Integrating Privacy Enhancing Services in Ubiquitous Computing Environments

Maomao Wu and Adrian Friday

Computing Department
Lancaster University
Lancaster
Bailrigg
LA1 4YR
UK

{maomao, adrian}@comp.lancs.ac.uk

1. Introduction

With the advances in pervasive wireless communications (such as GSM, WaveLAN, Bluetooth, etc.) and context-aware and 'smart room' prototypes (GUIDE [1], AT&T's Sentient Computing [2], Oxygen [3], Easy Living [4], the Aware Home [5], etc.), Mark Weiser's vision of ubiquitous computing seems closer than ever to reality. However, only until such systems are widely deployed and integrated with our everyday lives, will Weiser's vision be fully realised.

One of the big forthcoming challenges for those seeking to actually deploy ubiquitous computing (UbiComp) services on a significant scale will be making adequate provision for handling personal privacy. In environments with significant concentrations of 'invisible' computing devices gathering and collating sensorial data and deriving user context, the user should rightly be concerned for their privacy. To assuage this fear, we argue that future systems should provide a means to enable people to be aware of how they are being sensed and what that information is being used for. Furthermore, in the future service providers may well be legally bound to comply with privacy legislation [6,7].

In this paper we describe the initial motivations and challenges regarding a set of privacy enhancing services designed specifically for UbiComp environments. These services are designed to allow adaptive protection of users to meet personal privacy requirements without compromising their ability to receive personalised services and the service providers' needs to gather statistical data.

2. Background

2.1 The need for privacy management

In 1998, a survey of 1,400 web sites conducted by the Federal Trade Commission (FTC) showed that only 14 percent had a privacy policy explaining to consumers what might happen with their personal data. In their report [8], FTC proposed five principles for Fair Information Practices: 1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

The EU Directive on the Protection of Personal Data [7] prohibits the transfer of personal data to non-EU countries that do not have "an adequate level of privacy". In addition to the above principles, the EU Directive requires all member states to establish an independent authority to supervise the regulation of personal data. The US Privacy Act of 1974 [6] provided similar recommendations for openness and transparency, including no secret record keeping, individual participation, collection limitation, reasonable security, and accountability.

Both of the legislations proposed general principles for information practices. Although they were not intended or envisioned for UbiComp, they provide a clear set of guidelines for the design of UbiComp systems [9].

2.2 Managing Privacy

Privacy issues have already begun to surface on the Internet. W3C's Platform for Privacy Preferences Project (P3P) [10] provides a way to describe privacy policies for web sites in a machine and human-readable XML format. P3P enables web service providers to express their privacy practices regarding the collection, use, and distribution of personal information gathered from the user and their user agent. This policy can be automatically retrieved and interpreted by the user agent, which accepts or rejects services according to user's stated preference policy (typically security level).

In order to protect Internet users' privacy, a number of systems have begun to offer intermediary services (such as Anonymizer [11], Crowds [12] and Pseudonymity Networks [13]). Anonymiser dot com for example, allows people to browse the web anonymously, without personal information such as IP addresses or identities being harvested by the web servers they visit. One-time credit cards or electronic cash (e.g. PayPal) allow purchasers to protect their personal credit cards and identities by making one off payments via an intermediary. Pseudonymous email address services allow people to protect their real email addresses and identities from unsolicited commercial email, by providing pseudonyms for short term use. Identity and reputation services such as Microsoft Passport allow the secure and brokered storage of personal information under a single sign-on. As a trusted third party, such services can allow fine grained access control to personal information based on pseudonymous identities.

While these existing privacy enhancing services are all currently targeted at Internet browsing and shopping applications, we believe that similar services are required, tailored to UbiComp environments. In the following section we use a scenario to illustrate why such an approach is necessary.

3. Scenario

Imagine the wireless networked city - Lancaster - offers UbiComp services. The city council offers location-tracking service for tourist guide applications and the emergency services. Every shop also offers UbiComp services, such as location-aware special offer advertisements. The city also supports a number of privacy enhancing services, including Location Anonymiser and Identity Anonymiser.

Alice is a tourist visiting Lancaster, carrying her PDA in order to use the UbiComp services. The PDA has stored her privacy preferences regarding information gathering and distribution. For example, Alice has specified that any service can use the pseudonym stored on her PDA to deliver personalised services transparently without intruding by alerting her; but has also specified that any service asking for her mail address must have her explicit agreement.

As soon as Alice enters Lancaster's city centre, the city council location service advertises itself, the advertisement includes its privacy policy - what personal information it wishes to use, how it will be kept and distributed, and what services she will benefit from. The privacy agent on her PDA receives the policy, compares it with Alice's stated privacy preferences. If no conflict of interest is detected, the software will not intrusively notify or alert Alice. Where a conflict is detected, the agent will notify her of the privacy conflict and wait for Alice's approval or rejection.

Alice soon finds that too many of the services she is interested in compromise her wish for privacy. As she can't find any alternative services that meet her requirement, she toggles her privacy agent into 'adaptive' mode.

While Alice is walking past Sainsbury's, her PDA displays some special offers to her. She is sufficiently interested and enters the shop. The location-aware special offer advertisement service can be offered without requiring any personal information, but also offers a premium service that tailors advertisements based on stored profile information. Alice's privacy agent recognises the need for a unique identity to use this service, but continues to respect Alice's privacy by offering a pseudonym in place of her real identity. When Alice checks out, she presents her pseudonumous electronic reward card, which is also stored on her PDA.

4. Challenges

4.1 P3P is not the ultimate solution

P3P makes transparent use of privacy policies possible, but it is just the beginning, not the end. The intended application domain for P3P is Web browsing and applications, and the current definition does not extend to UbiComp applications. Significantly, P3P already provides simple mechanisms for extending the P3P vocabulary and it has already been proposed for UbiComp [14].

It is worth noting that P3P is only able to provide a technical mechanism by which services and their use of personal information are described. P3P does not provide mechanisms by which policies are enforced. Nor can policies be used to verify or prove that the services accurately reflect the stated policy. Legal protection mechanisms and independent adjudication is recommended to support P3P and protect against abuses by unscrupulous companies.

4.2 Privacy Enhancing Services for UbiComp environments

As discussed above, current privacy enhancing services are targeted at the Internet environment. We believe that new analogous services will be required, specifically tailored to support UbiComp environments. Examples of such services are:

- One-time identifier/ username generators
- Location anonymisers (or accuracy or temporal diffusors to reduce the precision with which users are tracked)
- Financial services, one-time payment mechanisms
- Communication anonymisers and rendezvous points (allowing unattributable exchange of information)
- Scalable persistent storage servers (required to allow users to conveniently manage their facades in a controlled way)
- Non-repudiation/ accountability services (trusted parties that audit interactions to allow back-tracing of operations, e.g. high priority access to locate missing persons, tracing of undesirable service usage and threat analysis, etc.)

This list is clearly not exhaustive. However, we believe that these services, services like them and the protocols that allow the services communicate should be an essential part of future UbiComp research.

Note that despite the best intentions of such services and protocols, using correlation and data mining techniques (e.g. mapping pseudonyms to known constants, such as hardware MAC addresses during communication), may allow the identity to be discovered. This is an important aspect for future work.

4.3 Adaptation

As identified in our scenario, we believe that although in the future large numbers of pervasive services will exist, it is unlikely that all the services a user wishes to use will match their privacy requirements. Where no alternatives exist, and the user still wants access to the service, adaptive protection mechanisms will need to be used. The default mechanisms of protocols such as P3P (accept, block, limited or user mediated) will not be sufficient. Alice can still have tailored, personalised information based on her spending habits or location, but without the need to divulge who she really is. Consistent use of such pseudonyms allows the service provider to gather statistical information and present information to the user as before, but without compromising her privacy.

5. Conclusion

In this brief position paper, we have outlined some of the challenges facing developers of UbiComp applications with regard toward personal privacy. We have set out the motivations for a range of new services that we believe will be required in the future to allow facilitate the deployment of such applications.

Our main contribution is the notion of ‘privacy enhancing services’ that adaptively provide protection for users as they enter and inhabit UbiComp environments, which allow for continued transparent use of services without compromising the users wish for privacy, nor the services providers ability to provide services. We are focusing our future researches on understanding these services and protocols.

6. References

[1] Davies, N., K. Mitchell, K. Cheverst, and G.S. Blair. "Developing a Context Sensitive Tourist Guide", Technical Report Computing Department, Lancaster University. March 1998.

[2] Sentient Computing Project, http://www.uk.research.att.com/spirit/.
[3] MIT Project Oxygen, http://oxygen.lcs.mit.edu/.
[4] Easy Living, http://research.microsoft.com/easyliving/.
[5] The Aware Home, http://www.cc.gatech.edu/fce/ahri/.
[6] US Privacy Act, 1974.
[7] EU Directive 95/46/EC.
[8] Privacy Online: A Report to Congress, http://www.ftc.gov/reports/privacy3/.
[9] Marc Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems.", Proc. Ubicomp 2001, Springer-Verlag, to be published Sep. 2001.
[10] Platform for Privacy Preferences Project (P3P), http://www.w3.org/P3P/
[11] Anonymiser, http://www.anonymizer.com/
[12] Crowds, http://www.research.att.com/projects/crowds/
[13] Rennhard, M., Rafaeli, S., Mathy, L., Plattner, B. and Hutchison, D., "Towards Pseudonymous e-Commerce", To appear in Kluwer Intl. Journal of Electronic Commerce Research.
[14] Marc Langheinrich , "A Privacy Awareness System for Ubiquitous Computing Environments", Submitted for publication, May 2002.
http://www.inf.ethz.ch/vs/publ/papers/privacy-awareness.pdf