Security and Privacy Issues in Health Monitoring Systems: eCare@Home Case Study

Thomas Wearing[1] and Nicola Dragoni[1,2(✉)]

[1] Technical University of Denmark (DTU), Kongens Lyngby, Denmark
ndra@dtu.dk
[2] Örebro University, Örebro, Sweden

Abstract. Automated systems for monitoring elderly people in their home are becoming more and more common. Indeed, an increasing number of home sensor networks for healthcare can be found in the recent literature, indicating a clear research direction in smart homes for healthcare. Although the huge amount of sensitive data these systems deal with and expose to the external world, security and privacy issues are surprisingly not taken into consideration. The aim of this paper is to raise some key security and privacy issues that home health monitor systems should face with. The analysis is based on a real world monitoring sensor network for healthcare built in the context of the eCare@Home project.

1 Introduction

With the development of new technologies such as mobile systems, embedded systems and wireless sensor networks, monitoring systems for healthcare are getting more and more common [1]. The rationale behind these systems is that elderly patients require systematic and continuous monitoring in order to promptly detect anomalous changes in their condition. Generally speaking, several wireless communication devices are employed and combined with medical sensors, to monitor elders from various points of view and according to different health parameters ([2–4] to mention only a few). However, the vast majority of the proposed systems are not taking into account what security threats the installation provides and which measures are needed in order to protect users' privacy. The security risks associated with such systems, indeed, can represent a high concern, because of the sensitive information these systems can deal with, like sleeping patterns, eating habits, heart rate and so on.

Methodology and Contribution of the Paper. In this paper we want to raise the awareness about the lack of concerns many solution providers show regarding such risks. To do so, we look at the main security and privacy weaknesses of a representative healthcare monitoring system, namely the home sensor network under development in the context of the eCare@Home project. The eCare@Home system is a made up of a collection of various sensors that monitor

Research partly supported by the eCare@Home project (www.ecareathome.se).

M.U. Ahmed et al. (Eds.): HealthyIoT 2016, LNICST 187, pp. 165–170, 2016.
DOI: 10.1007/978-3-319-51234-1_29

movements and activities. The aim of this is to measure several attributes of the tenants and their environment in order to infer various properties concerning the health of the tenants. This analysis should then be provided in a user friendly format to care-givers. The motivation behind choosing eCare@Home as case study is that the architecture of the eCare@Home sensor network is generic enough to represent the vast majority of health monitoring systems proposed in literature. In particualar, in this paper we examine the possible ways in which an attacker could gain access to the eCare@Home system, what could be exploited and how the system could be changed to prevent such attacks. With this paper we also aim at providing some key advice to other developments of similar healthcare monitoring systems that will surely encounter the same security flaws.

Outline of the Paper. Section 2 briefly introduces the system under analysis, namely the eCare@Home sensor network. Sections 3, 4, 5 focus on the performed privacy and security analysis, identifying attacks and possible countermeasures. Finally, Sect. 6 concludes the paper.

2 System Overview

The eCare@Home health monitoring system has currently been developed in a fully-functional room configured to replicate a real world apartment, containing a bedroom, a kitchen and a living room. As sketched in Fig. 1, the system consists of several sensor nodes distributed in the apartment varying from light, pressure and RFID. These sensors are connected to a small board running Contiki[1] which then connect to a base station over an 802.15.4 network. Once the data has been transmitted to the base station, it is converted into ROS[2] format and passed onto the internal ROS network within the base station. Collected data is stored in the base station but in future revisions the aim is to upload such data to a cloud repository.

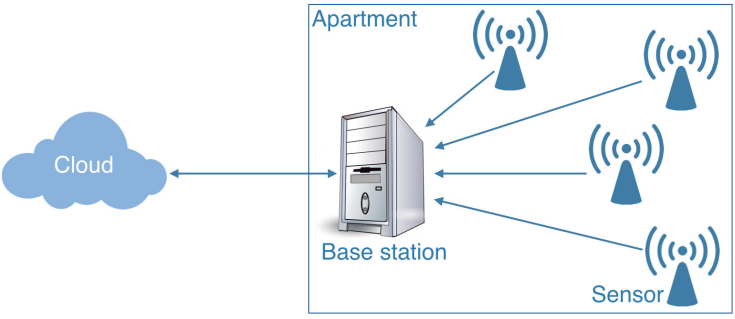

Fig. 1. eCare@Home sensor network

[1] An OS developed for the Internet-of-Things, http://www.contiki-os.org.
[2] Robot Operating System, http://www.ros.org.

Fig. 2. Data flow diagram of patient data within the boundary of the apartment

To aid in highlighting areas of interest for the security assessment, Fig. 2 shows the data flow diagram concerned to the points of ingress and egress of the patient data. As mentioned earlier, the security assessment has been limited to the network within the apartment, as the method of uploading the data to the cloud has yet to be developed.

3 Wireless Communication

Attack: Wireless Sniffing. An observed vulnerability of the system is the ability to wirelessly sniff the communication on the 802.15.4 network. An attacker is able to use readily available equipment to promiscuously sniff the wireless network and gather patient data. This requires the attacker to be within a 10–30 m (dependent on device) of the location but it is plausible that an attacker could plant a device such as a repeater to extend the range or a receiver with significant storage. Both of these methods would allow the attacker to remotely collect the data without physically being within the 10 m radius. This type of attack could lead to a breach of patient privacy impacting the confidentiality of the data. It is noted that this type of attack would be highly targeted as it requires an amount of physical effort that would produce results on a small number of targets. With this assumption we can assume that attackers who are aiming to gather large amounts of data on a wide range of people will not see this as a viable attack. However due to the minimal amount of skill required to access the information it could be viable attacker for someone with a more personnel motive against the victim. It would be possible for an attacker to infer various states from the data that may be to their benefit. For instance, if someone is attempting to burgle the property, he can monitor the wireless network to determine if the occupant is at home or to determine the tenant's daily schedule in order to plan the best time for the malicious activity.

Attack: Spoofing of Data. In this attack, the attacker would require a more detailed knowledge of the system and protocols used but it is still plausible. It would be possible to inject packets into the network that are not genuine in an attempt to negatively impact on the patients data for the attackers benefit. This attack has greater implications when considering the future of healthcare monitoring systems, when such systems will not only have sensors that read from the environment but they will also incorporate actuators. These actuators may come in the form of embedded insulin pumps or pace makers. This means the security of the system does not just have to protect the confidentiality and

integrity of the patient's data but also their life. Even in less severe case such as actuators for opening doors, there is still a significant increase in risk as soon as the system can interact with the environment.

Recommendations. As part of Contiki, the introduction of LLSEC provides link layer security across the 802.15.4 network [5]. This allows for the use of AES encryption across the network providing an added layer of security from sniffing. This method also allows for authentication and non-repudiation to protect from replay attacks. The authentication can be done in two ways, either authentication with a network-wide key or a pairwise key. The pairwise key is recommended as if that is discovered it will only affect the communication between one sensor and the base station where the network-wide key would result in all of the sensor data being compromised. This is a trade off between ease of deployment and security though, if the network-wide key is used it would be easier to enrol new devices as you would not need to setup a new key on the base station. For the encryption scheme AES 256 would be recommended but due to the low power environment this system operates in AES 128 would be a sufficient deterrent. Currently NIST still approve of using AES in CBC mode [6]. Key management for this network is somewhat difficult to balance, static keys within the network could prove troublesome as a sensor device could be stolen and have its key extracted from the flash if it is not made to be tamper proof. This tamper proofing though will inevitably increase the cost of each sensor. The use of certificates could help with this, each certificate would be unique to each device and could be revoked if the device is stolen. The trade off with this method is the increase cost of computing that is required as part of asymmetric encryption. Using certificates for authentication and then generating a static key between the two devices would provide a better level of security for the network. Unfortunately, this functionality is not currently available in Contiki's current build.

4 Base Station

Attack: Theft of Patient Data. In this attack, the attacker gains access to the base station by either remote or physical means and obtains the patients data. The current system stores all of its recorded patient data on the base station in clear text. This could result in the data being compromised if the base station is physically stolen or remotely hacked into. In the case of the base station being physically stolen the only data that would be obtained would be regarding that patient, so the return on investment for the attacker would be relatively low. However if there is a common vulnerability across the base stations then an exploit could be weaponized and used to easily access a large amount of patient data. This style of attack could be conducted by a rival company, criminal business or government agency as it would require a lot of resources.

Recommendations. It is strongly recommend to move towards and encrypted storage platform. For instance, data could be stored in an encrypted database

such as SQLite this would allows for data to be easily written and read from the database whilst being stored in an encrypted manner. SQLite requires SQLite Encryption Extension (SEE) [7] to encrypt the entire database so that META data cannot be extracted. It is recommended to use AES 256 in OFB mode to provide the highest level of security using this framework. This does not address the base station being compromised but limits the impact of such a breach by restricting the attackers access to the information. Key management will be an essential part of the security of the system, deriving a strong key and storing it. It is not advised to store the key for the database on the base station but as these system will be possibly scattered over a large area it may be impractical to store the keys of site. Having a separate tamper proof key storage device connected to the base station can be a good option to get the best of both worlds but will incur an extra financial and maintenance cost.

5 Access Control

Attack: Unauthorized Access of Patient Data. In this scenario the attacker is an individual who has access to the system but is not authorized to access the patient data. Throughout the system there is an evident lack of access control, anyone with access to the base station can access all the data with no accountability. This is a detrimental to the privacy and confidentiality of the patients data. In the scenario where the application is deployed in the real world many people may have access to the base station such as carers, technicians and field engineers. Many of these people should not have direct access to the patient's data. To protect the privacy of the patient the access to the data needs to restricted so that only care providers and doctors have the rights to. Furthermore, this access should be monitored and logged so that accountability can provided if legitimate access has been abused. This type of exploitation would be far more likely to occur at the cloud level of the data storage. An individual who is allowed to access to patient data could steal a vast quantity of personnel data to sell to insurance companies or similar parties [8].

Recommendations. The SQLite framework supports access permissions so the DBMS could help control access to the raw data [9]. This will only be able to control access to the data that is stored on the base station but could be used to delegate different levels of access to different users. Logs should be forwarded to an external server as well as locally being stored so that tampering with them is discouraged. If the logs a merely contained on the base station there is the possibility that they will be modified or deleted. This access control and logging needs to be extended to protect the cloud storage as well. Indeed, the cloud needs a form of access control system that limits the amount of data the users of the system have access to. For example, a doctor should not be able to access all patients data just because he is a doctor, they should be limited to their own assigned patients. Logs should be stored and analyzed to spot any suspicious activity such as requesting large bulks of data.

6 Conclusion

In this paper, we have highlighted some of the basic security and privacy issues that a healthcare monitoring system should deal with in order to protect users and their sensitive data. The analysis has not been based on theoretical healthcare frameworks, but on a real-work healthcare monitoring sensor network developed under the context of the eCare@Home project. The main flaws we have identified are the lack of encryption on the wireless network used for the sensors, the improper storage of the patient data and the unrestricted access of the patient data. These flaws are common to the majority of similar systems proposed in the literature so far, as security and privacy are not sufficiently taken into consideration by the healthcare community.

Key recommendations resulting from the analysis includes: to secure the wireless network through available encryption schemes; for both storage and access, to use an encrypted database that can store the patients data in a secure format as well as control access to the raw data. This assessment is by no means complete as there might be still various flaws within the system. However, although these recommendations will not create a fully secure system, they will significantly improve the security of the healthcare system. Indeed, most of the attacks against healthcare systems performed in the recent years have been successful not because of sophisticated attack strategies, but because of a complete lack of basic security and privacy protection in the targeted systems. We hope this paper can be regarded as alarm bells for all the healthcare professionals, by sending out a clear signal regarding the need to pay greater attention to security and privacy of future home health monitoring systems.

References

1. Pantelopoulos, A., Bourbakis, N.G.: A survey on wearable sensor-based systems for health monitoring, prognosis. IEEE Trans. Syst. Man Cybern. Part C (Applications, Reviews) **40**(1), 1–12 (2010)
2. Tsukiyama, T.: In-home health monitoring system for solitary elderly. In: Proceedings of EUSPN/ICTH'15, Procedia Computer Science, vol. 63, 229–235 (2015)
3. Kotz, D., Avancha, S., Baxi, A.: A privacy framework for mobile health and homecare systems. In: Proceedings of SPIMACS'09. ACM (2009)
4. Dasios, A., Gavalas, D., Pantziou, G., Konstantopoulos, C.: Wireless sensor network deployment for remote elderly care monitoring. In: Proceedings of PETRA'15. ACM (2015)
5. Contiki Pull Request Containing A.E.S. Encryption, July 2016. https://github.com/contiki-os/contiki/pull/557
6. Dworkin, M.: NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality 2002, July 2016. http://csrc.nist.gov/publications/nistpubs/800-38a/spp.800-38a.pdf
7. SQLite Encryption Extension: Documentation, July 2016. https://www.sqlite.org/see
8. Bloomberg: Your Medical Records Are for Sale, July 2016. http://www.bloomberg.com/news/articles/2013-08-08/your-medical-records-are-for-sale
9. SQLite, July 2016. https://www.sqlite.org/