Security Analysis of Medical Devices within Wireless Body Area Networks and Mobile Health Applications

Abdulkerim DEMİR[1], Emin İslam TATLI[2]

[1]Ziraat Technology, İstanbul, Turkey
[2]STM Defense Technologies Engineering and Trade Inc., Ankara, Turkey
abdemir@ziraatteknoloji.com, emin.tatli@stm.com.tr
(Geliş/Received:28.03.2017; Kabul/Accepted:03.12.2017)
DOI: 10.17671/gazibtd.301668

***Abstract*—** Body Area Networks (BAN) consisting of medical devices that interact with human body have been in recent years developed in accordance with technical developments in healthcare area. Thus, devices automatically measuring human blood pressure or insulin value and transmitting the measured data into hospital management systems have been started to be used in daily-life. These medical devices aim to improve health of patients, however they are also subjected to unauthorized access and manipulation which creates substantial risk for the patients. In this paper, the analysis results of medical devices used in Wireless Body Area Networks (WBAN) and mobile health applications are explained according to different security requirements and aspects. All threats and risks faced by remotely accessible medical devices in WBAN are identified by applying WBAN threat modeling. Performed security analysis and penetration testing of mobile health applications running on smart devices are presented in detail. In addition, secure architecture principles for WBAN designs are discussed in detail.

***Keywords*—** WBAN architecture, WBAN security analysis, mobile application penetration testing, health security

Vücut Alan Ağlarındaki Medikal Cihazların ve Mobil Sağlık Uygulamaların Güvenlik Analizleri

***Özet*—** Sağlık alanındaki teknolojik gelişmelerle birlikte insan vücudu ile etkileşimde bulunan medikal cihazlardan oluşan Vücut Alan Ağları (BAN) geliştirildi. Bu sayede örneğin insan kan basıncını ya da insülin değerini otomatik ölçen ve hastane yönetim sistemlerine aktaran mobil cihazlar günlük hayatta kullanılmaya başlandı. Bu medikal cihazlar bir yandan sağlık yönetimini iyileştirirken diğer taraftan bunlara yapılacak izinsiz müdahale ile insan sağlığını riske atabilmekte hatta ölümlere neden olabilmektedirler. Bu çalışmamızda Kablosuz Vücut Alan Ağları (WBAN)'nda kullanılan medikal cihazların ve mobil sağlık uygulamalarının güvenlik analizleri gerçekleştirildi. Öncelikle WBAN'ın tehdit modellemesi yapılarak WBAN'da ki özellikle uzaktan erişilebilir medikal cihazların karşı karşıya kaldıkları bütün tehditler ve riskler belirlendi. Akıllı cihazlar üzerinde çalışan mobil sağlık uygulamaları için güvenlik analizleri ve güvenlik sızma testleri gerçekleştirildi. Ayrıca, WBAN sistem tasarımı için güvenli mimari prensipleri belirlendi.

***Anahtar Kelimeler*—** WBAN mimari, WBAN güvenlik analizi, mobil uygulama sızma testi, sağlık güvenliği

1. INTRODUCTION

Today, wireless sensor networks have vital importance in our lives since they are utilized in various fields. Solutions are present for many issues in health area with the use of this technology combined with medical technologies. Significant changes have been made to traditional patient monitoring systems with wireless sensor networks. Developing a patient monitoring system generally requires transmission of patient data to a medical server at hospitals. Doctors and other medical staff can access required patient data on medical servers. The data is collected by intelligent sensors placed on the body or inside the tissues of patients. The technology that enables the transmission of data from sensors to a server over a wireless connection for analysis or storage is called Wireless Body Area Network. WBAN

technology enables monitoring medical patient data without temporal and spatial limitations but security risks of this technology can bring several disadvantages as well. The vital functions of monitored patients may be in danger if these vulnerabilities are misused and even death cases might occur.

In this study, the threats and risks that remotely-accessible medical devices in body area networks face were primarily identified. Security penetration tests for mobile health applications, which can be downloaded from official application stores and run on smart devices, were performed. In addition, sharing of personal health data between these health applications and cloud computing environments were evaluated from security and privacy perspectives.

The paper is organized as follows: Section 2 explains the related work. Section 3 provides a general information about WBAN architecture layers and patient monitoring systems. In Section 4, security risks of WBAN system are given based on a secure architecture threat catalog. Section 5 explains the results of security testing of a WBAN mobile device as well the penetration test results of its management mobile apps. Penetration testing results of 15 mobile health applications are explained in Section 6. In Section 7, the required security controls of WBAN system and mobile health applications are evaluated. The Section 8 concludes the paper and discusses the future work.

2. RELATED WORKS

The data collected from all BAN sensors are sensitive personal data. The security requirements for intra- and extra- BAN transmissions of this data, the secure storage of the data and the availability of access on demand have increased interests of researchers in this area. Due to use of wireless technologies, WBAN technologies are more likely to contain security vulnerabilities. Many studies have been published so far by researchers and system designers in this area.

Jang et al. [8] proposed a new security model and security framework for information protection in wireless body area networks. This work was intended to be a guideline for ensuring proper security and privacy of wireless communication in WBAN. Garcia-Morchon et al. [9] developed a distribution model for wireless sensor networks based on the concept of patient living area and medical sensor networks used in the widespread patient care services. This group offers a complete and effective secure structure consisting of three levels of operation and safety requirements in patient area network, medical sensor network and back-end levels. Glucose monitoring and insulin delivery systems are becoming increasingly popular among diabetic patients. These devices use wireless networks that are often subject to security attacks. In 2011, Li et al. [10] studied an insulin pump in a laboratory environment, which is on the market and also controls glucose. They proposed defense methods against various attacks. The use of Implantable Medical Devices (IMD) increases with the medical needs of patients. IMDs designers work on safety, reliability, ease of use, power consumption and cost. Burleson et al. [11] specified design challenges by examining published work on safe and implantable medical devices. They discussed the implementation of security principles and avoiding common security risks. The safety and privacy features of an Implantable Cardioverter Defibrillator (ICD) device have been examined by Halperin and coworkers [12]. This device with cardiopulmonary technology uses wireless communication and is easily found on the market.

Silva et al. [13] developed a basic patient model related to Medical Cyber Physical Systems (MCPS). The purpose of this work is to provide patient safety and verify the MCPS. They introduced a patient model that can be used to verify health care systems without jeopardizing the health of the patient. Ramli et al. [14] studied the use of biometric characteristics in secure data communications in WBAN and power efficiency as well as reduction of computational complexity. They used hybrid authentication model as a conceptual framework for the system. In addition, Ramli et al. published another study [15] in the same year that could be an example for this study. They use ECG signals as biometric data for secure WBAN technology.

3. WBAN ARCHITECTURE

Various technologies are used based on the type and distance of communication end-points to ensure a reasonable communication in patient monitoring systems. Patient monitoring system networks are grouped as short-range wireless technologies (WBAN), medium-range wireless technologies (HAN, WLAN) and long-range wireless technologies (WMAN, WWAN).

The most commonly used examples of these grouped devices and the relative distance map for human-body are illustrated in Figure 1.

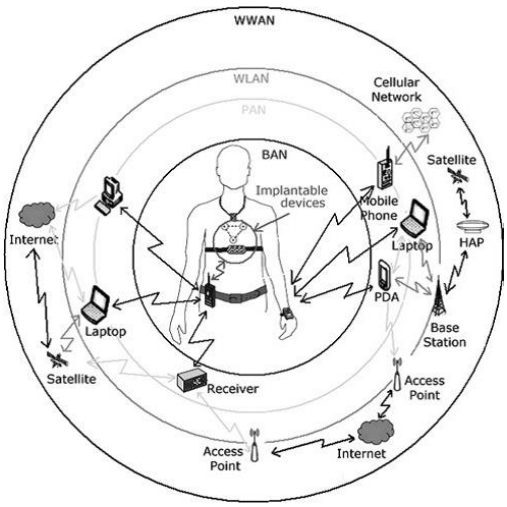

Figure 1. The relative distance map from human-body [1]

Wearable computers, wireless local area networks, personal area networks, BAN, GSM / GPRS, Wimax and

cognitive radio technologies are widely used in patient monitoring systems. From these technologies, BAN attracts attention in terms of lower cost and applicability. Generally a BAN contains components such as sensor, microprocessor, chip and battery. Communication between BAN components is called Intra-BAN and communication between BAN and remote monitoring medical server is called extra-BAN. The gateway facilitating extra-BAN communication is defined as Mobile Based Unit (MBU) [2]. Sensors are responsible for collecting data. Physical events such as patient movement, muscle activity, or blood flow are first converted to electrical signals, then these signals are amplified, recorded, digitized and transmitted via extra-BAN.

The architecture of a patient monitoring system generally consists of three layers. The first layer is called BAN layer. It generates raw data via wearable computers. In this layer, signals from wireless sensor that are placed on patient's body surface or in tissues are collected by a network controller. Personal area network technologies such as Bluetooth, ZigBee, Ultra-Wideband (UWB) in connection with a BAN server can be used as a network controller. The second layer is a BAN server collecting data from sensors. This layer is responsible for transmitting data from sensors to medical server layer, which is the last layer. In addition, some data types can be evaluated in this layer and results can be delivered. The BAN server can be Personal Digital Assistant (PDA), personal computers or mobile phones. Wimax, GSM/GPRS, EDGE, 3G and LTE technologies named as wireless wide area networks are widely used between BAN servers and medical servers. The third layer is medical server layer. The data sent by BAN servers is processed and stored in this layer. This layer also depends on hospital information management systems. Thus, the processed data is transmitted to the relevant personnel (e.g. doctor, nurse, ambulance, etc.) as an alarm or a report [3].

WBAN consisting of sensors in personal body area is a short-range wireless communication technology. In WBAN technology, data from biomedical sensors placed in or on the body is transferred to a server using a wireless connection for analysis or storage purposes. Usage of short-range wireless network technology to transmit signals from sensors to BAN servers distinguishes it from other technologies. WBAN technology is based on the IEEE 802.15.6 standard [4].

4. SECURITY RISKS OF WBAN SYSTEMS

We have developed a Secure Architecture Threat Catalog (see Figure 2) which is grouped into four different categories for detailed threat analysis of WBAN architectures. The four categories of the threat catalog are Person and Process Layer, Network Layer, System and Application Layer and Physical Layer.

The security risks identified during our analysis have been evaluated according to Microsoft STRIDE Threat Methodology [5]. In this methodology, S refers to Spoofing identity, T refers to Tampering with data, R refers to Repudiation, I refers to Information disclosure, D refers to Denial of service and E refers to Elevation of privilege.

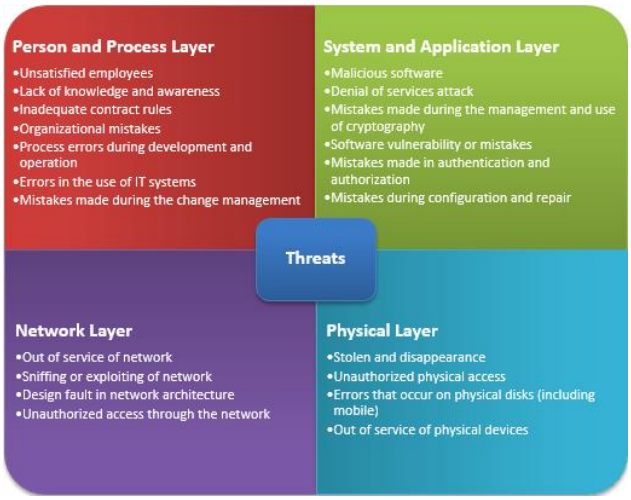

Figure 2. Secure architecture threat catalog

Based on our security analysis, the security risks of WBAN layer are given in Table 1, the security risks of WBAN server layer are given in Table 2 and the security risks of medical server layer are given in Table 3 respectively in detail.

Table 1. Security Risks of WBAN Layer

Security Risks	S	T	R	I	D	E
Being infected with a malware, a WBAN sensor becomes unavailable and cannot send data from patient-body to the WBAN server.		X		X	X	
As a result of a denial of service attack performed towards a WBAN sensor, it cannot receive data from patient-body or transmit data to the WBAN server.					X	
Due to incorrect usage and configuration of cryptography methods, a WBAN sensor exchanges insecurely data over network channel.	X	X	X	X		X
Vulnerabilities within sensor firmware can be exploited for data leakage.	X	X	X	X	X	X
Security weaknesses in authentication process can be misused for data leakage and data manipulation.	X	X	X	X		X
Security weaknesses in authorization process can be misused for privilege escalation.			X	X		X
Misconfiguration of smart sensors can be exploited.	X	X	X	X	X	
Due to network unavailability, smart sensors cannot communicate with a WBAN server and exchange data.					X	
As being physically out of service (distortion, fracture, etc.) of a smart sensor, it cannot transmit data.					X	

Table 2. Security Risks of WBAN Server Layer

Security Risks	S	T	R	I	D	E
In case system operators have insufficient knowledge and lack of awareness, attackers can get unauthorized access to sensitive health data on WBAN servers.	x	x	x	x	x	x
Being infected with a malware, a WBAN server becomes unavailable and can share personal health data with unauthorized persons.		x		x	x	
As a result of a denial of service attack performed towards a WBAN server, health data cannot be accessed.					x	
Due to incorrect usage and insecure configuration of cryptography methods, protected data that are stored on WBAN servers and exchanged through the network can be endangered.	x	x	x	x		x
Vulnerabilities in server firmware can be exploited for data leakage.	x	x	x	x	x	x
Security weaknesses in authentication process can be misused for data leakage and data manipulation.	x	x	x	x		x
Security weaknesses in authorization process can be misused for privilege escalation.			x	x		x
In case of network unavailability, the communication and data exchange with a WBAN server becomes not possible.					x	
Misconfiguration of communication network with server can be exploited.	x	x	x	x	x	
In case attackers get unauthorized access to WBAN servers, they can get access and even manipulate sensitive data stored on the servers.	x	x		x	x	
In case attackers get physical access to WBAN servers, they can shut-down the servers and stop all communication.		x		x	x	
In case of hard disk failures, data stored on servers cannot be accessed.				x	x	

Table 3. The Security Risks of Medical Server Layer

Security Risks	S	T	R	I	D	E
Staff dissatisfaction at the medical server layer can cause negative results.	x	x		x	x	
In case system operators have insufficient knowledge and lack of awareness, attackers can get unauthorized access to sensitive health data on medical servers.	x	x	x	x	x	x
As a result of organizational errors that may occur in the medical server layer, misinformation can be given to healthcare staff.		x		x	x	
Being infected with a malware, medical server layer becomes unavailable and personal health data can be shared with unauthorized persons.		x		x	x	
As a result of denial of service attacks performed towards a WBAN server, health data cannot be accessed and healthcare staff cannot perform any operation.					x	
Due to incorrect usage and insecure configuration of cryptography methods, protected data that are stored on medical servers and exchanged through the network can be endangered.	x	x	x	x		x
Vulnerabilities in server firmware can be exploited for data leakage.	x	x	x	x	x	x
Security weaknesses in authentication process can be misused for data leakage and data manipulation.			x	x		x
Security weaknesses in authorization process can be misused for privilege escalation.			x	x		x
Misconfiguration of systems in the medical server layer can be exploited.	x	x	x	x	x	
In case of network unavailability, the communication and data exchange with a medical server becomes not possible.					x	
Misconfiguration of communication network between medical server layer and WBAN server can be exploited.	x	x	x	x	x	
In case mobile devices get stolen, sensitive data can be accessed and manipulated by the attackers.	x	x		x	x	
In case attackers get physical access to medical servers, they can shut-down the servers and stop all communication.		x		x	x	
In case of hard disk failures, data stored on servers cannot be accessed.				x	x	

The security risks that can be encountered at each layer of WBAN technology were examined in detail as well. This examination shows that more attention should be paid to security requirements while designing WBAN systems.

5. SECURITY TESTS OF A WBAN DEVICE AND EXPERIMENTAL RESULTS

In this step, a commercial mobile WBAN medical device with features such as regular sleep monitoring, heart rate measurement and calorie counting was procured and its security analyses were performed. The device comes along with an official mobile Android application for remote management. We performed security penetration testing of the official mobile app as well. The device and the mobile application communicates over Bluetooth version 4.0 BTLE (BTLE, Bluetooth Smart) technology. It transfers its collected data from various sensors to the communicated mobile device.

In the security analysis of the mobile WBAN device, we checked security details of its Bluetooth configuration used between the WBAN device and the mobile application. Our analysis showed that the tested medical devices does not provide sufficient security for secure communication. Even though Bluetooth v4.0 supports all security modes, the default BTLE mode of the device is set to "Security Mode 1" which is the most insecure mode. This configuration is not recommended for a reasonable security. It cannot protect against traffic sniffing and man-in-the middle attacks. By sniffing Bluetooth network traffic, it is possible to grasp clear text values such as BD_ADDR (Bluetooth Device Address), RAND (Random Number), SRES (Signed Response)) and even PIN VALUE. With this PIN value, crafted packets can be injected into the traffic and sent to the device for manipulation.

In addition to the Bluetooth configuration, we also tested security aspects of the official Android application from the vendor as well as three non-official Android apps from other third party play stores. All four applications support storing data on cloud-based backend servers.

We performed mobile penetration testing based on OWASP Mobile Security Testing Guide methodology [16]. Using this methodology, we checked existence of several security controls for the categories like secure architecture, secure storage, secure network communication, cryptography, authentication, session management, access control, etc. For instance, it was checked if critical data is stored in the databases in unencrypted forms. It was checked if the mobile applications validate backend SSL certificates correctly. It was checked if sensitive data is leaked in the logging process. It was checked if code obfuscation is applied or not. Usage of critical permissions were checked as well. We also applied reverse engineering methods on the Android *.apk* files and checked both required permissions for execution and deobfuscated source codes for sensitive data like hard-coded passwords or keys. During the security tests, we utilized the tools such as Android SDK, Genymotion Emulator, Burp Suite Free Version, Wireshark network sniffer, and Vezir v2 Linux distro.

We could identify several security vulnerabilities during our penetration tests. Considering secure storage of sensitive personal health data, none of the mobile apps provides encryption of the locally stored data. On the other hand, all four applications establish a secure SSL channel before sending data to the cloud servers. Android permissions are very critical for privacy. It is also known fact that Android apps misuse permissions since end users are incompetent at management of permissions [17]. Three of the four mobile apps contained dangerous permissions such as ACCESS_NETWORK_STATE, SEND_SMS, READ_CONTACTS etc. One of the mobile apps supports MAC authentication instead of username-password authentication, but it allows manual entry of MAC addresses. This is an insecure practice for authentication.

6. PENETRATION TESTING OF MOBILE HEALTH APPLICATIONS

In this step, we aimed to check security status of mobile applications used for health management. We identified 15 mobile health applications from the official Android application store and other third-party Android application stores for penetration testing. The selected applications can be considered as security-critical applications since they process and store sensitive personal health data like heart rate and insulin value. Some of the applications exchange data with remote hospital information systems. As explained in the previous section in detail, we applied also OWASP Mobile Security Testing Guide methodology for penetration testing of these 15 mobile Android apps. The penetration test results of the fifteen mobile health applications are summarized in Table 4.

Table 4. Penetration Testing Results of the Selected Mobile Apps (Y: Yes, N: No)

App. Name	Unauthorized database access possible	Obfuscation applied	Authentication enforced	Sensitive data exists in Source Code	Logging of sensitive data	Encrypted data transmission	# of dangerous permissions
Healthiply [18]	N	N	Y	N	Y	N	3
mMR [19]	N	N	Y	N	Y	N	0
Nfc Medic [20]	N	N	Y	N	N	N	3
Patient Chart [21]	N	N	Y	N	N	N	0
Zibdy [22]	Y	N	Y	N	N	Y	3
Yalova Devlet [23]	N	N	Y	N	N	N	0
Diagnose [24]	Y	N	N	N	N	N	0
Health Files [25]	N	N	N	N	N	N	0
Pedometer	Y	Y	N	N	N	N	0
Smart Medical [26]	N	N	N	N	N	N	2
Health Records [27]	Y	Y	N	N	N	N	1
Caddy [28]	Y	N	N	N	N	Y	1
Medical History [29]	Y	N	N	N	Y	N	1
WebMD [30]	Y	N	N	N	N	Y	2
Medical History [31]	Y	N	Y	Y	N	N	2

Access to application databases without password authentication was possible for certain apps. Only two apps applied code obfuscation which makes reverse engineering more difficult. Therefore, the original source codes of the remaining applications are easily accessible. Certain applications did not enforce authentication to access mobile app data. Some mobile apps contained sensitive hard-coded passwords in their source codes. Logging of sensitive data was also another vulnerability that exist in some mobile apps. It was realized that personal health data

including user name and password information were kept in the local storage area in clear text. It is known that this is insecure for confidentiality principle. Most apps did not establish a secure channel for secure communication with the back-end servers.

There were also various permissions required at different levels according to the capabilities of the tested applications. Some applications violated user privacy because of the permissions they requested. By misusing such permissions, they could make phone calls, access the data stored in the user calendar, access user's daily program, access and read the device contacts guide and even add entries into contacts. Some applications have RECEIVE, SEND, and C2D_MESSAGE permissions required for the GCM function that is susceptible to exploitation. It has been found that there are a number of applications incorporating some of the ten most dangerous permissions that are effective in the exploitation of security and privacy, as presented at Google I / O 2012 [6].

For more detailed information about the performed tests, you can refer to the master thesis titled as "*Security Analyzes of Medical Devices in Body Area Networks and Mobile Health Applications*" [7] of the authors.

7. SECURITY CONTROLS OF WBAN SYSTEM AND MOBILE HEALTH APPLICATIONS

Considering the overall security risks of WBAN technology, the results of our WBAN security test and related studies on this subject, we have identified several security controls for WBAN and WBAN server layers. These security controls are listed in Table *5*. While designing a mobile health system enabling communication of several parties, these controls should be taken into consideration and all required security controls should be enforced carefully.

Table 5. Security Controls of WBAN and WBAN Server Layers

No	Security Controls
SC1	Users must be educated about security weaknesses caused by lack of information and awareness.
SC2	Users must be informed about security risks that can arise from unauthorized physical access to used devices (sensor, WBAN server).
SC3	Technologies providing security controls such as authentication, encryption must be selected for wireless communication between smart sensors and WBAN servers.
SC4	Before transmission, data must be encrypted with strong cryptographic algorithms and sent over an encrypted channel.
SC5	Smart sensors and running software on WBAN servers must be subjected to secure software development processes and security tests must be performed.
SC6	No other applications must be installed on a device used as a WBAN server. If installed, security tests of those applications must also be done.
SC7	Authentication and authorization must be applied for access to sensors and WBAN servers.
SC8	Configurations of sensors must be made in accordance with the system used.
SC9	The network used for data transmission must be protected against denial of service attacks.
SC10	The network used for data transmission must be secured against sniffing and exploiting.
SC11	Considering the risk of being stolen, devices used as WBAN servers must be evaluated and precautions such as backing up according to the criticality of the stored data must be taken.
SC12	Precautions must be taken about errors that may occur on the device disk of a device used as a WBAN server.

As a result of our mobile app security tests, a checklist of security controls for mobile health applications have been developed as well (see Table *6*).

Table 6. Security Controls for Mobile Health Applications

No	Security Controls
SC 1	It must be checked that mobile applications request only the required permissions.
SC 2	Only the data that an application will use for its business needs must be collected.
SC 3	Code obfuscation must be applied to the code of the mobile application being developed.
SC 4	An authentication process must be performed in order to keep personal health data in application.
SC 5	It must be kept in mind that sensitive data must not be held on the device and all data held on the device may be accessed and altered by unauthorized persons.
SC 6	Sensitive data (GPS tracking information, etc.) must be deleted on the device when the application is closed.
SC 7	Even if it is temporary, sensitive data must not be kept in places accessible by third party or applications.
SC 8	Sensitive data must not be stored on external storage areas such as on SD Card.
SC 9	If an application communicates with a backend server and keeps the data there, it must explicitly be approved by the user. Otherwise, privacy is violated.
SC 10	Without authentication control, access to the databases used in the application must not be allowed
SC 11	An application must be developed by considering the security requirements of the mobile application and different types of security tests must be done.
SC 12	Application logs must not contain critical data (e.g. username-password credentials, etc.).
SC 13	The data held on an application must be encrypted with strong encryption algorithms and must be transferred only over encrypted channels.
SC 14	Validity of the application certificates must be checked.

No	Security Controls
SC 15	HTTP Strict Transport Security (Strict-Transport-Security: max-age=15724800) must be included in all requests and access to the application over the insecure HTTP protocol must be blocked.
SC 16	An application must run only if the user explicitly declares that he or she has understood the risks of jailbroken or rooted devices.
SC 17	Server configurations must be configured securely, and all operating system, web server, and other application component patches must be up-to-date on time.
SC 18	The maximum number of requests that can come from a specific person / IP within a certain period of time must be limited against Denial of Service attacks.
SC 19	CAPTCHA must be used on authentication forms.

8. CONCLUSION

In this study, penetration tests of a commercial medical device using WBAN technology, mobile applications used for the device management and fifteen mobile health applications downloaded from official and non-official application stores were performed. The results of penetration tests were evaluated. As a result of these evaluations, security controls for WBAN layer, WBAN server layer and mobile health applications were listed.

We have evaluated WBAN and WBAN server layers. The Medical Server Layer in WBAN Architecture and Hospital Information Management System included in this layer should be in the future examined in another study in terms of the security features. Medical devices such as remotely managed insulin pumps, blood pressure monitors, heart pads, defibrillators are used in daily life. Such a study should be applied to all these devices in order to develop security features. Medical devices designed or developed according to these security requirements will enhance the quality of use by providing protection of personal health data.

REFERENCES

1. H. F. Rashvand, V. T. Salcedo, E. M. Sanchez, D. Iliescu, “Ubiquitous Wireless Telemedicine”, *Communications, IET*, 2(2), pp.237-254, 2008.
2. R. Bults, K. Wac, A. Van Halteren, D. Konstantas, V. Jones, I. Widya, “Body Area Networks for Ambulant Patient Monitoring Over Next Generation Public Wireless Networks”, **3rd IST Mobile and Wireless Communications Summit**, Lyon, France, 27/30, 27-30 June, 2004.
3. M. Li, W. Lou, K. Ren, “Data Security and Privacy in Wireless Body Area Networks”, *IEEE Wireless Communications, ISSN 1536-1284*, 17(1), pp.51-58, 2010, doi: 10.1109/MWC.2010.5416350.
4. IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks, *IEEE Std 802.15.6-2012*, pp.1-271, Feb. 29 2012, doi: 10.1109/IEEESTD.2012.6161600.
5. Internet: Microsoft STRIDE Threat Model, https://msdn.microsoft.com/library/ms954176.aspx, 19.04.2016.
6. Internet: D. Galpin, I. Lewis, Google I/O 2012 - Ten Things Game Developers Should Know, https://www.youtube.com/watch?v=WDDgoxvQsrQ, 13.12.2015.
7. A. Demir, **Vücut Alan Ağlarındaki Medikal Cihazların ve Mobil Sağlık Uygulamalarının Güvenlik Analizleri**, Master Thesis, Istanbul Şehir University, Graduate School of Natural and Applied Sciences, 2016.
8. C. s. Jang, D. G. Lee, J. w. Han, “A Proposal of Security Framework for Wireless Body Area Network”, **Security Technology, International Conference on’08**, Los Alamitos, CA, USA, pp. 202-205, December, 2008, doi: 10.1109/SecTech.2008.32.
9. O. Garcia-Morchon, T. Falck, T. Heer, K. Wehrle, "Security for Pervasive Medical Sensor Networks," **2009 6th Annual International Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous**, Toronto, ON, pp. 1-10, July, 2009, doi: 10.4108/ICST.MOBIQUITOUS2009.6832.
10. C. Li, A. Raghunathan and N. K. Jha, "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System," **2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO**, pp. 150-156, June, 2011, doi: 10.1109/HEALTH.2011.6026732.
11. W. Burleson, S. S. Clark, B. Ransford, K. Fu, "Design Challenges for Secure Implantable Medical Devices," **DAC Design Automation Conference 2012, San Francisco, CA**, pp. 12-17, June, 2012, doi: 10.1145/2228360.2228364.
12. D. Halperin et al., "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," **2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA**, pp. 129-142, May, 2008, doi: 10.1109/SP.2008.31.
13. L. C. Silva et al., “A Baseline Patient Model to Support Testing of Medical Cyber-Physical Systems”, **MedInfo, Studies in Health Technology and Informatics**, vol:216, Editor: Indra Neil Sarkar et al., IOS Press, pp. 549-553, 2015, doi: 10.3233/978-1-61499-564-7-549.
14. S. N. Ramli, R. Ahmad, M. F. Abdollah, E. Dutkiewicz, "A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)," **2013 15th International Conference on Advanced Communications Technology (ICACT)**, PyeongChang, pp. 998-1001, January, 2013.
15. S. N. Ramli, R. Ahmad, M. F. Abdollah, "Electrocardiogram (ECG) Signals as Biometrics in Securing Wireless Body Area Network," **8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)**, London, pp. 536-541, December, 2016,doi: 10.1109/ICITST.2013.675025

16. Internet: OWASP Mobile Security Testing Guide, https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
17. M. Ogul, S. Baktir and E. I. Tatli, "Abused Android Permissions by Advertising Networks," *IEEE International Conference on IT Convergence and Security (ICITCS), Beijing*, 2014, doi: 10.1109/ICITCS.2014.7021726.
18. Internet: Healthiply. Healthiply professionals, https://play.google.com/store/apps/details?id=com.health.doc, 2016.
19. Internet: KloudData Inc. mMR, https://play.google.com/store/apps/details?id=com.klouddata.mmr.main, 2016.
20. Internet: NFC MEDIC. Nfc medic, https://play.google.com/store/apps/details?id=com.gn4me.apps.NFCMedic2, 2016.
21. Internet: VitalHub Corp. Patient chart, https://play.google.com/store/apps/details?id=com.vitalhub.vitalchart, 2016.
22. Internet: Zibdy Inc. Zibdy health, https://play.google.com/store/apps/details?id=com.zibdy.VPB.client, 2016.
23. Internet: Tıpnet Yazılım. Yalova devlet hastanesi uygulaması, https://play.google.com/store/apps/details?id=com.yalovadh.monaca, 2016.
24. Internet: Diagnose Software Inc. Diagnose, https://play.google.com/store/apps/details?id=com.DiagnoseSoftware.diagnose, 2016.
25. Internet: Greenway Family Practice. Healty files, https://play.google.com/store/apps/details?id=com.healthfilesapp.mobileandroid, 2016.
26. Internet: Smart Medical Apps. Smart medical, https://apkpure.com/smart-medical-apps-h-p/com.smartmedicalapps.checklist, 2016.
27. Internet: AvvaStyle. Health records, https://apkpure.com/health-records/com.AvvaStyle.medcard, 2016.
28. Internet: Caddy. Medical & health records caddy, https://apkpure.com/medical-health-records-caddy/com.medicalcalculations, 2016.
29. Internet: Tanya White. My medical history, https://apkpure.com/my-medical-history/com.droidcasa.tanyawhite, 2016.
30. Internet: LLC WebMD. Webmd, https://apkpure.com/webmd-for-android/com.webmd.android, 2016.
31. Internet: LifeGuard Global Ltd. My medical history, https://apkpure.com/my-medical-history/com.pirolor.steven.medhitory, 2016.