User Identity and Ubiquitous Computing: User Selected Pseudonyms

Craig Chatfield
Griffith University
School of ICT
Brisbane, Australia
c.chatfield@griffith.edu.au

René Hexel
Griffith University
School of ICT
Brisbane, Australia
r.hexel@griffith.edu.au

ABSTRACT

As ubiquitous computing environments become more prevalent they will cover more and more of our public and private lives. Users will be able to interact with these environments to purchase goods, receive services and share information in ways unheard of today. But the success of these environments will be dependent on users' willingness to accept and manage the privacy risks of sharing their personal information within this new digital world.

This paper describes the concept of User Selected Pseudonyms, a method of allowing users to manage their identity in ubiquitous computing environments. This method of interaction allows users to control, either directly or through privacy preferences, what information about themselves they share with an environment to manage the risks to their privacy. The selected user information can then be used by the environments to personalise delivery of information and services. User Selected Pseudonyms allow personalised delivery of intelligent environment services while allowing users to maintain their desired level of anonymity.

Keywords

Intelligent Environments, Identity, Privacy, Security

1. INTRODUCTION

Intelligent environments are ubiquitous computing environments that use contextual information to provide users with personalised environmental information and services. These environments have been suggested for our homes, work places, public spaces and transportation systems [1]; potentially covering all areas of our lives in pervasive information sensing networks previously unimagined outside the realms of science fiction. This collection of information about users' and their environment is such a concern for user privacy that the management of this issue is imperative for the successful development of these environments [2].

Different intelligent environments differ in their purpose and intended audiences. Some environments are designed for use in commercial environments, typically tracking users' whereabouts and providing services to improve their productivity. These environments have limited populations, and an existing trust relationship is implied between the users and the environment's owner. Other environments provide services to the general public, and are open to anyone that wishes to make use of these services. These environments present more privacy concerns to users as there is no existing trust relationship between the user and the environment's owner. Personalisation of services from these environments is difficult, because users must provide information to the system without breaching their required levels of privacy.

In order for an environment to provide a personalised service to a user, it must be able to record a user's interests and behaviour over time. But this recording of user information and interactions open users up to a range of privacy attacks. Kobsa and Schreck [3] identify the privacy benefits of using pseudonyms within adaptive systems, and suggest that users be allowed to adopt multiple pseudonyms to improve their privacy. This research examines user's interactions with intelligent environments, and seeks to identify an interaction technique to improve user's privacy and to promote their use.

The present paper examines user identity and privacy within intelligent environments, and suggests a potential solution to the management of user identity and maintenance of user privacy within intelligent environments. Section two examines the relevant research on this topic, and identifies existing methods of handling user identity within intelligent environments. Section three and four describes User Selected Pseudonyms, a potential solution to identity management in intelligent environments. Section five and six concludes this work and looks forward to the development and evaluation of this identity management solution.

2. PRIVACY & IDENTITY MANAGEMENT

The management of personal information within intelligent environments is an important social and technical research challenge. Users determine what information they wish to share based upon the current context of the exchange and the identity of the information receivers [4], and their privacy preferences and goals for the current information exchange [5]. Privacy enhancing technologies seek to allow users effective control of their information without burdening them with excessive feedback or interaction requirements. Users must also be allowed to share the minimum information possible to achieve their goals, to use pseudonyms and be allowed anonymity where possible [6, 7].

The use of anonymity in these systems is good for both users and the environment's owners. Records of users' interactions with a system are a valuable source of information for an environment's owners. This data can be utilised without risk to user's privacy, as long as it cannot be linked to a specific user with data mining techniques [8]. This type of collection of information is more likely to be palatable to users then a more centralised storage of personal information, e.g. Microsoft Passport. This system gives the service provider access to huge amounts of user information and the privacy concerns brought on by this collection of information has lead to Passport's widespread rejection, e.g. [9].

Allowing users to be anonymous in intelligent environments improves their privacy, but it can make user adaptive systems much less effective [3]. Using pseudonyms has been identified as a method of allowing users to use adaptive systems, while maintaining some anonymity [3]. This idea seeks to allow users to utilise pseudonyms in a way that will protect their privacy from any historical data mining attacks, and should be used with other forms of security (e.g. encryption, Mix Zones [10], etc).

Users must receive appropriate feedback on the usage of their information if they are to make informed choices regarding their privacy and the sharing of information in intelligent environments [2]. This management of information is especially important in environments with multiple service providers. The EU disappearing computer privacy design guidelines call for systems to require minimum amounts of user information, provide effective users feedback and to make the user aware of the trade-offs between functionality, privacy and security [7]. The development of usable, effective privacy management interfaces for ubiquitous computing systems are essential for the development of environments that provide useful services while maintaining user privacy.

The management of the flow of user information is essential to prevent the breaches of privacy that occur when information crosses personal boundaries of privacy [11]. Any use of personal information must restrict its flow across the natural, social, spatial and ephemeral borders of privacy. These systems should restrict the flow of information outside of the physical location where it was provided, used only for the purpose it was collected and deleted after a stated timeframe. Variations to these principles should only be allowed with explicit user consent. These measures are essential if these systems are to respect the expectation of privacy by individuals in public spaces [11].

Intelligent environments should avoid active collection of user information through environmental sensors, especially without the user's consent. If contextual information is used to personalise services, it should focus on the interaction and not sensed details about the user or their handheld device. Service based intelligent environments should not double as security systems, and active sensing of users' information should only be used in special, well defined environments (e.g. emergency rooms, aircraft hangers etc) [12]. Intelligent environments that provide benefits to the user without invading their privacy will be much more useful than the traditional security and sensing environments currently under development.

3. USER SELECTED PSEUDONYMS

User Selected Pseudonyms is a method of managing user identity across multiple intelligent environments in a way that provides the benefits of personalised interaction with the security of using user controlled pseudonyms. When entering an environment users have the option of providing the environment with a previously used pseudonym (or history of interaction), to create a new pseudonym or to remain anonymous. User can maintain many different environmental pseudonyms, allowing them to effectively choose their required level of anonymity at any given time. This opt in approach to identity management allows users the flexibility to use these environments as they wish, sharing information about themselves only when given an incentive to do so.

When a user enters an intelligent environment for the first time, their handheld computer provides the environment with a random identification number, similar to a user placed 'cookie', with which it can store any personal details or user preferences recorded throughout the user's interaction with the environment. The handheld computer could automate the storage of the ID number, or the user could annotate the ID reflecting its intended use or privacy exposure, e.g. 'Anonymous News Gathering', 'High Risk', etc. The account linked to the ID number remains within the intelligent environment, and the interaction information within this account can be used to inform the environment's designers on the usage of the environment. The usability of the interface used to manage these pseudonyms will be critical to the success of this pseudonym management solution.

By allowing the users control over what information they share with intelligent environments, they can effectively control their involvement and interaction with this emerging form of computing. This suggests a new type of interaction with ubiquitous computing environments that allows users access to a range of services without privacy concerns. Users will be able to automate information gathering and service usage, like receiving updates on public transports scheduling and news bulletins while travelling to work, or ordering 'breakfast to go' at your favourite café while still on the train.

3.1 Usage Example

Consider the case of Belinda, a postgraduate student using an interactive bulletin board outside her school's office. This bulletin board could be used to access local school or university information or provide information accessed from other sources, e.g. bus timetables. When approaching the board, her mobile device recognises the request for identity information from the board and seeks to supply this information in accordance with her privacy preferences. Belinda's mobile device selects a pseudonym (or identity account), previously placed in the bulletin boards database, that contains her desire to only see post-graduate or general university notices.

The bulletin board is able to use the information within the identity account to personalise the displayed information, without breaching Belinda's privacy by sensing, evaluating or recording personal information. If Belinda had her preferences set differently, then an alternate account may have been provided, possibly containing a list of her subjects so she could receive any notices relevant to her studies. This selection of accounts allows the user to clearly see what information the intelligent environment, in this case the interactive bulletin board, is using to personalise her interaction with the information services. This transparency allows users more control over their privacy, and potentially greater confidence when interacting with these environments.

4. SYSTEM DESCRIPTION

This system replaces more traditional methods of recognising a user in an intelligent environment, e.g. requesting a user name or through the detection of a devices' MAC address. Figure 1 describes the interaction between the user and the intelligent environment. Users interact with an environment with their personal device, which identifies itself to the intelligent environment by providing an existing account stored in the environment. The intelligent environment maintains a model of

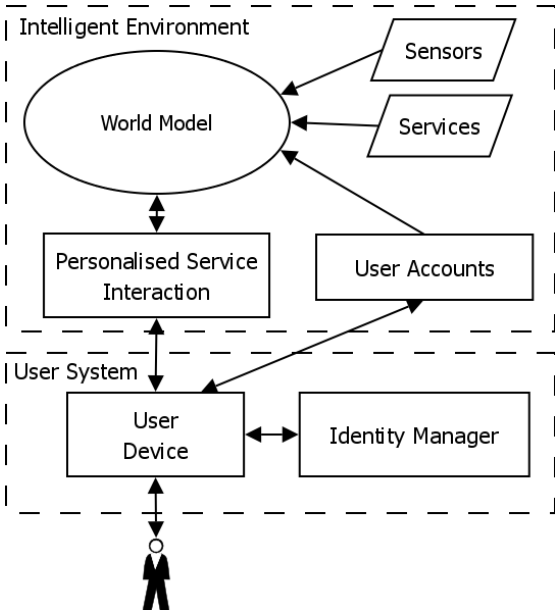

Figure 1: User Selected Pseudonyms Identity Manager

the environment based upon the information provided by hardware sensors, models of users present in the environment and the available services. Sensor data could include environmental conditions like the temperature, or the expected arrival of a particular bus at a bus station. Service information describes available services, and the information required for their use.

The 'User Accounts' database manages all accounts created by users for interaction within the environment. Information contained in these accounts would vary, depending on the purpose and privacy policy of the intelligent environment. The account would generally include records of previous interactions with the environment and user preferences for information or service delivery, but wouldn't normally include personal details like the users name unless this information was required to access a specific service. This user information is stored using an XML-based user modelling language [e.g. 13] allowing it to be easily utilised by all of the services required by the user.

The effectiveness of this system also depends on the user interface used to manage the user's accounts and information sharing preferences across potentially large numbers of intelligent environments [2]. This interface will be implemented on top of our system and evaluated in a user study. It will manage the Identity Manager's privacy preferences, which are responsible for selecting the account to be used in any given intelligent environment, and provide the user with the feedback required to identify potential risks to the user's privacy. Accounts containing sensitive information would be secured, either with a password or through other means, e.g. via voiceprint identification. The intelligent environment uses the information within the account and world model to develop a personalised service interaction interface. This personalised interface is then provided to the user to allow access to any required services.

When a user creates a new account with an intelligent environment they must provide information describing their service preferences and any required personal attributes. To improve this provisioning of information the intelligent environment will provide an information template when the user accesses the system without an existing account. This template describes the information required to access the services available in the intelligent environment, and its use could expedite the exchange of user information. This information is placed in the 'User Accounts' database and used by the intelligent environment to personalise the user's interactions with any available services.

While this system is most likely to be used with services available anonymously, services that require proof of particular personal details require some form of authorisation entity or signature provider [e.g. 14, 15, 16]. Hitchens *et al.* developed a system to allow private and secure provision of information to intelligent environments using a standard template published by an authorisation entity [16]. This system allows the third party to digitally sign user information confirming its accuracy. This allows the intelligent environment to have confidence in the information provided, without requiring the user to provide more information than is necessary. Any referenced third party may be required to prove its trustworthiness, e.g. via a trust network [17].

The use of user pseudonyms does allow the user some anonymity, but the longer a pseudonym is used, the greater the risk there is of the pseudonym being associated with the user. To avoid this, user accounts within the intelligent environment should have expiry dates to remove old data from the system [7]. Additional privacy safeguards could be built into the user interface, prompting the user to create new accounts after a default timeframe. A user's ability to effectively manage their privacy in these environments will be limited by the usability of their interaction interface. When an account is created it is associated with a particular privacy preference or persona that the user wishes to present. In any given environment the user could have multiple accounts, and the account used is that which reflects their required level of anonymity.

The easily discarded nature of these user accounts means that if a new level of privacy is required, users can simply create a new account, or provide new information to an existing account. The use of accounts with varying details allows the user to provide the minimum information required to achieve their interaction goals, as suggested by the EU disappearing computer privacy design principles [7]. The most effective method of managing these privacy preferences is an ongoing goal of this and other research [e.g. 2, 7].

Further privacy protection is provided by assigning expiration dates to each account, to reduce the risks of the user being associated with a pseudonym through historical data mining attacks, and through the creation of multiple accounts in an intelligent environment to allow the cycling through of these accounts at random intervals to prevent patterns of use being linked with the user. The ability to export personalisation data (e.g. interaction histories) from an account could also allow new accounts to be created without losing the personalisation benefits associated with a long history of use.

This system is especially useful for allowing users to interact with different environments based upon their current context. Users could use a different ID for a news delivery service, depending on what configuration of news they require (e.g. professional news, sports, business etc), or to manage the payment of goods using different identities (e.g. when using a personal or work account).

Using this system, the user is free to develop how they use intelligent environments, and to choose what information they wish to be associated with a given interaction.

5. DISCUSSION / FUTURE RESEARCH

User Selected Pseudonyms allows users to easily adapt their interaction with an intelligent environment to their current context. This allows users to automate interaction with environments by using different pseudonyms to personalise their interaction in different ways, e.g. by selecting the pseudonyms that gathers the correct bus timetables depending on their desired destination. Users can also maintain effective control over their exposure to privacy risks by selecting different pseudonyms to reflect their required level of anonymity. This system allows users to provide personal information or preferences without confirmation, unless it is required for a particular service, e.g. access to an 18+ movie. Existing methods of confirming parts of a user's identity [e.g.14, 16] can be used without requiring users to maintain traceable user accounts.

Further research in this area will seek to evaluate this method of managing user identity and privacy within intelligent environments. To validate this approach this system will need to be implemented to allow users to interact with these environments under normal use conditions. A user study investigating the use of these environments will be undertaken to investigate how effective this interaction method is at protecting user privacy. This study will examine what type of user interface and system feedback on the information usage is most effective at communicating the affect of sharing information on the user's privacy. It is hoped that the development of this technology will promote new methods of social interaction brought on by allowing users to dynamically identify themselves in different ways in different environments. This method of interaction moves users closer to being able to interact with ubiquitous computing environments without risking their privacy.

6. CONCLUSIONS

This paper has described User Selected Pseudonyms, a method for managing users' interactions with multiple intelligent environments. This interaction method allows users to mange which pseudonyms they use in a given intelligent environment, and allows users more control of their exposure to privacy risks. But the benefits of this system are not restricted to allowing private interaction with one intelligent environment. This system also allows users to automate interactions with individual intelligent environments, selectively interacting with services that provide tangible benefits to their lives.

The selective interaction with these environments will force developers to ensure value is added to an environment by the implementation of an intelligent environment. The privacy concerns associated with intelligent environments are numerous, with the predominate user concern seemingly that of a *big brother* like sensing network that knows their actions and location at all times. But these environments provide little benefit to end users, and are unlikely to be used. User Selected Pseudonyms allows users to control risks to their privacy, giving them the confidence to utilise the services provided by these environments while maintaining the same anonymity currently enjoyed without them.

7. ACKNOWLEDGMENTS

The authors would like to acknowledge the support of the Smart Internet Technology CRC.

8. REFERENCES

1. Lahlou, S., M. Langheinrich, and C. Röcker, *Privacy and trust issues with invisible computers.* Communications of the ACM, 2005. 48(3): p. 59-60.
2. Langheinrich, M. *Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems*. in *International Symposium on Ubiquitous Computing*. 2001. Atlanta, USA. p. 273-291.
3. Kobsa, A. and J. Schreck, *Privacy Through Pseudonymity in User-Adaptive Systems.* ACM Transactions on Internet Technology, 2003. 3(2): p. 149-183.
4. Lederer, S., A.K. Dey, and J. Mankoff, *A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments*, 2002, Technical Report, UCB-CSD-02-1188.
5. Adams, A. *Multimedia information changes the whole privacy ballgame*. in *Computers, Freedom and Privacy*. 2000.
6. Berendt, B., O. Gunther, and S. Spiekermann, *Privacy in E-commerce: State Preferences vs. Actual Behavior.* Communications of the ACM, 2005. 48(4): p. 101-106.
7. Lahlou, S. and F. Jegou, *European Disappearing Computer Privacy Design Guidelines v1.0.*, 2003, Disappearing Computer Initiative, Ambient Agoras Report, D15.4.
8. Canny, J. *Some techniques for Privacy in Ubicomp and Context-Aware Applications*. in *International Symposium on Ubiquitous Computing*. 2002. Göteborg, Sweden.
9. Bishop, T. *Microsoft's Passport to be tossed by eBay*, Seattle Post-Intelligencer, December 31, 2004.
10. Beresford, A.R. and F. Stanjano, *Location Privacy in Pervasive Computing.* Pervasive Computing, 2003. Jan - Mar: p. 46 - 55.
11. Marx, G.T., *Murky conceptual waters: The public and the private.* Ethics and Information Technology, 2001. 3(3): p. 157-169.
12. Langheinrich, M. *Privacy Invasions in Ubiquitous Computing*. in *International Symposium on Ubiquitous Computing Privacy Workshop*. 2002. Göteborg, Sweden.
13. Kay, J., B. Kummerfeld, and P. Lauder. *Managing private user models and shared personas*. in *Workshop on User Modelling for Ubiquitous Computing*. 2003. Pittsburgh, USA
14. Chatfield, C. and R. Hexel. *Privacy and Security within Intelligent Environments*. in *Australasian Conference on Computer-Human Interaction (OzCHI)*. 2004. Wollongong, Australia.
15. VeriSign, http://www.verisign.com/.
16. Hitchens, M., J. Kay, and B. Kummerfeld, *Secure identity management for pseudo-anonymous service access*, 2004, Technical Report, TR546.
17. Cahill, V., et al., *Using Trust for Secure Collaboration in Uncertain Environments.* Pervasive Computing, 2003. 2(3): p. 52-61.