Privacy Rights Management for Mobile Applications

A. K. Bandara, B. A. Nuseibeh, B. A. Price, Y. Rogers
Centre for Research in Computing
The Open University
Milton Keynes, MK7 6AA, UK
{a.k.bandara, b.nuseibeh, b.a.price, y.rogers}@open.ac.uk

N. Dulay, E. C. Lupu, A.Russo, M. Sloman
Department of Computing
Imperial College London
London, SW7 2AZ, UK
{n.dulay, e.c.lupu, a.russo, m.sloman}@imperial.ac.uk

A. N. Joinson
School of Management
University of Bath
Bath, BA2 7AY, UK
a.n.joinson@bath.ac.uk

1. INTRODUCTION

With mobile telephony and GPS devices becoming ubiquitous, there are many tracking and monitoring devices being developed that have a range of potential applications, from supporting mobile learning to remote health monitoring of the elderly and chronically ill. However, do users actually understand how much of their personal information is being shared with others? In general, there will be a trade off between usefulness of disclosing private information and the risk of it being misused. In this position paper, we describe the Privacy Rights Management for Mobile Applications (PRiMMA) project, where we are investigating techniques for protecting the private information typically generated from ubiquitous computing applications from malicious or accidental misuse. Consider the following scenario:

"Alice and Bob's son Charles is involved in many after school activities. Concerned for his safety whilst travelling to and from these activities, Charles' parents buy him a new mobile phone that has a GPS tracking feature together with a Privacy Manager (PM) tool. To prevent Charles from unintentionally disclosing is location to others Bob configures the PM with a policy that states that only Alice and Bob can read Charles' location information.

One day Charles needs a lift home and uses a taxi firm, 'zCar', that allows customers to send SMS requests containing their location. However, when Charles tries to send a pick-up request, his PM informs him that this would violate his location privacy policy. Charles chooses to override his policy and soon a taxi arrives to take him home. The next time Charles needs a lift, he uses another firm offering the same service, 'qCab', and is again forced to override his policy. Over time, Charles' PM learns this behaviour and suggests a new policy that will disclose his location to taxi firms whenever he requests a pick-up."

This scenario illustrates the need for explicit privacy rights in mobile computing interactions, and the importance of being able to detect and resolve inconsistencies between user privacy policies and the information required to provide particular functionalities. It also raises the need to be able to analyse a collection of user privacy policies before making a decision to disclose private information. Together with the need for automated learning of privacy policies in order to minimise the overhead of requiring user intervention whenever there is an inconsistency between policies or between an information request and privacy policies.

We are investigating privacy requirements across the general population for a specific set of ubiquitous computing technologies and produce a reusable framework with demonstrator applications, based on the above scenarios, evaluated with participants across a wide population demographic. We aim to develop a Privacy Rights Management (PRM) framework that will enable users to specify and manage the privacy of personal context information generated by a pervasive system [1]. This framework will integrate users' privacy policies with their personal information to control how information is used. This is analogous to Digital Rights Management (DRM), which uses software solutions to protect digital information against copyright infringement and often incorporates information such as 'digital watermarks' in the data being protected or encapsulates the data such that it is self protecting [8]. Our work will identify how people perceive privacy in ubiquitous systems, how they would like to control it, and provide tools that will enable them to manage the privacy of the information they generate. To this end, we are will recruit a large cohort of over 1000 Open University (OU) students with a broad range of ages and backgrounds, both for identifying requirements and a smaller group of over 100 to evaluate the tools for privacy management prototyped in the project. We will focus on two types of ubiquitous computing privacy risks: the unidirectional risk, such as where a student is being monitored by his tutor, and the bi-directional risk where peers (e.g., students, friends, colleagues, spouses) are implicitly or explicitly exchanging context information. We will implement a PRM system that allows users to specify privacy preferences, to help visualize them, to learn from the user's behaviour what their likely preferences are, and to enforce privacy policies. We will develop simple interfaces that allow users to specify and understand what is being revealed about them. By providing an analysis and learning system within the framework, we believe that we can produce a usable system that does not burden users with complex privacy rule sets.

2. RESEARCH ISSUES & OBJECTIVES

The overall objective of the project is to determine how users perceive privacy issues related to information they will generate in pervasive systems, and to develop a Privacy Rights Management (PRM) System to enable them to specify privacy controls which will be enforced by the system. Interface evaluation, especially for novel interfaces, typically involves small numbers of users (usually computer science or psychology undergraduates) who have been trained on the experimenter's equipment and perform a lab-based or other brief evaluation. Our work will move the evaluation of novel interfaces to the next level by allowing many more users from the general population to use their own equipment (mobile phones) doing real world tasks over a period of weeks. The research issues and questions related to the above objectives include:

- Determining how users perceive privacy of information they generate. Who will they share it with? What sort of controls do they want over the information?
- What is the granularity of context information that users are willing to divulge in the different contexts of work, learning, and play?
- What mechanisms are needed to automate the control of privacy and how should these be distributed between mobile devices and the infrastructure?
- Can we predict the privacy requirements over a range of users from monitored information and how do these change over time?
- Can we detect and resolve inconsistencies in users' privacy requirements?

3. APPROACH

We propose to develop four distinct components to address the problem of privacy control in ubiquitous computing: both large and small screen user interfaces for privacy management; information models for context data and privacy policies; privacy policy languages and enforcement mechanisms; and learning and analysis techniques for automating specification, derivation and validation of privacy policies. A high-level architecture diagram of our proposed framework illustrating how these components would interact is shown in Figure 1.

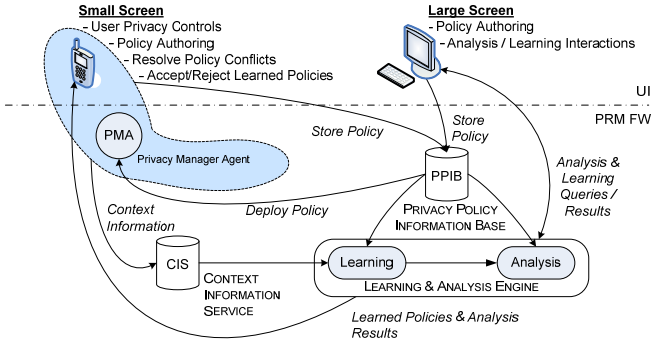

Figure 1: High-level PRM Architecture

A key output of this project will be an implementation of this PRM framework, including demonstrator applications together with a comprehensive evaluation with >100 participants across a wide demographic. Before starting detailed design and implementation of the components shown, we will conduct a large scale requirements gathering exercise to elicit initial privacy requirements for ubiquitous computing involving over 1000 people. These requirements will guide the interaction/interface design which will produce a reusable privacy user interface for both handheld devices and visualization on large screen devices. The requirements will also guide the development of models for the context and policy information used by the privacy management framework and will also provide input to the design of a specialised privacy policy.. Our framework will include a privacy manager agent which is able to interpret and enforce the policies deployed on the user devices. We will also evaluate what functionality can be incorporated on portable devices and what needs to be offloaded to more powerful computers. For example, can policies be learned in real-time or only as an offloaded background activity; can detailed analysis results be shown on a mobile display; etc? Finally, although not shown explicitly in the architecture diagram, we will also implement requirements monitoring mechanisms for evaluating how users' stated requirements change in ubiquitous computing environments once applications are in use.

4. RELATED WORK

Hong and Landay [3] identify a number of privacy requirements for end users, including simple and appropriate control and feedback. They address this concern in their Confab architecture by adding digitally signed privacy tags to shared data items with retention and use policies. This approach corresponds to the European data protection model of data being licensed for a specific purpose and no other. The idea of combining data with metadata in Confab is the starting point for the DRM-style of PRM that we propose. Other DRM-style approaches include Gunter et al. [4] who combined a method using a formal access control matrix with Personal DRM (PDRM). Their PDRM system combines the features of P3P with the eXtensible rights Markup Language (XrML) [5] to create digitally signed contracts licensing the use of personal data for specific purposes and for fixed periods of time. Our approach extends this idea to incorporate actual user requirements, context awareness, and a practically tested user interface. Despite these results, the problems of privacy control in mobile or ubiquitous computing remain largely unaddressed.

5. ACKNOWLEDGEMENTS

This work is funded by the UK EPSRC (Grant # EP/F024037/1) and is supported by IBM Research as part of their Open Collaborative Research (OCR) initiative. We are grateful to our OCR partners, Jorge Lobo (IBM), John Karat (IBM), Lorrie Cranor (CMU) and Elisa Bertino (Purdue) for their input into this work.

6. REFERENCES

[1] Fahrmair, M., W. Sitou, and B. Spanfelner. *Security and privacy rights management for mobile and ubiquitous computing*. in *Workshop on UbiComp Privacy: Privacy in Context at UbiComp'05*. 2005. Tokyo, Japan.

[2] Lessig, L. *The Architecture of Privacy*. in *Taiwan Net'98*. 1998. Taipei, Taiwan.

[3] Hong, J.I. and J.A. Landay. *An Architecture for Privacy-Sensitive Ubiquitous Computing*. in *Proceedings of the 2nd Int. Conf. on Mobile systems, applications, and services*. 2004. Boston, MA, USA

[4] Gunter, C.A., M.J. May, and S.G. Stubblebine. *A Formal Privacy System and its Application to Location Based Services*. in *Workshop on Privacy Enhancing Technologies*. 2004. Toronto, Canada.

[5] ContentGuard.com, *XrML Version 2.0*. 2005