

Privacy and Security within Intelligent Environments

Craig Chatfield, René Hexel¹

Griffith University, Brisbane, Australia
{c.chatfield,r.hexel}@griffith.edu.au

Abstract

This paper discusses the current research in maintenance of user's privacy within an intelligent environment. The need to ensure user privacy within an intelligent environment means the development is as much a socio-technical challenge as a technical one. Users must have complete confidence in the ability and willingness of an intelligent environment to keep their information private before the system will be used. The consideration of user privacy at the design stage is therefore essential to an intelligent environments success.

The paper presents a privacy aware intelligent environment architecture that seeks to incorporate the user privacy and security design requirements for an intelligent environment. The architecture uses secure communication and user pseudonyms to maintain user privacy, and trusted third parties for secure identity management. User information is managed by the user's privacy preferences, and the intelligent environment's services are utilised in a way that minimises the risk to a user's privacy.

Keywords

Intelligent Environments, Privacy, Security

INTRODUCTION

Intelligent environments are ubiquitous computing environments that interactively provide services based on contextual information such as user characteristics and environmental data. The potential dangers to users' privacy are increasingly being addressed in the literature surrounding ubiquitous computing and intelligent environments. Users unwillingness to trust ubiquitous computing systems is seen as the major impediment to the acceptance of these systems (Langheinrich, 2001). Intelligent environments infringe on user privacy, but the effects can be minimised with effective system design and implementation.

User privacy can be managed within an intelligent environment in many ways. Users must have control over exchanges of information, but this must be accomplished in a way that doesn't burden users with excessive amounts on information. The context of the information exchange (Dey, 2001), the use of aliases or pseudonyms to obscure the user's identity (Kobsa and Schreck, 2003) and the identities of the receivers of any shared information (Lederer et al., 2002) all have an impact on the affect of an information exchange on a user's privacy. Trust and reputation has also been suggested to help manage the exchange of personal information between unknown users and intelligent environments (Goecks and Mynatt, 2002).

The security of an intelligent environment is an equally important design consideration, ensuring the environment is protected against unauthorised access of user information and the illegal use of the intelligent environments services. The level of security required in an intelligent environment will depend on the environment's purpose and location, but users should retain control over their information security. We suggests that all security encryption and resources should be located outside of the intelligent environment, with trusted third parties such as the user's own information domains or with an identity broker.

This paper acknowledges these influences upon user privacy and information security, and presents an architecture that allows users to control their personal information. This architecture seeks to control the flow of information within the environment, and to allow the users to interact with the environment in a seamless, non-burdensome way.

PRIVACY AWARE INTELLIGENT ENVIRONMENT ARCHITECTURE

This privacy-aware architecture (Figure 1) describes an interaction framework for users within an intelligent environment, and between users and the environment's services. The architecture allows all users to remain anonymous, sharing only the information they choose with the environment and other users. It is assumed that all information passing through the intelligent environment is secure, and no recording of user details is carried out.

¹ The authors would like to acknowledge the support of the Smart Internet Technology CRC.

To guarantee user privacy, an intelligent environment must secure all user information and all references to user identity. To ensure these references are secured, the intelligent environment temporarily assigns each user in the environment with an alias. This alias can be used to request information about the user from the user's personal domain, through an identity manager. Each user's personal domain contains (amongst other information) the user's profiles that are displayed for different types of users. A user modelling tool similar to the Personis user modelling system (Kay et al., 2002) could be utilised to provide different audiences with different user profiles.

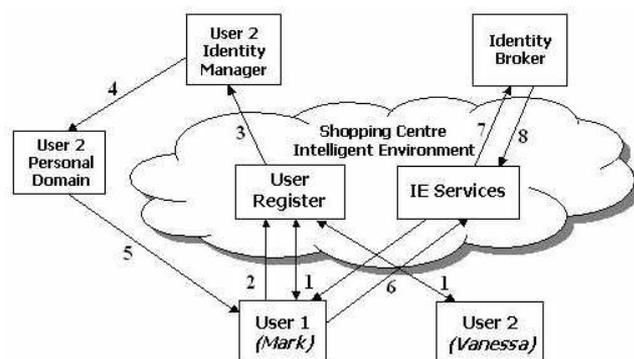
Users can request information about another user through their identity manager. This request is processed through the intelligent environment, which securely exchanges the user's temporary alias with their unique identifier (e.g. the user's Mac Address). Users could provide the intelligent environment with a pseudonym if they wanted more identifiability, or could utilise a randomly generated MAC addresses for more anonymity.

The identity manager takes the user's unique identifier and directs the request to the user's personal domain. This domain will then securely provide a selected profile based upon the user's privacy preferences, and the identity of the inquirer. The results of this information request are again passed through the intelligent environment, ensuring no identifying information (beyond that provided by the user) is available to the inquirer. Trust and reputation could be used to enhance the effectiveness of user's privacy preferences. A user or system with an outstanding reputation, either globally or amongst the user's friends, is potentially more appealing from a trust point of view, and may affect the profile returned.

Details of the services provided by an intelligent environment are described to the user's mobile device, including any information required from the user. To take advantage of these services, the users must (either actively, or through the setting of personal preferences) provide a service request, and any required information, to the intelligent environment. If a service requires verifiable information, users can make use of an identity broker to verify user information in a secure way. An Identity Broker is an accredited third party that maintains an account verifying some or all of the user information (e.g. VeriSign's Consumer Authentication Service (VeriSign, 2004)).

An identity account enables external systems (e.g. intelligent environments) to confirm necessary details about the user (e.g. name, age, etc). This system works in much the same way as an electronic ID card issued by a trusted source (e.g. bank, government department). So whenever a user wants to prove his identity, he simply provides a secure key for the system to query. A user could potentially have multiple relationships with an identity broker, each representing a different persona, or a different subset of their personal information. To further facilitate user privacy, an identity broker should only provide the minimum information necessary to authenticate the request (e.g. confirming the user is over 18, but not providing the user's birthday).

For trustworthy information to be stored at the identity broker, an account must first exist for the enquiring user. Depending on the account, and the information being verified (e.g. financial payment, proof of legal name, allergies etc) additional verification of the facts managed by that account may be required. This would be handled through the provision of verifiable data through independent channels such as personal inspection of a photo ID, fingerprint matching, etc. The intelligent environment would not store this verification information, but would instead route it between the institution that maintains and verifies the account and the requesting systems.



1. Users connect to IE, Aliases assigned, IE services sent to user
2. Mark requests information on Vanessa from IE
3. Information request passed to Vanessa's Identity Manager
4. Mark's information forwarded to Vanessa's Personal Domain
5. Vanessa's selected 'persona' returned to Mark
6. Request for Service, ID #
7. Request for confirmation of ID
8. Identity Broker's ID confirmation

Figure 1: Privacy Aware Intelligent Environment (IE) Architecture

EXAMPLE SCENARIO

The following scenario illustrates how the users are able to interact anonymously with each other and the services within the intelligent environment. This scenario shows the information flow within the environment, and the interaction between two users, Mark and Vanessa, and their environment. This scenario describes an interaction with the architecture described in Figure 1. The numbered description describes the flow of information within the intelligent environment, and reflects the events in this scenario

Mark and Vanessa are users who have just entered the entrance of a large shopping complex. Both have mobile devices that wirelessly connect to the intelligent environment that exists throughout the complex. At this time, each user is given a temporary alias by the intelligent environment, which the environment can match to the device's unique identifier (and thus to the user). Each temporary alias is initially available to all users within the intelligent environment. The intelligent environment can track a user while within the environment, but doesn't know who the user is beyond this temporary alias. The available services are displayed on the user's personal device when they enter the environment.

While shopping, Mark recognises Vanessa as someone that attends the same local university. Hoping to find some common interests, Mark supplies Vanessa's temporary alias and his personal details to the environment, along with a request for more information. The intelligent environment substitutes the alias with Vanessa's identity manager ID number and directs the request, with Mark's personal information, on to the identity manager. A simple URL could be used to access the identity manager. Depending on the required level of anonymity, this URL could access a service within the users' personal domain or an anonymising server or proxy.

The identity manager would then examine the user information forwarded from the intelligent environment, and use this to determine what action to take. This could be a simple look up table, or a sophisticated relationship manager utilising measures of trust, reputation, current contextual information and other forms of association (i.e. recent proximity or matching of any available interests) to construct a dynamic persona. Actions could range from the referral to some or all data about a persona within the users personal domain, through to complete refusal of contact.

Mark receives a representation of Vanessa's personal information, which has been transmitted through the intelligent environment. In this case, Vanessa allows Mark to see that she is from Brisbane (Australia), but he doesn't get her exact address, where (but not what) she studies, and he sees an anonymised contact email address. If Mark and Vanessa were friends, this would be recognised by her identity manager and he would possibly also see Vanessa's actual address and phone number (and possibly other information such as her appointments for today). With different privacy preferences Vanessa's response could her include interests and a brief description.

INTELLIGENT ENVIRONMENT MODEL IMPLEMENTATION

This section describes in more detail our model for development of scalable intelligent environments that support and protect user privacy and security. In particular we examine the interaction between users within an intelligent environment and the ownership of the user's contextual information.

User Interaction and Context Information

In our scenario above, Vanessa and Mark are represented in the intelligent environment using a temporary user alias. These aliases would be assigned to a current, temporary identity manager ID that gets associated with a static unique ID such as the MAC address of the handheld device they are carrying. This temporary number is similar to a phone number, but unlike a phone number, it only has meaning in a particular session, preventing ID triangulation. All entities enquiring to or about the users within the intelligent environment will only receive these temporary aliases. Furthermore, to prevent breaches in privacy through location tracking history, the relationship between the temporary alias and the user is destroyed when the user leaves the environment.

Any information exchanged between an external source and a user, as in the case of Mark requesting information on Vanessa, is routed anonymously through the intelligent environment. This ensures that Mark only receives the information Vanessa (or her privacy preferences) want him to see. A similar path for information sharing would occur if Mark were outside of Vanessa's current intelligent environment, with the results again based upon her privacy preferences. A voice call for example could, depending on the originator, connect directly with Vanessa's mobile device, or more securely be routed via a voice service within the intelligent environment.

The ownership of context information is an important concern when considering the scalability of intelligent environments. To avoid breaching user privacy, intelligent environments should maintain existing barriers to protect user privacy. Intelligent environments should respect the natural borders of observation (Langheinrich, 2002) and not provide context information to entities outside these borders. Therefore the current context of a user within an intelligent environment should be restricted to that environment, and to users within that environment. Practically this means that this context can only be used by people within the environment, e.g. to determine how their mobile device should react, or by the environment itself, e.g. to determine whether a user is within range of a potential service.

Context should only be passed outside these borders in clearly defined ways, and when approved by the user's privacy preferences (e.g. using the LocServ service to provide location information to external entities (Myles et al., 2003)). Therefore no contextual information should be passed outside the environment, except by the users interacting with their personal information domain.

CONCLUSIONS AND FUTURE RESEARCH

The identity management privacy architecture (Figure 1) maintains user privacy through the use of pseudonyms and secure identity management. The use of user privacy preferences allows users to be completely anonymous to both the environment and to other users. The anonymity and control of the flow of their information will promote greater user confidence in ubiquitous computing systems, and improve the systems' ability to support social systems. It is hoped that this architecture will form the basis for future intelligent environment architectures.

Further research directions must consider the role of the identity manager and broker in this model. The use of trust and reputation in the identity manager could allow for more effective management of information requests. The knowledge of friends' contacts (to determine a local reputation) requires access to your friends' contact lists. Access to global reputation systems could also take many forms, but would require access to user's contacts and personal information to be effective.

The role an identity broker will play in securely identifying users must also be examined. This confirmation of identity could take a number of different forms. The user might provide a simple identity number, encrypted to prevent this key being collected through various data mining techniques, which will server as a pointer to a specific representation of their identity on the identity broker's server. Identity provisioning should not be limited to proving a user's name or physical descriptions. Identities could contain any number of attributes or secure information, e.g. Medical History, Financial Information and Environment specific preferences of any kind. The content and purpose of these identities could differ with different interaction designs.

Finally, this architecture must be developed to allow user interaction with the intelligent environment. The management of privacy information is not only a technical, but, perhaps more importantly, a socially bound problem that is deeply rooted in user perceptions. Usability remains the biggest challenge before the goal of a scalable, distributed intelligent environment that ensures user privacy and security can be realised. Implementation efforts are currently underway that seek to incrementally test and refine the viability and usability of this intelligent environment architecture.

REFERENCES

- Dey, A. K. (2001), Understanding and Using Context, *Personal and Ubiquitous Computing*, 5.
- Goecks, J. and Mynatt, E., (2002), Enabling Privacy Management in Ubiquitous Computing Environments through Trust and Reputation Systems, In Proceedings of the Computer-Supported Cooperative Work
- Kay, J., Kummerfeld, B. and Lauder, P., (2002), Personis: a server for user models, In Proceedings of the Adaptive Hypertext, pp. 203-212
- Kobsa, A. and Schreck, J. (2003), Privacy Through Pseudonymity in User-Adaptive Systems, *ACM Transactions on IT*, 3.
- Langheinrich, M., (2001), Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, In Proceedings of the Ubicomp, pp. 273-291
- Langheinrich, M., (2002), Privacy Invasions in Ubiquitous Computing, In Proceedings of the UbiComp Privacy Workshop, Göteborg, Sweden, pp.
- Lederer, S., Dey, A. K. and Mankoff, J., (2002), A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments, Technical Report, University of California
- Myles, G., Friday, A. and Davies, N. (2003), Preserving Privacy in Environments with Location-Based Applications, *Pervasive Computing*, Jan - Mar.
- VeriSign (2004) <http://www.verisign.com/>, 7 June, 2004

COPYRIGHT

Chatfield, C., Hexel, R. © 2004. The authors assign to OZCHI and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to OZCHI to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.