Commercial Home Assistance (eHealth) Services

Milica Milutinovic, Koen Decroix, Vincent Naessens, Bart Decker

Commercial Home Assistance (eHealth) Services

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

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

Abstract. In this paper, we describe the software architecture of a commercially run home assistance system that allows patients or elderly people to stay longer at home. Since such systems often have to handle sensitive medical information, the protection of the privacy is a major concern. Also, legislation often restricts access to health information to qualified persons (i.e. medical personnel), who are not always available in a commercial company.
The home assistance system can offer several services, going from scheduling necessary tasks and following up their execution, to monitoring the patient's health status and responding promptly to requests for help or to emergency situations, and all this without the need to maintain personal medical data or identifying information in the home assistance center.
This paper focusses on how the commercial home assistance center will keep track of the anonymized patients' networks. A network consists of all the caregivers of a patient; each member of the network has been assigned a role, which is used in course-grained authorization decisions. The protocols involve anonymous credentials for the caregivers and smartcards for patients.

Keywords: eHealth, privacy, caregiver, commercial

1 Introduction

The average life expectancy in the Western world has risen well above 80 years. Also, the limited birth rate has resulted in a greying population and caused the population pyramid to flip upside down or at least to become more cube-like. The progress of medicine has made many diseases and disorders curable or at least less life-threatening. However, the downside of this evolution is that the government's social security budget needs to expand year after year and may grow faster than the country's economic growth. One way to cut costs is to have elderly people stay at their homes much longer instead of moving them to nursing homes and dismiss patients sooner from hospitals. However, these elderly people or patients often need extra care or have to be followed-up from time to time or monitored continuously. Luckily, technology can fulfill these needs.

There are many initiatives for designing and building such advanced home assistance centers. Often, hospitals are involved since they have skilled employees who are qualified to handle medical data and to make the correct assessments. However, hospitals are not the best players to run these home assistance centers. They often lack the technicians who are necessary to install and maintain the necessary equipment on a large scale. Moreover, these assistance centers should also offer support for non-medical services such as catering, cleaning, shopping, etc. These services are already provided by specialized organizations or companies. Hence, it is very likely that in the near future commercial businesses will start to operate home assistance centers. There is one important impediment for a commercial deployment, however. Many countries have legislations that limit the access to medical data to qualified personnel (e.g. doctors, paramedics, etc.). That means that if the home assistance centers (HACs) have to process medical data, they also have to employ medical personnel. Also, home assistance systems are by definition distributed systems (part of the system is deployed at the patient's home and part at the center) with many access points, which makes it much harder to restrict access to sensitive (medical or health) data. Therefore, the system should preferably be designed in such a way that HACs never see or process such data.

Protecting the privacy of the elderly person or patient is of utmost importance. Even when the patient's medical data is properly protected, information about the patient's health could be indirectly deduced if one knows which specialist is treating the patient (e.g. when the doctor in attendance is an oncologist, one can easily deduce that the patient suffers from cancer). Therefore, not only the medical data needs to be protected, but also the patient's social network should remain hidden as much as possible. We have seen in the past many cases of accidental or deliberate leakage of privacy sensitive information; often because of the loss or theft of storage media or laptops. Hence, the system should avoid to store as much as possible identifying information about patients, doctors, etc. On the other hand, in case of an alert or emergency situation, the appropriate caregiver needs to be notified as soon as possible.

In this paper we propose a novel system architecture aiming to fulfil the requirements mentioned above. We give an in-depth overview of the system and evaluate functional requirements. We also focus on organizing the network of patient's caregivers. The protocols that lead to improved privacy compared to existing systems are discussed in detail.

The rest of this paper is organized as follows. Sect. 2 describes the architecture of the system, the functional requirements and the patient's social network. In Sect. 3 the security and privacy requirements are listed and the attacker model is discussed. Sect. 4 gives an overview of the protocols used by the system to protect the patients' privacy. Sect. 5 evaluates the design and Sect. 6 gives an overview of related work. Concluding remarks and future work are given in Sect. 7.

2 Functional description of the system

The home assistance system offers different services which patients can subscribe to. For a system providing pervasive care, services offered to the patient should include:

- **Monitoring the health status** of a patient. Depending on the patient's requirements, a network of different sensors can be deployed in his household. It has a task of monitoring different health parameters of the patient, such as blood pressure, heartbeat rate or pulse oximetry, detecting falls, or monitoring environmental parameters, such as temperature or humidity. In addition, each patient should have a hand-held control unit that would allow him to indicate emergencies, request for help/advice or cancel an alarm. The device can further be equipped with a speaker and a microphone in order to allow for a conversation between the patient and a caregiver and to provide the patient with an automatic reminder or advice.
- **Scheduling and following up on tasks** that need to be performed by the patient's caregivers. Those include both daily tasks, such as catering, cleaning or scheduled visits, but also help in emergency situations. Tasks that are assigned are dynamic and patients or their guardians can always enter new tasks, remove or modify the existing ones. For every task, minimal skills may be required (e.g. medical expertise), a time frame within which the task should be performed may be defined, and a set of preferences regarding caregivers may be suggested. The tasks are assigned via the home assistance center (HAC) that makes a schedule according to the caregivers' availability, skills and preferences. It also supports last-minute changes and immediate substitutes for caregivers not able to perform an assigned task in a timely manner.

  As explained in the introduction, this service is often performed by the patient's close relatives. However, since the number of single persons are growing, chances are that no family members are available to coordinate this service.
- **Choice of services** should be provided to the patients by the HAC. All organizations may publish their services through the system, so that patients can anonymously browse through the database in order to choose appropriate service providers. The payment for the services can be made directly to the organizations or through the home assistance system which would subsequently charge the patient.
- **Remote access to patient's health information** is a service provided to the caregivers. Authorized caregivers should be able to access the sensor readings remotely in order to assess them. Patient's policies would govern the access control for this service.
- **Privacy-protected social networks** are meant to organize self-help groups for the patients. They would allow exchange of information between patients with similar illnesses, but also medical personnel specialized in the particular field. This service would help the patients reducing their solitude or providing

information relevant to them. All users should be able to stay anaonymous, while strict access control needs to be imposed in order to make sure that only authorized individuals can communicate with their peers.

It is clear that the patient's caregivers are not only individuals, such as relatives or neighbours, but organizations can also be integrated into the system in order to offer a wider range of services to the patient. Examples are businesses providing catering or cleaning, but also medical institutions – hospitals or organizations offering nursing services.

2.1 The patient's social network

The home assistance center handles scheduling of tasks to the patient's caregivers and mediates communication between them. Therefore, it needs to maintain all the patient-caregiver connections. The connections are represented by *patients' social networks*. These networks are patient-centric and all the caregivers belonging to a network are assigned a role, such as relative, neighbour, GP, specialist, etc. Roles are assigned by the patients and are used for coarse grained access control in the home assistance center. In order to prevent misuse, caregivers need to provide proof of their expertise in order to have certain roles assigned to them. Examples are roles of medically trained caregivers.

In order to preserve privacy in the system, all users, both patients and caregivers, need to be pseudonymous in the network. Therefore, all the information that is handled in the system can only be linked to the pseudonyms and no identifying information would be available to unauthorized parties.

2.2 System architecture

The system functionalities are separated into several entities, as shown in Fig. 1.

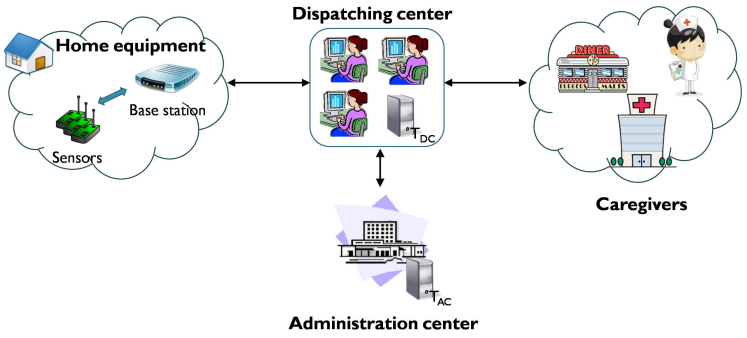

Fig. 1. The global architecture.

In order to provide services to the patient, a *base station* is installed at the patient's home. It acts as a gateway towards the rest of the system and stores and controls access to patient's data. It also records the patient's dynamic privacy policies. All the recordings of the sensor network, including the signals from the fall detector and the hand-held control unit are sent to the base station, where they are assessed (Fig. 2). As a result of the assessment, the base station can request a caregiver's intervention or start an automatic task. The base station also controls a door system that allows authorized caregiver to enter the patient's house, thereby circumventing the need for distributing physical keys, which cannot be easily controlled or revoked. Authorization to enter the patient's home is represented by access tokens assigned to caregivers and can be provided or revoked dynamically. They are also characterized by a time slot in which they can be used.

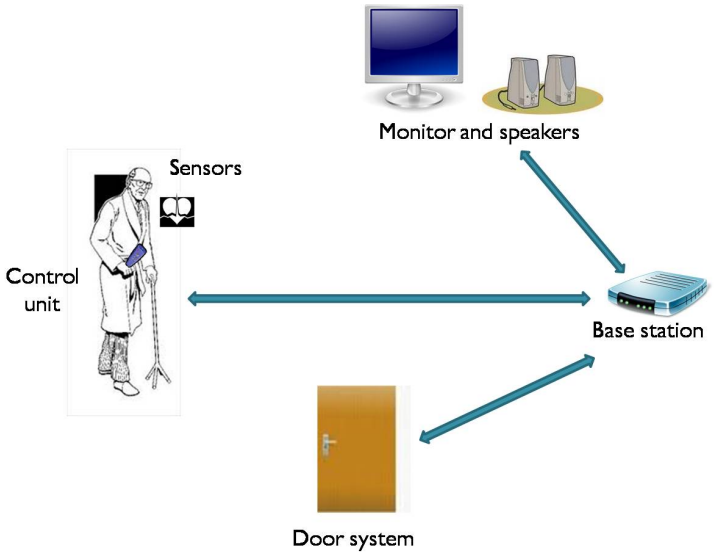

Fig. 2. Patient's home equipment.

All the communication between the base system and the caregivers is mediated by a *dispatching center* (DC). The center is therefore responsible for maintaining the anonymized networks of patient's caregivers, assigning and/or scheduling tasks, monitoring the proper working of the base stations, notifying caregivers in case of alert or emergency situations and following up on their responses, providing authorized caregivers with access tokens for the door system, exercising (course-grained) access control to the resources controlled by the base stations, and collecting and archiving evidence of actions taken by the DC. Be-

cause it does not have access to medical data of the patient, it does not need to employ medically trained personnel.

Finally, a separate entity, namely the *administration center* (AC), handles all the administration tasks, such as registration of users, invoicing or receiving payments. This separation of functionality allows the system to be privacy-friendly and circumvents the need to keep identifying information about the users in the dispatching center and allows anonymization of patient's connections.

Trusted devices are also a part of the system architecture. They need to be deployed in the dispatching (T_{DC}) and the administration center (T_{AC}). They perform conversion of encrypted data into data encrypted with another key, or provide (part of) the encrypted plaintext under certain conditions. Examples are re-encrypting the patient's address information with a public key of an authorized caregiver who needs to assist the patient or decrypting the patient's identity in case of a misuse. However, before performing these actions, the trusted devices perform predefined checks in order to detect attacks and prevent unauthorized parties from obtaining patient's private information.

2.3 Functional requirements

System's functional requirements can be defined according to the overview of the offered services presented above.

1. The system should provide the *scheduling of tasks*.
   - In order to create schedules for patient's caregivers, it should maintain all the connections between patients and their caregivers.
   - The system should keep a profile for each caregiver stating his qualifications, willingness to perform certain tasks and availability.
   - According to the available information, the system should be able to assign regular or one-time tasks to the members of the patient's social network and make up a schedule according to the caregivers' stated availability. In addition, some members, such as organizations, should be self-scheduling. They should be able to assign the received tasks to their personnel themselves.
   - Another very important property, is timely response to last-minute changes. An example is a caregiver that cannot keep an appointment, so that the system needs to assign the task to another caregiver, or – in the worst case – notify a close relative or neighbour.
2. The system should support *continuous monitoring* and *communication* with the patient.
   - The system should be able to interface with different sensors, such as a fall detector, heatbeat sensor or motion sensor. Some sensors may be sophisticated and able to detect anomalies (e.g. exceeding a threshold) and raise an alarm; others may merely measure body parameters and send these measurements to the base station at regular intervals, where they will be assessed by special tasks.

- The assessments performed by the system should be dynamic. They can be pre-defined, or performed on-demand. Demanding computations could also be performed remotely, e.g. on hospital computers.
- According to the assessment results, the system should be able to raise alerts and report emergencies. Some actions could be pre-defined and automatically executed. Examples are playing a prerecorded advice to the patient or notifying caregivers.
- Communication means, such as a microphone and a speaker should be available (possibly incorporated in the control unit) so that verbal communication is possible.
- Video cameras installed in different rooms of the patient's house allow for assessing the situation when the patient does no longer respond to stimuli from the system. Access to the video stream requires strict access control.
- All the above communication means should be easy to handle and have a simple interface.

3. The system should provide *flexible access control*.
   - The patients should be able to define privacy policies that control the access to the sensor data. Authorized caregivers would be able to see and assess the sensor measurements. Some caregivers should also be allowed to specify automatic actions to be performed and conditions for their initiation. Examples are setting thresholds for sensor measurements and defining tasks to be performed in case of detected problems.
   - Flexible access control to the patient's home should also be provided by the system. Since different caregivers may need access to the patient's home, using physical keys is not desirable. Not only many copies of the same key are necessary, but they also give the bearer the possibility to enter the house at any time. Moreover, some services (such as nursing, catering, cleaning) are offered by organizations that may not always send the same caregiver to the patient. Therefore, virtual keys (or access tokens) are preferable. They provide more fine-grained access control, as the validity can be limited to a specific time interval and they can be dynamically provided or revoked.

3 Security and privacy requirements

As the system handles personal medical data, which is exceptionally privacy sensitive, the following requirements need to be fulfilled:

- Only authorized individuals, such as medical personnel or explicitly authorized caregivers of a patient, should be able to *access the personal medical data*. Even more so, since legislation in many countries imposes this rule. Therefore, strict access control must be provided.
- The patient's *network* should be *anonymized*. This requirement arizes from the fact that knowledge of some of the caregivers of a patient's network

sometimes allows one to deduce the illness the patient suffers from. It will not be possible to hide everything, though. In general, one cannot hide that someone has health problems or needs permanent care, since passers-by may notice and recognize caregivers who enter or leave the patient's house. However, the amount of deduced information should be limited. If someone gets hold of the database of the patients' networks, because of a deliberate leak by a disgruntled employee or a break-in into the system, he should not be able to learn privacy-sensitive information.

– Actions that are performed in the system should be *logged*, and treated as extremely *confidential*. Except to a trusted (external) party in case of disputes, these logs should not be accessible to anyone. If such logs are necessary to check the proper working of the system, then they should be anonymized previously.

3.1 Attacker's model

There are three kinds of attackers the system should be secure against, differing in their roles in the system and authorizations:

The first kind of attacker is an **entity external to the system**. They do not have authorized access to any data handled by the system and can try to acquire information by passive observation, but can also illegally break into the system. Deducing any private information should not be possible for them.

Another kind of attacker is a **caregiver** who belongs to one or more patient's networks. A distinction needs to be made between medical professionals and other caregivers, since the former typically have access to the medical data of the patient. However, they are bound by a duty of professional confidentiality. On the other hand, non-medical caregivers without special authorization should never get access to the patient's medical data. Moreover, the system should only allow access to medical professionals that belong to the patient's social network.

Finally, another kind of attackers are **employees** of the home assistance center. Clearly, since they have to install the system at the patient's house and keep it running, they already have some background information that others do not have (e.g. they know which sensors are being used by which patient). However, the system should not provide them with more information than necessary, namely what they learned at the patient's house. Medical data –if kept at the home assistance center– should not be readable to employees. That requires its encryption with a key which employees cannot obtain. Also connections between patients and their caregivers should be anonymized. In order to limit the information that can be deduced by observing the available data about connections – the companies and individuals that belong to several patient's networks are represented by different pseudonym in each network. Hence, indiscretions about one network do not reveal anything about other networks. As a consequence of the listed requirements, disclosing the complete network database would not reveal more than a set of random numbers associated with general attributes, such as roles and rights.

It is, however, difficult to prevent the employees from learning some information by observing the system (e.g. the mobile phone number of the patient's GP), since the system may need to contact a caregiver and his phone number would need to be provided to a dialing device. Therefore, the design of the system should make it extremely difficult to link these phone numbers to pseudonyms of the networks.

In short, the employees should not be able to modify the data in the system or tamper with the software so that programmed checks are eliminated or that identifying data (such as phone numbers or email addresses), which may be temporarily kept in volatile memory is continuously recorded.

4 System protocols

In this section we describe the protocols for user registration, the creation and extension of patients' social networks.

4.1 User registration

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

Patients subscribe to a certain set of services offered by the home assistance center, and possibly sign a contract with a service provider. A Service Level Agreement (SLA), listing the subscribed services and the conditions, will be agreed upon. The users also prove their identity and contact information (possibly with their eID card), so that the administration center can personalize and issue a new *patient smart card* (SC_{PT}). The patient's identity, address information and SLA are stored on the card, which will generate a new pseudonym (Nym_{PT}) and two new key pairs (SK^i_{PT}, PK^i_{PT}), (i = enc or sig), one to be used for encryption/decryption, the other for signing/verification. The administration center certifies the public keys PK^i_{PT} and the certificates are stored on the card during personalization. Every patient card will also have a public key of the trusted devices running in the dispatching and the administration center.

All issued cards will share a common authentication key pair (SK_{co}, PK_{co}) (cfr. also [15] for the rationale behind this privacy–friendly identity card). The card is necessary to authenticate the base station towards the dispatching center and the caregivers, and to sign or decrypt information. Hence, the base station will only run as long as the $SC_{PT}$is inserted in the card reader.

After patient registration, the administration center stores the patient's pseudonym, certificates, SLA and the encrypted patient's identity and address information (encryption is done with the public key of T_{AC}; see further). The home equipment can then be installed at the patient's home.

Individual caregivers, such as relatives, neighbours or self-employed doctors, often perform registration after being invited to join the network of a patient. As patients, caregivers need to provide proof of identity and address (contact) information. That can be done using their eID card. Also, medically trained

caregivers would need to provide signed qualifications in order to be allowed to assume such roles in patient's networks. For verification of contact information, the administration center would send an authentication code to each address and expect for it to be returned within a limited time interval. The caregiver can then generate and send to the administration center a pseudonym (Nym_{CG}) and a commitment ($Comm_{CG}$) to a secret, random number ($Rand_{CG}$). In return, the caregiver is issued an anonymous credential ($Cred_{CG}^{anon}$) certifying the pseudonym, identity, qualifications, contact information and the committed random value.

After the registration, the administration center records the caregiver's pseudonym, along with all the identifying information encrypted with the public key of the trusted device.

Organizations offering paid services to the patients do not need to be anonymous in the system. They can register with the administration center disclosing their identity, contact information, certified public key (PK_O^{enc}) and list of offered services. If the registration is accepted, the organization can send a commitment ($Comm_O$) to a random value $Rand_O$. An anonymous credential is then issued to the organization certifying the exchanged information.

The administration center will record the identity of organization and related information, so that the patients can browse through the database and choose an appropriate organization.

4.2 Creation of the patients' network

When a base station has been installed at the patient's home, he can initiate connections with his caregivers and the creation of his social network. This is depicted in Fig. 3. Firstly, mutual authentication is performed between the patient and the dispatching center. Authentication of the patient is anonymous and is done using the patient's smart card (SC_{PT}) and the common authentication key pair (SK_{co}, PK_{co}). After a successful authentication, an end-to-end secure (SSL) channel is created between the base station and the dispatching center. The patient's pseudonym, public key certificate, SLA and a vault containing his pseudonym, identity and address information (encrypted with the T_{DC}'s public key) is sent over this channel. Since the patient's card is trusted, the contents of the vault is assumed to be correct.

In the dispatching center's database a new network is created, consisting of one node characterized by the patient's pseudonym, certificate (binding his pseudonym to his public encryption key PK_{PT}^{enc}), SLA and a vault with encrypted identity and address information.

4.3 Extension of the patients' networks

If a patient wishes for a specific caregiver to join his network, he needs to send him a specific request. All connections are initiated by patients and if a caregiver responds positively to the request, the patient is presented with his real identity, so he can verify that the connection was established with the intended individual.

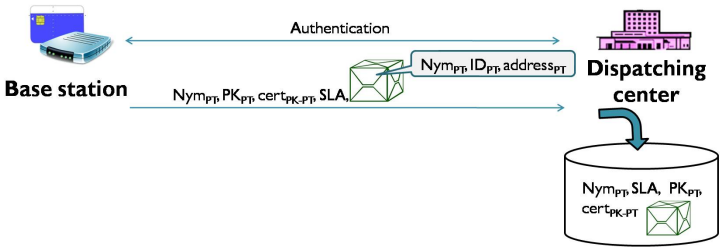

Fig. 3. Creation of the patient's network.

This is important to make sure that an unauthorized person cannot pose as a legitimate caregiver and endanger the patient's privacy. The protocol describing the extension of patient's network is depicted in Fig. 4.

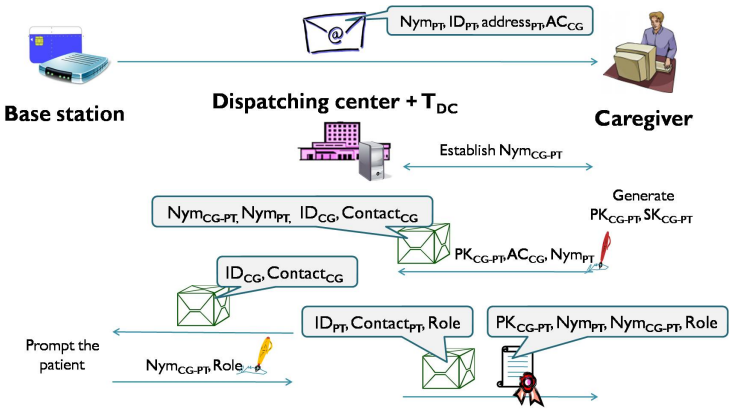

Fig. 4. Extending the patient's network.

Initially, the patient will contact the dispatching center and request *access codes* in order to connect to his caregivers. Fresh access codes are generated and issued to the patient, but a fingerprint and validity period of every access code is recorded and linked with the patient's pseudonym.

After obtaining access codes, the patient can send a connection request to a desired caregiver. That request contains patient's identity, pseudonym, address, access code, and possibly additional information and can be sent to the caregiver via email. It is assumed that the patient does not hold caregiver's certified public key, and therefore, the information that he sends in the request is encrypted with a known public key of an applet used by the caregivers.

This applet is used at the caregiver's side, when he wants to respond by accepting the request for connection. When the caregiver starts the applet, it first loads the data received via email and the caregiver's anonyous credential. Note that if the caregiver is not yet registered with the administration center, he would need to perform that step in order to connect to the patient. In the next step, the applet establishes a new pseudonym Nym_{CG-PT} with the dispatching center, using the patient's pseudonym $Nym_{PT}$and the random number contained in the credential ($Rand_{CG}$). That allows the caregiver to subsequently prove possession of the pseudonym, by proving that it was properly generated using data contained in his credential. Next, the applet generates a new key pair (SK_{CG-PT}, PK_{CG-PT}) and verifiably encrypts the new pseudonum, the patient's pseudonym and the caregiver's identity and contact information with the public key of a trusted device T_{DC}. It also signs this information, together with the patient's pseudonym, the public key PK_{CG-PT}, and access code (AC_{CG}) with the caregiver's anonymous credential, thereby proving that the Nym_{CG-PT} was correctly generated and that the verifiably encrypted information contains the corresponding values from the credential (i.e. identity and contact information is correct). The dispatching center verifies the signature and the proofs mentioned above and checks the validity of the access code. If all the checks pass, the access code is marked invalid and the public key and the encrypted information are stored with the new pseudonym Nym_{CG-PT}.

In the next step, all the exchanged information is given to the trusted device T_{DC}, together with the certificate linking the patient's public key and his pseudonym. The trusted device performs the same checks in addition to which it checks whether the pseudonyms in the certificate and the encrypted vault are the same. If all the checks pass, the trusted device re-encrypts the caregiver's pseudonym, identity and contact information from the vault with the public key of the patient, PK_{PT}^{enc}. This vault is sent to the patient and decrypted by the SC_{PT}. The patient is then presented with the caregiver's identity, so he can confirm the connection and assign a role to the caregiver. This confirmation is sent to the dispatching center as a signature on the caregiver's pseudonym and the new role.

After receiving the confirmation, the dispatching center records the new caregiver's pseudonym as a permanent node in the patient's network and the trusted device will generate a certificate confirming membership (with a certain role) of the patient's network. It also prepares a vault with the patient's identity, which is sent to the caregiver (for verification).

In case the caregiver is a registered organization, the protocol slightly differs, as the user can obtain its certified public key and the initial request can be encrypted using that key.

5 Evaluation

In this section, we investigate the security and privacy properties of the system and protection against the different types of attackers described above.

The first requirement in this system is that unauthorized individuals should never have access to the medical data of a patient. Since neither the dispatching, nor the administration center store any medical data of patients, employees or attackers breaking into the system cannot see any private health information. In addition, any party accessing patient's data in the base station is authenticated and authorizations are checked. The patient or his guardian can specify policies defining the authorizations of different caregivers or roles.

However, indirect information can also lead to unintentional disclosure of private information. For instance, knowing a specialist who treats a patient can be used to deduce the illness of the patient. However, the patient's networks are anonymized and all identifying information is not readable at the dispatching or the administration center, in order to counter these risks. Moreover, caregivers belonging to different patient's networks are assigned different pseudonyms in each network, ensuring that indiscretions about one network do not reveal information about other networks.

It is also not possible for an attacker with access to the dispatching center data to try to infiltrate into a patient's network, since every patient is presented with the real identity of the caregiver before confirming the connection. An attacker that is not a patient's caregiver could try to plant his own public key to the trusted device in order to have some secret patient's data re-encrypted with this public key. However, the trusted device performs sufficient checks, as explained in Sec. 4, which prevents this attack.

Finally, actions that are performed in the system should be logged. It is required to keep all the logging information confidential. Indeed, the dispatching center will sometimes send text messages or emails to caregivers. Hence, phone numbers or address information used need to be kept confidential. This can be fulfilled by encrypting all logging information with the public key of an external trusted third party. Also, trusted devices log their actions for later auditing.

6 Related work

There is a significant body of research focusing on eHealth systems for providing care in the patient's household. Most research initiatives in this area focus on the remote monitoring service that allows supervising the patient's health status. However, security and privacy problems in these systems are not fully tackled.

The research in this field typically assumes a three-tier system architecture. Patient monitoring can be bootstrapped using sensors that measure physiological parameters such as EEG, ECG or GSR, or environmental parameters such as temperature and humidity. Furthermore, system can incorporate sensors detecting user indicated alarms [12]. Video monitoring was also explored for deployment in these systems, as it allows communication with caregivers [5], but also fall detection [13] and movement, posture and gait analysis [10]. Sensors performing health monitoring can be deployed as a personal area network [7] or can be integrated in a single device [2]. Desirable types of monitoring sensors were investigated in [11].

Proposed systems also incorporate a personal server, used to gather data recorded by the sensors. The collected data is then sent to a remote care center for assessment [3] [8] [6]. Recorded data can also be forwarded to another predefined care provider. Although relaying the data to a central station assures greater resources for data analysis, if all the tasks are performed in the central station, the patient has no substantial control over the disclosed information and services that are deployed.

Other research initiatives consider interoperability in these systems. [4] proposes a novel architecture in order to tackle cross-context identity management in eHealth systems with the goal to improve interoperability between providers. Interoperability between relevant standards, namely HL7 and IEEE 1451 standard was explored in [9]. HL7 is a messaging standard for exchanging medical information and IEEE 1451 standard deals with various aspects of sensors, the format of data sheets and how to connect and disconnect the sensors from a system. This work is complementary with our proposal, as these standards can also be used for information exchange in our architecture.

Importance of security and privacy in these systems is widely recognized [1], [14], but research proposals do not solve those issues fully. Reliability is another important requirement, that needs to be tackled.

7 Conclusion and Future work

In this paper we propose a novel architecture for a home assistance system, providing care for the elderly or stay-at-home patients. Offered services of this pervasive system include continuous monitoring of patients, scheduling of patient-requested tasks to their caregivers, follow-up on the responses, help in emergency situations and remote access to the patient's data to authorized caregivers. This approach allows the system to be run by a commercial organization without the need to employ medically trained personnel. It is designed in such a way that the home assistance center cannot access patients' medical data. Instead, it maintains patients' anonymous networks and only mediates communication between patients and their caregivers. Protocols employed in the system, that lead to improved privacy and patient's control over his data, are described in detail.

Another important feature of this approach is openness of the system. New users, caregivers and even services and service providers can easily and seamlessly be integrated into the system.

A possible extension of the system are anonymous self-help groups that would allow the patients to anonymously communicate with their peers with similar health conditions. Strict admission procedures would be employed.

Acknowledgement

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

References

1. Health Insurance Portability and Accountability Act (HIPAA). http://www.hhs.gov/ocr/privacy/.
2. M. N. K. Boulos, A. Rocha, A. Martins, M. E. Vicente, A. Bolz, R. Feld, I. Tchoudovski, M. Braecklein, J. Nelson, G. . 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, 2007.
3. 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, 2006.
4. M. Deng, D. D. Cock, and B. Preneel. An interoperable cross-context architecture to manage distributed personal e-health information. In M. M. Cunha, R. Simoes, and A. Tavares, editors, *Handbook of Research on Developments in e-Health and Telemedicine: Technological and Social Perspectives*, chapter 27, pages 576–602. Hershey, PA, USA: IGI Global, Inc., 2009.
5. B. Johnston, L. Weeler, J. Deuser, and K. H. Sousa. Outcomes of the kaiser permanente telehome health research project. In *Arch Fam Med. 2000;9(1)*, pages 40–45.
6. E. Jovanov, A. Milenkovic, C. Otto, and P. de Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and Rehabilitation*, 2(1):6, 2005.
7. 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.
8. 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*, volume 4061 of *Lecture Notes in Computer Science*, pages 473–479. Springer Berlin / Heidelberg, 2006.
9. W. Kim, S. Lim, J. Ahn, J. Nah, and N. Kim. Integration of ieee 1451 and hl7 exchanging information for patients sensor data. *Journal of Medical Systems*, 34:1033–1041, 2010. 10.1007/s10916-009-9322-5.
10. 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.
11. A. Lymberis. Smart wearables for remote health monitoring, from prevention to rehabilitation: current R&D, future challenges. *4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine 2003*, pages 272–275, 2003.
12. A. Sarela, I. Korhonen, J. Lotjonen, M. Sola, and M. Myllymaki. Ist vivago ®-an intelligent social and remote wellness monitoring system for the elderly. In *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on*, pages 362 – 365, april 2003.

13. 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*.
14. U. Varshney. Pervasive healthcare and wireless health monitoring. *Mob. Netw. Appl.*, 12:113–127, March 2007.
15. J. Vossaert, J. Lapon, P. Verhaeghe, B. De Decker, and V. Naessens. A smart card based solution for user-centric identity management. Aug. 2010. PrimeLife/IFIP Summer School 2010, Helsingborg, 2 - 6 August.