Security Analysis of an IoT Architecture for Healthcare

M. Teresa Villalba, Manuel de Buenaga, Diego Gachet(✉), and Fernando Aparicio

Universidad Europea de Madrid, 28670 Villaviciosa de Odón, Spain
{maite.villalba,buenaga,diego.gachet,fernando.aparicio}@uem.es

Abstract. Security issues of IoT devices are increasing with their massive use in healthcare. Recollection of data from devices is not clear to the users so far, and different problems arise including confidentiality, integrity and availability of the information. We analyze security issues mainly related to IoT data storage and transmission in our proposal of healthcare system architecture including cloud services and big data processing of information. We identify protocols needed and security problems including authentication, transmission of data to the cloud, as well as their insufficient anonymization process and the opaque procedure for users in order to control the storage of their data.

Keywords: Internet of Things · Security · Privacy · Wearable · Healthcare

1 Introduction

Nowadays society is demanding new services and technology allowing citizens to better manage their own health and disease, resulting in more cost effective healthcare systems and alleviating the issues of an increasing aging population. New emerging technologies can be combined with other widely deployed ones to develop such next-generation healthcare systems.

According to World Health Organization, chronic diseases are the leading cause of death worldwide, as they cause more deaths than all other causes together. While these diseases have reached epidemic proportions, they could be reduced significantly by combating the risk factors and applying early detection, the indoor and outdoor monitoring joined with prevention measures and a healthier life style. For both chronic and pre-chronic people several dangerous clinical situations could be avoided or better monitored and managed with the participation of the patient, their caregivers and medical personnel [1].

In this paper we present main issues in the security analysis of an IoT architecture for healthcare in the framework of the project IPHealth [2], including key aspects of security in the Internet of Things in healthcare, the description of our system architecture proposal with a significant focus on IoT elements, and the analysis of security key aspects of main IoT components.

B. Mandler et al. (Eds.) IoT 360° 2015, Part I, LNICST 169, pp. 454–460, 2016.
DOI: 10.1007/978-3-319-47063-4_48

2 Security in the Internet of Things in Healthcare

According to Gartner, wearable fitness and personal health devices will be $5 billion market by 2016 [3]. In spite of this expected growth, just as "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data" [4] reveals, the majority of healthcare organizations do not spend enough resources to protect patient data. Moreover, the last "Internet Security report of Symantec" estimates a 125 % growth in healthcare cyber-attacks over the past five years, and reported that a 37 % of security incidents affected to healthcare organizations [5], with the largest number of data breaches for the fourth year in a row. The huge amount of personal information coupled with this lack of resources to protect them, turn health data into an attractive and lucrative objective.

Currently the devices being used in healthcare to collect biometric data are usually smartphones with sensors or specific wearable devices. Both of them are commonly combined with apps to process data, interpret the signals, and show statistics to users. These apps carry out simple processing, so the functionality is sometimes extended by transferring the data to the cloud to be processed with complex algorithms. Security issues in this scenario can be categorized into three major areas: security, or as is widely accepted confidentiality, integrity, and availability; privacy or the appropriate use of the information; and legal issues, i.e. security concerns related to laws. Regarding security, three points of risks can be identified in the general architectures previously shown: device, data transmission (sensor to smartphone and smartphone to cloud) and cloud storage.

- Devices are individual and personal, so the motivation for data theft is smaller. Still malware can be used to automate the task of enabling a massive theft of data. Moreover the physical device can be stolen or lost. Wearable sensors do not include protection, and mobiles need to be configured by users (phone locking, tracking …). Mobile devices use apps to extend functionality to users. Symantec reviewed 100 health apps finding that 20 % transmit user credentials without encryption, 52 % not use any privacy policies and each one connects with an average of 5 websites while using usually with advertisement and analytics services [5].
- During transmission, data can be captured by using different attacks in the same way than in other architectures. The solution is to use strong encryption to avoid reading the data if they are capture, and authentication to confirm that data are sent to the true receptor. But there are some issues related to encryption and strong authentication to be solved, such as they slow down data transfer, are difficult to use, and are heavy energy-consumers.
- Finally, cloud computing architectures store data on database. Cloud services are provided by third party vendors who are exposed to attacks from insiders. But in addition, these databases are exposed to the Internet network in order to receive data from users. So the risks are similar to other similar databases, and depend on the configuration. Solutions involve multi-factor authentication, access control methods, strong passwords, etc. Again these methods make the systems more difficult to use and slower.

3 IoT Architecture Proposal for Healthcare

Our proposal of architecture for collecting data in order to promote wellbeing and physical activity is based on the need for a scalable data storage and high-performance computing infrastructure for efficiently storing, processing and sharing of health and activity sensor data. With this situation in mind we propose a simple and coherent activity monitoring solution. That solution takes into account several factors like using noninvasive sensors, allowing the processing of high volumes of data coming from them (including information from other sources as for example clinical texts); searching and retrieval of medical related information from forums, and designing appropriate visualization interfaces for each user type (patients, healthcare professionals, caregivers, relatives, etc.)

According to the above features, our general architecture for activity monitoring as well as its associated services are presented in Fig. 1: the components shown are being developed under the project ipHealth [2]. The architecture allows monitoring of both chronic and non-chronic patients, as well as healthy people that need to be monitored by different circumstances in both, home and external environment. Moreover it allows interaction with their family, the emergency systems and the hospitals through the application of Cloud computing, Big Data and Internet of Things approaches. IoT plays a key role in our architecture allowing users benefit from the utilization of different wearables and sensors devices.

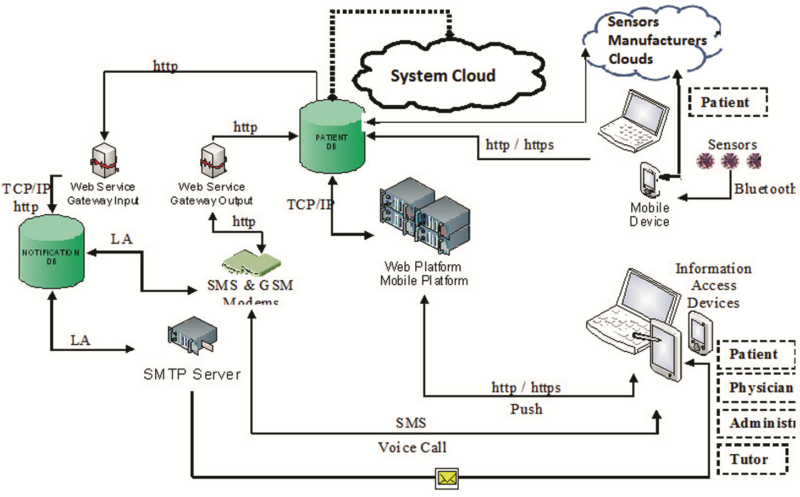

Fig. 1. Proposed architecture for patients monitoring

The architecture includes as main elements the following: smart mobile phones which in turn accepts data from wearable vital signs or activity sensors, a cloud based (public as Amazon Web Service or private) infrastructure for data store and an analytic module for activation of alarms to be sent to the patient and/or patient's caregivers, access to the different sensors of cloud manufacturers, an interoperability and messaging

platform for delivery of information to all involved actors in the system, and a website platform that allows to consult the associated patient information from desktop computer as well as from mobile devices.

4 Security Analysis of the Architecture

For our system, health and activity data are mainly taken from the clouds of sensor's manufacturers using different APIs that allow developers to establish a connection between applications and health data generated by users with their products. At present time we are conducting tests for monitoring physical activity and cardio-vascular status using iHealth BP7 bluetooth enabled blood pressure sensors, iHealth PO3 pulse oximeters, and Fitbit flex wristbands. Since the other components of the architecture here presented are common to other Internet connected architectures and, due to space limitations, in this paper we will focus on the wearables segment of the architecture. Specifically we will take FitBit as a representative element of wearable.

FitBix Flex [6] is a wrist monitor with a MEMS 3-axis smart accelerometer that collects data about user's movement such as steps taken, distance walked, and calories buried. Collected data are sent to a cloud to provide more detailed information to users through an online website. A free app, FitBit, extend the functionality syncing the sensor statistics with the mobile through BLE (Bluetooth Low Energy) 4.0 among others. An API to integrate third-party applications getting and modifying user´s data from Fitbit.com is provided. Moreover, the user can create an account to keep in touch with other users.

Figure 2 shows the specific architecture of Fitbit. We separate the different components according to the division mentioned in Sect. 2: (1) and (3) devices, (2) and (4) data transmission, and (5) cloud storage.

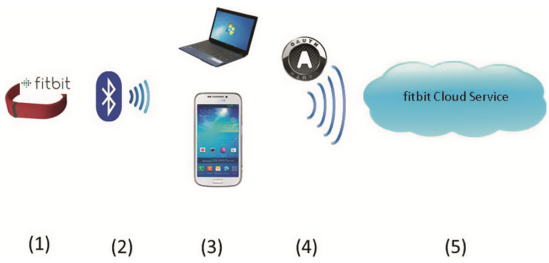

Fig. 2. Fitbit architecture

Regarding the device, logs stored in the mobile phone with more data than shown to users were found in [7], in contrast to what they declare in their privacy policy [6]. Moreover, more data than needed are requested to users, for example date of birth instead to only the year. On the other hand, the provided API uses OAuth 1.0 (version 2.0 is in beta state) which has several discovered vulnerabilities [8].

Otherwise, synchronization between Fitbit and mobile devices or personal computers is done over BLE 4.0. BLE supports encryption and authentication.

In addition, it provides a mechanism which allows a device to use and change private addresses as frequently as needed to avoid tracking [9]. However, Fitbit does not take advantage of this feature, and consequently it is possible to track activities of specific users, even when the user has the location functions inactivated. Additionally, BLE credentials are sent to the mobile device in plaintext over TLS [7]. Finally, in [9] it has been reported that none of the pairing methods used by BLE protects against passive eavesdropping, although in the BLE specification claims its future versions will resolve this issue [12].

Regarding the data transmission between the mobile device and the cloud, during the connection the mobile device notifies to the server all the Fitbit devices within the range [7]. This can lead to privacy issues by providing more information than necessary.

Fitbit provides access to its social network to share results with friends. As the same of other social networks, privacy preferences should be well configured in order to preserve data privacy. Although the privacy preferences are right configured, a social engineering attack is possible too. Education and awareness of users are the only way here to avoid these kinds of attacks.

On the other hand, the Fitbit privacy policy just claims to use a combination of security technical controls, so users cannot know the level of protection of their data neither of the stored data in the device nor the cloud [6]. They declare that the users will be notified if their data would be made publish, but they do not let users the option of

Table 1. Summary of compliance for privacy and security properties

Security and privacy properties [13]	Fitbit compliance (yes/no/ partially/not informed)	References
P1. Inform Patients about collected and stored data (what, why, where, who can access, …)	Partially	[6, 7]
P2. Enable Patients to review storage and use of their PHI	Yes	
P3. Enable Patients to control, through informed consent	No	[6]
P4. Provide access to PHI to read, modify and delete their registers	Partially	
P5. Provide easy-to-use interfaces to review and control all their data	Partially	
P6. Limit collection and storage of PHI	No	[7, 9]
P7. Limit use and disclosure of PHI to those purposes previously specified	No	[6]
P8. Ensure quality of PHI (freshness, integrity, completeness and authenticity)	Partially	[9, 10]
P9. Hide Patient identity	Partially	[10]
P10. Support accountability through robust mechanisms	Not informed	
P11. Support mechanisms to remedy effects of security breaches or privacy violations	Not informed	

objecting. Moreover, they claim to use anonymization techniques for some data (do not specify which ones), and that they can share or sell those anonymized data without option for user to participate in the decision. However, anonymization techniques have proved to be insecure [11, 12]. In addition, Fitbit does not provide users any control of their data stored in the cloud [6]. Table 1 shows a summary of the privacy and security according to the properties following the model defined in [13].

5 Conclusions and Future Work

We have studied main issues in the security analysis of an IoT architecture for healthcare in the framework of the project IPHealth. Common IoT architectures involve as main security vulnerability issues the storage in device (sensor and/or smartphone), data transmission (sensor to smartphone and smartphone to cloud) and cloud storage. As wearables are being connected to social networks, the risks to reveal private and sensitive information are higher. It is important to identify vulnerabilities of these devices in order to avoid attacks.

As a reference to carry out the security analysis, we have presented our architecture involving IoT devices, cloud architectures and big data components. Using FitBix Flex as representative of the sensors manufacturers we integrate, we have eventually found several important security risks and vulnerabilities impacting to nowadays users. After the analysis and following a common model of privacy and security properties, a table with the compliance of Fitbit to these properties is provided. The results show that the privacy provided by Fitbit is clearly insufficient.

Although more devices need to be analyzed, this results make us suspect that there is a long way to go in regards to security of the devices used in healthcare, here analyzed.

References

1. Gachet, D., Aparicio, F., de Buenaga, M., Padrón, V.: Personalized health care system with virtual reality rehabilitation and appropriate information for seniors. Sensors **12**(5), 5502–5516 (2012)
2. Gachet, D., Aparicio, F., de Buenaga, M., Ascanio, J.R.: Big data and IoT for chronic patients monitoring. In: Hervás, R., Lee, S., Nugent, C., Bravo, J. (eds.) Ubiquitous Computing and Ambient Intelligence. Personalization and User Adapted Services. LNCS, vol. 8867, pp. 416–423. Springer, Heidelberg (2014)
3. Angela McIntyre, J.E.: Gartner, Market Trends: Enter the Wearable Electronics Market with Products for the Quantified Self, July 2013
4. Ponemon Institute LLC: Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data (2015)
5. Symantec: Internet Security Threat Report (2015). http://www.symantec.com/security_response/publications/threatreport.jsp
6. FitBit: FitBit Flex (2015). http://www.fitbit.com/es/flex. Accessed June 2015
7. Cyr, B., Horn, W., Miao, D., Specter, M.: Security Analysis of Wearable Fitness Devices (Fitbit). Massachusetts Institute of Technology (MIT), December 2014

8. Hsu, Y., Lee, D.: Authentication and authorization protocol security property analysis with trace inclusion transformation and online minimization, pp. 164–173 (2010)
9. Gomez, C., Oller, J., Paradells, J.: Overview and evaluation of bluetooth low energy: an emerging low-power wireless technology. Sensors **12**, 11734 (2012)
10. The Bluetooth Special Interest Group: Specification of the Bluetooth System, Covered Core Package, Version: 4.0. Kirkland, WA, USA (2010)
11. Backstrom, L., Huttenlocher, D., Kleinberg, J., et al.: Group formation in large social networks: membership, growth, and evolution, pp. 44–54 (2006)
12. Sweeney, L.: K-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness Knowl.-Based Syst. **10**, 557–570 (2002)
13. Avancha, S., Baxi, A., Kotz, D.: Privacy in mobile technology for personal healthcare. ACM Comput. Surv. **45**, 31–354 (2012)