Personal Information Disclosure Management in Smart Home Tele health care

Umar Rashid and Woontack Woo

***Abstract*— Recent advances in ubiquitous computing technologies have stimulated interest in the prospects of using context-aware applications in home environments for tele-healthcare purposes. However, very few research activities have addressed the issues related to the privacy of patients-at-home in such smart computing environments. We propose a theoretical framework that empowers the patient-at-home control over access to personal information, allows for fine-tuning of disclosed information, ensures that disclosure of information is dependent upon the context of the user and provides a default information disclosure mechanism under emergency situation (which can be adapted by user according to his needs).**

***Index Terms*— Privacy, Situation-aware, interactive systems, interactive computing**

I. Introduction

The emerging advances in ubiquitous computing technologies offers the promise of significant improvements in the user's quality of life. However, many critics have expressed concerns over the potential privacy breaches in smart computing environments [1]. Context-aware application developers need to provide the users with flexible means to control when, to whom and at what level of detail they can release their personal information to environment.

To ensure the seemingly contradictory goals of privacy and quality-of-service, users must not just be able to restrict access to their personal information but also to fine-tune the details of disclosed information. Jason & Hong [2] describe granular control over release of context information as a desirable feature for privacy protection. Moreover, they also mention the need for special exceptions for emergency. Palen and Dourish [3] describe privacy management as a "dynamic response to circumstance rather than a static enforcement of rules".

Some previous works in the area of privacy protection allow for granular control over release of personal information under different situations in context-aware computing environments [1, 4, 5]. However, they fall short of mechanisms to assess the benefit users may gain by disclosing their personal information in and automate the disclosure process accordingly. In this paper, we present a theoretical framework for users in a smart home tele-health care systems to publicize their health information in relation to their privacy concerns. We provide users default privacy settings in relation to the expected benefit that is assessed on the basis of the context of the user and the health literacy of information receiver. The key features of our proposed framework are as follows:

- Explicit user control over access to personal information
- Granular control over disclosure of personal information
- Disclosure of information according to user's context
- Default privacy policies in relation to user's context (stress level, time) and health literacy of information receiver
- User control to amend the default policies at his/her discretion (In parallel to MSN Internet Explorer which has default privacy settings but also provides users the flexibility to regulate these settings according to his/her own needs)

II. Personal Information Disclosure Management

Our theoretical framework helps user regulate disclosure of their personal information to different requesters under different situations. The constituents of the framework are described below:

A. *Personal Information*

Personal information consists of the data collected from the wearable physiological sensors attached to user's body and stress level of user according to oriental medical science analysis. To determine stress level, physiological data is collected from the wearable sensors and then analyzed using oriental medical science techniques.

Stress level information is classified into 5 levels (0-4) with level 4 being the most critical.

The granularity stress level information is specified at different temporal levels as follows:

- Minute
- Day
- Past Days

In addition to that, data from physiological sensors is collected available at second level.

B. *Context of User*

The context of the user is signified by the current stress level of the user, and the time of disclosure.

This work was supported by Seondo Project of MIC, Korea.

Both with GIST, Gwangju 500-712, S.Korea, (e-mail: {urashid,wwoo}@gist.ac.kr).

C. *Information Receivers*

Based on the study by Wanda et al[6], we classify the receivers of user’s health information into the categories as follows:

- Healthcare related (doctors)
- Professional (employers, coworkers)
- Social (family, friends)

The classification of receivers is needed to help the system understand the health literacy and disclose user’s health information to them accordingly. Disclosing irrelevant and low-level granularity information to people with low literacy is not anything of benefit for user. If the information recipients belong to *professional* or *social* networks, they may be unable to understand the meanings of galvanic skin response, pulse rate or temperature, but may understand the user’s stress level at a particular moment and tension and based upon this information, provide *benefit* to the user (boss may grant him leave, family members may call on him).

D. *Time*

Time is also important factor in disclosure control framework. Under specific days, user may allow the access to his/her health information to be laxer or tightened (working hours vs. weekends).

A sample of default settings in theoretical framework is presented in the fig. 1:

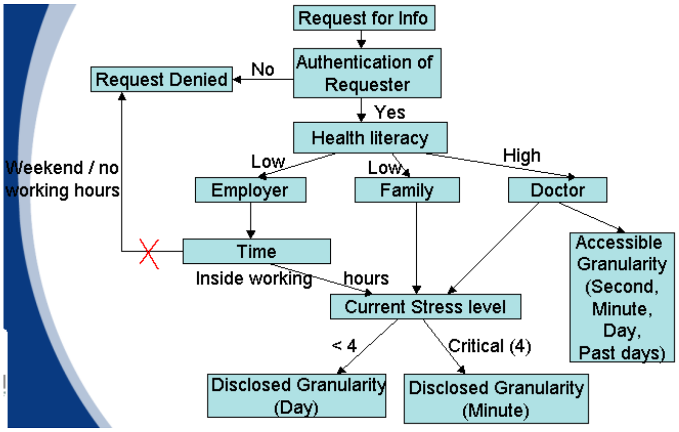
Request for Info
Authentication of Requester
No
Request Denied
Yes
Health literacy
Low
Low
High
Weekend / no working hours
Employer
Family
Doctor
Time
Inside working hours
Current Stress level
Accessible Granularity (Second, Minute, Day, Past days)
< 4
Critical (4)
Disclosed Granularity (Day)
Disclosed Granularity (Minute)

Fig. 1 Theoretical framework for personal information disclosure management

III. Demo Scenario

We will illustrate our theoretical framework through the following demo scenario:

A user-at-home receives a request from Bob (receiver) requests for the personal information (stress info). If stress level is 4 (critical), the granularity of stress information is set at minute level. If the Bob belongs to “ Healthcare related ” category, this implies that his Health Literacy is High. Hence, allow him to access user’ s stress info at all granularity levels including sensor level data (at second level). If Bob comes under ” social ” category, this implies that his Health Literacy is low. Hence, disclose information at minute level but no need to provide him info at finer granularity levels. If Bob is employer and comes under “ professional ” category ,this implies that his Health Literacy is low. Check if it a working day and user had some appointment scheduled with him (info from user’ s personal calendar). If yes, allow him information access at minute level otherwise deny the request.

On the other hand, if stress level is less than 4 (not critical), the granularity of stress information is set at day level. If the Bob belongs to “ Healthcare related ” category, then allow him to access user’ s stress info at all granularity levels including sensor level data (at second level). If Bob comes under ” social ” category, then disclose information at day level but no need to provide him info at finer granularity levels. If Bob is employer and comes under “ professional ” category, then check if it a working day and user had some appointment scheduled with him (info from user’ s personal calendar). If yes, allow him information access at day level otherwise deny the request.

IV. Discussion

We have presented a theoretical framework for the management of personal information disclosure in smart home tele healthcare. The framework provides user control over access to personal information, allows for fine-tuning of disclosed information, ensures that disclosure of information is dependent upon the context of the user and provides a default information disclosure mechanism under emergency situation (which can be adapted by user according to his needs). In future works, we tend to implement this framework and evaluate it with users in real time.

References

[1] Saadi Lahlou, Marc Langheinrich, Carsten Roecker1. “Privacy and Trust Issues with Invisible Computers**”,** Communications of the ACM, Volume 48, number 3 (March 2005) pp. 59–60

[2] J.I. Hong and J.A. Landay. An architecture for privacy-sensitive ubiquitous computing. *Proceedings of the 2nd Int’l Conference on Mobile systems, applications, and services*, pp. 177-189, ACM Press, 2004.

[3] Palen, L., and P. Dourish. Unpacking Privacy for a Networked World. *Proceedings of the Conference on Human Factors in Computing Systems* (CH 2003), ACM Press, Fort Lauderdale, FL, USA, pp 129-136

[4] Scott Lederer, Jennifer Mankoff, Anind Dey, and Christopher Beckmann, “Managing Personal Information Disclosure in Ubiquitous Computing environments,” Technical Report IRB-TR-03-015, Intel Research Berkeley, 2003.

[5] Ryan Wishart, Karen Henricksen, and Jadwiga Indulska, “Context Obfuscation for Privacy via Ontological Descriptions,” Proc. Of LoCA, 2005.