Annual ADFSL Conference on Digital Forensics, Security and Law

2016
Proceedings

May 26th, 9:00 AM

WBAN Security Management in Healthcare Enterprise Environments

Karina Bahena
REU Student Fellow, Department of Biological Science, Morton College

Manghui Tu
Department of Computer Information Technology & Graphics, Purdue University Calumet

WBAN SECURITY MANAGEMENT IN HEALTHCARE ENTERPRISE ENVIRONMENTS

Karina Bahena[1], Manghui Tu[2]

[1]REU Student Fellow, Department of Biological Science, Morton College
[2]Department of Computer Information Technology & Graphics, Purdue University Calumet

ABSTRACT

As healthcare data are pushed online, consumers have raised big concerns on the breach of their personal information. Law and regulations have placed businesses and public organizations under obligations to take actions to prevent such data breaches. Various vulnerabilities have been identified in healthcare enterprise environments, in which the Wireless Body Area Networks (WBAN) remains to be a major vulnerability, which can be easily taken advantage of by determined adversaries. Thus, vulnerabilities of WBAN systems and the effective countermeasure mechanisms to secure WBAN are urgently needed. In this research, first, the architecture of WBAN system has been explored, and the vulnerabilities within the system have been identified and analyzed. After that, issues on existing federal regulations related to WBAN are discussed. Finally, scenarios are described where vulnerabilities, threats, and countermeasures are analyzed.

1. INTRODUCTION

The advances in Internet technologies, the proliferation of mobile devices, and the development of electronic healthcare records have driven healthcare services online, and are ubiquitous to provide convenience and flexibility to users and patients (Johnson & Willey, 2011; Tu, Spoa-Harty, and Xiao, 2015). Wireless communication has played a critical role in this process since it can provide anytime and anywhere access, and the WBAN (Wireless Body Area Network) has been integrated into the healthcare environment in the last two decades. WBAN has popular applications in military, law enforcement, fire departments, sports, and even hotels, due to its extensive flexibility to monitor vital signs such as blood pressure, glucose level, heart rate, and body motion. An essential part of WBAN is biomedical sensors, which are very lightweight and small devices can be implanted by a physician, or worn by the patients to monitor and send the patients' data to medical personal (Patel, Park, Bonato, Chan, & Rodgers, 2012).

However, due to the untrustworthy internet environment, and especially the wide adoption of wireless devices and technologies, as well as sophisticated healthcare service and business processes involved, healthcare sector faces severe challenges on securing protected healthcare information (El Emam et al., 2010; Ernst & Young, 2011; Halbesleben, Wakefield, and Wakefield, 2008; Johnson & Willey, 2011; Tu, Xu, Butler, & Schwartz, 2012, Tu et al, 2015; Wakefield & Wakefield, 2008). Over the past few years, millions of sensitive data records in healthcare and other private and

public sectors were exposed (Ernst & Young, 2011; Halbesleben, Wakefield, and Wakefield, 2008; Johnson & Willey, 2011; Ramzan, 2008; RSA SECURITY, 2008; Wakefield & Wakefield, 2008) and have resulted in substantial financial and operational loss, which greatly hurts the confidence of customers, business partners, and stakeholders (Ernst & Young, 2011; Hoffman, 2007, Johnson & Willey, 2011; Seltxer, 2006). The average total cost per data breach has risen to $7.2 million or $214 per record lost (Ernst & Young, 2011) and the estimated total cost of data breach in healthcare industry is 6 billion dollars annually (Johnson & Willey, 2011). According to RSA's (RSA Security LLC) annual Consumer Online Fraud Survey, consumers are concerned, more than ever before, about online private businesses and public organizations putting their data at risk (Hoffman, 2007). Meanwhile, over the last two decades, government and industry bodies around the world have issued many laws and regulations such as HIPAA 1996, to ensure the security, integrity, and confidentiality of healthcare records, business data, and healthcare IT infrastructures. These mandates have placed businesses and organizations in healthcare industry under obligations to undertaken programs to ensure the compliance with these laws and regulations; therefore, securing protected healthcare information and healthcare IT infrastructures, including the wireless network infrastructure such as WBANs, to prevent data loss including, data breach and industrial espionage, is critical.

However, a few challenges exist and need to be appropriately addressed. First, even though the general theory of vulnerabilities and threats of wireless networks may be well understood, the specific knowledge of WBAN system vulnerabilities and threats have been remained unclear due to the complexity of the WBAN system and the supported healthcare business processes. Second, even though system risk assessment methodology has been well documented, security risks of WBAN systems have not been formally studied due to the relative insufficient effort on WBAN systems.

The objective of this research is to conduct a systematic research on the security management of WBAN systems in healthcare enterprise environments. Specifically, a systematic analysis of WBAN system vulnerabilities and threats, risk assessment involving WBAN system security risks, and healthcare laws and regulations will be conducted.

2. SYSTEM MODEL

An abstraction of classical healthcare enterprise environment is modeled as a multi-tier system that consists of multiple data access or management parties, including a data module, service providers, business users, data management team, and client party. The overview of the system is shown in Fig. 1.

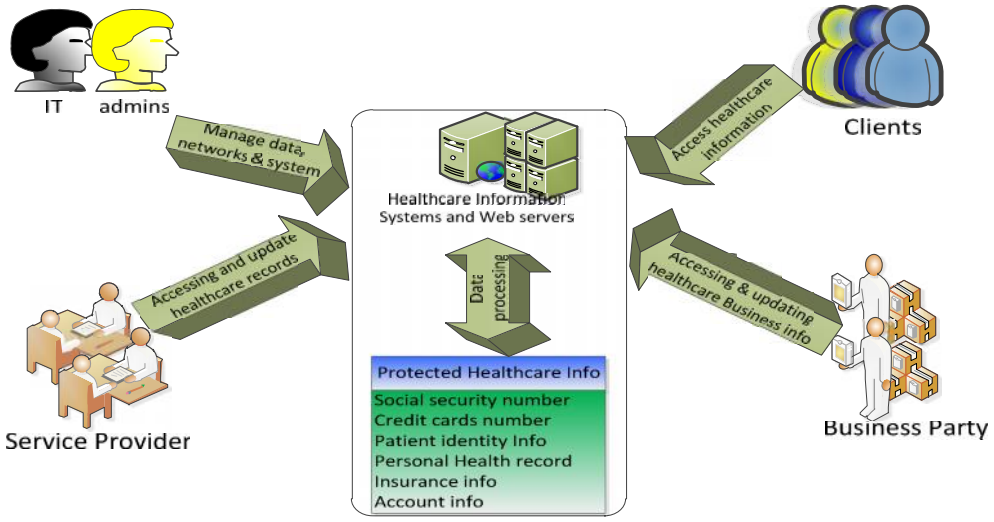

Figure 1. An architecture overview of the healthcare enterprise system.

The data module is a central and critical part of this architecture and is composed of a data storage system, a data process module, and a data access module. The data storage module is essentially databases and files that contain the information to be protected. The data process module is composed of a healthcare information system which processes the information stored in the data storage module for business clients, patients, government agencies, and healthcare service providers. The data access module is essentially web-based interfaces for users. The service provider party is composed of different services that are provided by the healthcare business, including hospital services, lab test services, health prevention care services, disease diagnosis and treatment services, nursing, etc. These services involve many human users such as doctors, technicians, and nurses. The business party is essentially the interactions between the healthcare business entity and other entities such as other healthcare service providers, government agencies, insurance companies, healthcare equipment/pharmacy providers. The data management party is fundamentally the IT teams including database/web/network/computer system administers, and the security/compliance team. The client party is basically the patients and their legal guardians.

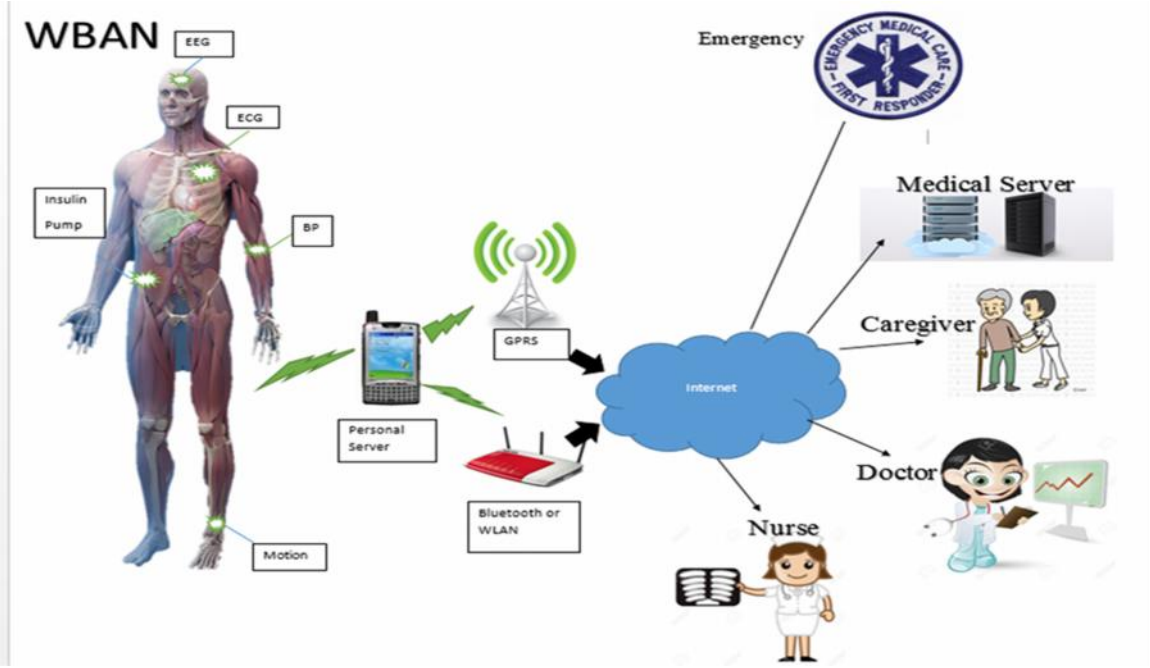

Figure 2. An architecture overview of the WBAN

A WBAN system is part of the healthcare IT infrastructure and is composed of three tiers. The first is composed of the nodes that will transmit patients' physiological data to the second tier. The second tier is mainly composed of a PS (Personal Server), which will communicate with body sensors in tier one through wireless personal network; either Bluetooth or WiFi. The PS will not, however, upload the gathered data until a secure link becomes available. The third tier is composed of the entities to whom the information should be distributed, such as the physician, nurses, emergency techs, the caregiver, and medical servers. A medical server stores electronic medical records for registered users to provide services for hundreds of users, including the informal caregivers, medical personnel, and patients. It is the personal obligation of the medical server to authenticate its users, accept of the uploads from health monitoring sessions, format and insert data retrieved from the sessions in the appropriate medical records, analyze of different data patterns, and have the ability to detect alarming health abnormalities to provide contact to urgent care givers within the area (Feng, 2008). The overview of the abstractive architecture of the WBAN system is illustrated in Fig. 2.

3. WBAN SECURITY VULNERABILITY ANALYSIS

Privacy and security are top concerns in healthcare environment. Data stored, transmitted, and processed in the healthcare system can be corrupted, manipulated, intercepted, and extracted. The loss of data, hacking, extraction of data, patient endangerment, and loss of money are just some of the risks of the WBAN. These risks, amongst others, can lead to future attacks if ignored. WBAN systems, similar to other forms of wireless networks, are more vulnerable to Denial of Service and eavesdropping

compared to wired networks. Such vulnerabilities can lead to serious safety concerns because of the significant risk of affecting overall performance, networks, transmission of data, amongst others (Hugher, Wang, & Chen, 2012). If the issues with the security of the networks and WBAN systems persist, it is in the hands of the provider to make sure that all of the information is confidential, available, and authentic.

3.1 WBAN Vulnerabilities & the Impacts on Confidentiality

Ensuring confidentiality of patient data stored, transmitted, and processed in WBANs are crucial to healthcare vendors to be compliant with laws and regulations such as HIPAA. However, threats and attacks to breach confidentiality of WBAN systems are common, due to the nature of the wireless communication in WBAN networks, the power and CPU constraint of WBAN nodes, the complexity of healthcare work flow, and non-technical end users.

An adversary with a powerful antenna can easily pick up data transmitted in the WBAN networks, which contain physical location of the patient, timestamps, source, and destination addresses (Kumar & Lee, 2012). Passive attacks are some of the most popular attacks taken place during the process of routing the data packets. The intruder can manipulate the final destination of the packets to enable the eavesdropping, and the data can be stolen through the wireless communication data and additionally pin-pointing the location of the user (Ameen, Liu, & Kwak, 2012). There have been plenty of cyber-attacks throughout the years; many with the hopes of compromising identities. If the attacks are active, then they are much more harmful. Like most cyber-attacks, the purpose is to steal identities for malicious activities. When medical records get involved, critical data is at risk of being fully exposed and takes things to another level. The healthcare providers and the patients will suffer from that extraction of data. It has been proven that a person with a low-costing device can easily eavesdrop and pick up on the data exchange of a pacemaker (Picazo-Sanchez, Tapiador, Peris-Lopez, & Suarez-Tangil, 2014, Kumar & Lee, 2012). The extraction of the patients' data will only worsen any scenario. Following the theft of the patient information, such information can precede into impacting their personal lives (Ameen, Liu, & Kwak, 2012).

3.2 WBAN Vulnerabilities & the Impacts on Integrity

The devices in a WBAN system can be compromised and the information can be altered or processed by an unauthorized attacker or in an unauthorized way (Picazo-Sanchez, Tapiador, Peris-Lopez, & Suarez-Tangil, 2014). An implantable cardioverter defibrillator may experience unauthorized alteration of information stored, transmitted, or processed, including patient personal information and health related data, as well as the setting of therapy for when and how shocks are administered. Such unauthorized alteration can lead to the production of cardiac arrest, or the reduction or increase of the amount of insulin pumped, which can cause the patient to die. The WBAN devices are also vulnerable from people with malicious intent and from natural causes such as wear and tear (Ameen, Liu, & Kwak, 2012). The system may malfunction, or processes flow may be changed to produce unexpected results, which may pose serious problems to the overall system operation. Thus, it is extremely important to design these devices to be tamper-proof.

3.3 WBAN Vulnerabilities & the Impacts on Availability

The availability of WBAN ensures that the WBAN networks, devices, data, and services

are always available to the authorized user in authorized way when it is needed. An adversary can break in a WBAN network and capture or disable the Electrocardiogram (ECG) node – which monitors electrical activity of a patient's heart. The loss of the monitoring data of a patient's heart behavior could result in the loss of the patient's life. A WBAN network can be physically jammed by injecting large amount of radio signals, or the data link frame headers can be corrupted which will lead to the discordance of the data being transmitted. Spoofing is one of the most common attacks against traffic routing. During the spoofing attack, the intruder is capable of causing complications within the networks by manipulating the system into creating new routing loops, and complicate overall process-forwarding. The flooding then begins and confuses the network into recognizing it as one of its own nodes; granting it access without being identified as being malicious, or exhausting the memory to prevent the normal WBAN communication (Saleem, Ullah, & Yoo, 2009). Moreover, a risk on the end of the patient is blockage of localization. Dependent upon the frequency that the wireless sensors can communicate, the human body itself is capable of causing blockage of all, or a select few of the wireless signal required for localization (Cornelius & Kotz, 2010). Such vulnerability can result in a conflict when the patient is in a life-or-death situation. These are just some of the examples of the risks regarding the WBAN. There are many other vulnerabilities that exist in WBAN systems, for example, some vulnerabilities can result in the loss of MRIs and X-ray images (Cornelius & Kotz, 2010).

4. WBAN SYSTEM RISK ANALYSIS

Safety precautions and regulations have been established to further protect all identities and information. Regulations have been well established for the WBAN since WBAN has been a popular technology for more than two decades. Regarding to WBAN, the US FDA (US Food and Drug Administration) has its share in the regulation process, but FCC (Federal Communications Commission) and HIPAA (Health Insurance Portability and Accountability Act) played the bigger role in regulating the WBAN and how it should secure the data storage, transmission, and processing. Any non-compliance of such regulations could lead to financial and reputational losses, and even lead to civil litigations.

4.1 FCC Regulations

Table 1
FCC regulations regarding WBANs.

WBANs should only be used for the specifically for diagnostics and therapeutic devotions
WBANs should be provided to the patients but should be only through the direction appropriately of a verified physician
WBANs are not allowed to provoke harmful interferences to other approved stations that operate within the band of 2360-2400 MHz.
WBAN needs to accept interferences from any additional certified stations who are operating under 2360-2400 MHz
All WBAN devices must be made available for inspection upon request by an authorized FCC representative.
As it is indicated in Part 95 rules, control or programmer WBAN transmitters need to be labeled with statements. These statements provide the warning that the device should not be the cause of interference and it has an obligation to accept interference from devices that are under the same operation WBAN programmer/control transmitters. The statement can be placed in the manual of the transmitter where it is not viable to placing the statements on the device itself.
WBAN controller/ programing transmitters need to be individually identified with the use of a serial number that will be assigned by the manufacture of the specific device. The corresponding serial number can be place on the device itself or place in the instructional manual of the transmitter.
(Federal Communications Commission, 2014).

The FCC has concluded in their 2014 report that the "FCC will initially adopt a 'permit but ask' policy that is typically associated with new technology, where devices are required to be tested and approved directly by the FCC test lab, which can be applied to devices in WBAN systems. In addition to the FCC approval, WBAN devices will also need to receive FDA approval before they can be used in hospitals" (Buckiewicz, 2015). These regulations mainly deal with the technical aspects of WBAN technology, such as device certification, signal transmission, and interferences. The availability assurance and user access control falls in the scope of cybersecurity. The WBAN restrictions and compliances in accordance to the FCC is shown in the following as Table 1.

4.2 HIPAA

In healthcare sector, one of the most important regulatory criterion is HIPAA (Health Insurance Portability and Accountability), which was introduced in the year 1996. HIPAA has established criterial and regulations on how healthcare information should be handled such that availability, integrity, and confidentiality can be assured. Covered entities must put into place critical protections for the ability to protect every person's healthcare information, while also assuring that they don't disclose or misuse people's health information. Also, these same entities must train employees to protect the information- all while rationally limiting disclosure and use down to a minimum necessity for accomplishment of intended purposes (Federal Communications Commission, 2013). The patients may also be held accountable if they sign disclosure agreements. Business Associates (including IT personal and anyone with medical field relations) additionally, are required to establish safeguards to shield health information and assurance of not disclosing healthcare

information improperly (U.S. Department of Health & Human Services, n.d.); however, even a covered entity is capable of disclosing health information that is supposed to be protected for treatment (or other activities) when another provider needs data to proceed with procedures, which includes providers who are not covered through the Privacy Rule (U.S. Department of Health & Human Services, 2003). Failure to follow HIPAA regulations to protect patient information could lead to a financial penalty of 11,000 dollars, per violation, per patient. In addition, in regards to the security, since the establishment of HIPAA, over 29 million records have been wrongfully disclosed.

Table 2
Crucial WBAN security requirements, as been described in ((Li, Lou, & Ren, 2010)).

Critical Security Requirements	Description
Data Access	
Access Control	A well-constructed data access policy will have to be enforced in order to prevent any unauthorized parties from having the possibility of accessing any of the patient data the WBAN generates.
Accountability	A user who abuses the privilege to discharge any unauthorized acts regarding patient data needs to be identified and be held liable for their actions
Non-repudiation	Sources that generate patient related data can't deny their origin
Revocability	Privileges pertaining to WBAN user nodes ought to be deprived soon enough if found guilty of malicious behavior or involved in compromising of data.
Data Storage	
Confidentiality	All data in relation to the patient must remain confidential throughout periods of storage.
Dependability	The patient data must be willingly retrievable during data erasure or during node failure.
Dynamical Integrity Assurance	Throughout periods of storage, any patient related data may not be tempered with. During the storage periods the data will be reviewed and can be identified
Other Important Requirements	
Authentication	The appointed patient related sender needs to be authenticated any addition of data outside the WBAN needs to be prohibited.
Availability	Patient data needs to be accessible at all times even when it is under DoS attacks.

All the measures and regulations are established in hopes of further protection and minimization of confiscation. The Officer for Civil Rights on behalf of the HHS has stated

"We hope the healthcare industry will take a close look at this agreement and recognize that OCR (US Office for Civil Right) is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information" (Wisniewski, 2011). Super-confidential medical records containing drug and alcohol, mental health, and HIV information are subject to more stringent federal and state laws under HIPAA. As a result, physician practices must determine if medical records contain super-confidential information before releasing them. Generally, a physician practice can release these super-confidential records only upon a court order or upon receipt of a HIPAA Authorization signed by the patient which explicitly acknowledges the records which contain drug and alcohol or mental health record information (Medical Records, n.d.).

Data security systems pertaining to HIPAA are usually installed on computer systems and networks of healthcare providers; this also includes firewalls to further prevent any wrongful access, and electronically-inspecting systems are also used for individual identification, logging, and specifying all records each individual can access (Medical Records, n.d.). Additionally, transmitters in the WBANs have to be certified by the FCC or the Telecommunications Certification Body. The certification processes consists of submission of a certification application followed by measurement reports demonstrating compliance with FCC technical requirements, or Telecommunications Certification Body (Federal Communications Commission, 2013). Moreover, more key security requirements are included in HIPAA and a partial list of such regulations are listed in Table 2, which has been described in the works by Li, Lou, and Ren (2010).

5. WBAN SECURITY SCENARIO ANALYSIS

In this section, we will mainly describe three generic healthcare workflow scenarios to illustrate the potential security risks related to the WBAN systems.

5.1 Scenario One

Let us assume that a patient Luna, who has a life threatening heart disease and is currently out of the US has a pacemaker, and notices a change in cardiac rhythm which usually indicates a danger to the patient with such a disease. This is where the WBAN plays its important role for communication between patient and healthcare provider in a healthcare application. In this scenario (shown in Fig. 3), the first response unit will identify Luna's tag in order to obtain her medical records and existing information in the medical database. Next, her vital signs will become available to access for healthcare professionals, which can speed up and enhance the treatment. With this information now stored in the system, it will instantly become accessible to anyone to intervene and help. An intern, per se, has been left in charge of monitoring all alarming notifications for WBANs. The intern is now able to upload a report from her WBAN to the personal device that is transmitting the signal in her area. Configurations are then made to her network in order to configure who will be able to have access to her WBAN. An adaptation will soon take place and allow several others to be able to operate her device and access all her medical information.

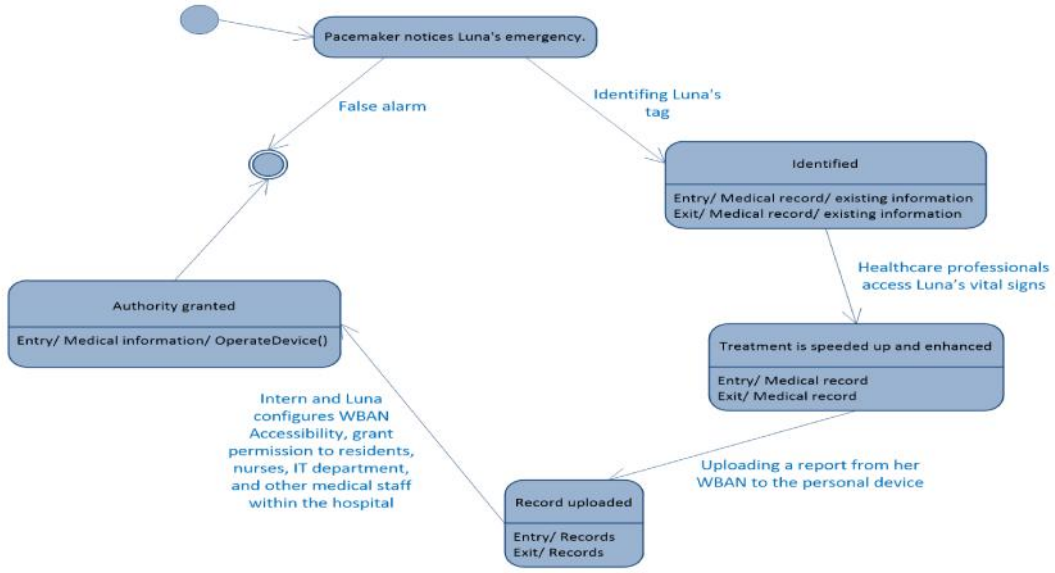

Figure 3. Overview of WBAN workflow including sensitive information in Scenario One

People who have access include: interns, residents, nurses, IT department, and other medical staff within the hospital. Luna herself can also change her access policy and manage who gains access to sensitive information. For example, only a doctor could be able to see drug abuse history and HIV history, where a nurse may not have access to this sensitive information. What is actually stored as medical data is dependent on the nodes and their storage capacity. The original data and the update can be transferred to a wireless network in the hospital; however, the data will not be uploaded until a secure link is provided. Luna's WBAN and the local wireless server will allow access to updated data to be accessed rapidly and on-the-spot to help assist her better.

The problem now is how to guarantee that the information stored on nodes is not accessed or modified by an unauthorized user and/or in an unauthorized way. An adversary can take advantage of various vulnerabilities in the system to compromise a less secured node, and can then manipulate the information in transition within the WBAN system. This could lead to the genuine information unreachable to the medical staff, or the pacemaker not to function as expected. Therefore, all this information, as well as her insurance and medical records, should all be encrypted for storage and it is important to keep this network as safe as possible.

5.2 Scenario Two

Activity and mobility of a patient should be monitored and the results should be evaluated and accessed in time, especially for those cases that patient actions can lead to the risk of falling. A sample scenario is illustrated in Fig. 4. In such a scenario, the communication between patient and healthcare providers through a wearable 3-axis accelerometer is observed and data is analyzed offline since no immediate action is required (Büsching, Bottazzi, Pöttner, & Wolf, 2013). In this case, it is desirable to acquire a dataset completed without missing key data pertaining to the overall length of the monitoring session. However, radio transmission will not be

possible if the patient leaves their home, since the data will surpass the communication range and become lost (Büsching, Bottazzi, Pöttner, & Wolf, 2013). If the data gets lost or corrupted and the patient suffers from a crisis, the provider might not be become aware.

However, in real world, wireless communication could suffer from malicious attacks or unintentional interferences, which could lead to denial of services and the compromise data integrity. Without appropriate protection, such attacks or interferences could lead to the risk of loss of life and health degradation for patients, and in turn could result in financial loss and civil litigation for service providers.

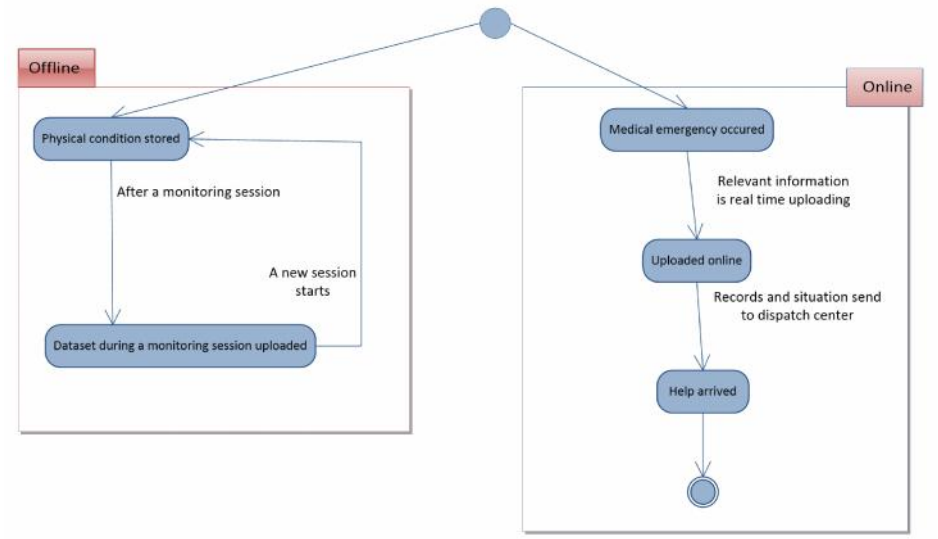

Figure 4. Offline and online monitoring

5.3 Scenario Three

It is always advised to ensure separate network access control for volunteers, patients, healthcare professionals, staffs, network administrators, and other users. Strong password and username combinations for user authentication and accountability should be enforced. In a typical hospital environment, as illustrated in Scenario Three (as shown in Fig. 5), an open network is provided for patients and guests to entertain themselves and relax while they wait for assistance. A volunteer should have a different access than an intern, physician, and a resident. A normal person waiting for assistance should not be able to connect to the same network as a physician. Open networks, as stated before, are perhaps one of the most obvious, but neglected vulnerabilities.

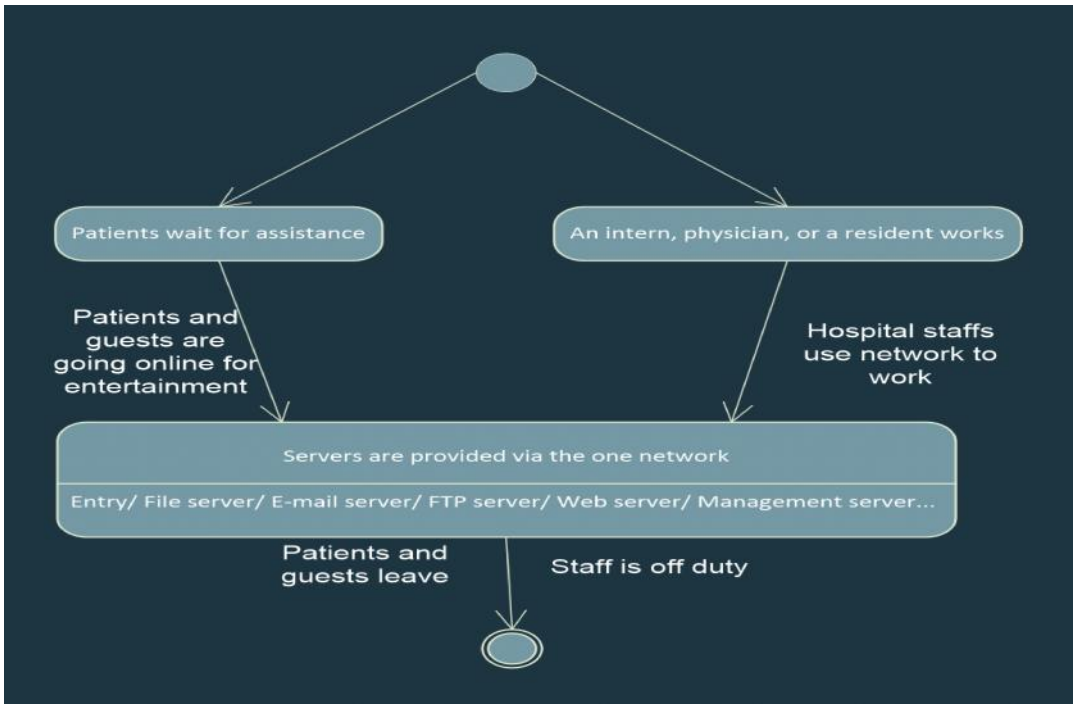

Figure 5. Guest connecting to open and shared network gaining access to sensitive information.

Even though such wireless network is not part of WBAN systems, it could lead to a data breach or other risks to WBAN systems. The wireless network is vulnerable to various attacks, and users of wireless networks could be also the same users using WBAN systems. The compromise of the wireless network could lead to the compromise of the WBAN system and lead to the data breach and unauthorized alteration in WBANs.

5.4 Discussion on Potential Solutions

When encountering a disrupting a situation or event, not every situation has a fundamental solution that can be pinpointed easily. Just like medical decisions, wireless security solutions should be proposed confidentially and not impulsively. As wireless communications continue to expand daily, the struggle to keep up with the security arises; the solutions that are proposed to help the WBAN security varies. The critical data that is encrypted is to be used only for medical purpose, but once in the wrong hands it can be fatal, and lead to a costly loss on the practitioners' side. One of the proposed solutions for which security has not been fully explored, and not quite understood, is body-coupled communication. A proposed requirement is extent proof that the data comes from only one monitored body. The reason being that some doctors may rely on data collected from the WBAN for procedures. It is critical to have assurance that the data being analyzed is specifically collected from that patient (Cornelius & Kotz, 2010). Since the eavesdropper can access the personal area network of the patients, it is proposed and encouraged to encrypt the data with a secretive private key which will only be shared in a channel of secure communications that will consist specifically between receiver and the sender (Dr. Rangaraj, 2011). This appointed key will have the capability to decrypt and encrypt. In order to further prevent future flooding attacks, and the hacker

falsifying information, all of the messages should be required to be authenticated. The authentication process would be able to help prevent many incidents on all ends of a WBAN. It can be viewed as going onto a site, clicking "claim your prize," entering your personal information, being scammed, and resulting with a virus. However, with an appropriate anti-virus software installed, the detection would be immediate and block the transmission of data. Also, the wireless networks used by medical professionals should be restricted to certain group of users and not made accessible to guests. However, this can be a critical flaw in which that most places are partaking and no appropriate access control nor security protection in place. Currently, the most popular proposal to enhance the safety of WBANs is a cloud -based frame.

6. CONCLUSION

The healthcare field is now moving forward and adapting the wireless to take full advantage of the rapid advancement of technology. The WBAN has been around for over two decades and has been very popular in the healthcare environment. Due to the sensitivity of the information stored, transmitted, and processed, security and privacy have been the top concern; however, the system is fundamentally flawed in security and needs improvement as discussed in this paper. Action to harden and secure the WBAN system is therefore critically needed.

In this paper, we focus on addressing the security management of WBAN systems in healthcare enterprise environments. First, a logic view of a typical healthcare enterprise environment and WBAN system has been described. WBAN security vulnerabilities were discussed and identified. Second, the risks of information security and privacy were assessed and WBAN related regulations and standards, e.g., FCC and HIPAA, have been discussed in detail. Finally, healthcare scenarios involving WBAN system have been illustrated to discuss security vulnerabilities, risks, and corresponding countermeasures.

The following research topics will be further investigated in the future. First, a comprehensive modeling should be developed based on field experiences on a real world healthcare enterprise environment with WBAN system. Vulnerability identification, attacks/threats enumeration, and financial and regulatory risk analysis will be systematic studied. A modeled enterprise healthcare cyber-infrastructure design with appropriate security and privacy controls will be developed.

ACKNOWLEDGEMENT

This research was support in partial by NSF-REU Program (CNS1461296).

REFERENCES

Ameen, M. A., Liu, J., & Kwak, K. (2012). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of Medical Systems, 93-101.

Buckiewicz, B. (2015). Overview of Medical Body Area Networks. Retrieved from LSR: http://www.lsr.com/white-papers/overview-of-medical-body-area-networks

Büsching, F., Bottazzi, M., Pöttner, W.-B., & Wolf, L. (2013). DT-WBAN: Disruption Tolerant Wireless Body Area Networks in Healthcare Applications. 1st International Workshop on e-Health Pervasive Wireless Applications and Services (eHPWAS'13), (pp. 197-203).

Cornelius, C., & Kotz, D. (2010, August). On Usable Authentication for Wireless Body Area Networks. Retrieved from Darthmouth.edu: http://www.ists.dartmouth.edu/library/471.pdf

Dr. Rangaraj, G. V. (2011, April 17). Tutorial on Wirless Security of medical devices By Dr G V Rangaraj. Retrieved from Slideshare: http://www.slideshare.net/gvrangaraj/tutorial-on-wirless-security-in-medical-devices-icrtit2011

Federal Communications Commission. (2013, May 13). Medical Body Area Networks. Retrieved from Federal Communications Commission: https://www.fcc.gov/document/medical-body-area-networks

Federal Communications Commission. (2014). Small Entity Compliance Guide Medical Body Area Networks. Washington, D.C.: Federal Communications Commission.

Feng, D. D. (2008). Biomedical information technology. Amsterdam: Elsevier/Academic Press.

Hugher, L., Wang, X., & Chen, T. (2012). A Review of Protocol Implementations and Energy Efficient CrossLayer. Sensors.

Kumar, P., & Lee, H. (2012). Security Issues in Healthcare Applications Using Wireless Medical SEnsor Networks: A Survey. Sensors, 55-91.

Li, M., Lou, M., & Ren, K. (2010). Data Security and Privacy in Wireless Body Area Networks. IEEE Wireless Communications, 51-58.

Medical Records. (n.d.). HIPAA Compliance for EMR / EHR Systems. Retrieved from Medical Records: http://www.medicalrecords.com/physicians/compliance

Medical Records. (n.d.). HIPAA Requirements. Retrieved from Medical Records: http://www.medicalrecords.com/physicians/hipaa-and-medical-records

Picazo-Sanchez, P., Tapiador, J. E., Peris-Lopez, P., & Suarez-Tangil, G. (2014). Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks. Sensors.

Saleem, S., Ullah, S., & Yoo, H. S. (2009). On the Security Issues in Wireless Body Area Networks. International Journal of Digital

Content Technology and Its Applications, 179-184. Retrieved from Academia.edu.

Toorani, M. (n.d.). On Vulnerabiliites of the Security Association in the IEEE 802.15.6 Standard. Retrieved from http://fc15.ifca.ai/preproceedings/wearable/paper_1.pdf

U.S. Department of Health & Human Services. (2003, April 3). Health Information Privacy. Retrieved from U.S. Department of Health & Human Services: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html

U.S. Department of Health & Human Services. (n.d.). Guidance Materials for Consumers. Retrieved from U.S. Department of Health & Human Services: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/

Wisniewski, C. (2011, February 25). Retrieved from Naked Security: https://nakedsecurity.sophos.com/2011/02/25/hipaa-fines-prove-the-value-of-data-protection/

