Using Personalization to support Privacy in Ubiquitous Systems

Elizabeth Papadopoulou, Sarah McBurney, Nick Taylor, M. Howard Williams
Heriot-Watt University
Riccarton, Edinburgh, UK
{ceeep1 ceesmm,nkt, mhw}@macs.hw.ac.uk

INTRODUCTION

In order to develop a pervasive computing system that is acceptable to the end user, it is important that it should satisfy two end user requirements:

(1) It should adequately protect the privacy of the user. Much work has been done on the design of privacy aware ubiquitous systems (e.g. [1], [3], [4]), including analysis of end-user requirements and the approaches needed to satisfy them. Such systems should not reveal information about the identity of the user nor allow access to any of the user's personal data without the user's permission, and there should be simple and appropriate mechanisms for the user to control this. The notion of pseudonymity provides a simple and practical solution to concealing the real identity of the user from the services he/she uses. By using different pseudonyms for different service transactions, pseudonymity provides a balance between protecting user privacy and offering advanced personalization practices. Different implementations include *separate personas*, private and public [1], which place different restrictions on information they release to services, and *virtual identities*[2]

(2) It should take account of user needs and preferences in any relevant decision making and adapt its behaviour accordingly. The importance of incorporating user preferences has been recognized in a number of projects, where preferences are entered manually by the user (e.g. Intelligent Home, AURA and Blue Space [6]) or where learning is used to support the acquisition of preferences (e.g. Adaptive House, MavHome and GAIA [7]).

Daidalos is an EU project in the final stage of developing a pervasive system [5], which uses user preferences to personalize system decisions relating to user privacy. This paper focuses on the problem of determining what information about the user can be shared with a service.

CHI 2008, April 5–10, 2008, Florence, Italy.

USING USER PREFERENCES TO SUPPORT PRIVACY DECISIONS

Pseudonymity is achieved in Daidalos through the use of multiple Virtual Identities (or VIDs) [2]. These VIDs form subsets of the user's profile and are used to authenticate the user with services. For any user the set of VIDs may be viewed as a set of different user names, which the user may use for different purposes, and which may conceal all or part of his/her personal data. Each user may have any number of VIDs. None of these can be linked to any of the others so that if a user uses two VIDs with the same service, that service will treat these as two different users. This also allows for good personalization practices since users can use services for different activities and have different preferences for each.

Initially one could simply assume that the user will always select the appropriate VID for any service. However, this is an arduous task, especially if the number of VIDs grows. The situation is more complex if one takes account of changing context conditions (e.g. location) which can affect the choice of VID. Thus in order to provide a user-friendly pervasive environment the system should manage the automatic selection of VIDs wherever possible, resorting to user decision or intervention only when really necessary.

The process of selecting a VID depends in part on the personal data that the system wants to access (e.g. location, credit card details) and in part on the user's preferences. This process can be divided into three steps:

(1) *Negotiating use of data*. One of the main factors that affects the choice of VID for any situation is the access that is needed to user data. Thus, before a service is used, it is important to know what user data the service will want to access. The pervasive system must then negotiate with the service between the user data that is requested and what the system is willing to disclose based on the user's wishes. This is called Privacy Policy Negotiation (PPN). For this purpose one may have a set of user preferences, referred to as *PPN preferences*, that define what the user wishes in each situation. These may depend on external factors such as context conditions (e.g. the user's location, activity, people in his/her proximity, etc) or service-specific conditions (e.g. reputation of service) or internal service trust levels for each user. In each case, the PPN preference outcomes tell the system whether or not a piece of personal data can be disclosed. The evaluation of these PPN preferences for all the requested user data results

in a privacy policy. This privacy policy is used to negotiate with the service on behalf of the user the terms of use based on these outcomes.

(2) *Matching PPN outcomes with potential VIDs.* The result of the negotiation is a list of data items (i.e. context attributes, preferences, personal information) that the service can access. The second step in the process of VID selection uses this list to identify the set of possible VIDs that allow access to all of the items in the list and only those items in the list. This results in the identification of one or more VIDs that can be selected for use with this service.

(3*) Final VID Selection*: User VID selection preferences are used to select the actual VID to be used. The result of this step has the form "select VIDa".

Thus the process of selecting a VID involves two types of preference rules: *PPN preferences* and *VID Selection Preferences*.

FORMATS OF USER PRIVACY PREFERENCES

The format of the privacy policies is based on the industry standards P3P and XACML, including the possibility of creating custom privacy preferences. On the other hand the PPN preference rules have the same "if-then(-else)" format as for all preference rules in the Daidalos system,.

A PPN preference lists the conditions under which a piece of user data is disclosed to a service. These include the status and attributes of other services being run by the user, attributes of the service requesting access to the data, etc. The outcome of such a preference would be either positive (i.e. disclose this piece of data), negative (i.e. do not disclose it) or a conditional expression of "positive if a list of requirements is met". These latter requirements are conditions such as the data retention policy of the requesting service, the data usage policy of the requesting service and other such conditions subject to negotiation with the service. This has been fully specified but constraints on space do not permit a fuller discussion on this here. The following example shows a PPN preference.

IF location = 'work' AND time.between(0900,1700) AND LocalTrustLevel(requestor) >0.5 AND GlobalTrustedReputationLevel(service) > 0.7

THEN PrivacyPolicyRule:

Effect: "allow"

Obligations: 1) Data_Retention_Policy < 12 hours

2) Share information with 3rd parties: NO

Evaluating this results in a privacy policy that specifies under which circumstances access to user data should be granted. The resulting privacy policy is used to start negotiation with the service. This negotiation should result in an agreement that meets all the requirements in the privacy policy. The format of VID selection preferences is similar although the outcome specifies a VID.

SOME RESEARCH CHALLENGES

Some major challenges with this approach include:

(1) No service should have access to more information on a user's VIDs than is absolutely necessary for its functioning. This has consequences for the design of the preference subsystem.

(2) The user must be engaged in the process of VID selection. There are problems if it is either completely automatic or completely manual. A compromise is to take the decision for the user but give him/her the opportunity to intervene and change the VID selected or create a new one.

(3) By monitoring user actions and applying machine learning techniques, user preferences can be built up and maintained automatically. However, one is still faced with the problem of distinguishing between short-term and long-term changes in preferences.

This approach forms an important part of the way in which privacy is handled within the Daidalos system

REFERENCES

1. Brar, A. and Kay, J.: Privacy and Security in Ubiquitous Personalized Applications, in: *Proc. User Modelling Workshop on Privacy-Enhanced Personalization*, Edinburgh, (2005)
2. Girao, J., Sarma, A. and Aguiar, R.: Virtual identities - a cross layer approach to identity and identity management, .in *Proc. 17th Wireless World Research Forum*, Heidelberg, Germany, (2006).
3. Hong, J.I. and Landay, J.A. An Architecture for Privacy-Sensitive Ubiquitous Computing, in *Proc. 2nd Int. Conference on Mobile Systems, Applications, and Services (MobiSYS)*, Boston, Massachusetts, USA, (2004).
4. Langheinrich, M.: A privacy awareness system for ubiquitous computing environments, in *Proc. 4th Int. Conf. on Ubiquitous Computing*, London, UK (2002), 237--245.
5. Williams, M. H., Taylor, N. K., Roussaki, I., Robertson, P., Farshchian, B. and Doolin, K.: Developing a Pervasive System for a Mobile Environment. In *Proc. eChallenges 2006 – Exploiting the Knowledge Economy* (2006), 1695 – 1702.
6. Yoshihama, S., Chou P. and Wong D.: Managing Behaviour of Intelligent Environments. In *Proc. First IEEE Int. Conf. on Pervasive Computing and Communications (PerCom '03)* (2003), 330-337
7. Ziebart, B. D., Roth D., Campbell R. H. and Dey A. K. Learning Automation Policies for Pervasive Computing Environments. In *Proc. 2nd Int. Conf. on Autonomic Computing (ICAC '05)* (2005) 193-203.