*

컨텍스트 인식 헬스케어 어플리케이션을 위한 개인화된 정보 공개 기법

우마 라쉬드, 최아영, 우운택
광주과학기술원 U-VR 연구실
{urashid, achoi, wwoo}@gist.ac.kr

Personal Information Disclosure Control in Context-aware Healthcare Applications

Umar Rashid, Ahyoung Choi and Woontack Woo
GIST U-VR Lab.

Abstract

There is a tradeoff between user's privacy and utility of context-aware services in ubiquitous computing environments. Many privacy models have been proposed to support the disclosure of personal information at different levels of detail, in ubiquitous computing environments. However, most of these models do not allow for explicit criteria to assess the benefit users are likely to reap by disclosing their personal information. In this paper, we propose an automated decision making mechanism that evaluates the "benefit of disclosure" for the users based on trust relationships between users and information requesters and manages the disclosure of user's personal information accordingly. Unlike other trust models, we do not regard the reputation of an information requester as sufficient to determine his/her trustworthiness. Instead, we represent trustworthiness as a function of information requester's reputation in the eyes of the user and his/her competence in a given context. To validate our mechanism, we apply it to context-aware healthcare application that monitors physiological condition of a user.

Keywords: Context awareness, Privacy, Trust

1. Introduction

Disclosure of personal information is inevitable to personalize context-aware services and applications in pervasive computing environments. More personal information a user discloses to service provider, more customizable and beneficial the service becomes. This phenomenon calls for users' control over disclosure of their personal information. Context-aware application developers need to provide the users with flexible ways to control when, to whom and at what level of detail they can disclose their personal information to different information requesters. Traditional disclosure paradigms, which restrict the disclosure of information to "nothing or everything" options, can no longer satisfy the users' needs in pervasive computing environments as pointed out by Lederer et al [1].

In recent years, many research activities have been focused on providing privacy solutions for users in ubiquitous computing environment [1]-[6]. Most of these proposed solutions provide the users with granular control over the release of their personal information according to their specified preferences. However, they do not offer explicit criteria to assess the benefit users may gain by disclosing their personal information.

To address this problem, we propose an automated decision making mechanism that evaluates the "benefit of disclosure" for the users and manages the disclosure of personal information accordingly. The theme behind

* *This was supported by Seondo project of MIC, Korea.*

the proposal is that *people compromise privacy in proportion to gained benefit*. A user should give up as much personal information as indispensable for gaining benefit. Since different entities may contribute to user's benefit at different levels (or no benefit), therefore, the detail level of personal information disclosed to different entities should also be different accordingly.

Applying Locke's definition of *trustworthiness* as "*the capacity to commit oneself to fulfilling the legitimate expectations of others*" [7], the "benefit of disclosure" is evaluated in relation to the *trustworthiness* of information requesting entity. The more *trustworthy* an information requester is, the more *beneficent* it is likely to be. Many research activities make use of trust relations between interacting parties to provide privacy solutions [8-12]. However, most of the trust models determine the *trustworthiness* of information requester on the basis of his/her *reputation* of in the eyes of the user (or user's acquaintances). Our contention is that in order to assess the "benefit of disclosure" for subsequent disclosure of personal information, the system must be aware of not only be aware of the *reputation* of information requester in the eye of the user but also of his/her *competence* in a given *context*. To demonstrate the significance of our proposed model, we apply it to context-aware healthcare application that monitors physiological condition of a user.

The paper is organized as follows. In section 2, we review the related works that deal with the issues of privacy in pervasive computing environment. In section 3, we describe our method of managing disclosure of personal information based upon the assessed "benefit of disclosure". We explain the architecture of our application in section 4 and experimental results in section 5. Finally, we sum up the conclusions and future works in section 6.

2. Related Works

As described by Alan Westin, "*privacy is the claim of individuals, groups or organizations to determine for themselves when, how and to what extent information is communicated to others*" [13]. Users in context-aware systems should be able to disclose personal information at different levels of detail to different entities, according to his/her preferences. For example, during a business trip, Bob may restrict his location information to be shared with his colleagues up to the level of city he is currently visiting. However, he may disclose to his family members his exact location e.g., district, street number, building he has made a stopover.

In recent years, many research activities have been aimed at protecting the users' privacy by granting them with fine-grained control over the disclosure of their personal contextual information [1,5,6]. As argued by Palen and Dourish [4], privacy is not simply a problem of access control, but it is an ongoing and organic process of negotiating boundaries of disclosure, identity, and time. Jiang et al. [3] propose "principle of minimum symmetry" for a privacy-aware system that calls for minimizing the information symmetry between users and observers. Other research activities propose trust-based approaches for managing privacy [9,10].

Our proposed mechanism is inspired by all of the aforementioned concepts. Our goal is to enable the users to evaluate the benefit they can attain by going public with their personal information and automate the process of information disclosure with respect to "benefit of disclosure". We discovered that the previous works in the areas of privacy and trust management are helpful yet insufficient to achieve that goal. In the trust models we surveyed [8-12], *trustworthiness* is calculated solely in terms of *reputation*. We refine our trust model to incorporate an entity's competence in a specific *context* along with its *reputation*. In this way, we are able to assess the user's "benefit of disclosure" in terms of *trustworthiness* of information requester. For example, a user can share his tax information with a trusted *information requester* (who has good *reputation* in the eye of user) but if *well-reputed* information requester also holds *competence* in financial dealings (*context*), then for user, it will be a bonus sharing tax information with him. In that case, information requester is more *trustworthy*, and the user is likely to gain more *benefit* by disclosing personal information to him.

3. Personal Information Disclosure Automated by "Benefit of Disclosure"

We present an automated decision making mechanism that manages disclosure of personal information according to the gained *benefit* i.e. calculated based upon the *trustworthiness* of information requester. *Trustworthiness* per se is evaluated based upon the information requester's *reputation* and *competence* in given *context*, as shown in fig. 1.

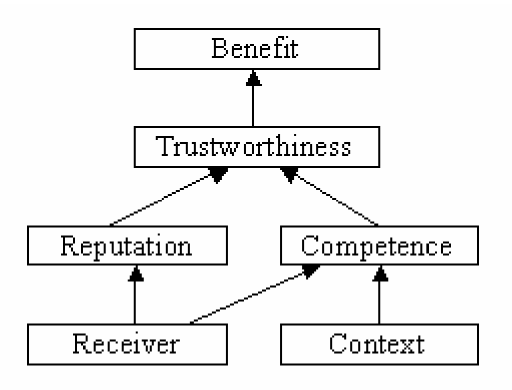


Fig. 1. Evaluation of Benefit

Rehman et al [8] define reputation as, *"Reputation is an exception about an agent's behavior based on information about or observations of its past behavior"*. In real life, reputation information about others plays a great role in making our effective decisions about them. In the words of Misztal [14], "[Reputation] helps us to manage complexity of social life by singling out trustworthy people – in whose interest it is to meet promises". Strictly speaking, reputation represents our personal opinion about a person and is formed by our interactions with him/her.

Re *competence*, we borrow its definition from American Heritage Dictionary i.e. "*the state or quality of being adequately or well qualified*". Competence is strictly dependant on *context*. A person competent to in one context may be quite inept in another. For example, a doctor is competent to tackle physiological information but may be incompetent regarding tax information.

Benefit of disclosing personal information in a given *context* to an *information requester* who holds *trustworthiness* on account of his/her *reputation* in the eye of the user and *competence* in given *context* is represented as:

Benefit ← Trustworthiness (Requester, Reputation, Competence, Context)

In order to demonstrate the efficacy of our information disclosure mechanism, we apply it to a context-aware healthcare application that monitors the physiological condition of a user. If the user finds his health condition disturbed, he may inform his doctor or friends about it. The detail level of physiological information is adjusted in accordance with the expected benefit as follows:

1). If the information requester is a *well-reputed* doctor, user is likely to get more *benefit* by disclosing physiological information at "Expert" level detail (pulse rate, temperature etc.). It can be shown as:

Benefit (High) ← Trustworthiness (Doctor, High Reputation, High Competence, Physiological Context)

2). If the information requesters are user's family members or colleagues, who command *high reputation* but are *incompetent* about technical aspects of physiological condition, user is likely to gain *less benefit* from them. They may be unable to understand the meanings of galvanic skin response, pulse rate or temperature, but may understand the stress and tension and based upon this information, provide *benefit* to the user (boss may grant him leave, family members may call on him). This situation can be represented as:

Benefit (Low) ← Trustworthiness (Non-expert, High Reputation, Low Competence, Physiological Context)

Information can be disclosed on user's discretion or on request. The process goes through the steps as shown in fig. 2 below:

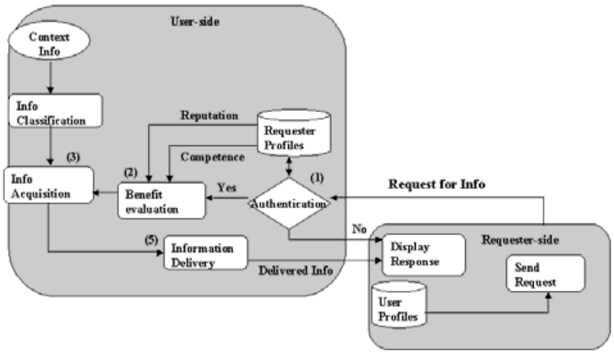
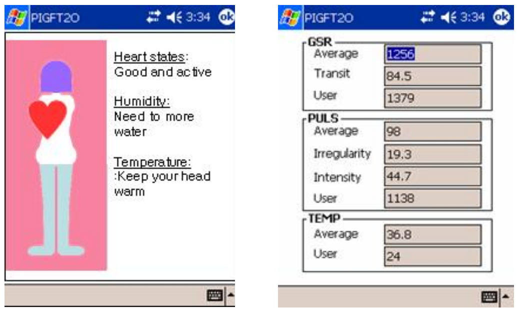


Fig. 2. Personal Information Disclosure Control Mechanism

1. *Authentication*. Requester is authenticated (if it exists in requester profiles on user's system). If no, then no information is sent to the requester.
2. *Benefit evaluation.* If requester is authenticated in step 1, then system determines the *trustworthiness* in relation to the requester's *reputation* and *competence* about physiological information (*context)*, and evaluates the "benefit of disclosure" based upon trustworthiness.
3. *Context Acquisition*. The system acquires the context information at relevant level of detail in relation to the "benefit of disclosure" calculated in step 2.
4. *Information Delivery*. Physiological info is sent to the requester at appropriate detail level

4. Implementation

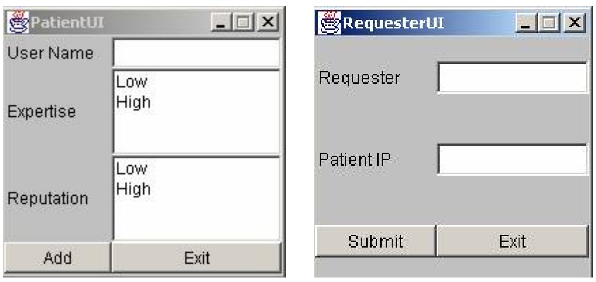
In our application, a user's physiological information is collected from a wearable wrist type multi-physiological sensing system consisting of PPG, GSR and SKT sensors. The physiological signal is transferred to the personal station for signal processing where we categorize the detail levels of physiological signal information in terms of parametric information ('Expert' level data) and whole state indication ('Layman' level data) as shown in fig. 3. We follow the general physiological signal procedure and analysis methodologies with the view of general statistics and mathematics. The wrist type physiological signal sensing part has been implemented using embedded visual C++.



(a) (b)

Fig. 3. Level of details in physiological context (a) layman level context (b) expert level context

This information is transferred to the user's Personal Digital Assistant (PDA). Interfaces are provided on user's PDA to specify requester's credentials and on requester's system to submit request to access user's physiological info, as shown in fig.4 below:



(a) (b)

Fig. 4. User Interface (a) for specifying requester credentials (b) for submitting request to view user's physiological information

A user can use the interface to add an authorized requester, specify his/her expertise and trust levels. User's PDA also runs an "information disclosure server" to process requests from different requesters. The requestor access rights are verified based on the privacy policy specified by the patient and then the context information is sent to the requestor accordingly. User interfaces and "information disclosure server" have been implemented using JDK 1.1.8.

Requesters can send request for accessing user's physiological information by entering user's name and IP address of PDA. The request is forwarded to "information disclosure server" running on user's PDA and is further processed there. If the requester is not found in the profiles of authorized requesters on patient's system, then no physiological info is sent to the requester and the appropriate message is displayed on requester's platform. Otherwise, the user's physiological information is sent at the appropriate detail level, in accordance with requester's reputation and competence.

5. Evaluation

We compare our proposed model with other privacy control models for ubiquitous computing environments based on four factors. Table 1 shows the result of evaluation.

Table2: Privacy Model Evaluation

Privacy Models	Granu-lar control	Context Types	Levels of Disclos-ure	Benefit of Disclosu-re
Lederer [1]	Yes	Multiple	Limited	Excluded
Wishart [6]	Yes	Multiple	Arbitrary	Excluded
Umar	Yes	Multiple	Arbitrary	Included

Our proposed model supports granular control over disclosure of multiple context types at arbitrary detail levels. Moreover, it evaluates the "benefit of disclosure" and discloses the context information at appropriate detail level in accordance with the evaluated benefit.

We are conducting a questionnaire-based survey to determine the importance of two factors - reputation and competence of the information requester - in determining the *trustworthiness* of information requester. So far, 16 people have responded to our questionnaire. The respondents are in the age group of 22 - 35 and consist of 6 females and 10 males. We noticed that all respondents agree on the *reputation* as being a necessary factor to determine the *trustworthiness* of information requester while a significant majority also included *competence* as the determining criterion. As shown in Table 2, About 80% people argued that they see no benefit in disclosing personal information to people who have high *reputation* but low *competence*. Majority of respondents welcomed the idea of applying this mechanism to ubiquitous health monitoring applications.

Table2: Factors affecting trustworthiness

	Yes	No	Doesn't matter
Reputation	16 (100%)	0	0
Competence	13 (81%)	1	2

6. Conclusion and future works

We have presented an automated mechanism that evaluates the benefit users can gain by disclosing their personal information and then adjusts the detail level of disclosed information accordingly. To validate our mechanism, we applied it to context-aware healthcare application that monitors physiological condition of a user. In addition, we evaluated our system with several subjects for analyzing the effectiveness of this system. We discovered that it has wide acceptance among users for privacy protection systems. In future, we intend to include the "risk of disclosure" along with benefit factor in our model and automate the decision making process based on risk/benefit analysis**.** Moreover, in evaluation step, we will extend our experiment with a larger sample size of users in natural daily life.

6. Reference

[1] 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.

[2] Marc Langheinrich, " Privacy by design – principles of privacy-aware ubiquitous computing systems," Proceedings of Ubicomp 2001, pp. 273-291, 2001.

[3] X. Jiang, J. Hong, and J.Landay, "Approximate

Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing," Proceedings of Ubicomp 2002, pp. 176-193, 2002.

[4] L. Palen, and P. Dourish, "Unpacking privacy for a Networked World," CHI Letters, pp. 129-136, 2003.

[5] Hang and Landay, "An Architecture for Privacy Sensitive Ubiquitous Computing," 2nd ACM International conference on Mobile systems, applications, and services, pp. 177-189, 2004.

[6] Ryan Wishart, Karen Henricksen, and Jadwiga Indulska, "Context Obfuscation for Privacy via Ontological Descriptions," LoCA 2005.

[7] J. Dunn, "The Concept of Trust in the politics of John Locke," Philosophy in History, Cambridge University Press, 1984.

[8] Abdul-Rahman, and Hailes, "Supporting Trust in Virtual Communities," International Conf. System Sciences, 2000.

[9] Brian Shand, Nathan Dimmock, and Jean Bacon, "Trust for Ubiquitous, Transparent Collaboration," 1st IEEE International Conference on Pervasive Computing and Communications, 2003.

[10] Jeremy Goecks, and Elizabeth Mynatt, "Enabling privacy management in ubiquitous computing environments through trust and reputation systems," ACM Conference on Computer Supported Cooperative Work, 2002.

[11] F. Azzedin, and M. Maheshwaran, "Evolving and Managing Trust in grid computing systems," IEEE Canadian Conference on Electrical and Computer Engineering, 2002.

[12] Mui, Mphatshemi, and Halberstadt, "A Computational Model of Trust and Reputation," 35th Hawaii International Conference on System Sciences, IEEE, 2002.

[13] Westin, "Privacy and Freedom," New York NY: Atheneum, 1967.

[14] Misztal, "Trust in Modern Societies," Polity Press, Cambridge MA, 1996.