Forensics Readiness for Wireless Body Area Network (WBAN) System

Abdul Fuad Abdul Rahman[1], Rabiah Ahmad[2], Sofia Najwa Ramli[3]

[1]*National Vulnerability Assessment Centre (MyVAC), Department of Security Assurance, Cybersecurity Malaysia, Seri Kembangan, Selangor, Malaysia*
[2]*Centre for Research Innovation Management (CRIM), Universiti Teknikal Malaysia Melaka (UTeM), Malaysia*
[3]*Centre of Advanced Computing Technology (C-ACT), Faculty of Information Technology and Communication (FTMK)*
abdfuad@cybersecurity.my, rabiah@utem.edu.my,sofia.najwa@yahoo.co.uk

***Abstract*— Wireless Body Area Network (WBAN) is a wireless network that can be attached or implanted onto the human body by using wireless sensor. Since WBAN developed for medical devices, the system should be design for a wide range of end user with different professional skill groups. This require WBAN system to be open, accurate and efficient. As from our previous experienced, any open system is vulnerable, similar to any other current available wireless systems such as Wireless Local Area Network (WLAN). However, currently there were not many discussions on the WBAN security vulnerability and security threats and if there is any, the issues were discussed through theoretical, concept and simulation data. In this paper, we discuss potential WBAN security vulnerability and threats using Practical Impact Assessment (PIA) conducted in real environment so that we are able to identify the problem area in details and develop potential solutions to produce a forensics readiness secure network architecture for WBAN system.**

***Keywords*— Forensics Readiness, Information Security, Practical Impact Assessment, Secure Network Architecture, Wireless Body Area Network (WBAN)**

I. INTRODUCTION

The empowerment in wireless technologies and sensors have developed the Wireless Body Area Network (WBAN). Many medical devices such as Electrocardiography (ECG), Insulin Pumps, Pacemakers, Implantable Cardioverter Defibrillators (ICD) and temperature and pulse sensors, all have been moved to WBAN technologies [1]. The deployment of WBAN technologies in the medical healthcare industry is target to replace wires to increase patient's comfort and most of all, provide the ability for healthcare professionals to monitor patients remotely [2]. However, as the WBAN technology expand and advances, security and privacy concerns have increase rapidly [2]. The nature of wireless technology has bequeathed security and privacy issues to WBAN [3]. Since WBAN must be a user friendly and a low operating powered system, this provide further challenge to develop a technology based security mechanism to combat WBAN security threats [3]. However, the current research only discussed the theoretical and the concept of the security threats and not practically proven [3].

The objective of this paper is to prove that inputs from practical approach can be used to develop a forensics readiness secure network architecture for WBAN system. In this paper, there are two main phase. First, the security of WBAN system will be assess by using a new practical approach, Practical Impact Assessment (PIA). The PIA will measure the impact from WBAN security threats based on the Three Main Security Pillars (C.I.A) concept [4]. Which represent Confidentiality, Integrity, and Availability of the system. In second phase, by using inputs from PIA, we develop an effective forensics readiness architecture for WBAN. This proposed forensics readiness architecture for WBAN will help prevent WBAN security threats and also to determine the attacker if an attack occur.

II. PRACTICAL IMPACT ASSESSMENT

The Practical Impact Assessment (PIA) is a practical testing to assess the impact of WBAN security threats. Each testing will be conducted practically by imposing other wireless technologies security threats to WBAN system, in order to prove that other wireless technologies bequeathed security threats to WBAN [3]. A set of wireless security threats was selected based on Explanatory Report of Convention on Cybercrime. The method use in the Convention on Cybercrime was accepted by 51 country including United Kingdom, United State of America and Australia [5]. The set of four wireless security threats selected, PIA_m as shown in Table 1.

TABLE 1. SET OF FOUR PIA_m

m	PIA_m	Attack
1	PIA_1	Eavesdropping

2	PIA_2	Denial of Service (DoS)
3	PIA_3	Authentication Bypass
4	PIA_4	Role Bypass

During the PIA process, two parameters will be measured. The first parameter is the time taken to execute a successful PIA_m, and the second parameter is the distance between the attacker and WBAN target system as shown in Figure 1. The PIA conducted from various distance to measure the minimum and maximum distance required, to execute a successful PIA_m. Only set of parameters from a successful PIA_m will be recorded.

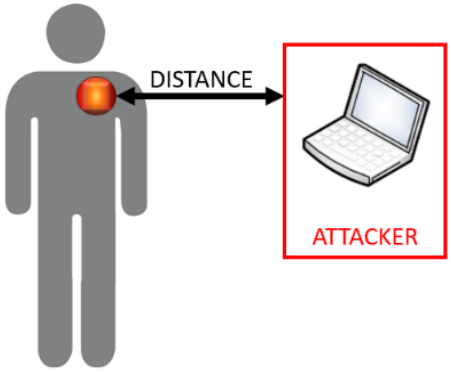

Figure 1. Distance between attacker and WBAN target system

If the PIA_m conducted was not successful, the whole process will be repeated. The success of the PIA_m was verified using logs recorded by WBAN target system, during the PIA_m execution process. The logs will also use to determine which impact was affected. The impact on WBAN security based on the C.I.A will be determined in the final stage of PIA process. The impact based on the C.I.A as shown in Table 2.

TABLE 2. IMPACT PARAMETERS

m	Parameter	Security Three Pillars
1	C	Confidentiality
2	I	Integrity
3	A	Availability

The PIA_m process simplified in flow chart as shown in Figure 2. Table 3 shows the result for all successful PIA_m conducted. The result in Table III successfully proves that imposing other wireless technology security threats to WBAN is achievable. The maximum distance between attacker and WBAN target system recorded for all successful PIA_m conducted was Five meters. The distance recorded in the manner of clear line of sight, which means there was neither objects, nor walls in between the WBAN target system and PIA setup. Table III shows that time taken to executed a successful PIA_1, PIA_2, PIA_3 and PIA_4 was 85.5 seconds, 123.23 seconds, 366.35 seconds and 529.66 seconds respectively. The time difference is influenced by various factors, but the main factor is the complexity of different security threats, PIA_m.

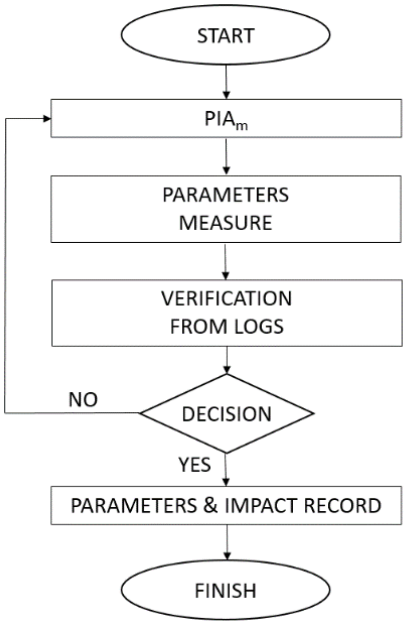

Figure 2. Practical Impact Assessment (PIA) Flow Chart

The Confidentiality of WBAN target system was compromised in PIA_1. The Availability of WBAN target system was compromised by PIA_2. Both PIA_3 and PIA_4 was affecting more than one impact, when the Confidentiality, Integrity and Availability of the WBAN target system was compromised.

TABLE 3. PIA RESULT

m	PIA_m	Parameters Measure		Impact Parameters		
		Maximum Recorded Distance (m)	Time to Execute (s)	C	I	A
1	PIA_1	5.0	85.50	1	0	0
2	PIA_2	5.0	123.23	0	0	1
3	PIA_3	5.0	366.35	1	1	1
4	PIA_4	5.0	529.66	1	1	1

III. FORENSICS READINESS FOR WBAN

Forensics Readiness means a forensically ready system that has the ability to investigate post incident event [6]. Figure 3 shows the architecture for system forensics readiness in Hospital Internal Network proposed by Brian Cusack and Ar Kar Kyaw study in 2012 [1]. The Hospital Internal Network is enhanced by adding a forensic server and drone within the wireless network [6]. The drone applied within wireless network

is hidden from other wireless clients, but has the ability to record communication within their network and forward it to the forensic server [6].

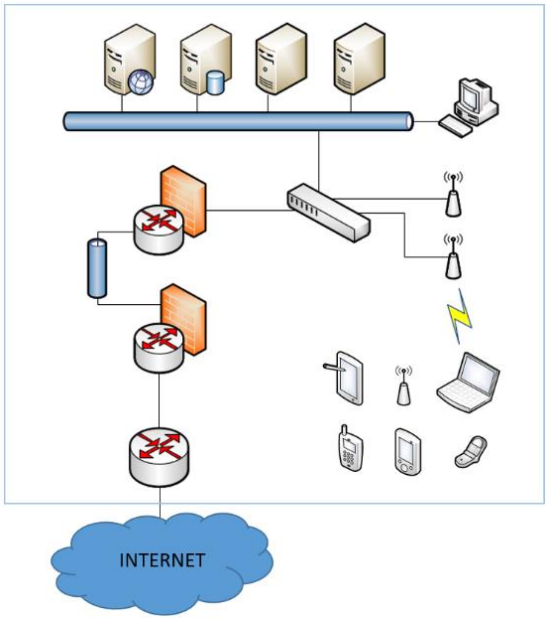

Figure 3. Forensics Readiness for Hospital Internal Network [1]

In order to implement WBAN system to the Hospital Internal Network securely, this study proposed a new set of Hospital Internal Network Architecture. From this study, the PIA has shown results that a successful security threat can be executed not more than five meters radius from the WBAN target system. To date, a WBAN system installation is recommended to have a minimum distance of six meters radius from other wireless system and devices as shown in Figure 4. The minimum distance of six meters will create a secure 113.14286m^2 space to ensure WBAN system security.

IV. TECHNIQUE TO DETERMINED ATTACKER

It is proposed that the minimum 113.14286m^2 space created also equipped with Surveillance Cameras or Closed Circuit Television (CCTV) for monitoring purposes. As shown in Table III, if an incident such as PIA_1, PIA_2, PIA_3 or PIA_4 were to occur, we can estimate that the incident was executed within a five meters radius. With the support of CCTV, this allows us to estimate the location where the attack was executed. We can determine whom the attacker was, and detect which attack was executed by using the information in Table III. For example, a DoS attack detected. Based on the CCTV recording, there were two people using wireless device within the radius of four meters from the WBAN target system. One of the suspect spend only 10 seconds in the crime scene, and the other spend more than 150 seconds. This allows us to narrow down our investigation to one person only. In order to validate our findings, the logs recorded in forensics server and drone installed within wireless network can be used to provide further information such as MAC address for investigation purposes [5].

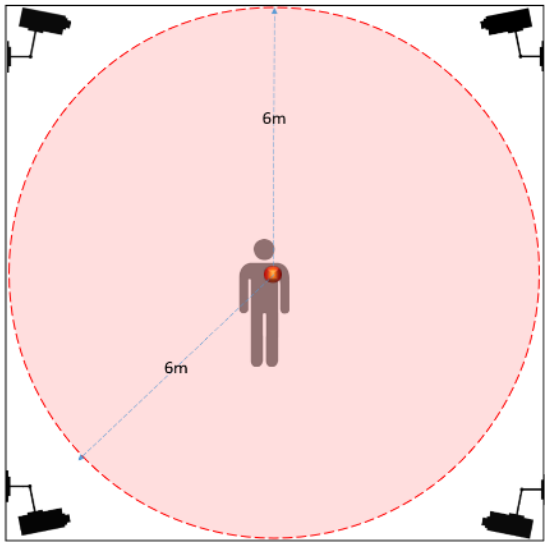

Figure 4. Six meters radius distance

V. CONCLUSIONS

The PIA results shown on Table III are both highly influenced by other factors. Although conducted on clear line of sight, interference of other signals or frequencies operated on the same spectrum may affected the accuracy of the results, as WBAN exists on the air [7]. This study purposely conducted without sweeping the floor for interference in order to study the WBAN vulnerability in real environment [7]. The parameter for time taken to execute, depends highly on human skills. It is known that initial level of skilled performance will drops considerably without proper human motor skill practiced [8]. Although the PIA was conducted multiple of times in order to provide an accurate and reliable data, the PIA still much depends on the human skills who perform it [8]. It is highly recommended to conduct a further research on this parameters in order to understand the PIA in depth.

The objective of this paper to develop a secure architecture for WBAN implementation in Hospital Internal Network using practical approach, Practical Impact Assessment is achieved as shown in Figure 5.

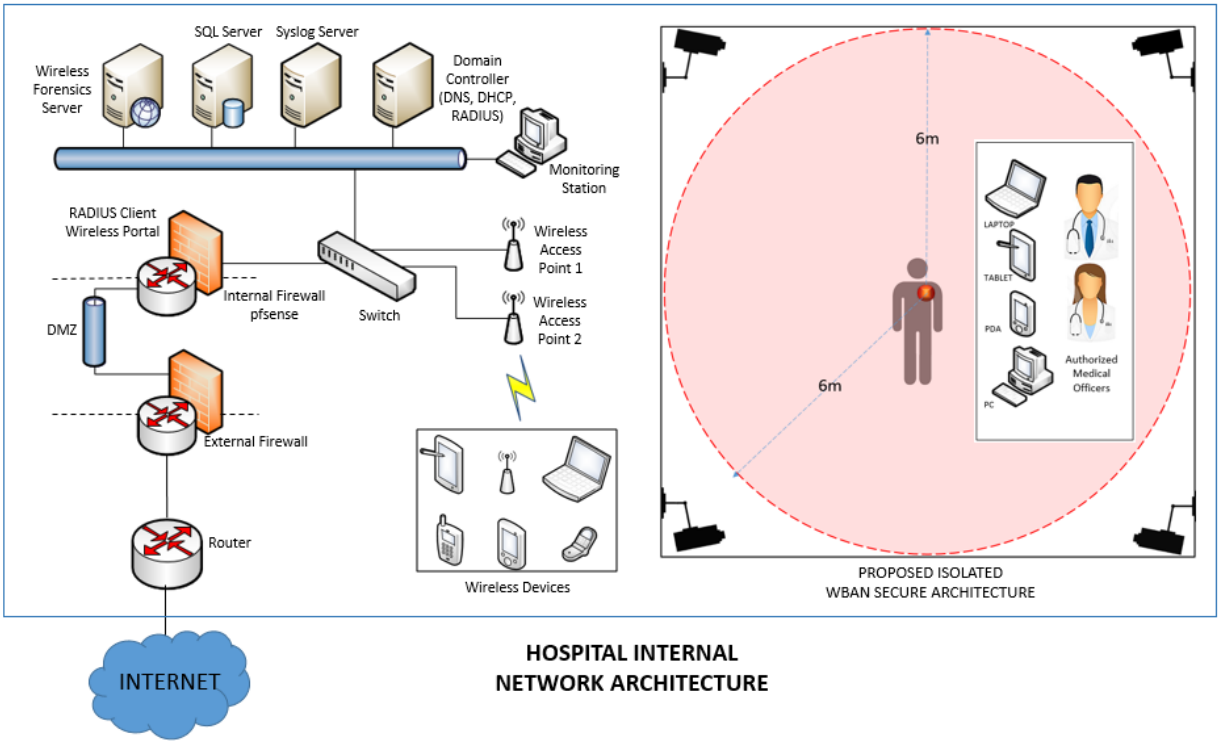

Figure 5. Proposed Forensic Readiness for Secure Hospital Network Architecture

ACKNOWLEDGMENT

The authors would like to thank all the reviewers for their helpful comments. We also would like to thank the Universiti Teknikal Malaysia Melaka (UTeM) that provides the research grant for this project. This research is currently supported by the ERGS/2011/FTMK/PK02/1 under the Exploratory Research Grant Scheme (ERGS) funding by the Ministry of Higher Education Malaysia (MOHE) and National Vulnerability Assessment Centre (MyVAC) of Cybersecurity Malaysia, an Agency under Ministry of Science Technology and Innovation Malaysia (MOSTI) for their contribution.

REFERENCES

[1] B. Cusack, A.K. Kyaw, Forensics Readiness for Wireless Medical Devices, Published in the Proceedings of the 10th Australian Digital Forensics Conference, 2012, http://ro.ecu.edu.au/adf/108

[2] H. C. Keong and M. R. Yuce, "Analysis of a multi-access scheme and asynchronous transmit-only UWB for wireless body area networks," in Proc. EMBC'09, pp. 6906-6909, 2009.

[3] A. F. A. Rahman, R. Ahmad, Hybrid Method to Measure Vulnerability in Wireless Body Area Network, Published in the Proceedings of the 6th International Conference on Sensor Asiasense 2013

[4] S. Saleem, S. Ullah and H. S. Yoo "On the Security Issues in Wireless Body Area Networks", International Journal of Digital Content Technology and its Application 2009.

[5] Council of Europe, Explanatory Report of Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Reports/

[6] S. Ngobeni, H.Venter, I. Burke, Forensics Readiness For Wireless Networks, IFIP Advances in Information and Communication Technology, Vol 337, 2010, pp 107-117 ISBN 978-3-642-15506-2

[7] F. Tufail and H. Islam, "Wearable Wireless Body Area Networks", Information Management and Engineering, ICIME '09, pp 656-660, 2009.

[8] R Ajemian, AD Ausillio, H Moorman, E Bizzi, Why Professional Athlete Need A Prolonged Period Of Warm-Up And Other Peculiarities Of Human Motor Learning, Journal of Motor Behaviour, Vol 42, No 6, 2010, http://web.mit.edu/ajemian/www/Ajemian_et_al_Motor_learning.pdf

[9] B. Dolan, C. Psychol, Barrister, " Medical Records: Disclosing Confidential Clinical Information", The Psychiatrist, Vol 28, pp 53-56, URL:http://pb.rcpsych.org /content/28/2/53.full, 2004

[10] C. Cornelius and D. Kotz, "On Usable Authentication for Wireless Body Area Networks", Proceedings of the 1st USENIX Workshop on HealthSec 2010.

[11] M. Al Ameen, N. Ullah, M. S. Chowdhury, SM. R. Islam, K. Kwak, "A power efficient MAC protocol for wireless body area networks" EURASIP Journal on Wireless Communications and Networking 2012, http://jwcn.eurasipjournals.com/content/2012/1/33

[12] A. Milenkovic, C Otto, P. D. Groen, B. Johnson, S. Warren, and G. Taibi, "A WBAN System for Ambulatory Monitoring of Physical Activity and Health Status: Applications and Challenges", 27TH Annual International Conference of the Engineering in Medicine and Biology Society, pp 3810-3813, 2005.