth information security architecture which include weak authentication and authorization, and weak encryption with which sometimes optional in the older versions of Bluetooth. Therefore with this architecture Bluetooth enabled mobile phone users are not assured of their information security. Bluetooth is therefore a threat to security of user information. This therefore lead the development of an information security framework for Bluetooth enabled phones that improves user awareness through an appropriate policy that includes device configuration guidelines, security policies, and enforcement mechanisms for the use of Bluetooth devices.

7. SUGGESTION FOR FURTHER STUDY

This research is based on the current Bluetooth version 4.2 and not the older versions. Therefore a backward compatibility with older Bluetooth specifications with the updated specification could also be determined since there are a numbers of users using the older version of Bluetooth. Bluetooth SIG has also decided to adopt Wi-Fi technology as a stopgap measure prior to implementing its ultra wideband (UWB) technology. This would incorporate 802.11 into future Bluetooth device functionality. It would provide Bluetooth with high speed, allowing the capability of switching to 802.11 radio connectivity for better connection speeds but then also fall back to Bluetooth when 802.11 connectivity is not needed. The information security implications of combining Bluetooth and Wi-Fi connectivity would need to be examined and the potential information security risks identified. Integration of the updated Bluetooth specification and Wi-Fi with fixed network infrastructures in both the private and public environments would need to be assessed, along with the improving ability of Bluetooth-enabled mobile phones. As handheld devices continue to converge with cell phones and become more complex, the Mobile phones will evolve into a handheld device with highly complex abilities, allowing mobile access via a range of wireless communication standards.

REFERENCES

[1] Colleen, R., (2006). Bluetooth Security: East Carolina University. International Journal of Computer Applications July 2006, 26, (1):6-9

[2] Lewis, J., 2005. Bluetooth Security.

[3] Bluetooth, (2001). Specification of the Bluetooth system, version 1. Bluetooth Special Interest Group: retrieved from website, http://www.bluetooth.com.

[4] Register T. (2003), Bluetooth to outnumber wifi five to one; Retrieved April, 2013 from http//www.theregister.co.uk/2003/06/18/Bluetooth-to-outship-wifi-five.

[5] Mohamed H. (2009), Threats to Mobile Phone Users' Privacy; St John's, NL, Canada A1B 3X5, 21(5): 402-409.

[6] Yasir Arfat Malkani and Lachhman Das Dhomeja, "PSim: A tool for analysis of device pairing methods", International Journal of Network Security& Its Applications (IJNSA),1(3), October 2009

[7] Bauknecht K. (2004). Information Security Services ISO 7498/2. Website. http://www.ifi.unizh.ch/ikm/Vorlesungen/sec/02.pdf. 25 February 2004

[8] Gehrmann, C. Persson, J and Smeets, B. (2004) Bluetooth security, Boston, Mass. London

[9] Haartsen J, (2013), The Bluetooth radio system. IEEE Personal Communications, 7(1): 28-36.

[10] NSA. (2010) Bluetooth Security, Available at: http://www.nsa.gov/ia/_files/factsheets/I732-016R-07.pdf (Accessed 18/03/2010)

[11] Raquel H and Billy F (2008), "Bluetooth Wireless Technology Security Threats and Vulnerabilities", Indiana University Bloomington, 3(4): 7-8

[12] Lynn T. (2007). "Symantec Warns Users over Bluetooth Security": CNET News; http://news.cnet.com/Symantec-warns-users-over-Bluetooth-security/2100-1029_3 6209361.html.

[13] Alexander G. (2006), Bluetooth-enabled Devices is Security Threat: 2nd Edition, New York, Wiley & Sons, 2006: 342-354.

[14] Neoease, IT & Security Portal. (2006). http://www.itobserver.com/bluetooth-enabled-devices-are-security-threat.html

[15] Naima. C.(2009). The Unintended Consequences of Technological Innovation: Bluetooth Technology and Cultural Change; internet journals, 22(7):200-210.

[16] Shirley R. (2012) security of Bluetooth systems and devices: (NIST); Itl bulletin august 2012,3(6):231-236

[17] Komal R. and et al (2013). Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA: International Journal of Computer Applications (0975 – 8887), 71(22), 1512-1534.

[18] Wuling Ren and Zhiqian Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", Second International Conference on Modelling, Simulation and Visualization Methods, 2010.

[19] Joakim P, (2009), Bluetooth Baseband Security Concept. Proceedings Bluetooth, 5(3):287-298.

[20] Ford-Long Wong and et al (2007), Repairing the Bluetooth pairing protocol. University of Cambridge Computer Laboratory, available at: http://www.cl.cam.ac.uk/research/dtg/~fw242/publications/2005-WongStaClu-bluetooth.pdf

[21] Loo, A. (2009), "Security threats of smart phones and Bluetooth", CACM, Vol. 52 No. 3, pp. 150-2.

[22] Dell, P. and Ghori, K.S. (2008), "A simple way to improve the security of Bluetooth devices", International Symposium on Applications and the Internet, IEEE Computer Society,

[24] Herfurt, M. and Milliner, C. (2004), "Remote device identification based on Bluetooth finger printing techniques", available at: http://bluehack.elhacker.net/downloads/paper/171-blueprinting-paper.pdf accessed November 2011.

[25] Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V. and Iftode, L. (2010), "Root kits on smart phones: attacks, implications and opportunities", Proceedings of the Hot Mobile Eleventh Works hoping Mobile Computing Systems and Applications, ACM, NewYork, NY, 49-54.

[26] Potter, B. (2006), "Bluetooth security moves", Network Security, 3:19-20.

[27] Black T.R. (1999). Doing Quantitative Research in the Social Sciences. 1st Edition, SAGE Publications, May 17, 1999 - Social Science:743-751.

[28] Kothari, C. R. (2004). Research Methodology: Methods and techniques, 2nd edition. New Age Publication, New Delhi ISBN: 81-224-1522-9.

[29] Brian A. (2009). Combined Qualitative-Quantitative Research Methods; Star Tribune (Minneapolis, MN) 5(3): 321-325.

[30] Creswell, J.W. (2003). Research design: Quantitative, qualitative and mixed approaches (2nd Ed.). Thousand Oaks, CA: Sage publications:230-245

[31] Sandelowski. M. (2000) Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques in Mixed-Method Studies: 7460 Carrington Hall, Chapel Hill, NC 27599, USA

[32] Levi A. and et al (2004), Relay Attacks on Bluetooth Authentication and Solutions. Computer and Information Sciences (ISCIS'2004), 19th International Symposium, Kemer-Antalya, 5(6):345-349

[33] Lofland, J. & Lofland, L. (1984). Analyzing Social Settings. Belmont, CA: Wadsworth Publishing Company, Inc.

AUTHOR PROFILE

Chrispus Kimingichi Wanjala received his bachelor's degree in Computer Science from Masinde Muliro University of Science and Technology in 2008. He is a Network Administrator at Kibabii University. Currently, he is a Masters student at Masinde Muliro University of Science and Technology.

Samuel Mungai Mbuguah PhD, Currently Lecturer .and Director ICT at Kibabii University. He received his PhD in Information Technology from Masinde Muliro University of Science and technology, Kenya in 2013.

Mr Juma Kilwake, Currently senior lecture