Security And Privacy Issues in Healthcare Monitoring Systems: A Case Study

Daniel Tolboe Handler, Lotte Hauge, Angelo Spognardi and Nicola Dragoni
DTU Compute, Technical University of Denmark, Richard Petersens Plads, 2800, Kongens Lyngby, Denmark

Keywords: Security, Privacy, Pervasive Healthcare.

Abstract: Security and privacy issues are rarely taken into account in automated systems for monitoring elderly people in their home, exposing inhabitants to a number of threats they are usually not aware of. As a case study to expose the major vulnerabilities these systems are exposed to, this paper reviews a generic example of automated healthcare monitoring system. The security and privacy issues identified in this case study can be easily generalised and regarded as alarm bells for all the pervasive healthcare professionals.

1 INTRODUCTION

Health monitoring systems are getting more and more common (Pantelopoulos and Bourbakis, 2010). In particular, elderly patients require systematic and continuous monitoring in order to promptly detect anomalous changes in their health. With the development of new technologies such as mobile computing and wireless sensor network (WSN), many solutions specifically aimed at elder persons have been proposed. Generally, several wireless communication devices are employed and combined with medical sensors, to monitor senior citizens from various points of view (Tsukiyama, 2015; Kotz et al., 2009; Dasios et al., 2015). Surprisingly, many of the proposed systems are not taking into account what security threats the installation provides and which privacy measures are needed. The security risks associated with such systems, indeed, can represent a high concern, because of the sensitive information these services can deal with.

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 will look at the main weakness of one of these systems, namely a general monitoring system for elderly (Dasios et al., 2015) . This system has been chosen because it is generic enough to provide a good representation of the health monitoring systems available, which are mostly surveillance, only wearable, or mostly environmental sensors. Common for most systems is that none of them have taken security into account, except for adopting encryption for the network protocols. In this paper we want to show which security measures should be investigated in all kind of monitoring systems, by making a risk analysis and threat model for the mentioned system. We also investigate which privacy measures should be stated before implementing the systems. One major contribution will be stating which impact can have the traffic analysis on a health care system, when burglars are planning a break-in. The case study aims at identifying a number of main guidelines to follow in order to propose e-health monitoring systems that should guarantee a reasonable level of security.

Outline of the Paper. We describe the case study in Section 2 and then we focus on what impact the health monitoring system can have (Section 3). In Section 4 we present different attacks, as well as vulnerabilities the used network protocols raise. Then we analyse which privacy measures should be taken into account in Section 5. Section 6 concludes the paper.

2 ENVIRONMENTAL SENSOR NETWORK

The system we are going to asses is the environmental sensor network described in (Dasios et al., 2015) (sketched in Fig. 1). This monitoring system aims to give an overall health estimation of the elderly at a low cost, without using cameras and microphones, which according to the paper are ”commonly perceived as privacy violators”. They also seek

Handler D., Hauge L., Spognardi A. and Dragoni N.
Security And Privacy Issues in Healthcare Monitoring Systems: A Case Study.
DOI: 10.5220/0006224603830388
In *Proceedings of the 10th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2017)*, pages 383-388
ISBN: 978-989-758-213-4

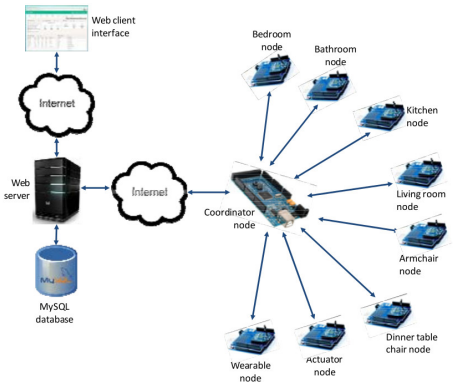

Figure 1: Architecture of the considered environmental sensor network (picture taken from (Dasios et al., 2015)).

a minimal amount of wearable devices. These goals are obtained by a WSN of nine nodes. Four room nodes measure movement, light, temperature, electricity consumption, water flow, and pressure, in order to give an overall assessment of what the senior citizen is doing. Sensors on the chairs detects the presence of a person seating on a chair. A wearable sensor serves as fall detector and as a panic button to call for help. An actuator enables remote control of certain electrical installations such as climate control. Lastly, a coordinator node works as a sink for the WSN, handling data from the network to a web interface and vice versa. The WSN uses ZigBee (see Section 4) to communicate to the sink, that, in turn, uses a wired internet connection sending all the data to a MySQL database and deploying the data on a Web site.

3 THREAT MODEL

The threat model is essentially composed by assets, threats, attackers, attacks and vulnerabilities of the system. The final aim is to enable an informed decision-making about application security risk.

Assets. The reason for installing monitoring health care systems, is to be able to take care of the elderly. The system reviewed in this paper strives to detect life threatening events and preserving good health, which must be the main assets for the elder. Installing such systems should give the elder a secure feeling of living on their own, while not using an extensive amount of communal resources in salary for health care personnel. Other assets for the elder which are not taken into account in the considered health monitoring system are dignity, possessions of the elder and revealing of activities and location. The environmental sensor network presents a possibility of remotely changing the climate, which they state as an asset for the elder, but with modern technology, this should not be a problem to handle by the elder. In Fig. 2 we list all the considered assets with respect to what we think would be their value for the elder, where we adopted a scale from 1 to 5: very low value (1), low value (2), medium value (3), high value (4), very high value (5).

Assets

- Life (5)
- Good health (4)
- Feeling secure (4)
- Communal resources (4)
- Dignity (3)
- Possessions (3)
- Revealing of activities (2)
- Revealing of location (2)
- Indoor Climate (1)

Attackers

- Inheritor (1) / (2)
- Criminals (2) / (3)
- Burglars (4) / (2)

Figure 2: Considered assets, with priorities related to their value for the elder and attackers, with existence likelihood and technical knowledge to exploit a system.

Threats. When looking at the system, the major threats of the assets are false positives, false negatives, or exposure of data. In particular, the exposure of personal health data, location of the elder, and activities. False positives and false negatives are related to the considered assets. A false positive is when the monitoring system misunderstands the status of the elder (for example, raising a false alarm). Conversely, a false negative is when the system fails to detect situations in which the assets are threatened.

Attackers. We have defined three main types of attackers (inheritors, criminals and burglars) as summarized in Fig. 2, where also their existence likelihood (from 1: very low, to 5: very high) and related technical knowledge to exploit a system (from 1: very low, to 5: very high) are reported.

Inheritor. The most important assets defined, such as life, good health and feeling secure are very dear to the elder, but not something that a lot of others have interest in taking. The only identified attacker for these assets is the inheritor, who would benefit from an early exit for the elder. The inheritor is defined to have less technical (that is, user level) knowledge of the system and very small probability of existing.

Criminals. Dignity and indoor climate could be used as blackmailing material and cons for criminals in order to get to the elders possessions. According to Danish police statistic over criminal charges[1] there are about 125 con thefts in inhabitants every year,

[1] https://www.politi.dk/NR/rdonlyres/87ADE11F-C8EE-4249-A64B-7D4B7FDFC7EE/0/Centralenoegletal2014.pdf

and these are mostly committed against elder people. Since it is limited how much value the elder posses, the major criminals are probably not going after the elders homes. Due to this we asses the likelihood of this as small, and the technical knowledge a bit higher than the inheritor, since the criminals have a network where they can distribute malicious tools.

Burglars. Possessions are also of great value to burglars. Burglars are becoming more organized, and according to a Danish assurance company they often know what is valuable, and are quick to find and take these items. Knowledge of where values are kept could be fatal in a burglary, which often takes short time. According to Danish police statistic over criminal charges thefts happens more than 20 times as much as robberies, which indicates that burglars tries to avoid people when breaking in. Danish assurance companies also advice their costumers to make their home look inhabited when away, which includes not stating their vacation on Facebook (Alka Ensurance, 2013). This indicates that knowledge of location and activities can have a large impact for burglars when choosing a place to break in. We asses the likelihood of a burglar as high when the burglars are defined to having little technical knowledge (see Fig. 2).

Attacks. We have identified five types of attack, which are considered in this paper. These are chosen because they show how serious and diverse can be the attacks available for this types of systems.

Man in the Middle. Man-in-the-Middle (MITM) is an attack type where the attacker relay and possibly modify or permutate the communication between two parties (Erickson, 2008). If the attacker is capable of intercepting or modifying the communication into or out of the house, he will be capable of preventing critical system updates, and prevent critical information of going of the house. Additionally is a man in the middle capable of sending fake messages, stating that the elderly has fallen, hence summon the health care company to assist the elderly without reason. If the health care system uses cameras to monitor the elderly, these pictures can be intercepted, and used either for blackmailing the elderly or for locating possession of value in the home of the elderly.

Denial of Service. If the health care systems are targeted by a successful denial of service attack, it will have severe consequences. All three health monitoring systems rely on sending information out of the house, if the user has fallen or anomalies is detected. If a denial of service attack prevents this, the whole system is compromised. The environmental sensor network relies on communication between the sensors and the sink. If this is prevented the system will become useless, hence the denial of service would be discovered, since the normal behavior sends steady flow of information, not only when a problem arrives. Compromise of the system in such way can lead to death or injury of the elderly, or a decrease in feeling secure.

Traffic Analysis. If the communication flow in the system is analyzed, it might be possible to know whether the elderly is home, is asleep or similar. This information can be useful to a burglar, who doesn't want to be disturbed when breaking in.

Malware. Malicious software can be used to modify the system, such that it doesn't fulfill the intended purpose. This can be used to make denial of service or man-in-the-middle attacks. Additionally malware can be used for simple traffic analysis as well.

Social Engineering. Attacking the human directly instead of the system has plenty of functions. It can be used to get access to the barebone computer or the sink to install malware, or it can be used to locate the sensors of the network. Elderly people are more vulnerable to social engineering than younger people (Lahtiranta and Kimppa, 2006), hence it is a obvious attack vector for the criminals.

Fig. 3 resumes the relations between threats attacks and attackers we have above detailed.

Asset	**Threat**			**Attacker**	**Attack**
	False negative	False positive	Exposure of		
Life	X			Inheritor	DoS
Good Health	X			Inheritor	DoS
Feeling secure	X		Possession	Inheritor	DoS
Communal resources		X			MitM
			Skin		MitM
Dignity			Activities	Criminals	SE
			Possessions	Criminals	SE
Possessions			Activities	Burglars	MitM
			Location		MitM
Revealing of activities			Activities	Burglars	TA
Revealing of location			Location	Burglars	TA
Indoor Climate		Climate adjustments		Criminals	MitM

Figure 3: Threat model for a health monitoring system, linking assets to the different threats, attacks and attackers.

Vulnerabilities. The attackers can exploit several vulnerabilities in order to realize the above attacks on the assets, that can be related to the different protocols or to the human being, as the social engineering-based attacks. The considered vulnerabilities are discussed in great detail in the following Section 4.

4 SECURITY AND PROTOCOLS

This Section addresses some security issues and vulnerabilities that occur when implementing the system. The network protocol used in the environmental sensor network is ZigBee. This Section reviews how MITM attacks, Denial of Service (DOS) attacks,

and traffic analysis can occur. Then, we generically describe how malware attacks and social engineering can occur. We use the acquired information to provide a risk assessment of the system.

ZigBee. ZigBee is widely used in pervasive computing due to its low bandwidth, low cost, and low power consumption (Stelte and Rodosek, 2013). Our vulnerability analysis is based on KillerBee[2], in particular on its *zbtumbler* tool, which detects active ZigBee networks, records and display information about the found devices. This makes it easy to detect whether or not ZigBee is in use.

MITM Attacks. zbreplay lounges a replay attack, which is countered in (Stelte and Rodosek, 2013). Another MITM attack is explained in (Choi et al., 2013) and exploits a vulnerability in the key distribution. In ZigBee the key is occasionally updated over the air in standard mode, which makes this attack quite realistic. The counter measures proposed involve using public key encryption instead of symmetric encryption. A greater modification is needed, and public key encryption.

DOS Attacks. zbassocflood uses a vulnerability in ZigBee's association method for new nodes joining the network. This floods the coordinator node, creating denial of service from the coordinator note, which is the sink of the sensor network. A counter measure for this problem has been proposed in (Stelte and Rodosek, 2013), by filtering the incoming traffic.

Traffic Analysis. zbsniff is a tool that sniffs and analyses the network traffic, thus making network-analysis easy to do. This is very difficult to prevent, due to how easy ZigBee is to detect.

Malware. Unintended, malicious software is a problem in all the communication technologies described above. If an attacker is able to inject malware into the system, the attacker will be able to compromise the whole system. Injection of the malware can be done by physically plugging in the malware (e.g. by a USB-stick) or using social engineering to get into the house of the system. Alternatively is it possible to access a wireless router, and through this get access to a computer to inject the malware on. A firewall and a strong security on the wireless network would be a countermeasure to this.

Social Engineering. The last attack vector we address is social engineering, covering actions where the human is the target of the attack, rather than the system (Bellovin, 2015). Examples of social engineering attacks are phishing, elicitation and simple phone calls, where the attacker pretends to be someone else (e.g. the IT department) (Hadnagy, 2011). According to Danmarks Statistik[3] the average age of the victims of trick theft (which can be assimilated to social engineering) is 75 years. It is important to keep social engineering in mind when implementing the health care systems, where users primarily are elders. It is impossible to make a comprehensive list of actions to prevent social engineering, however some recommendations can be given:

- Make sure the user of the system (the elderly people) gets information about: system updates, visits from technicians, who in call, if in doubt.
- As far as possible use technicians the user knows, or send a known employee from the health care organization together with the technician.
- If possible configure the system, such that the elder doesn't have to know passwords, etc., such that a social engineer cannot trick the password from the elder.

Attackers. Based on the analyses in Sections 3 and 4 we will now define which attackers who are able to carry out which attacks:

Inheritors. The computationally skills of the inheritors is limited according to our description in section Section 3. Since the assets the inheritors are targeting are the health and life of the elderly, denial of service attack is their only obvious attack vector. Malware to perform these attacks are considered to hard computationally for the inheritors to do, hence inheritors rely on jamming equipment or similar to perform the attack.

Criminals. Social engineering is the first and most obvious option of the criminals. Since their target is to blackmail the elderly, a lot of information is needed. This information can be gathered by man-in-the-middle attacks or traffic analysis. Malware is an option for these attacks.

Burglars. The location of the elderly is the main concern of the burglar. Traffic analysis is a good tool for locating the elderly. Man-in-the-middle attacks can be used to intercept pictures of the home of the elderly to locate possessions of value, such that the burglar knows where to look. Malware is one way to conduct a traffic analysis or a man in the middle attack, however it is difficult for the burglar to to able to plant the malware in the system.

[2]https://github.com/riverloopsec/killerbee

[3]http://www.dst.dk/da/presse/Pressemeddelelser/2002

4.1 Risk Assessment

As a final evaluation of the above analysis, having defined the risks and threats of the systems in Section 3 and the vulnerabilities of the system in the above sections, we can propose an overview of the five different attack vectors in the system of the considered case study. We start considering easiness and availability of performing the attack, proposing a score for each attack vector. The final outcome is shown in Fig. 4, where, again, we used a scale from 1 to 5, where 1 means very low risk and 5 means very high risk. It is quite clear that the proposed system is most vulnerable to traffic analysis, as well as the social engineering, even if this is a more general problem, not only related to the specific system.

- Man-in-the-middle (4)
- Denial of Service (3)
- Traffic analysis (5)
- Malware (2)
- Social engineering (4)

Figure 4: Easiness and availability of the different attacks, given the vulnerabilities of the system.

The challenges of traffic analysis are that it is very hard to prevent. The use of wireless protocols is always detectable. Even if the data in the communication is encrypted, it is still possible to detect the presence of the data flow.

The full overview of how critical each security issue is, with respect to the assets, can be found in Fig. 5. The scores are calculated as follows.

Probability Score. The probability score is a measure of probability of compromising the asset. The value is calculated as the average of the product of the each attackers value (found in Fig. 2) and the linked attack vectors scores (found in Fig. 4) divided by 5 and rounded up. As an example the probability of compromising dignity is:

$$\frac{1}{5}\left\lceil \frac{\textit{Likelihood of criminal} \cdot \textit{ease of MitM}}{2} + \frac{\textit{Likelihood of criminal} \cdot \textit{ease of Social Engineering}}{2} = \right\rceil$$
$$= \frac{1}{5}\left\lceil \frac{2 \cdot 4}{2} + \frac{2 \cdot 4}{2} \right\rceil = 2$$

Value Score. The values are defined as the assets value and are scored similar to the score applied to each asset in Fig. 2.

Final Score. The final score reveals the overall risk for compromise of this asset the score is calculated as the probability score multiplied by the value score. This reveals a new assessment scale from 1 to 25. Since we do not get above 9 in our assessment we have only colored the scale from 1 to 9, introducing dark green as better than green, dark red as worse than red, and brown as worst in order to easily distinguish between the risks. This is justifiable since everything above 10 could cause serious health problems because of the sensitive subject of health care is, taking care of the already weakened citizens.

Asset	Prob.	Value	Final
Life	1	5	5
Good health	1	4	4
Feeling secure	1	4	4
Dignity	2	3	6
Possessions	3	3	9
Revealing of activities	4	2	8
Revealing of location	4	2	8
Indoor Climate	2	2	4

Figure 5: Final results of the risk analysis, stating the different risks for the different considered assets.

Fig. 5 reveals that the must critical asset for the elderly is possession, followed by revealing of activities, and revealing of location. The assets most compromised are targeted by burglars doing traffic analysis. It is not impossible to imagine a scenario where a one of the health care systems is widely used, and a burglar will walk around a neighborhood, and use traffic analysis to find out where the systems are used. If the burglar knows in which houses the systems are used, he will be able to determine if the elderly is home, or not, and can then conduct a break-in, without being disturbed.

5 PRIVACY AND EQUIPMENT

This Section deals with the privacy issues occurring when monitoring the elderly (*the user* from now on). We use the Common Framework by Markle Foundation (Markle Foundation, 2008) as a base for the analysis, since it has been recommended for health systems in an extensive analysis for privacy frameworks (Kotz et al., 2009).

Openness and Transparency. It is important that the user of system knows exactly what data that is collected about her and how this data is used. Furthermore it is important to state who has access to this data and where and how the data is stored.

Purpose Specification. It is important that the collected data is used only for its purpose. If the data is intended to be used for new purposes it should be accepted by the user beforehand. If the user is unable to make that decision, it should be clear who can vouch for the decision (children or other next-of-kin).

Collection Limitation and Data Minimisation. The stored data should be limited to a minimum. Example: there is no need for storing fall detection data, as long as the user hasn't fallen. It is important to inform the user of the amount of stored data and how long time the data is stored.

Use Limitation. The collection of health data is very personal information for the user, and it is important that the integrity of the data is ensured, and that the data in no situation is made available to other than authorized users of the system.

Individual Participation and Control. Users should be able to access their own stored data, and should be able to control who else have access to these data.

Data Quality and Integrity. Only relevant data should be stored and should be up-to-date. Old and irrelevant data should be removed as soon as possible.

Security Safeguards and Controls. All means for protecting the data should be taken, when collection, analyzing, transmitting and storing the data.

Accountability and Oversight. The company or people in charge of the health care system must be held accountable for any breach of the security or privacy issues of the system. The system uses many different sensors, and it is important for each type of sensor to tell the user exactly what is stored. The system is used for detecting and analysing the environment the user lives in, hence a certain amount of data will have to be collected and stored for the system to be sufficient. If compromised this system will reveal a great amount of personal data about the user, and it is important that the user is aware of this, and that security measures are launched and maintained.

6 CONCLUSION

In this paper we have considered a reference health monitoring system for elderly people as a case study to state the security and privacy risks one should be aware of before implementing such kind of systems. In particular, we have identified attack vectors and groups of attackers, who could compromise the health monitoring system. Moreover, we have raised some privacy issues to address when people are monitored in their own home. Due to the fact that personal data is transmitted and stored on external servers, it should be stated who can access the data and who can be held accountable if data is lost or leaked.

Our major contribution has been the identification of the burglar threat, which could be very prominent if one healthcare system is used in large scale, because traffic analysis is not something a communication protocol can secure, the defence needs to be implemented as a part of what is communicated, which is easy to oversee by the developer.

The aim of the paper is to raise the levels of awareness and understanding of the cyber risks related to home monitoring systems. The hope is that the issues identified in this case study will be regarded as alarm bells for all the pervasive healthcare sector.

REFERENCES

Alka Ensurance (2013). Her er man mest udsat for indbrud! (retrieved on http://www.alka.dk/).

Bellovin, S. M. (2015). *Thinking Security - Stopping Next Year's Hackers*. Addison-Wesley.

Choi, K., Kim, M., and Chae, K. (2013). Secure and Lightweight Key Distribution with ZigBee Pro for Ubiquitous Sensor Networks. *IJDSN*, 9(7).

Dasios, A., Gavalas, D., Pantziou, G., and Konstantopoulos, C. (2015). Wireless sensor network deployment for remote elderly care monitoring. In *Proc. of PETRA'15*. ACM.

Erickson, J. (2008). *Hacking: The Art of Exploitation*. No Starch Press.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Wiley Publishing, Inc.

Kotz, D., Avancha, S., and Baxi, A. (2009). A privacy framework for mobile health and home-care systems. In *Proc. of SPIMACS'09*. ACM.

Lahtiranta, J. and Kimppa, K. (2006). Elderly people and emerging threats of the internet and new media. In *Proc. of I3E 2006*. Springer.

Markle Foundation (2008). Common framework for networked personal health information: Overview and Principles. Connecting for Health.

Pantelopoulos, A. and Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, 40(1):1–12.

Stelte, B. and Rodosek, G. (2013). Thwarting attacks on zigbee - removal of the killerbee stinger. In *Proc. of CNSM'13*.

Tsukiyama, T. (2015). In-home health monitoring system for solitary elderly. In *Proc. of EUSPN'15/ICTH'15*. Procedia Computer Science, Elsevier.