Security of Mobile Health (mHealth) Systems

Fatma Zubaydi, Ayat Saleh, Fadi Aloul, Assim Sagahyroon
Department of Computer Science & Engineering
American University of Sharjah, UAE
{g00056871, g00060689, faloul, asagahyroon}@aus.edu

Abstract - **mHealth is a growing field that enables individuals to monitor their health status and facilitates the sharing of medical records with physicians and between hospitals anytime and anywhere. Unfortunately, smartphones and mHealth applications are still vulnerable to a wide range of security threats due to their portability and weaknesses in management and design. Nevertheless, mHealth users are becoming more aware of the security and privacy issues related to their personal healthcare information. This survey discusses the security and privacy issues in current mHealth systems and their impact. We also discuss the latest threats, attacks and proposed countermeasures that could support secure sensitive mHealth systems. Finally, we conclude with a brief summary of open security problems that still need to be addressed in the mHealth field.**

Keywords — **mHealth, mobile health, cyber security, healthcare applications, mobile applications.**

I. INTRODUCTION

Mobile health (mHealth) is a recent technology innovation in which mobile devices are utilized to support medicine and public health practices. Ideally mHealth-based services should allow patients and healthcare professionals to easily access their medical data anytime and anywhere. Also, patients may easily manage their health needs at home and accordingly the number of visits to hospitals and the cost of healthcare are reduced. Moreover, physicians can remotely monitor their patient's health and give advice with no need for physical meeting with their patients. Today, monitoring mobile devices that were previously only available at hospitals have reached the hands of patients who are using them to a monitor, manage and communicate from home.

Smart phones are considered attractive platforms for healthcare practices due to several features 1) pervasiveness, 2) computational capabilities, 3) user-friendly interface, 4) built-in sensors, 5) availability, 6) mobility, and 7) connectivity. By 2019, it is estimated that there will be nearly 1.5 mobile devices per capita according to Cisco Visual Networking Index [1]. mHealth aims to make healthcare accessible and cheap for everyone especially in urban regions by making use of this remarkable smart phones penetration. Research2guidance [2] reported that there were more than 97,000 mHealth applications listed on 62 full catalogue app stores in 2013. The majority of these applications are general health and fitness apps that provide individuals with basic health and fitness related information, and sometimes it could be guidance. Moreover, they reported that by the end of 2017, the total mHealth market revenue will grow by 61% to reach US$26 billion.

Many healthcare organizations are expressing interest in mHealth and conducting studies on the effective role, limitations and future of mHealth as the World Health Organization (WHO) did in one of their recent publication [3]. According to WHO reports, mHealth seem to have more impact and shows more promising results in middle or low income countries. For example, Bangladesh worked on raising health awareness among its residents using SMS campaigns. One of these campaigns targeted pregnant women in remote villages by allowing them to register their mobile numbers to receive useful prenatal advice that is appropriate to their gestation stage.

This campaign was a part of a group of campaigns in Bangladesh that achieved a decrease in maternal deaths from 322 per 100,000 in 2001 to 194 in 2010, a 40 percent decline in 9 years according to USAID report [4]. The Ministry of Health and Family Welfare of Bangladesh achieved this result by simply taking the advantage of the rapidly increasing number of mobile telephone subscribers in the country to improve the health of its citizens and overcome existing communication barriers.

Nevertheless, recent research have drawn attention to the fact that smart phones are vulnerable to a wide range of security threats, and they are becoming target of malware authors and several types of security attacks due to weakness in management and design. The majority of security concerns come from the fact that smart phone devices could run different applications which can have full access to the data on the phone and communicate with other apps on the phone in addition to external entities. An mHealth application must ensure that data will not flow internally to untrusted applications or externally to untrusted hosts. Unfortunately, at present, mHealth apps are outside the bonds of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [5].

In this survey, we discuss security and privacy issues of mHealth systems. In Section II, we present the security requirements for safe mHealth applications. Section III lists possible threats that have to be considered in the mHealth field. Section IV, discusses the nature of some attacks and effective countermeasures. The paper is concluded in Section V.

II. mHealth Security Requirements

The HIPAA security rule, which became effective on April 2005, enforces administrative, physical, and technical safeguards to ensure *confidentiality, integrity* and *availability* of electronic health care information that is stored or transferred electrically [5]. *Confidentiality* requires assurance that electronic personal health information is not made available or disclosed to unauthorized parties. *Integrity* requires assurance that electronic personal health information has not been modified or destroyed without authorization. Finally, *Availability* means the usability and accessibility of electronic personal health information by an authorized party at anytime from anywhere. As we indicated previously, mHealth is still not restricted by HIPAA, but developers can benefit from HIPAA security rule standards to achieve higher security level of mHealth applications.

Recently, the increasing awareness by mHealth users toward the security of their personal healthcare information motivated researchers to conduct studies that reflect on the current situation of mHealth security levels and outline security requirements for mHealth systems [6-9]. Typical security requirements of mHealth systems should include the following:

- *Confidentiality*: Health data should be confidential and available only to authorized physicians in addition to the original user. Confidentiality violation could cause damage to the patient, since the attacker could use the eavesdropped health data in illegal activities. Therefore, this requirement is essential for any mHealth system.
- *Integrity*: mHealth system needs effective mechanisms to secure stored data, verify that data hasn't been altered by unauthorized party and verify that data were sent by a trusted party.
- *Audit Control*: mHealth system needs to record and examine the activities of the system.
- *Effective User Authentication*: mHealth system needs to verify that patient or physician has the identity he claims before accessing any sensitive health information.
- *Access Control*: Access to patient's health data could be requested by many users such as nurses, physicians, insurance companies, medical centers, etc. Therefore, effective and accurate access control mechanisms are required to restrict access to personal health care information.
- *Data availability*: Health data should be available to the patient and responsible entities such as physicians at any time and from anywhere.
- *Freshness of Health Data*: mHealth system is very sensitive to time and depends on recent and accurate health data. Therefore, freshness of physiological data and healthcare data is essential. Otherwise, mHealth system functionality could affect the patient negatively.
- *Patient Consent*: A patient's permission is critically needed in mHealth systems whenever sharing of data with external entities is required.

The aforementioned security requirements are paramount for any mHealth system. In order to achieve these requirements, mHealth developers should take these aspects into consideration while designing the system, they can achieve these requirements by following specific mechanisms. Recent study [6] suggested controlling remote communication, preventing data sharing with other applications, protecting insecure data storage and detecting user consent steps to achieve the needed security requirements.

Several important traditional methods and concepts for ensuring security within the mHealth context do exist. First, having a good encryption algorithm for handling sensitive information such as Advanced Encryption Standard (AES). Second, using public key cryptography for exchanging the encryption key such as Elliptic Curve Cryptography (ECC). ECC is known to be an *efficient* public key cryptography system that is suitable for mobile devices. Third, having a multi-level authentication system that grants specific access privileges to users based on their identity or type.

III. mHealth Security Threats

Electronic health information stored on mobile devices is vulnerable to a wide range of security threats which include:

- *Malware Infections*: Malicious software may exploit vulnerability in an application or use social engineering techniques to trick the user and install itself on a mobile device. The installed malicious software on the device could obtain stored sensitive health information, damage it, alter it, or send it to an untrusted entity.
- *Application Developers*: In case they don't take appropriate mechanisms to ensure data security, vulnerabilities can exist in a poorly implemented application which opens the doors for hackers to take advantage of.
- *Mobile Devices*: Devices are vulnerable to unauthorized usage or physical theft in case they left unintended, which could lead to the disclosure of health information or lack of availability of medical application services.
- *Human Users*: In case they share the passwords of their devices with others, an unauthorized user can consequently get access to the phone. People use their own smart phone for work, at the same time at house or café for personal reasons. A recent study [10] reported that about 41 percent of those who use smart phones in the health sector have no password protection on their phones. Furthermore, 53 percent admitted they have used unknown networks with their devices. Another scenario involves the user emailing

personal health information to a wrong recipient rather than the correct one, leading to the revealing of personal health information to unauthorized recipients.

- *Health Insurance Companies*: Such companies may seek to gain advantage by learning health information which is not normally part of their review procedures [11].
- *Data Intelligence Companies*: Such companies accumulate and sell demographic information about individuals and their health conditions [11].

IV. mHealth Security Attacks and Countermeasures

mHealth applications are vulnerable to a wide range of security attacks [6, 10, 12-15], which may include the following:

- *Eavesdropping on unencrypted internet*: mHealth applications may send information over internet without encryption, therefore an intruder can eavesdrop and capture a message which contains personal health information. Additionally, an intruder can discover the fact that an individual might be using a specific health monitoring application and accordingly the intruder can guess that individual is suffering from a specific disease, this case could happen in case the sender's and receiver's details are not encrypted while the health records itself are encrypted.
- *Eavesdropping on logged sensitive health information*: poorly implemented mHealth applications may put sensitive user information into unsecured locations such as server logs, mobile application logs, browser history. This action could lead to personal information leakage.
- *Eavesdropping on unencrypted SD card storage*: mHealth applications may store unencrypted data files, e.g. audio files from a sleep monitoring application, on an external storage like an SD card. The SD card might be later accessed by unauthorized users.
- *Tampering with personal health data*: An intruder may alter the personal health data that is recorded or reported by an mHealth application.
- *Third party attacks*: mHealth applications may use or communicate with a third party, e.g. hosting services, social media and web servers and share private information. This could lead to possible violations of the privacy requirements.
- *Bluetooth attacks*: mHealth applications may communicate with external devices like health sensors via Bluetooth. An attack called external device *misbonding* (DMB) [16] exists for Bluetooth-enabled Android devices, which can allow an external device to steal private data or inject fake data into the original application.
- *Application owner attacks*: Some application owners may keep records of who has downloaded their applications and hence reveal the user's medical conditions. Also, application owners may publish user ratings which accordingly can reveal who is using the application.
- *Fake mHealth applications*: A fake mHealth application may aim to collect personal health information from individuals.
- *Security concerns while developing the mHealth applications*: Developers may insert trackers into application to observe user behavior which can also lead to private data leakage.
- *An intruder with physical access to smartphone*: An intruder with physical access to the smartphone may be able to extract SD card and access unprotected data or delete the application or damage the phone and hence impact the availability requirement.
- *Smartphone owner mistakes:* The owner of the smartphone may wittingly or unwittingly release data.
- *Fake user consent*: A malware may exist on a mobile device that is capable of executing scripted actions on the mobile as though the user generated a response [6]. Usually, user consent is required when data may flow to untrusted application; a malware may take a role and generate response instead of authorized user.
- *Denial of Service* (DoS) attacks: Health monitoring applications usually need to be continuously on. Attackers can flood the network to stop the communication between the application and external servers.

We notice that the sources of the above security threats and issues may be the smartphone, smartphone's user, mHealth application developer or malware infections. In order to build secure mHealth systems, it is critical that we take security into consideration while designing the system and at all levels. Researchers have recommended security mechanisms and proposed secure mHealth systems to overcome the addressed issues.

Elkhodr et al. [17] proposed a trust negotiation approach to ensure the privacy of personally sensitive information and secure Electronic Health Records (EHRs) during the transmission in remote monitoring systems. The suggested approach is based on Ubiquitous Health Trust Protocol UHTP and runs on Android operating system, it contains three levels of authentications: the authentication of health care professional, the authentication of device in use and the authentication of the environment of access. When a client wants to communicate with the server he must first authenticate his mobile using the following six factors: user name, password, serial number of patient's SIM card, international Mobile Equipment Identity (IMIE), longitude and latitude. The patient is allowed to communicate with the system if he is only in an allowed location.

Y. Choh et al. [18] proposed the design and implementation of a cross-platform mobile activity monitoring system on the cloud. The suggested system incorporates HTTP 2.0 with SPDY to enable fast and secure medical information push by server to individual users. The system consists of four parts: mobile, SPDY server, database for storing information, and MATLAB to analyze user's data. SPDY is an experimental open networking protocol developed by Google, it aims to reduce the amount of latency involved in loading web content using header compression, multiplexing and prioritized requests. Moreover, it uses multiple client certificates within the same SPDY session. By using this feature, after using MATLAB for analysis, the server can send notifications or events to clients, without the need to open application.

Pfeifer et al. [19] introduced a new approach called reverse cloud approach. The new suggested approach allows the transfer for the applications to the mobile instead of sending data to be processed on the cloud. This ensures that the data never leaves the mobile phone and hence is more secure. The Hybrid cloud architecture is currently evaluated in seven European hospitals called "Fi-star". Also, this concept can be applied in other sensitive areas like electronic government, defense industry, and law enforcement.

Naveed et al. [16] recommended applying encryption to the personal medical data stored on mobile devices and using TLS/SLL through the internet transmission session regardless that network transmission is encrypted or not.

Tan et al. [7] suggested recommendations to enhance the security of emerging remote obstetrics monitoring systems. They suggested the following three recommendations to enhance emerging monitoring systems to better meet HIPAA Security Rule requirements:

1. *Restrict smartphone capabilities:* Smartphones are incorporated into emerging monitoring systems due to their computing capabilities. On the other hand, their computing capabilities and flexibility increases the risk of possible vulnerabilities being introduced to the mobile due to user activities, such as installing malicious applications. Therefore, restricting the smartphone capabilities by removing unnecessary applications and preventing the user from installing new applications will help reduce the risk of a compromised smartphone.
2. *Perform both user and device authentication:* User and device authentication are both necessary to provide integrity protections. Ideally, all components in the system should be authenticated. However, only the smartphone in this system is a general purpose computing device where the user can install additional programs. This action makes the smartphone more vulnerable than other components existing in this system. Therefore, the system needs to authenticate the smartphone before allowing the health data to be stored into the server.
3. *Better Feedback:* Improvement of the user feedback process in the data transfer process and the data collection process.

In summary, mHealth systems are suffering from major security issues which affect all entities of system such as patient and physician with varying degrees. Sources that lead to the previously discussed security issues are: connectivity and mobility of smartphones, poor design of mHealth systems, weak use of passwords, plain text storage and transmission of data, lack of standards and infrastructures for mHealth systems security, and lack of supervision on mHealth applications. Therefore, effective steps should be taken towards overcoming the existing security issues in mHealth systems.

V. Conclusion and Recommendations

mHealth systems have the potential to replace some traditional healthcare services and practices and lower the cost of providing healthcare by taking advantage of the mobility, computing and sensing capabilities of smartphones and other handheld devices. However, this also comes with additional security risks that are absent from traditional healthcare approaches. In this survey, we discussed the security issues in mHealth systems. Specifically, we discussed the latest possible threats, attacks and countermeasures in mHealth systems. Security requirements for the development and use of safe mHealth applications were also presented. It has been shown that several aspects should be taken into consideration in order to improve the quality and practicality of mHealth systems. First, security standards should be enforced to ensure security of mHealth systems. Second, guidelines for effective building and testing of secure mHealth systems are required to help developers overcome security concerns that result from poor design. Third, mHealth applications on different app stores need supervision to evaluate their legality and authenticity. Finally, users must be aware of the security concerns and the steps needed for safe use of such mHealth applications. Many security issues in mHealth systems still need to be explored more, and we hope that this survey will motivate researchers and healthcare organizations to come up with more effective mechanisms for future mHealth systems.

References

[1] "Global Mobile Data Traffic Forecast Update 2014–2019," *Cisco Visual Networking Index, White Paper*, February 2015.

[2] "Mobile Health Market Report 2013-2017," *research2guidance*, 2013.

[3] World Health Organization, "mHealth - New horizons for health through mobile technologies," *Global Observatory for eHealth series*, vol. 3, 2011.

[4] "Bangladesh: Maternal Deaths Decline by 40 Percent in Less Than 10 Years," *USAID's Global Health Bureau*, March 2011.

[5] B. Pieper, "An Overview of the HIPAA Security Rule," *Journal of the American Optometric Association,* 75(11), 728-730, 2004.

[6] M. Ahmed and M. Ahamad, “Protecting Health Information on Mobile Devices," in *Proc. of the second ACM Conference on Data and Application Security and Privacy*, 229-240, February 2012.

[7] C. Tan, L. Bai, D. Mastrogiannis and J. Wu, “Security Analysis of Emerging Remote Obstetrics Monitoring Systems,” in *Proc. of the IEEE Int’l Conference on e-Health Networking, Applications and Services (Healthcom)*, 329-334, October 2012.

[8] P. Sahoo, “Efficient Security Mechanisms for mHealth Applications Using Wireless Body Sensor Networks,” *Sensors,* 12(9), 12606-12633, September 2012.

[9] D. Luxton, R. Kayl, and M. Mishkind, “mHealth Data Security: The Need for HIPAA-Compliant Standardization,” *Telemedicine and e-Health Journal,*18(4), 284-288, May 2012.

[10] Cisco mConcierge, “BYOD Insights: A Cisco Partner Network Study,” March 2013.

[11] K. Knorr and D. Aspinall, “Security Testing for Android mHealth Apps,” in Proc. *of the IEEE Int’l Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, Graz, Austria, 1-8, 2015.

[12] N. Deursen, W. Buchanan and A. Duff, “Monitoring information security risks within health care,” *Computers & Security,* vol. 37, 31-45, September 2013.

[13] D. He, M. Naveed, C. Gunter and K. Nahrstedt, “Security Concerns in Android mHealth Apps,” in *American Medical Informatics Association (AMIA) Annual Symposium*, November 2014.

[14] D. Kotz, “A threat taxonomy for mHealth privacy,” in *Proc. of the Int’l Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, 1-6, January 2011.

[15] M. Plachkinova, S. Andres and S. Chatterjee, “A Taxonomy of mHealth apps – security and privacy concerns,” in *Proc. of the Hawaii Int’l Conference on System Sciences*, Kauai, HI, 3187-3196, 2015.

[16] M. Naveed, X. Zhou, S. Demetriou, X. Wang and C. Gunter, “Inside job: understanding and mitigating the threats of external device mis-bonding on Android,” in *Proc. of the Annual Network and Distributed System Security Symposium* (NDSS), February 2014.

[17] M. Elkhodr, S. Shahrestani and H. Cheung, “Enhancing the security of mobile health monitoring systems through trust negotiations,” in *Proc. of the IEEE Conference on Local Computer Networks*, Bonn, 754-757, October 2011.

[18] Y. Choh, K. Song, Y. Bai and K. Levy, “Design and implementation of a cloud-based cross-platform mobile health system with HTTP 2.0,” in *Proc. of the IEEE Int’l Conference on Distributed Computing Systems Workshops* (ICDCSW), Philadelphia, PA, 392-397, July 2013.

[19] T. Pfeifer and S. Covaci, “Active protection of patient data by reverse cloud approach,” in *Proc. of the IEEE Int’l Conference on e-Health Networking, Applications & Services* (Healthcom), Lisbon, 716-718, 2013.