Privacy preserving mechanisms for a pervasive eHealth system

Milica Milutinovic[1], Koen Decroix[2], Vincent Naessens[2] and Bart De Decker[1]

[1] KU Leuven, Dept. of Computer Science, DistriNet/SecAnon,
firstname.lastname@cs.kuleuven.be
http://www.cs.kuleuven.be/~distrinet/
[2] Katholieke Hogeschool Sint-Lieven, Dept. of Industrial Engineering,
firstname.lastname@kahosl.be
http://www.msec.be/

Abstract. In this paper we propose a privacy-friendly eHealth system design providing pervasive care for the elderly or stay-at-home patients. The system integrates services of health status monitoring, organizing assistance and remote access to medical data. The proposed architecture is open and allows seamless integration of new services, service providers and users. The focus of this paper is on privacy preserving mechanisms that provide protection of the sensitive data handled by the system.

Keywords: eHealth, privacy, pervasive health care, commercial

1 Introduction

The average age of individuals has risen significantly in the past decades. The economy is under a growing pressure to sustain support and provide sufficient social security budget for the elderly population. One way to reduce costs is to allow them to stay at their homes for as long as possible. This is also complementary to their reluctance to leave home. The contemporary trend is thus moving from hospitalization of elderly or patients, to care in the community and development of smart homes. However, providing complete care and organizing help at the households is not a trivial task. It can, in fact, be a great burden for the guardians of the elderly or stay-at-home patients. Therefore one important initiative is to develop home assistance systems that provide continuous monitoring of health parameters and organize the caregivers' help. Even though there is a significant body of research focused on such systems, the privacy requirements are not fully tackled. Since individuals' medical data is handled by such systems, providing adequate privacy is an imperative. It is of utmost importance to ensure protection of sensitive data and allow only authorized personnel to access it. This is not a trivial issue because of possible need to access the health data remotely.

In order to tackle these problems and protect the privacy of vulnerable individuals, we have developed a novel approach to remote patient monitoring and scheduling of help. This paper focuses on privacy preserving mechanisms suitable

for such home assistance system providing complete and continuous monitoring of elderly or stay-at-home patients along with remote access to medical data and scheduling of tasks. Another important issue that we try to address is openness, i.e. seamless integration of new users, service providers or services into the system. In the remainder of this paper, we will no longer distinguish between stay-at-home patient and elderly person, and denote both by the term 'Patient'.

The rest of this paper is organized as follows: Next section discusses related work and Section 3 provides a brief description of the proposed system. Privacy requirements and mechanisms used to ensure them are described in Section 4 and evaluated in Section 5. Finally, concluding remarks are given in Section 6.

2 Related work

There is a significant body of research focusing on eHealth systems allowing care in the patient's household. Usage of sensors for monitoring health parameters or activity and raising alarms has been discussed in [4], [3], [2] and [5]. The sensors record different parameters ranging from user-indicated alarms [9], EEG, ECG signals to location data [1]. The optimal selection of parameters to be monitored is discussed in [8]. Similarly, using video technology for detecting patient's movement, posture or fall was explored in [6] and [10]. The proposed architecture of those systems usually consists of sensors monitoring the patient, a personal server gathering the sensor data and a central server - a monitoring center. The base station has a role in filtering and relaying the measurements to the monitoring center where it is assessed by the personnel. This approach clearly assumes employment of medical professionals at the monitoring center.

Even though privacy is an important requirement for such health care systems employing wireless health monitoring [11], the problem of its protection is not fully tackled. Encryption can be used for communication between the components, but a great amount of trust is placed on the monitoring center and its personnel. On the other hand, excluding medical personnel from the monitoring center would ease the commercial deployment and patients would be able to connect to their regular caregivers, instead of bounding the caregivers to the monitoring center.

3 System description

A pervasive home assistance system needs to integrate a range of services, such as health status monitoring, scheduling of assistance and remote access to patient's medical data. The system's functionalities are separated into several entities, as depicted in Fig. 1 and will now be explained in more detail.

Patients' health parameters, such as blood pressure or heart rate are continuously being measured by wearable, unobtrusive *sensors*. This sensor network is extended with a fall detector that records a sudden fall of the patient and a hand-held personal unit that captures patient's request for help and possibly incorporates an audio interface to allow communication with the patient. The

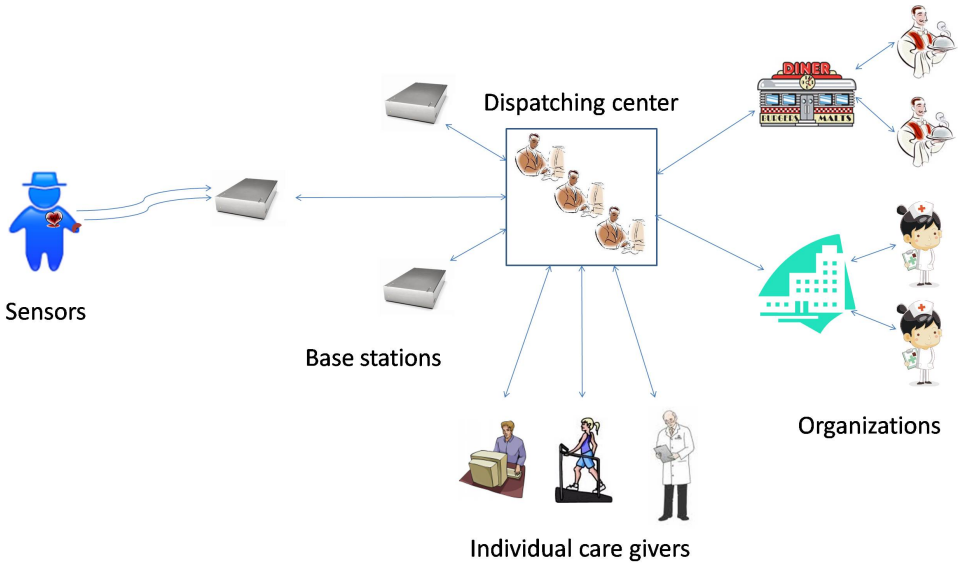

Fig. 1. System components.

measurements and signals from the sensor network are sent to a *base station* that logs and assesses them. The base station is also a part of the home equipment. It sends alerts if a problem is detected and controls access to the data according to patient-specific privacy policies.

All the communication with caregivers is mediated by a *dispatching center*. It is a commercial organization that is responsible for scheduling help for the patients and assigning tasks to caregivers (e.g. catering, doctor's visits), notifying caregivers of alerts and following up on their responses. It also performs coarse grained access control according to defined privacy policies and archives evidence of all actions, such as caregivers' requests or responses to alerts. The dispatching center also verifies that all of the connected home base stations and the links towards them are functioning and provides technical support. Besides the connection with patients' base stations, the dispatching center is connected with individual caregivers and *service providers*, such as hospitals or catering services. It is aware of their availability in order to schedule and assign all the tasks requested by the patients.

Finally, a separate entity, the *administration center* handles administrative tasks, such as user registration. This functionality is separated from the dispatching center for privacy reasons. Since the dispatching center mediates communication between patients and their caregivers and performs scheduling of tasks, combining that information with the identities of all users would reveal sensitive data. Therefore, all the users are identified in the dispatching center

by their pseudonyms and only reveal information on a need-to-know basis (e.g. medical expertise of caregivers, since it is relevant for assigning tasks).

Both dispatching and administration center are equipped with tamper-free devices. These *trusted devices* are used to re-key or decrypt (part of) sensitive information encrypted with their public key. These actions are performed under certain conditions and after strict checks in order to counter possible attacks and prevent leakage of private information. The role of these devices in establishing security and privacy is explained in more detail in the following text.

3.1 Patients' care networks

The dispatching center handles scheduling of tasks to caregivers and communication between caregivers and the home equipment. Therefore, it needs to keep track of all the patient-caregiver connections. It actually maintains the network of all caregivers of a patient, along with their roles (e.g. close relative, general practitioner, cleaning service) and their availability. These care networks are patient centric and each patient or caregiver are identified with their pseudonyms. This is a privacy-friendly solution, as the only distinction that can be made is between the role of a patient and the role of a caregiver. In addition, the caregivers that belong to multiple care networks are assigned different pseudonyms for each network. Thus, no additional information can be deduced by observing the connections between the users of the system.

All caregivers that are a part of a patient's care network have one or multiple roles assigned to them. The system accordingly maintains a *hierarchy of caregivers*. Coarse grained separation can be done according to medical training. Medical staff are strictly separated from the others, since they have certain privileges regarding access to the patient's medical data. More fine grained separation can be done between close relatives, guardians, neighbors, general practitioners, specialists, etc. The patient's (privacy) policies, kept on the base station, specify what access privileges are assigned to each role or caregiver.

4 Privacy as preserved by the system

In this section we will list the privacy requirements of a home assistance center and propose mechanisms that can be used to ensure them.

4.1 Security and privacy requirements

Personal medical data is exceptionally privacy sensitive. Therefore, the following requirements need to be fulfilled:

1. Strict control of access to personal medical data should be employed. Only medical personnel or individuals authorized by the patient should be able to get access to that data. This requirement is unavoidable, since legislation in many countries imposes this rule.

2. All connections of a patient, or patient's care network should be anonymized. This requirement arises from the fact that knowledge of some of the caregivers of a patient sometimes allows one to deduce the illness the patient suffers from.
3. Actions that have been performed in the system should be logged for possible future auditing and those logs should be treated as extremely confidential. They should only be accessible by a trusted (external) party in case a dispute arises.

4.2 User registration

All parties using this system first need to be registered with the administration center. Depending on their role in the system, different procedures are followed.

Patients subscribe to a certain set of services and possibly sign a contract with one or more service providers. They also need to prove their identity and contact information. In return, they receive a smart card containing the service level agreement, patient's identity and contact information, two key pairs for encryption and signing and certificates for the public keys issued by the administration center. The identity and contact information stored on the card will only be released to the dispatching center encrypted with the public key of a trusted device. In case of an emergency, the trusted device will re-encrypt this information with a public key of a caregiver that is requested to assist the patient or it will relay the information to the calling module, so it can send it to the authorized caregiver (see Section 4.4). Therefore, this identifying information is only available to an authorized person and cannot be retrieved by the dispatching center personnel.

After the home equipment is installed, the card is inserted into the base station to anonymously authenticate the base station towards the dispatching center and since keys for encryption/decryption and signing/verification are stored on the card, the functioning of the base station is only possible as long as the card is present. The administration center's database records the patient's pseudonym, certificates, service level agreement and the identity and address information encrypted with public key of a second trusted device that decrypts it only in case of a dispute and for billing purposes.

Individual caregivers (such as general practitioners, relatives, neighbors) that wish to register prove to the administration center their identity and address information (possibly via their eID card). Also, for medical personnel, additional proof(s) of qualifications must be provided. That is necessary to allow them to assume appropriate roles in the system (such as general practitioner or specialist). Upon registration, the caregiver receives an anonymous credential that includes his or her identity, qualifications and contact information. The credential also records a random number chosen by the caregiver, which is not disclosed to the administration center. Similarly as for the patients, the administration center keeps a record of the caregiver's pseudonym, qualifications, public key and encrypted identity and contact information.

Organizations (such as hospitals) or *service providers* (such as a catering service) provide the administration center with identity and contact information, a list of offered services, a certified public key and a commitment to a random number. If the administration center accepts the registration, the organization receives in return an anonymous credential, which includes all the previously exchanged information. The administration center's database will list the organization, related information and its recertified public key. Note that these registrations are not anonymized. Patients can browse this database and look for services they want to use.

4.3 Establishment of connections

Before the creation of the care network, each patient needs to register with the dispatching center. Initially, the smart card anonymously authenticates with the dispatching center and a secure end-to-end channel is established. Over this channel, the card will send the patient's pseudonym, public keys with the certificates and identity and contact information encrypted with the public key of the trusted device. The dispatching center creates a new node identified with the patient's pseudonym and records all the received information.

Later, if a patient wishes for a specific caregiver to join his or her care network, the patient or an authorized guardian sends a request, e.g. via email. The request specifies the patient's pseudonym, public key and an access code, which is used to limit the validity of the request and to prove that the caregiver has indeed received the request and is not the initiator of the connection. These access codes are obtained from the dispatching center on request and can only be used once. A fingerprint of each access code is stored and linked with the patient's pseudonym to allow later verification of validity.

If the caregiver wishes to accept the request, he or she contacts the dispatching center via a special applet, designed to ease the establishment of connections for the caregivers. The applet loads the caregiver's anonymous credential and the information received in the request, namely patient's pseudonym and the access code. It then establishes a new pseudonym for the caregiver using the patient's pseudonym and a random number contained in the caregiver's credential. This new pseudonym will only be used for tasks regarding the inviting patient. The applet then sends the newly generated pseudonym, received access code and caregiver's identity information verifiably encrypted with the trusted device's public key to the dispatching center. Using verifiable encryption allows the caregiver to prove that it is a valid encryption of the information contained in his or her anonymous credential, without disclosing it. The dispatching center verifies the access code, the validity of the credential and the encrypted data. If all the checks are validated, the public key is certified and the certificate and the encrypted data are stored with the new node linked with the caregiver's pseudonym. The complete transcript is then relayed to the trusted device for similar verification and re-encryption of the caregiver's identity information with the patient's public key. The re-encrypted data is then sent to the patient's base station. In order to make sure that an attacker cannot plant his or her public key in place of

the legitimate caregiver's key, the trusted device is also provided with the newly generated certificate linking the caregiver's new pseudonym and public key.

Upon receiving the response, the base station decrypts it and prompts the patient about this connection. The patient verifies the caregiver's identity, approves and assigns a role to the caregiver. When a connection is established, the base station records the pseudonym of the caregiver. The pseudonym is linked with the real identity of the caregiver, so the patient can specify the caregiver using the real identity and does not have to deal with complicated pseudonyms. On the other hand, when a request is sent to the dispatching center specifying a caregiver, the pseudonym is used.

For a detailed description of the protocols for creating and extending a patient's network, we refer the reader to [7].

4.4 Handling patients' requests

When a patient wishes to send a request for scheduling a task, he or she uses the smart card to authenticate and reveal the pseudonym to the dispatching center. The request that is sent to the dispatching center specifies the task and additional information (such as time slot, preferred caregivers or undesired ones). The dispatching center checks the schedules of caregivers, their preferences and qualifications and chooses one of them. A request is sent to the chosen caregiver and the response is awaited. The trusted device may provide the contact information to an appropriate system module that sends the request, or the request is delivered to a local mail box, where the caregiver can retrieve his or her assignment. Some caregivers such as organizations can be self-scheduling. They receive tasks and make a schedule for their personnel.

If an alert is raised and a caregiver needs to respond promptly, the system notifies the caregiver about the problem and the patient's identity and contact information. After detecting an alert, the base station sends this data encrypted with the public key of a trusted device to the dispatching center. If the caregiver is logged in the system and can receive the notification on-line, the trusted device is requested to re-encrypt all the information with the public key of the chosen caregiver. In order to prevent attacks, the caregiver's pseudonym sent in the request needs to be signed by the patient and linked to the current time or a fresh nonce, to prevent replay, so the trusted device can verify that the request for re-encryption is valid. It also verifies that the given public key of the caregiver indeed belongs to a specified caregiver's pseudonym, with an appropriate certificate. If, however, the caregiver needs to be contacted using other means, such as an SMS, it is assumed that decryption on his or her side is not possible. Therefore, the trusted device will decrypt and relay the alert message and the phone number of the caregiver to a calling module. This information is encrypted with a key that is embedded in the calling module (through white box cryptography[1]) and will be deleted immediately after sending, so that an attacker would not be able to capture this data.

[1] The private encryption key is hidden in the cryptographic software using obfuscation.

4.5 Handling caregivers' requests

A caregiver who wishes to access medical data in the base station, sends a request to the dispatching center. In order to prove its freshness, the caregiver incorporates the current date and time in the request, or a challenge-response protocol is used between the dispatching center and the caregiver. If the verification succeeds, the dispatching center checks the caregiver's role and accordingly decides whether this request can be relayed to the base station. Some roles, such as catering or cleaning service, are never allowed access to patient's medical data. Upon reception of the request, the base station verifies that the request is fresh, checks the pseudonym and decides whether to grant access according to the patient's policies. If the request is confirmed, all the data sent to the caregiver is encrypted with his or her public key, so that it cannot be decrypted in the dispatching center.

4.6 Handling emergency situations

The monitoring equipment installed at the patient's home allows automatic detection of alert or emergency situations. The thresholds or normal boundaries for measured health parameters are usually specified by patient's general practitioner or specialist. Some sensors can be sophisticated enough to detect anomalies, while other simply send their measurements to the base station which performs the assessment. If a health parameter surpasses a threshold, or if the patient requests for help using the hand-held device, or in case a fall is detected, then the system starts a set of predefined steps for handling alerts. The patient's policies determine how the alerts need to be handled. They are composed by the caregivers, patients and/or their guardians.

As an example, a fall of the patient can be observed. When the fall detector records a fall, this information is sent to the base station. If the policies specify so, the patient is signalled via his or her hand-held unit that an alert was detected and is given a chance to cancel the alert. If the patient does so, the system cancels the alert, but performs an additional check after some time by prompting the patient about his or her condition. If, however, the patient does not reply or requests for help via the personal device, a caregiver will be alerted. Since the base station records all the policies, it will determine which caregiver needs to be notified. The pseudonym of the chosen caregiver and the alert message encrypted with trusted device's public key are sent to the dispatching center. The dispatching center checks the validity of the request (see Sect. 4.4) and relays the message together with the encrypted contact information of the caregiver to the trusted device. The trusted device performs the verifications and decrypts and relays the message and the phone number to the calling module. The calling module will use the number and send the message. The base station records the time in which the response from the caregiver is expected, so it can alert another caregiver if the response is not received or the caregiver states that he or she is unable to assist the patient.

In order to protect this privacy-sensitive information, some additional mechanisms need to be employed. A mechanism is needed to prevent any software changes at the dispatching center, so that checks are eliminated or that these messages and phone numbers are continuously recorded. Since an attacker is assumed not to have complete control over the system and is not able to follow the data flows inside the system, the linking identifying information and leakage of private data can be considered highly unlikely.

4.7 Billing

The patients registered in the system will need to pay a monthly fee for the dispatching center's services and possibly an additional amount for the equipment installation and initialization. Payments are handled by the administration center. As it stores the encryption of the identity, contact and service level agreement information for every patient, it would be able to access this relevant information monthly and create a bill that is sent to the patient.

On the other hand, payment to the caregivers should be performed directly. Monthly fees may depend on the used services and revealing the invoices to the system could be used to deduce some private information. Therefore, these payments should not be mediated by the system. Moreover, the caregivers already know the patients that use their services, so there will be no additional information disclosure.

5 Evaluation

In order to protect the privacy in the system, the dispatching center only knows users' pseudonyms and is not aware of their real identities. In addition, the exchange of data between patients and caregivers is performed using public key encryption. The initial communication between patients and caregivers is performed via email and is not mediated by the dispatching center, so the authenticity is ensured. All the subsequent communication can be performed over the dispatching center which is not able to see the data passing by, because it is encrypted with users' public keys.

A possible attack to users' privacy is breaking into the database of the dispatching center. However, due to the use of pseudonyms and encrypted storage of identifying data, the attacker would not be able to obtain any relevant data. Additionally, since the caregivers belonging to different networks have different pseudonyms in each of them, leakage of information about one network would not reveal any information about other networks.

An attacker can also try to join a patient's care network posing as a certain caregiver. Even if he or she obtains a valid access code issued for the patient, the patient needs to confirm the connection after being presented with the caregiver's real identity. Since an attacker cannot obtain an anonymous credential of a caregiver, this attack will not succeed, as the user can see that an intruder is trying to connect with him or her. An attacker can also try to plant his or her

own public key in place of a public key of an authorized caregiver to whom some private information needs to be re-encrypted and sent by the trusted device. However, the trusted device first checks the pseudonym of the caregiver in the signed request from the base station, verifies that it is linked to the given public key in a certificate and only then performs the re-encryption. Therefore, this kind of attack is also countered. The medical or monitoring data is only available to authorized caregivers, even though it is sent to them via the dispatching center. Due to encryption with the authorized caregiver's public key, it is not readable by any other party, even staff of the dispatching center.

Finally, an important property of the system is that even though the users' identities are protected, if a misuse is detected, it would be possible to identify the perpetrator by an external trusted party using logged data.

6 Conclusions

In this paper we have described a pervasive eHealth system providing care for the elderly or stay-at-home patients. Our focus was on the privacy preserving mechanisms that would allow this system to handle sensitive medical data of users in a secure and private way. This system also allows the users to control the access to their medical data by utilizing dynamic privacy policies. Another important feature of this system is openness, or seamless integration of new patients, caregivers or service providers in the system. Furthermore, different sensors can be added to the home monitoring system. In addition, the architecture circumvents the need for employing medical personnel at the dispatching center, as this is an important impediment for its commercial deployment.

Acknowledgement

This research is partially funded by the Interuniversity Attraction Poles Programme Belgian State, Belgian Science Policy, Belgian Fundamental Research on Cryptology and Information Security (BCRYPT), and by the IWT-SBO project (DiCoMas) "Distributed Collaboration using Multi-Agent System Architectures".

References

1. M. Boulos, A. Rocha, A. Martins, M. Vicente, A. Bolz, R. Feld, I. Tchoudovski, M. Braecklein, J. Nelson, G. O Laighin, C. Sdogati, F. Cesaroni, M. Antomarini, A. Jobes, and M. Kinirons. Caalyx: a new generation of location-based services in healthcare. *International Journal of Health Geographics*, 6(1):9, 2007.
2. R. Chakravorty. A programmable service architecture for mobile medical care. In *Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, PERCOMW '06, pages 532–, Washington, DC, USA, 2006. IEEE Computer Society.

3. J. Corchado, J. Bajo, D. Tapia, and A. Abraham. Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare. *Information Technology in Biomedicine, IEEE Transactions on*, 14(2):234 –240, march 2010.
4. E. Jovanov, D. Raskovic, J. Price, J. Chapman, A. Moore, and A. Krishnamurthy. Patient monitoring using personal area networks of wireless intelligent sensors. *Biomedical Sciences Instrumentation*, 37:2001, 2001.
5. H. Kim, B. Jarochowski, and D. Ryu. A proposal for a home-based health monitoring system for the elderly or disabled. In *Computers Helping People with Special Needs*, Lecture Notes in Computer Science. 2006.
6. B. P. L. Lo, J. L. Wang, and G. zhong Yang. From imaging networks to behavior profiling: Ubiquitous sensing for managed homecare of the elderly. In *Adjunct Proceedings of the 3rd International Conference on Pervasive Computing*, 2005.
7. M. Milutinovic, K. Decroix, V. Naessens, and B. De Decker. Commercial home assistance (ehealth) services. LNCS 7039, pages 28–42, Luzern, CH, June 2011. IFIP International Federation for Information Processing, Springer Verlag.
8. A. Rodriguez-Molinero, A. Catala, M. Diaz, J. Rodriguez, E. Fernandez de la Puente, A. Tabuenca, J. Jose De la Cruz, A. Yuste, L. Narvaiza, and the CAALYX consortium. Caalyx: Evidence-based selection of health sensors for elderly telemonitoring. In *Proceedings of the 6th Conference of the International Society for Gerontechnology*, June 2008.
9. A. Sarela, I. Korhonen, J. Lotjonen, M. Sola, and M. Myllymaki. Ist vivago reg; - an intelligent social and remote wellness monitoring system for the elderly. In *Information Technology Applications in Biomedicine, 2003.*, april 2003.
10. A. M. Tabar, A. Keshavarz, and H. Aghajan. Smart home care network using sensor fusion and distributed vision-based reasoning. In *Proceedings of the 4th ACM international workshop on Video surveillance and sensor networks*, VSSN '06, pages 145–154, New York, NY, USA, 2006. ACM.
11. U. Varshney. Pervasive healthcare and wireless health monitoring. *Mob. Netw. Appl.*, 12:113–127, March 2007.