Privacy-Preserving Scheduling Mechanism for eHealth Systems

Milica Milutinovic, Vincent Naessens, Bart Decker

Privacy-Preserving Scheduling Mechanism for eHealth Systems

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

[1] IBBT-DistriNet, KU Leuven, Belgium,
{Milica.Milutinovic,Bart.DeDecker}@cs.kuleuven.be
http://www.cs.kuleuven.be/∼distrinet/
[2] Katholieke Hogeschool Sint-Lieven, Dept. of Industrial Engineering, Belgium
Vincent.Naessens@kahosl.be
http://www.msec.be/

Abstract. In this research, we designed a privacy-preserving scheduling service in eHealth applications. The scheduling service is envisioned as part of a pervasive home assistance system. The mechanisms that we propose protect all sensitive information that is handled by the system, but at the same time allow for a fair distribution of tasks and restricting the task assignment to caregivers with required qualifications. Therefore, this service can be offered by a commercial company without fear for privacy issues.

Keywords: eHealth, scheduling, privacy, fairness, commercial

1 Introduction

The continuous rise of the average age of individuals in the western countries is creating a need to provide some form of home assistance to a growing number of individuals. As an efficient and cost-effective solution, eHealth systems have been brought into the spotlight. The services these systems need to provide include monitoring of health parameters, their automatic assessment or remote access to this data by authorized individuals. Additionally, the patients need to be able to request assistance and these specific tasks should be assigned to their caregivers.

For a pervasive system that handles sensitive patient's data, such as health parameters or contacts with caregivers, one of the most important requirements is privacy protection. Therefore, we have designed privacy-preserving protocols that describe the scheduling service in a pervasive eHealth system. The developed protocols surpass the need to disclose any identifying information to the scheduling service, which allows for a commercial deployment. However, the patients are still able to specify required medical qualifications and their preferences regarding caregivers. The design also ensures a fair distribution of tasks.

2 The system architecture

The scheduling mechanisms are integrated into a pervasive eHealth system. The system provides a range of services, such as monitoring of health related param-

eters, communication of patients and their caregivers (which can be individuals such as a relative, neighbour, GP, or organizations such as a catering or cleaning service) and remote access to the health related data. The architecture of this home assistance system is described in more detail in [1] and a brief overview is given in this section.

The home equipment consists of *wearable sensors* that measure the patient's health parameters and a *base station*, which records these measurements and controls access to them. Next, a remote *dispatch centre* provides technical support and mediates communication for all patients and their caregivers. Finally, an *administration centre* handles user registration and other administrative tasks[3]. Once a patient wishes to start using the services of the system, she would register with the administration centre, have the required equipment installed and obtain a smart card that records her personal information and key pairs for encryption and signing. The caregivers obtain an anonymous credential with their personal information when they register. With the obtained credentials, the users can pseudonymously register with the dispatch centre. The connections between patients and caregivers are also recorded (pseudonymously) at the dispatch centre and are created after mutual agreement of both parties.

3 The scheduling service

The scheduling service allows for a fair allocation of patient-requested tasks to their caregivers, making sure that every task is assigned and confirmed by a caregiver with appropriate qualifications. It also allows the patients to specify the preferred caregivers or undesired ones. Therefore, the scheduling is offered by the system as a service the patients can subscribe to. The scheduling provider can be an external entity that registers with the dispatch centre or the dispatch centre itself. If a patient wishes to use the services of a scheduling provider, it becomes one of the caregivers of her network with an appropriate role.

The base station of every patient maintains a schedule of the caregivers' tasks. For every task, the schedule contains its identifier, the time frame within which it should be performed, other details and the chosen caregiver. Until a caregiver confirms the assignment of a task, it remains conditional. In order to allow the scheduling service to be deployed in the system, caregivers specify their availability and store this information in a profile at the dispatch centre. Their profiles are encrypted with a fresh symmetric key and the key is encrypted along with the patient's and caregiver's pseudonyms with the public key of the trusted device of the dispatch centre. When the scheduling service obtains authorization to access caregivers' profiles in order to assign tasks, the trusted device re-encrypts the symmetric keys with the public key of the service. However, this is performed only after thorough checks.

[3] Both administration and dispatch centre are equipped with trusted devices that are programmed to perform certain tasks, such as re-encrypting data that is stored encrypted with their public keys, with a public key of an authorized party, after verifying the authorizations.

As an example protocol, we will observe the creation of schedules for the caregivers as a response to the patient's request. If one or more tasks need to be assigned, the base station sends a request to the scheduling service via the dispatch centre. For every task, the base station creates a request that contains the specified task, the time frame, the required caregiver's role and/or qualifications and preferred or undesired pseudonyms, and signs it with the patient's smart card. This request is sent via an encrypted link (cfr. [1]). It is then used by the scheduling service to prove its authorization to retrieve the profiles of the concerned caregivers. After verifications, the trusted device of the dispatch centre (TD_{DC}) reveals the profiles' encryption keys to the service, by re-encrypting them with the public key of the scheduling service. If special qualifications are necessary for a task, the service can prompt TD_{DC} whether a particular caregiver has these qualifications. The TD_{DC} will access and check the caregiver's information that is stored encrypted with its public key and reply 'Yes' or 'No'. When the scheduling provider obtains the profiles, it can assign the task, taking into account the required role of the caregiver and patient's preferences. Additionally, along with the initial request, the base station sends to the scheduling service relevant policies which are to be taken into account. Examples are limitation of hours that can be assigned to a role or a caregiver, restrictions on using commercial providers and additional requirements. In order to ensure a fair distribution of tasks, the base station also sends a summary (e.g. total number of hours) of current and past assignments for each of the caregivers. This way, the scheduling service can consider the load that is placed on each of the caregivers.

The assignments are then sent via an encrypted link to the base station. They are stored in the schedule, but remain conditional until a caregiver approves them. The base station also adds to each task some additional data that should be communicated directly to the caregivers. This way the specific information about each task is not revealed to the scheduling service, but is only sent to the caregivers when they retrieve their assignments.

For a detailed description of the protocols of task assignment, retrieval and contacting a caregiver and an evaluation of the complete design we refer the reader to [1].

4 Conclusion

In this research we have designed a scheduling mechanism that can be integrated into a pervasive eHealth system. The focus of the design was preserving privacy of patients, but also their caregivers. Furthermore, the disclosure of information is performed on a need-to-know basis, allowing the service to be offered by a commercial company, which is an important step towards large scale deployment.

References

1. Milica Milutinovic, Vincent Naessens, and Bart De Decker. Privacy-preserving scheduling mechanism for ehealth systems. CW Reports CW618, Department of Computer Science, KU Leuven, March 2012.