Developing the Security Zone for Wireless Body Area Network (WBAN) Implementation Using Practical Security Assessment (PSA)

Abdul Fuad Abdul Rahman and Madihah Zulfa Mohamad

***Abstract*—Wireless body area network (WBAN) is a wireless network similar to wireless sensor network (WSN). The WBAN uses body sensor to transmit and received wireless communication. The WBAN has recently emerged as one of the premier research topics in enhancing healthcare industry. However, since WBAN requires it to be a low powered sensor node, it will be extremely difficult to put through any advanced security mechanism due to the restriction of power use in WBAN devices. Therefore, this research proposed a different approach in securing WBAN. This research is designed to assess the confidentiality, integrity and availability of WBAN and measure the attack perimeter of the WBAN implementation, using a practical security assessment (PSA). In this paper, the idea of conducting PSA before designing WBAN security solution will be used. The WBAN security solution aimed to enhance the physical security of the WBAN by developing a Secure Zone for WBAN.**

***Index Terms*—Practical security assessment (PSA), security zone, wireless body area network (WBAN), wireless sensor network (WSN).**

I. Introduction

Wireless Body Area Network (WBAN) is a wireless network that can be attached or implanted in the human body. The idea is to replace wires connected to human body sensors, to increase patient's comfort and most of all, provide the ability for healthcare professionals to monitor patients remotely. Therefore, WBAN has become an important part of modern medical devices [1]. Recent research work by Rahman *et al*. 2014, showed that WBAN communication can be exploited to compromise Confidentiality, Integrity and Availability (CIA) of WBAN Sensors [2]. The research shows the importance of a practical security assessment (PSA) before designing security solutions and countermeasures. However, WBAN security is not as easy as the security on conventional desktop computers [3]. There are challenges exist. In other systems, designers use cryptographic approach to protect confidentiality and prevent unauthorized access [1]. However, adding advanced cryptography to WBAN, will be extremely difficult due to the limitation of power consumption [1]. Despite the challenges, security is important for WBAN Sensor. Therefore, a different approach to securing WBAN is needed.

A. Theory

There are factors that influence the reliability of WBAN sensors and its network. These factors are inspired from the WBAN characteristics and WBAN physical deployment [4]. The most influence characteristic of WBAN is the limitation on power source [4]. A study conducted by Mansouri *et al.* 2010, discovered that for the transmitting power on the distance estimation, between a target and a low transmission power sensor node, the distance estimation error (RMSE) is at its highest value at around 6 meters [4]. The study was conducted on a tracking application using the Variational Filtering (VF) based on quantized proximity sensors [4]. In other words, based on the Mansouri *et al*. 2010, any low powered sensor is only capable of transmitting data within 6 meters radius.

B. Approach

Based on Mansouri *et al*. 2010, it is known that RMSE is at its highest value at 6 meters. Therefore, this paper will adopt the discovery in the Mansouri *et al.* 2010 with an approach to securing WBAN. The approach of this paper is to explore the feasibility of protecting WBAN security without modifying them, by implementing a physical security mechanism by harnessing WBAN surroundings. Such an approach are expected to enhance the security of WBAN without altering or adding other security mechanisms to the existing WBAN medical devices. The idea of conducting practical security assessment before designing WBAN security solution will be the core element in this paper. The practical security assessment will be conducted on a WBAN Sensor prototype developed as a testbed.

C. Testbed

In this paper, the development of the WBAN Sensor prototype adheres to the ISO 13485:2003 medical device requirements outline by the International Organization of Standardization (ISO), and adheres to the Malaysian Laws of Medical Device Act 2012 (Act 737). The WBAN sensor prototype designed in minimal weight, miniature form-factor, limited processing power, storage, bandwidth and standard based interface protocols [3]. The prototype WBAN sensor deployed, designed with the details as shown in Table I. Throughout this paper, this prototype will used as the testbed [4]. The testbed was set as the target during the practical

Manuscript received November 19, 2014; revised April 16, 2015. This work was supported in part by the Malaysian Ministry of Education under Grant ERGS/2011/FTMK/PK02/1 Exploratory Research Grant Scheme (ERGS).

A. F. A. Rahman is with the National Vulnerability Assessment Centre (MyVAC), Department of Security Assurance, Cyber Security Malaysia, Malaysia (e-mail: abdfuad@cybersecurity.my).

M. Z. Mohamad is with the My Cyber Security Clinic (My CSC), Department of Industry and Business Development, Cyber Security Malaysia, Malaysia (e-mail: madihah@cybersecurity.my).

DOI: 10.7763/JACN.2015.V3.152

security assessment [4]. In this paper the practical security assessment conducted, adhere to the convention on cybercrime, and the vulnerability assessment and penetration testing (VAPT) methodology from the Cyber Security Malaysia.

TABLE I: WBAN SENSOR PROTOTYPE

No	Components	Description
1	Antenna	1dBi built in antenna
2	Rate	Transmitting up to 250kbps of data
3	Battery Power	3v battery
4	Sensor's Weight	20g of weight
5	Bandwidth	2.4GHz
6	Program + Data Memory	8KB SRAM
7	External Memory	128KB Flash ROM

II. PRACTICAL SECURITY ASSESSMENT

The practical security assessment (PSA) is a practical testing to assess the impact of WBAN security threats. Each testing will be conducted practically by imposing other wireless technology security threats to WBAN system. A set of wireless security threats was selected based on explanatory report of convention on cybercrime. The four wireless security threats, PSA (x_m) as shown in Table II. These selected PSA (x_m) is an act of causing security breach and is considered as cybercrime based on the convention on cybercrime. The convention on cybercrime are accepted in 51 countries, including the United Kingdom and Japan [5].

TABLE II: SET OF FOUR PSA

m	PSA (x_m)	Attack
1	PSA (x_1)	Eavesdropping
2	PSA (x_2)	Denial of Service (DoS)
3	PSA (x_3)	Authentication Bypass
4	PSA (x_4)	Role Bypass

A. Changeable Variable

Based on the Convention on Cybercrime, traffic data are referred as any data relating to a communication by a computer system that formed a part in the chain of communication, indicating the origin of the data, the destination of the data, the data route, the time stamp, the size of the data and packet of data, duration and type of the data or service [6]. In any cybercrime cases, it is crucial for the digital forensic team to analyze and determine the location of the crime and also the time of the crime committed [7].

TABLE III: CHANGEABLE VARIABLE

No	Changeable Variable	Description
1	Distance	The distance between the attacker and WBAN target systems as shown in Fig. 2.
2	Time to Execute	The time taken to execute a successful PSA (xm)

Therefore, during the PSA (x_m) process, two variables will be measured. The first variable is the time taken to execute a successful PSA (x_m), and the second variable is the distance between the attacker and WBAN systems as shown in Table III. The time measured will provide inputs to estimate the amount of time taken for each PSA (x_m) conducted. The PSA (x_m) conducted from various distances to identify and investigate the minimum and maximum distance required, to execute a successful PSA (x_m). The Distance variable will be use to developed the Security Zone.

B. Impact Variable

The council of Europe adopted the convention on cybercrime aimed at deterring action against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data [5]. Furthermore, according to the convention on cybercrime, any impairment to the confidentiality, the integrity and the availability of the WBAN system are considered as security breached [5]. In a study conducted by Perrig *et al*. 2010 also formalized the Confidentiality, Integrity and Availability as the security requirements for sensor [4]. Therefore, for this reason, the Confidentiality, the Integrity, and the Availability will be used to gauge the successfulness of an attack and will be set as impact variable as shown in Table IV.

TABLE IV: IMPACT VARIABLE

Impact Variable	Security Three Pillars	Description
C	Confidentiality	Protect the information to be disclosed only to authorized persons or organization
I	Integrity	Protect the information accuracy, authenticity, reliability, and completeness
A	Availability	Protect the information to be accessible to authorized users when required.

C. Testbed Setup

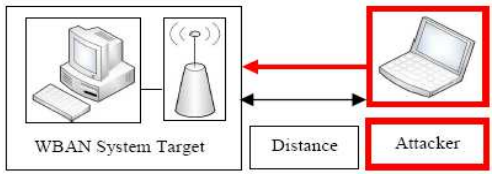

Fig. 1. Testbed setup.

All four wireless security attacks, PSA (xm) will be setup based on the testbed setup as shown in Fig 1. The setup deployed no other security mechanism such as Firewall, Intrusion Detection System, and Intrusion Prevention System between Attacker and WBAN Sensor prototype [2]. An attacker will be setup in a manner of clear line of sight location between the WBAN Sensor prototypes [2]. In this paper, the development of the Attacker prototype adheres to the requirements outline by the Federal Communication Commission (FCC) and adhere to the Malaysian Sirim regulation. The Attacker prototype designed with the details as shown in Table V [8].

TABLE V: ATTACKER PROTOTYPE

No	Components	Description
1	Antenna	1dBi built in antenna
2	Rate	Transmitting up to 250kbps of data
3	Power	External Power Source
4	Bandwidth	2.4GHz
5	Program + Data Memory	128 KB
6	External Memory	256KB

D. Eavesdropping

Fig. 2. Eavesdropping process.

Eavesdropping is an activity of secret listening to the other computer communication and in this paper, is the communication between WBAN Sensor and WBAN Base Station [9]. The Eavesdropping in this paper is similar to the other network tapping process done in wireless local area network (WLAN) and local area network (LAN) as shown in Fig. 2.

E. Denial of Service

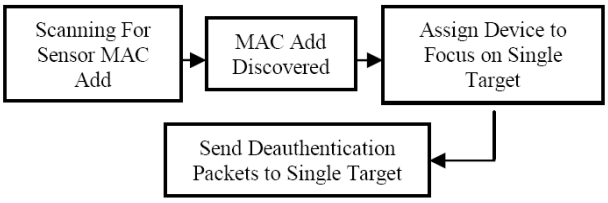

Fig. 3. Denial of service process.

Denial of service (DoS) is an activity to make assets of the WBAN unavailable to its intended user [10]. In this paper DoS is an activity to make the WBAN sensors unavailable and unable to transmit its WBAN signal towards the WBAN base station. A sensor can be DoS using the Hello World packets as Deauthentication packets in an attempt to flood the network as shown in Fig. 3 [11].

F. Authentication Bypass

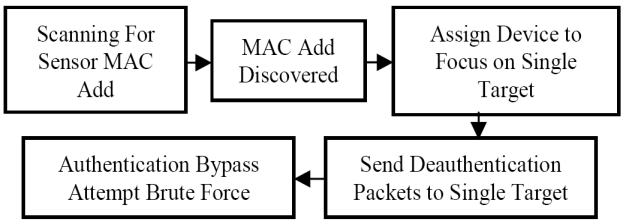

Fig. 4. Authentication bypass process.

Authentication Bypass is an activity of exploiting the authentication system vulnerability in order to skip the authentication challenge process [12]. Based on the research conducted in 2010, a Stolen Verifier attack against a system will exposed authorized user credentials as shown in Fig. 4 [13].

G. Role Bypass

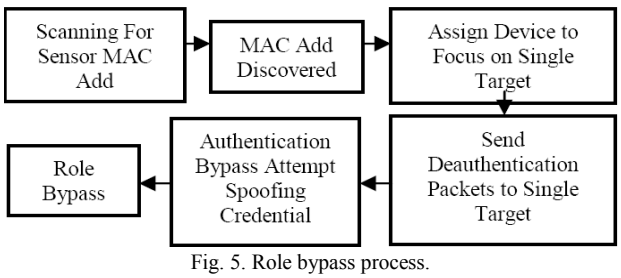

Fig. 5. Role bypass process.

In this paper a role is similar to an access control system providing access restriction. This Role can be exploited to bypass the access restriction [14]. In this paper, the Role Bypass is executed by using the Spoofing Credentials Attack [15]. An authorized user credential was obtained using the DoS attack and Eavesdropping attack [14]. The unauthorized user will then use the obtained authorized credentials to access the WBAN sensor as an authorized user as shown in Fig. 5.

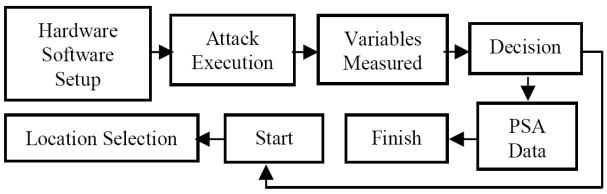

Fig 6. Practical security assessment (PSA) flow chart.

The PSA process simplified in flow chart as shown in Fig. 6. The only set of variables from a successful PSA will be recorded. If the PSA conducted was not successful, the whole process will be repeated. The success of the PSA was determined by the impact of the affected WBAN system, and the impact was verified using logs recorded by the WBAN system during the execution period of PSA. The logs generated by the WBAN system will be used to verify which impact was affected. At this stage, the inputs recorded is the Changeable Variables as shown in Table III and the Impact Variables as shown in Table IV.

TABLE VI: ATTACKER PROTOTYPE

Process	Description
Location Selection	During this process, the location of the WBAN Target System will be fixed and the location of the Attacker will be varied. The distance between the Attacker and the WBAN Target System will be measured and recorded as shown in Fig 1.
Hardware & Software Setup	During this process, all the hardware and software used in the PSA will be set up accordingly and switch on.
Attack Execution	The process of PSA (x_1), PSA (x_2), PSA (x_3) and PSA (x_4) as shown in Fig 2 to Fig 5 will be executed and during this whole process, the variable for Time will be recorded.
Variables Measured	During this process, the Time variable will be measured simultaneously with the PSA. All variables measured will only be recorded if the attack was successfully executed. If the PSA conducted was not successful, the whole process will be repeated.
PSA Data	PSA data will be recorded from a successful PSA only.

III. PIA RESULT

The result of PSA (x_m) was presented in Table VI. The result in Table VI successfully proves that imposing other wireless technology security threats to WBAN is achievable. Table VI shows that time taken to execute a successful PSA (x_m). The time differences were influenced by various factors, but from the result the main factor is the complexity of different security threats, PSA (x_m). Distance seems not affect the time of execution. There are slightly different, but it is still within the range of 1 to 13 seconds adrift for each distance. The distances were set from 1 meter, 2 meter, 3 meter, 4 meter,

and 5 meter. The maximum distance between the attacker and the WBAN target system recorded for all successful PSA (x_m) conducted was five meters (5m). The PSA (x_m), unable to produce any result beyond this 5m distance

TABLE VII: PSA RESULT

PSA (x_m)	PSA Changeable Variable		PSA Impact Variables			AVF Value
	Distance (meter)	Time to Execute (s)	C	I	A	
PSA (x_1)	>5.0	-	-	-	-	-
	5.0	85.50	1	0	0	1
	4.0	86.16	1	0	0	1
	3.0	85.32	1	0	0	1
	2.0	85.32	1	0	0	1
	1.0	86.34	1	0	0	1
PSA (x_2)	>5.0	-	-	-	-	-
	5.0	123.23	0	0	1	1
	4.0	122.44	0	0	1	1
	3.0	122.26	0	0	1	1
	2.0	126.69	0	0	1	1
	1.0	128.09	0	0	1	1
PSA (x_3)	>5.0	-	-	-	-	-
	5.0	366.35	1	1	1	3
	4.0	370.13	1	1	1	3
	3.0	375.87	1	1	1	3
	2.0	378.67	1	1	1	3
	1.0	379.59	1	1	1	3
PSA (x_4)	>5.0	-	-	-	-	-
	5.0	529.66	1	1	1	3
	4.0	543.34	1	1	1	3
	3.0	540.50	1	1	1	3
	2.0	540.32	1	1	1	3
	1.0	540.76	1	1	1	3

IV. DISCUSSION

The changeable variables are both highly influenced by other factors. Although conducted on clear line of sight, radius distances are very much affected by the interference of other signals or frequencies operated on the same spectrum, as WBAN exists in the air [2]. This study purposely conducted without sweeping the floor for interference in order to study the WBAN security in a real environment [2].

As discussed in previous section, a study conducted in 2010 discovered that for the transmitting power on the distance estimation between a target and a low transmission power sensor node, the distance estimation error (RMSE) is at its highest value at around 6 meters [4]. The study was conducted on a tracking application using the Variational Filtering (VF) based on quantized proximity sensors [4]. However, from this study, the PSA has shown results that a successful security threat can be executed not more than five (5) meters radius from the WBAN target system.

In this 5 meters distance, the communication of the standard WBAN sensor node was tested using PSA and the result was negative and providing no data or readings [2]. It can be concluded that no PSA testing that can be conducted beyond this 5 meter barrier [2]. This barrier justified if the discovery of highest RMSE on low power sensor node applied. However the explanations of the slight difference between those two distances can be researched further in the future. To this date, for the purpose of this study, it saves to recommend that a WBAN system installation to have a minimum distance of 5 meters radius from other wireless system and devices as shown in Fig. 7 [2]. The minimum distance of 5 meters will create a secure 78.5714m^2 space to ensure WBAN sensor node security.

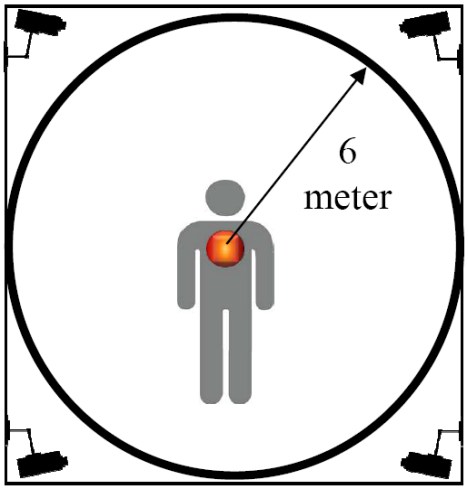

Fig 7. Security zone.

The Time variable also depends highly on human skills. It is known that without proper human motor skill practiced, it is well known that initial level of skilled performance will drop considerably [16]. Although the PSA was conducted multiple of times in order to increase the rate of accuracy, reliable data and reduce the error rate, the PSA still much depends on the human skills who perform [16].

V. SECURITY ZONE

Previously, the PSA has shown results that a successful attack can be only executed from less than five meters radius from the WBAN target system. From this finding, we proposed a prevention technique to be applied in the WBAN secure network architecture. To date, it was discovered that a WBAN system installation is recommended to have a minimum distance of six meters radius from other wireless system and devices as shown in Fig. 7. The minimum distance of six meters will create a secure 78.5714m^2 space to ensure WBAN system security. No other device with the wireless technology capability authorized inside this 78.5714m^2 space except for the Authorized Medical Officers. These security measures are to provide the proposed architecture the ability to reduce the security risk and prevent an incident happen.

It is proposed that this minimum 78.5714m2 space created also equipped with Surveillance Cameras or Closed Circuit Television (CCTV) for Security purposes. As shown in Table V, if an incident such as PSA (x_1), PSA (x_2), PSA (x_3) or PSA (x_4) were to occur, from the PSA findings, we can estimate that the incident was executed within a five meter radius. With the support of CCTV recording, the location where the attack was executed can be estimated. We can determine where the attacker location, including which the attacker was, and detect which attack was executed by referring to the information in Table VII.

For example, a scenario of 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 suspects spends only 10 seconds in the crime scene, and the other spends 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 WBAN Sensor can be used to provide further information such as time stamp and MAC address for further investigation purposes [7].

VI. Conclusion

The idea of conducting practical security assessment (PSA) before designing security solution is achievable. The data obtained from PSA has been successfully converted to security zone to secure WBAN system. However, the Security zone is recommended to be researched and enhanced in future research in order to create a comprehensive security solution for WBAN.

Acknowledgment

The authors would like to thank all the reviewers for their helpful comments. We also would like to thank the Cyber Security Malaysia, an agency under the Ministry of Science, Technology and Innovation Malaysia (MOSTI) for their contribution. 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 Education Malaysia (MOE).

References

[1] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," presented at the ACM SIGCOMM 2011 Conference, Toronto, Canada, 2011.

[2] A. F. A. Rahman, R. Ahmad, and S. N. Ramli, "Forensics readiness for wireless body area network system," presented at the 16th International Conference of Advanced Communication Technology (ICACT 2014), Pyeongchang, South Korea, February 2014.

[3] A. Perrig, "SPINS: Security protocols for sensor networks," *Wireless Networks*, vol. 8, pp. 521-534, 2000.

[4] M. Mansouri, A. Sardouk, L. M. Boulahia, D. Gaiti, H. Snoussi, R. R. Amoud, and C. Richard, "Factors that may influence the performance of wireless sensor networks," *Smart Wireless Sensor Networks*, 2010.

[5] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai, and S. K. S. Gupta, "A wireless sensor network based health security infrastructure and testbed," in *Proc. IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2005, pp. 406-407.

[6] Convention on cybercrime. Council of Europe (CoE). (2001). [Online]. Available: http://conventions.coe.int/Treaty/en/Reports/Html/185.html

[7] E. Casey, *Handbook of Computer Crime Investigation*, *Forensic Tools and Technology*, San Diego, US: Elsevier Academic Press, 2007, ch. 1.

[8] J. Wright, *Wireless Network Ethical Hacking and Penetration Testing*, SANS Institute Training Notes, 2014.

[9] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor network," *Information Processing in Sensor Networks Lecture Notes, Computer Science*, vol. 2634, pp. 349-364, 2003.

[10] A. Wood and J. Stankovic, "Denial of service in sensor network," *Computer,* vol. 35, issue 10, 2002.

[11] D. R. Raymond and S. F. Midkiff, "Denial of service in wireless sensor networks: Attacks and defenses," *Pervasive Computing*, vol. 7, issue 1, pp. 74-81, 2008.

[12] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in Sensor Network," presented at the IEEE Symposium on Security and Privacy, 2004.

[13] M. K. Khan and K. Alghathbar, "Security analysis of two factor user authentication in wireless sensor networks," *Advances in Computer Science and Information Technology, Lecture Notes in Computer Science,* vol. 6059, pp. 55-60, 2010.

[14] T. Lee, C. Qiao, M. Demirbas, and J. Xu, "ABC: A simple geographic forwarding scheme capable of bypassing routing holes in sensor networks," in *Proc. the 17th International Conference on Computer Communications and Networks*, 2008, pp. 1-8.

[15] C. Cornelius and D. Kotz, "On usable authentication for wireless body area networks," presented at the 1st USENIX Workshop on Health Security and Privacy, 2010.

[16] R. Ajemian, A. D. Ausillio, H. Moorman, and E. Bizzi, "Why professional athlete need a prolonged period of warm-up and other peculiarities of human motor learning," *Journal of Motor Behavior*, vol. 42, no. 6, 2010.

Abdul Fuad Abdul Rahman is a senior analyst with the National Vulnerability Assessment Centre (MyVAC) of Cyber Security Malaysia. Prior to that, he has a system security certified practitioner (SSCP) from the International Information Systems Security Certification Consortium (ISC)^2, a GIAC assessing wireless network (GAWN) certification from SANS Institute of America and he is a certified network engineer IPv6 (CNE6). He is currently appointed as the technical advisor to the Cybercrime Legislation Committee chaired by the Attorney General's Chambers of Malaysia.

Madihah Zulfa Mohamad is a senior executive with the My Cyber Security Clinic of Cyber Security Malaysia. Prior to that, she has a certified ethical hacker (CEH) from EC-Council and she is a Microsoft certified system engineer (MCSE) from Microsoft. She is currently focused in the research field of digital forensic, especially in data recovery.