Secure Mobile Access to Homecare Patients' Data

Sven Heiberg
Peeter Laud
Cybernetica AS
{sven|peeter}@cyber.ee

Sigurður Másson
Skýrr
sigurdur.masson@skyrr.is

Claus Popp Larsen
Acreo AB
claus.popp.larsen@acreo.se

ABSTRACT

In this paper, we outline a security architecture for the health records of homecare patients and describe its possible implementation using the Android software stack. Our system provides adequate access for the caregivers visiting the patients, while ensuring the confidentiality and integrity of patients' data.

Categories and Subject Descriptors

H.4.3 [**Information Systems Applications**]: Communications Applications

General Terms

Security, Design

Keywords

Android, Homecare, Smart phones

1. INTRODUCTION

The goal of homecare services is to increase the amount of time while older people and patients are still able to live at their homes, as opposed to a nursing facility. The services can be provided by friends and family, but often, for patients living alone, by social or medical workers. These workers may both assist the elderly patient with housekeeping chores, as well as perform simple medical operations.

Quite obviously, the homecare workers need access to patients' medical data, both for reading and updating. Most often, this access has been via *paper notes* that are printed out before the worker departs to visit the patients. Similarly, notes are taken during the visits and entered into the medical information system afterwards. The usage of such an *ad-hoc* system is time-consuming and it cannot be very flexible or follow fine-grained security policies.

Computerizing the access to care information appears to be a good idea — the caregiver is able to obtain the information right in the patient's home and he/she can access the information stored in various information systems, e.g. the the department of social affairs, the hospital, etc. The access to information can be regulated with high precision. The information can be updated on the spot, hence the updates are more accurate. Updating and reading can be interleaved, with the updates influencing the reading policies.

Smartphones constitute a suitable platform for such access of patient information. On the one hand, they are flexible and powerful enough for the required functionality to be effortlessly installed and executed on the device. On the other hand, they are considerably less bulky than laptop or netbook computers, and sport a longer battery life. The continuing decrease of smartphone prices and increase of penetration is also not the least of the considerations. One can expect that in a couple of years, a significant number of caregivers already possess a smartphone, thereby reducing the necessary investment in hardware by the homecare organization.[1]

In this note we describe the architecture — the components and the security measures — of a system enabling the access to care information through smartphones using the Android software stack.[2] We are not aware of any similar systems. So far, we are only aware of the Android platform being used to inform the patient about the details of the upcoming services through his/her TV-set.[3]

2. PROPOSED SYSTEM

2.1 Design

The main components of the system are the client (caregiver) application running on a smartphone, the security server of the homecare organization, the connection servers of care-providing medical, social affairs, etc. institutions, and the registries maintained by those institutions. The client application hosts the user interface for homecare information access and the means to authenticate the caregiver to the rest of the system. The client application connects to the security server over GPRS or 3G Internet connection. It signs the requests for data access and sends them to the security server. The traffic between the client and server utilizes the standard HTTP over SSL protocol [6], provid-

ICEGOV 2011, September 26-28, 2011, Tallinn, Estonia
Copyright 2011 ACM 978-1-4503-0746-8 ...$10.00.

[1] `http://www.changewaveresearch.com/articles/2010/07/smart_phones_20100714.html` (last access: April 25th, 2011)

[2] `http://www.android.com`

[3] `http://www.opencare.se/index.php?option=com_content&task=view&id=84&Itemid=66` (last access: April 25th, 2011)

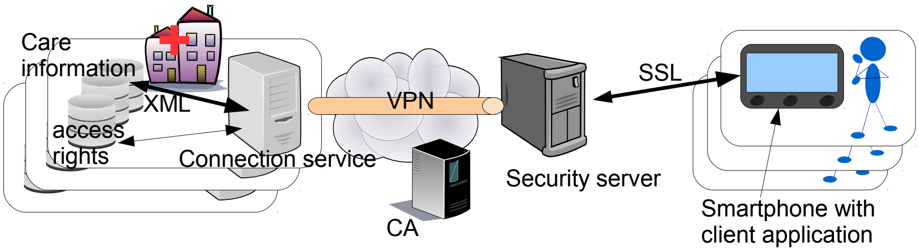

Figure 1: High-level architecture of the proposed system

ing the confidentiality of requests. The client and server authenticate each other through certificates, created by a designated certificate authority (CA).

When the security server receives a data access (read or write) request from a client, it first verifies the signature of this request. It then determines the institution to which this query has been addressed (included in the query) and forwards the query to the connection server of this institution. The information system of the involved institution contains a database of user access rights, against which it is possible to decide whether some query by some user can be answered or not, and what actions (e.g. logging) must be taken when this query is answered. The connection server again verifies the signature, then checks the access rights database and, if the query may be answered, forwards it to the internal information system of the institution. The answer to the query is sent to the user in the opposite direction. The answer is signed by the institution, and the signature is verified by the security server and by user. The overall architecture of the system is shown in Fig. 1.

We see that instead of the client application accessing directly the various registries of care-providing institutions, the traffic is routed through the security server and the connection servers. These components serve to reduce the heterogeneity of the whole system, as well as to define a clear perimeter of subsystems. The connection servers define a uniform query language for the client application; the backends for different care-providing organizations may need to be adapted. The security server is used route the messages, relieving the client application from that duty. There may also be several homecare organizations, each one with its own security server. The described architecture, especially the left part of Fig. 1 bears significant similarities to the eGovernment middleware “X-road” [1] deployed in Estonia. There are also some similarities between the homecare organization's security server and X-road's Citizen Portal, but the goals of these parts of the systems are different. Nevertheless, it may make sense to integrate the proposed system with X-road as much as possible, at least in Estonia.

As for the certificate authority, it makes sense to use the existing e-Identity infrastructure, should one be in place. This results in reasonably strong electronic identities without a significant up-front investment in a securely deployed CA. The advances in cross-border e-Identity interoperability[4] make this choice particularly attractive. Still, as the smartphone support for hardware tokens (e.g. smartcards) usually employed by these CA-s is yet lacking, our first prototype will use soft certificates for identification.

2.2 Conformance with Security Requirements

Health information systems may have very complex security policies, regulated by many different standards [5]. With the architecture we are proposing, much of this complexity is handled by the care-providing institutions' information systems and access control mechanisms. These systems make the decisions on whether to grant access to information to a particular user, whether to update the records, whether to log the transactions, etc. As these systems are already making those decisions now, the additional burden due to our proposal should be marginal.

Our system must ensure proper identification of all parties. We will achieve this through proper certificate granting process [4, 2] and the use of digital signatures. We also must make sure that the exchanged messages remain confidential, which we achieve through the use of provably secure protocols based on the TLS suite [3]. The security architecture of Android also helps to separate our client application from other programs running on the same device.

3. FURTHER WORK

This note reports on the general architecture of the planned system. Our current plans include the implementation of a part of the service on the Android platform and its usability tests.

Acknowledgements This work has been supported by VINNOVA, NordForsk, RANNIS, and MKM through the “Secure eHealth over Android” project, by ESF Grant #8124, and by ERDF through EXCS.

4. REFERENCES

[1] Arne Ansper. e-government from security viewpoint. MSc thesis, Tallinn Technical University, 2001.

[2] S. Chokhani, W. Ford. Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. IETF, RFC 2527, 1999.

[3] S. Gajek, M. Manulis, O. Pereira, A.-R. Sadeghi, J. Schwenk. Universally composable security analysis of TLS. In proceedings of ProvSec 2008 (LNCS 5324), Springer, pp. 313–327, 2008.

[4] Health informatics – Public key infrastructure – Part 3: Policy management of certification authority. International Standards Organization, ISO/TS 17090-3:2008.

[5] Report on current eHealth security standards. Deliverable 1.1 of BioHealth project (FP6/Europe Innova, contract no. 031121), 2007.

[6] E. Rescorla. HTTP Over TLS. IETF, RFC 2818, 2000.

[4] `https://www.eid-stork.eu/`