Privacy and security in ubiquitous personalized applications

Article

CITATIONS
37

READS
168

2 authors, including:

Judy Kay
The University of Sydney
387 PUBLICATIONS **6,215** CITATIONS

SEE PROFILE

Privacy and Security in Ubiquitous Personalized Applications

Ajay Brar, Judy Kay

School of Information Technologies
University of Sydney
{abrar1, judy}@it.usyd.edu.au

Abstract. Personalization systems provide customized service based on user preferences. In ubiquitous computing environments, personalization can be achieved based on user preferences stored on mobile devices. This requires a mechanism for capturing user information and making it available to users. However, storing and exchanging potentially personal information raises user privacy concerns. Past solutions to privacy in ubiquitous computing have been ad-hoc, application specific or partially implemented. This work explores a general framework to providing privacy-aware personalization in ubiquitous computing environments. A prototype implementation of the framework has been developed and evaluated. This paper describes the approach used and its underlying concepts.

1. Introduction

An important current development in the area of computing is the emergence of ubiquitous computing. Ubiquitous computing (or ubicomp) envisions a computational environment integrated into the physical world, featuring a multitude of heterogeneous computing devices interacting seamlessly to provide information when and where required. This proliferation of computing into the physical world suggests new paradigms of human computing interaction inspired by constant access and increase in information and computational capabilities [1]. Personalized services form one such interaction.

Personalization in ubiquitous computing environments would depend on detecting user characteristics and preferences and providing services based on these. User preferences may be stored on the user's mobile device, e.g. a PDA, and released in exchange for personalized services. Service providers would benefit from being able to provide improved and differentiated services, such as, targeted advertising and loyalty reward programs. Users would benefit from receiving information and services customized to their preferences. For example, a user could walk into a video store and receive information about latest releases in genres of his liking along with news about special offers that match his viewing preferences. The genre preferences and the user's viewing habits would be stored in a user model on his PDA and would form the basis of any personalization offered by the service providers, in this case, the video store.

User models provide a natural construct for storing, managing and communicating user information to personalize services in ubiquitous computing environments. However, maintaining user models and releasing them to service providers, raises privacy and security concerns relating to the storage, access and processing of the information contained within the model. Users may wish to limit and control the amount of information released to the service provider. The information stored is often personal and may potentially identify the user. Protecting user identity would require providing mechanisms to allow anonymous/pseudonymous interaction with personalized services. Service providers would also need to ensure the accuracy and authenticity of the information provided by the user. Mechanisms are thus required for defining relevant subsets of the user model, allowing users to control their release, and authenticating and protecting the integrity and confidentiality of the user information released to the service provider. These topics have been extensively researched in relation to the World Wide Web [8, 10], but have received much less attention [5] in the context of ubiquitous computing.

The majority of past work on privacy has focused on providing anonymity, hiding user identity and keeping personal information secret [7]. However, this addresses a narrow aspect of privacy and does not cover scenarios where users *want* to share selective information with others [7]. Participation in the social world requires disclosure of information; users need to provide information about them in order to personalize information and services. Thus, privacy needs to be seen in terms of a negotiated controlled disclosure of information. This paper addresses a wider notion of privacy that focuses on providing users with notice of data collection, choice regarding collection and informed consent, so they can make informed decisions regarding the disclosure of their personal information.

In this paper, we propose a framework for providing personalized services/information to users, based on user preferences stored in mobile devices while minimizing risks to user privacy. The framework, called Secure Persona Exchange (SPE), provides a set of tools for capturing, representing and storing user preferences as subsets of a user model, releasing the information to a user's mobile device, and restricting and controlling the release of the information to service providers while protecting user privacy.

2. Related Work

This work draws on research in the areas of user modeling and privacy mechanisms for the Web and in ubiquitous computing. User modeling has an important role in ubiquitous computing and is essential for personalization of user environments through user information (collected from sensors) stored in user models [9]. The information including location information, current activity, preferences etc can be used to provide tailored services to users. Kay et al describe the architecture of distributed, ubiquitous user models [9]. The architecture relies on the concept of partial user models, called *personas*, which are accessed by services in the ubiquitous environment. Personas implemented using the scaled-down user-modeling server, PersonisLite, can be stored on user mobile devices. Users can control the content of

each persona by defining access control at different levels: evidence source, component, view and context [9]. Personas were used to represent user information in the SPE framework.

The Platform for Privacy Preferences (P3P) [13] is a specification by the World-Wide Web Consortium (W3C) and provides a framework for informed online interactions on the Web, allowing users to negotiate agreements with services that declare their privacy practices and request data. P3P provides a vocabulary and standard machine-readable format to allow websites to declare their privacy practices and describe the data they collect. User privacy preferences are described using A P3P Preference Exchange Language (APPEL 1.0), defined in a companion specification [14]. Users can use this language to express their preferences as a set of rules (called a ruleset), which can then be used by their user agent to make automated or semi-automated decisions regarding the acceptability of machine-readable policies from P3P compliant Web sites [14].

There has been past work on adapting P3P to provide privacy in ubiquitous computing environments. Langheinrich suggests a P3P-style architecture to provide notice of data collection in ubiquitous computing environments [11]. Sensors and other recording devices can use a P3P declaration format to announce via one or more well-known mechanisms, their data collection practices. User agents on user mobile devices can release contextual information based on a comparison between the privacy declaration and user preferences encoded in a machine-readable format similar to APPEL The Privacy Awareness System (pawS) implements P3P in ubicomp environments to provide notice-choice based data collection [12]. The SPE framework includes a P3P style privacy awareness mechanism.

3. Framework Design

The Secure Persona Exchange (SPE) framework is based on P3P with an underlying notice-choice privacy model. Personas are used to represent user information and provide personalization. Machine-readable policies based on the P3P vocabulary are used to provide notice of data collection and decisions are based on user preferences expressed in APPEL. The framework also contains provisions to allow access to services with varying degrees of anonymity. The framework and its architecture is described in detail in [24]. This section describes the high level requirements and features of the framework.

3.1 End User Requirements

Table 1 summarizes the end-user requirements for the system. These requirements are based on analysis of research papers discussing user privacy preferences in ubicomp systems [6, 7, 15]; analysis of privacy laws and regulations [3]; and analysis of design guidelines for privacy-aware ubicomp systems [2, 4, 11].

Table 1. Summary of end-user requirements

End – user requirements
• Purpose specification • Openness • Simple and appropriate controls • Limited data retention • Pseudonymous interaction • Decentralized control

First, a mechanism is needed that allows users to view what benefits are offered by the personalized service and what personal information is needed to offer those benefits. They should be aware of the purpose of data collection [3]. This corresponds to the 'Clear value proposition' mentioned in [7]. The *PURPOSE* tag in P3P privacy policies can be used to describe the purpose of data collection and specify what benefits will be provided through personalized service.

Second, users should be aware of any data collection that takes place [3]. While this may seem to contradict the invisibility property of ubicomp systems, the requirement actually means that users should be able to view the data collected at any instant in time. A user agent may still perform actions on behalf of the user; but a log of all requests should be maintained and users should be able to configure the agent to prompt them for certain persona requests. This can be achieved using the PROMPT attribute of APPEL rules and corresponds to the "Notice/Awareness" principle mentioned by [11].

Third, users want simple control over the information disclosed and the entity to which this information is released [6, 7]. User information can be divided into personas based on the sensitivity of the information and the personalization, which can be provided based on it. For example, a user may have personal and public personas. Users may decide to disallow any access to the personal persona but allow any service to access the public persona. These access levels can be configured using APPEL rulesets.

Fourth, there have been user concerns over long-term retention of personal data [7]. Since, data is stored would be stored by service providers, limiting retention of personal data is outside the scope of the system. However, the P3P "RETENTION" tag can be used to discover the length of the period for which service providers would store user data and preferences can be specified to release information only to service providers with a limited data retention policy.

Fifth, users may prefer to interact with personalized services under assumed identities (pseudonyms), perhaps without divulging their actually identity. Pseudonymous interaction is supported: users can maintain a collection of user models (personas). Users can select one of these for use with a particular personalized service.

Finally users are concerned about systems that centralize data since sensitive data is stored on computers outside their control [6]. SPE follows a distributed architecture with user data stored on their mobile devices and thus under their control.

3.2 Personalization

The SPE framework implements client-side personalization where user information is provided to service providers through subsets of the user model known as personas stored on the user's mobile device. A persona thus captures the information regarding the user and their preferences that is needed for personalizing a particular service. Client-side personalization through personas addresses user concerns relating to the storage of personal data on systems outside their control. It also addresses legal requirements present in privacy laws and regulations relating to the storage of personal information. A major challenge for client-side personalization is ensuring the authenticity and integrity of user information. This is realized in the SPE framework through an Authorizing Entity responsible for creating user personas and releasing them to users. The Authorizing Entity signs the persona and also separately provides the service provider with persona templates (describing the structure of the persona) to allow them to interpret the information provided by the user, The Authorizing Entity is thus the trusted third party in the exchange and plays a role similar to the Certification Authority in PKI. An issue with client side personalization is the availability of user information. Since the information release is controlled by the user, the availability of the information cannot be guaranteed. This is, however, a business issue and is not addressed in this work.

3.3 Notice Choice Privacy Model

The SPE framework is based on the P3P notice-choice privacy model. Service providers issue requests for user information represented in one or more personas along with their privacy policy described using P3P vocabulary. The privacy policy describes the purpose of data collection, the entity collecting the data, all entities that shall have access to the data, the period for which the data will be stored and other statements required by P3P. This comprises the notice part. The privacy policy is evaluated against the user's privacy preferences and the user may configure these to prompt for action, release data or block data release based on the contents of the privacy policy. Default privacy preferences are provided for usability purposes but users can also define their own privacy preferences (based on the APPEL specification) and are thus not restricted to choosing the least intrusive of a set of preferences. This provides users with choice regarding data collection thus allowing them to make informed decisions regarding the release of his information. The P3P-like elements thus provide appropriate notice and user privacy preferences defined using APPEL provide appropriate choice.

3.4 Pseudonymous Interaction

The SPE framework can be combined with a network-level anonymizer to provide pseudonymous access to personalized services. Personalization systems may not need to know the actual identity of the person involved. All they need is some way of distinguishing different sessions and relating a particular set of interactions to some identity and maintain this across multiple sessions. The SPE framework supports pseudonymity through the concept of personas. Users may interact with services using different personas containing separate information, add new personas to their mobile

device and switch between them. Multiple users can store their personas on the same device and personalize services based on these.

3.5 Mobile Context

The core requirement underlying the SPE framework is personalization within a mobile ubiquitous computing environment. Thus user information is stored on mobile devices (the prototype was implemented on a PDA) and communicated to service providers across a wireless network (the prototype used WiFi).

4. Security Requirements and Mechanism

Security in user modeling is not a goal in itself, but an auxiliary means for realizing privacy [16]. The same principle applies to ubiquitous computing; security measures are designed to protect the privacy of the data exchanged and the entities involved in the system.

Requirements for security comprise requirements for implementing the four key attributes of security, i.e., authentication, confidentiality, integrity and non-repudiation [19]. Another key attribute of security is availability. Within the context of user modeling, availability refers to the amount of user modeling functionality available to user model client (in this case, the service provider) [16]. Since the functionality is adjustable depending upon user preferences, as expressed in APPEL, availability cannot be guaranteed. Similarly, ubiquitous computing applications depend on the availability of networking infrastructure (such as WiFi) and thus, availability of a particular ubiquitous system cannot be independently guaranteed. Thus, availability is not included as a security requirement.

The security requirements discussed here apply only to securing the communication between the participants of the system. Service providers would be responsible for securing the storage of personas and templates on their systems. The system also does not provide mechanisms for securing personas and templates stored on the user's mobile device. A solution may be to store encrypted personas along with a one way keyed hash of the persona. On a PDA, however, this may introduce additional processing delays. Similarly, the authorizing entity is expected to provide its own methods for securing the data storage.

Requirements for communication security are discussed below:

- Confidentiality: personas may contain personal information and thus their content needs to be kept secret from entities other than the participants in the system. Secrecy of exchange can be achieved through SSL.
- Integrity: personas and templates need to be protected against tampering during communication. This may again be achieved by using secure message digests and communicating over SSL. Users would be responsible for ensuring the integrity and confidentiality of personas stored on their mobile devices.
- Authentication: users need to authenticate personas and templates released by the authorizing entity. Similarly, service providers need to authenticate the templates released by the authorizing entity and the personas released by the user. Additionally, users need to authenticate the service provider prior to releasing their personas. Thus there are two kinds of authentication that is required: *entity* authentication to authenticate the participant in the exchange and *data*

authentication to authenticate the personas and templates exchanged. Note that users do not authenticate themselves while communicating with service providers. This allows them to preserve their anonymity. Entity authentication can be achieved through X.509 certificates and communicating over SSL while data authentication can be achieved through RSA signatures together with a Certification Authority. Note that data authentication implicitly provides data integrity (for if a message has been modified, the source has changed) [19].

- Non-repudiation: refers to preventing an entity from denying previous commitments or actions [19]. Non-repudiation is not a core security requirement of the system but may be required to prevent a service provider from denying data collection.

5. Conclusions and Future Work

The SPE framework provides privacy-aware personalization in ubiquitous computing environments. We have presented an analysis of user requirements, requirements for personalization, privacy and security based on past research. We also described how the Secure Persona Exchange (SPE) framework addresses these requirements. Current challenges in the implementation relate to the immaturity of software support for PDAs, including the serious issue of fixed MAC addresses.

References

1. Abowd, G. D. and E. D. Mynatt (2000). “Charting past, present and future research in ubiquitous computing.” ACM Transactions on Computer-Human Interaction, Special Issue on HCI in the new Millenium. 7(1): 29-58
2. Adams, A. (2000). “Multimedia Information Changes the Whole Privacy Ball Fame”. Proceedings of Computer, Freedom, and Privacy. Toronto, Canada. ACM Press.
3. Australian Privacy Act (1988). “Information Privacy Principles under the Privacy Act 1988.”
4. Belotti, V. and A. Sellen (1993). “Design for Privacy in Ubiquitous Computing Environments”. Proceedings of the Third European Conference on Computer Supported Cooperative Work (ESCW’93). Milan, Italy. Kluwer Academic Publishers.
5. Hitchens, M., J. Kay and B. Kummerfeld (2004). “Secure identity management for pseudo-anonymous service access”. University of Sydney School of Information Technologies Technical Report TR 546. June 2004
6. Hong, J. I., G. Boriello, J. A. Landay, D. W. Mc Donald, B. N. Schilit and J. D. Tygar (2003). “Privacy and Security in the Location-enhanced World Wide Web”. Proceedings of Fifth International Conference on Ubiquitous Computing: Ubicomp 2003 (Workshop on Ubicomp Communities: Privacy as Boundary Negotiation). Seattle, WA
7. Hong, J. I. and J. A. Landay (2004). “An Architecture for Privacy-Sensitive Ubiquitous Computing”. Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSYS). Boston, Massachusetts, USA.

8. Kay, J., R. J. Kummerfeld and P. Lauder (2003). “Managing private user models and shared personas”. UM03 Workshop on User Modelling for Ubiquitous Computing.
9. Kobsa, A. and J. Schreck (2003). “Privacy Through Pseudonymity in User-Adaptive Systems.” ACM Transactions on Internet Technology. 3(2): 149-183.
10. Langheinrich, M. (2001). “Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems”. Ubicomp 2001 Proceedings.
11. Langheinrich, M. (2002). “A Privacy Awareness System for Ubiquitous Computing Environments”. Ubicomp 2002.
12. Cranor, L. F., M. Langehinrich, M. Marchiori, M. Presler-Marshall and J. Reagle (2002). “The platform for privacy preferences 1.0 (p3p1.0) specification. W3C proposed specification.”
13. Cranor, L. F., M. Langheinrich and M Marchiori (2002). “A P3P Preference Exchange Language 1.0 (APPEL 1.0). W3C Working Draft.”
14. Lederer, S., A. K. Dey and J. Mankoff (2002). “Everyday Privacy in Ubiquitous Computing Environments.” Ubicomp 2002 Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing.
15. Schreck, J. (2003). *Security and Privacy in User Modeling.* Kluwer Academic Publishers.
16. Westin, A. F. (1970). Privacy and Freedom.
17. Menezes, A. J., P. C. v. Oorschot and S. A. Vanstone (2001). *Handbook of Applied Cryptography.* CRC Press.
18. Python Library Reference (2004).
19. Nielsen, J. (1994). *Usability Engineering*. Morgan Kaufmann
20. Whitten, A. and J. D. Tygar. Why Jonny Can’t Encrypt: A Usability Evaluation of PGP 5.0. 8th USENIX Security Symposium.
21. Fu, K., E. Sit, K. Smith and N. Feamster (2001). Dos and Don’ts of Client Authentication on the Web. !0th USENIX Security Symposium. Washington D.C., USA
22. OWASP (2002). A Guide to Building Secure Web Applications: The Open Web Application Security Project. 2004.
23. Brar, A. and J. Kay (2004). *Privacy and Security in Ubiquitous Personalized Applications*. Technical Report 561. School of Information Technologies, University of Sydney.