Handling Personalized Redirection in a Wireless Pervasive Computing System with Different Approaches to Identity

Yuping Yang, M. Howard Williams, Nick Taylor, Sarah McBurney and Elizabeth Papadopoulou

Abstract— **One important feature of a wireless pervasive computing system is to ensure that any incoming communication addressed to the user is dealt with according to the user's wishes – sent to an appropriate device, forwarded to another user, stored, etc. This is referred to as personalized redirection of communication. To do this it is necessary to maintain a profile of user preferences. However, in doing so, there is a natural risk to the security and privacy of the user. This paper considers two systems – one developed specifically to study personalized redirection and the other a wireless pervasive computing system which incorporates some of these ideas. Three different approaches to handling user identity that have been adopted in these two systems are described. The effects of these different approaches on personalization and the consequences for security and privacy in a wireless pervasive computing environment are discussed and compared.**

Index Terms— **personalized, pervasive, redirection, privacy.**

I. Introduction

THE environment for mobile users is rapidly increasing in complexity as the range of different services available explodes, the number of heterogeneous communication networks increases and the developments in sensor and device technologies lead to potentially large numbers of sensors and devices in the user's environment [1]. The goal of pervasive computing is to provide an intelligent environment to enable the user to manage this situation with minimal intervention [2], [3]. This includes dealing with services and resources in a dynamic fashion that best meets the user's needs and preferences [4].

Adaptability and personalization are two key aspects of a wireless pervasive computing system. In the case of adaptability, the system needs to adapt its functionality and behaviour depending on the context of the user. In particular, as the user moves around, a pervasive system should track the changing context of the user, and adapt its behaviour when necessary. In the case of personalization, the system needs to keep track of a user's personal preferences and their dependence on context [5]. This is essential in order to adapt the behaviour of the system to meet the needs of the user with minimal user intervention.

These two aspects are particularly important for telecommunication services in a wireless pervasive computing system. One facet of the functionality of such services, which relies on these two aspects, is that of personalized redirection. The latter is concerned with dealing with incoming communications addressed to the user. These may be simple messages, as in SMS or email, or more complex multimedia streams, including both audio calls and audio/video streams. Whatever form the communication may take, a pervasive system needs to deal with it appropriately.

PRCD is a system that was developed specifically to deal with the problem of personalized redirection [6]. Its aim was to build up a profile for each user, which stores the personal preferences and their relation to context, and to use these preferences to deal with incoming communications dynamically depending on the context of the user when the communication arrives.

This idea has been taken further in a large European research project called Daidalos. Daidalos [7] stands for "Designing Advanced Interfaces for the Delivery and Administration of Location independent Optimized personal Services". This project (which has some 45 partners) aims to integrate a range of heterogeneous networks in a seamless way and develop a pervasive service platform on top of this to provide the user with personalized dynamic behaviour with minimal user intervention. Dynamic personalized redirection is an important aspect of the functionality of the wireless pervasive computing system that is being developed.

One particular problem with any form of personalization, and personalized redirection of communication is no exception, is that of the risk to privacy and security [8]. To handle personalized redirection it is necessary to maintain a profile of user preferences as well as information on the context of the user. However, in doing so, there is a natural risk that some other user can gain unauthorized access to such information.

This paper is concerned with the use of different approaches to handling user identity in these systems and their effect on personalization and security. The next section provides some background on previous work done together

Manuscript received July 28, 2005. This work was supported in part by the European Union under the FP6 programme (Daidalos project) which the authors gratefully acknowledge.

M. H. Williams is with the School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK (phone: +44 131 4513430; fax: +44 131 4513327; e-mail: mhw@ macs.hw,ac.uk).

Y. Yang, N. Taylor, S. McBurney and E. Papadopoulou are with the School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK (e-mail: ceeyy1, nkt, ceesmm, ceeep1@macs.hw.ac.uk).

with a simple example to illustrate the notion of personalized redirection. Sections III and IV describe the two systems in question – PRCD, which is concerned solely with personalized redirection, and Daidalos, which is concerned with a pervasive computing system which incorporates some of these ideas. Section V describes the effects of different strategies for handling user identity adopted in these two systems and how they affect personalized redirection and security. Section VI summarizes and concludes.

II. Personalized Redirection

The ideas of message integration and of redirection of particular forms of communication to different devices have attracted growing interest. A number of research projects have been investigating techniques for achieving this and services are now emerging for simple message integration and redirection – e.g. email/SMS integration (SMSMate), email/voice integration (SonicMail), text/SMS integration (SMSMessenger), etc. Although these are fairly limited in the range of data sources that can be handled, more general services are beginning to emerge.

Some of the research prototypes on which current services are based include the following. The SPIN project [9] designed a messaging system to provide seamless integration of multiple mode formats, including voice, fax and email messages, based on the assumption that various data formats can be transformed into a standard text format. The Iceberg project [10] is based on service composition using Internet-based standards for flow routing. However, it depends heavily on a pre-existing network infrastructure, which requires a large number of nodes called Iceberg Access Points (IAPs).

TOPS [11] is focused on telephony-like applications and provides an architecture for redirecting incoming communications by a Terminal Tracking Server. IPMoA [12] makes use of mobile agents to integrate both aspects of user mobility - terminal mobility as well as personal mobility - into a single framework, which handles personal communication (e.g., MPA [13]) and personalizing operational environment (e.g., NetChaser [14]). A mobile agent is used as a Personal Communication Assistant (PCA), which may utilize some transcoding codes from the network's repository when conversion is required - although transcoding codes are usually platform dependent and hence there is no guarantee that transcoding code can run on any particular platform.

This paper focuses on the message redirection aspect. As previously explained, personalized redirection is the functionality which determines how to deal with incoming communications. To illustrate the complexity of this consider the following simple example. John is a university professor. While he is at work, he is prepared to receive communications from anyone – staff, students or family. The only exception is when he is in the lecture room. In this case any communication will generally be stored for later attention unless it is from his wife or from the vice chancellor of the university. In either of these cases it will be redirected to his secretary. On the other hand, when John is at home, any communications from students or staff (other than the vice chancellor) will be stored for later attention. John also suffers from diabetes and at all times wears a blood sugar monitor, which samples his blood sugar level from time to time and sends him a warning message if the level goes out of bounds (too high or too low). Any messages from the blood sugar monitor must be delivered wherever John is (even in a lecture). If John does not respond within a given period, the message is redirected to his wife/ colleagues/ close friends/ doctor depending on where he is at the time and who might be nearby.

Another aspect of redirection is the selection of an appropriate device to which to redirect the communication. For example, if the communication is a voice call and John is at home, he may prefer it to be directed to his home telephone. On the other hand, if he is in his car it should be directed to the car phone, and if he is neither at home nor in the car, it should be directed to his mobile phone. In general the process of selecting the actual device could become more complex and this is where pervasive systems play an important role.

This scenario illustrates some of the typical aspects of communication redirection. The action to be taken is generally dependent on the person from whom the communication originates (or device that generates the communication), but often also depends on the time of day or location of the addressee. In more complex situations it can depend on attributes of the person to whom the communication may be diverted, such as their location or availability. The communication may be a telephone call, an SMS, an email message, or some other multimedia object. Depending on the nature of the communication and the devices that are available in the environment of the recipient, an appropriate device needs to be selected that will suit the type of communication and the user’s preferences.

III. PRCD

The PRCD system [15] was designed specifically to handle personalized redirection and to support experimentation with the ideas. The system essentially operates as follows:

(1) Establishment of User Preferences. Since this was not a major focus of the system, a relatively straightforward graphical user interface was developed to enable users to enter, view or update their personal preferences. These were stored internally as Event-Condition-Action rules, which associate actions with particular events that satisfy the specified context conditions.

(2) Arrival of communication. When an incoming communication arrives, the system needs to determine how to deal with it. This may involve directing it to an appropriate device in the vicinity of the user, directing it to a different user, saving it somewhere or simply ignoring it altogether. The user preferences are consulted and an appropriate action is taken.

(3) Format conversion. Having decided to send the communication to a particular device, a format conversion may be required in order to achieve this. For example, images may need to be transformed to a size and format that can be handled by the device. An audio/video stream may need to be separated into two separate streams routed to two different devices. And so on.

In order to handle this, the architecture of the PRCD system is composed of the following components:

(1) The User Preference Registry manages the user preference profiles for the individual users. It enables users to update their preferences (with appropriate authentication for this) and provides the means for other modules to access this information.

(2) The User Context Tracking module keeps track of the current context of the user. For this purpose the two main attributes are the user's location and current activity. It also keeps track of the states of devices (switched off, busy or idle). Since the user's preferences may depend on the current context, this component provides essential information to take such decisions.

(3) A Conversion Server is a module that seeks to determine a converter or sequence of conversion operations to convert data from one format to another. There will in general be multiple Conversion Servers located on different machines in the system. Each will have associated with it a set of Converters. At the heart of a Conversion Server is the Conversion Plan Generator, which generates plans to perform any particular conversion. The Conversion Server selects the optimal plan on the basis of the user's preferences.

(4) The Conversion Manager is invoked when the data to be delivered to a device is not in a format acceptable to that device. It multicasts a request for conversion to the Conversion Servers registered on the Directory Server. Each Conversion Server returns an optimal conversion plan (if one can be found) from which the Conversion Manager selects the best and executes it.

(5) A Converter is a software component that converts from one format to another (for example, between different image formats).

(6) A Directory Server is used for the sake of efficiency to locate a user's service agents and map the user's device id to his/her person id.

(7) A Protocol Parser receives incoming communication and parses it accordingly before passing it to the Device Manager.

(8) The Device Manager receives the resulting communication from the Protocol Parser and sends it out to an application-specific end point.

(9) The Rule Engine plays a key part in the decision making process for handling an incoming communication. It determines whether to delete the communication or redirect it. If it is to be delivered, it determines which device and what display format to use. The Rule Engine uses three kinds of rules:

(a) User specified rules reflect a user's personal preferences in different circumstances.

(b) General system default rules handle situations for which the user has not specified an action to be taken.

(c) Device specific default rules are used to deal with the communications when users have not specified their own preferences.

IV. DAIDALOS

Daidalos is a large project whose main aim is to integrate a range of heterogeneous networks and to build a pervasive system on top of this to provide the user with ubiquitous access to services using the most appropriate devices and networks. To handle this, the architecture is divided into two major platforms – the Pervasive System Platform (PSP) at the upper level, and the Service Provisioning Platform (SPP) at the lower level.

The PSP is composed of six basic modules:

(1) Pervasive Service Management (PSM) is responsible for the discovery, selection and composition of services to satisfy user requests.

(2) Personalization (P) handles the user's preference and uses these to influence selection and composition of services, tailoring of services and personalized redirection.

(3) Context Management (CM) keeps track of the context attributes relating to the user and to any relevant objects that the user may wish to use.

(4) Security and Privacy Management (SPM) is responsible for maintaining security and privacy for the user.

(5) Rule Management (RM) handles the sets of rules that are used to determine what action to take under what circumstances.

(6) Event Management (EM) monitors events and alerts the appropriate modules when a relevant event occurs.

More details of the architecture are given in Williams et al [16].

This paper is concerned chiefly with the Personalization module, and the personalized redirection component in particular, as well as the underlying parts of the SPP that are used in the redirection process, although for its operation it depends closely on the CM, SPM, RM and EM.

In the first phase of the Daidalos project the focus has been on redirection of voice calls although the redirection software can also handle other forms of communication, such as those covered by the PRCD system.

V. Strategies for Handling User Identity

A. *Single Global Identifier*

The simplest strategy for managing user identity is one in which each user is assigned a single unique global identifier. This identifier is the sole route by which to access the user. Thus any message, voice call, etc., will be sent to the global identifier of the recipient.

A simple analogy might be that of having a single telephone number through which one may be contacted. However, note that this is a single telephone number as opposed to a single telephone. Although in the simplest case this global identifier might be associated with a specific device (as in the case of the telephone), more generally this need not be the case. One could regard the global identifier as a channel through which communication may be routed to the most appropriate device in the vicinity of the user.

Now each user can define his/her own rules for redirection, and these are associated with the single identifier for the user.

This is the strategy adopted in the PRCD system. The latter allows the user to specify what action to take depending on the source of the communication, the time and date, the recipient's current location, the identity of the sender, the nearest device of preferred type, and so on.

Thus in the case of the example described in section 2, John can set up preferences which have a condition part that tests for his location. For example, if he is at the University and he is not in a lecture room then deliver any communications to an appropriate device. If he is at University and is in a lecture room but the communication is from his wife or the vice chancellor, redirect it to his secretary. If he is at University and is in a lecture room, and the communication is not from his wife, the vice chancellor or his blood sugar monitor, store it for later attention. If he is at University and is in a lecture room and the communication is from the blood sugar monitor, deliver it to an appropriate device. And so on.

This could be further complicated by the fact if John is at the University outside normal working hours (e.g. over a weekend), he does not wish to be disturbed. In other words, this is not part of his normal working pattern. The rules then need to have both a location and a temporal condition associated with them.

Thus associated with each user identifier is a unique set of preferences pertaining to that user. One consequence from the point of view of personalization is that, although the system can handle the full range of functionality required to express user preferences, the rules can become very complex (as will be seen from the next section). In general this is not in the interests of the user and could put off users from using the system.

Although functionally personalization is not unduly affected by this, apart from complexity of the rules, the single user identity does provide a weakness in terms of security and privacy in general since all context and preference information relating to a user is accessible through a single identifier. This makes it easier for, say, a service provider to determine location information on the user or the preferences of the user even when the user may not wish it. Despite any reassurances on the trustworthiness of such a provider, the user will have greater confidence in the security and privacy provided by the system if this weakness could be minimized.

B. *Multiple Roles*

One way of reducing the complexity of user preferences and increasing overall security and privacy is by introducing the concept of multiple roles. This strategy is a simple extension of the single global identifier approach. In this case a user may have more than one role and may associate a different identifier with each role. Each identifier may have associated with it its own set of preferences.

Once again this is analogous to having several different telephone numbers – a work number for work calls, a home number for personal calls, etc. However, again each identifier is not necessarily associated with a single device but can be regarded as a channel through which communication may be routed to the most appropriate device in any particular context.

Returning to the example described in section 2, John could identify several different roles and set up several different identities corresponding to each of these. Thus he might have a work role, a lecturing role and a home role. In his work role, his preferences might be to deliver any communications to an appropriate device. In his lecturing role, if the communication is from his wife or the vice chancellor, it should be redirected to his secretary. If it is not from his wife, the vice chancellor or his blood sugar monitor, it should be stored for later attention. If it is from the blood sugar monitor, it should be delivered to an appropriate device. And so on.

As in section 3.1, suppose that one now adds the complication that if John comes in to the University over a weekend, he does not wish to be disturbed. At worst one can add a temporal condition to the existing rules, but often this is not necessary. One may define a new role or simply link this to an existing one (e.g. home role).

As can be seen from this example, this simplifies the specification of user preferences considerably. Instead of having a single set of complex rules, one has a number of simpler sets of rules, each set associated with a particular user role or mode of operation. This makes it easier for the user to understand and hence simplifies the task of personalization.

As far as security and privacy are concerned the approach breaks down the preferences into convenient subsets to which access can be more easily controlled. This is not unlike the idea of having separate telephone numbers for different roles. This overcomes the major weakness with the single identifier approach by ensuring that the preferences and other attributes associated with different roles may be kept by different providers and hence a greater degree of privacy and security can be ensured.

On the other hand, in order to make life easy for the user and to provide adequate support, one needs to incorporate some mechanism to assist the user in updating user preferences associated with different numbers. Just as with telephones that have their own telephone books incorporated, one sometimes needs the facility to transfer telephone numbers from one phone to another. Likewise in this case one needs to be able to transfer sets of user preferences between user identifiers. When a new preference is identified the system may ask the user whether it should be added to all sets of preferences, some subset of these or only the current one.

If one does maintain strict security over the different roles of a user, then the system will only be aware of a user's current role and have no knowledge of any other roles that the user may have. In this case the system would have to ask the user each time to enter details of each role that a preference should be added to. However, this is not very realistic. At the very least the user would expect the system to have some knowledge of his/her roles, and to present these as a drop-down list or provide a default that propagates to all roles, or something similar.

If one does this, it means that the boundaries between the sets of preferences are no longer watertight. This does present a slight problem from the point of view of security and privacy as it means that some central system must be aware of the different roles of the user so that preferences can be propagated when necessary. In this respect it does differ from the idea of having separate telephone numbers, which cannot necessarily be linked to the same person.

Another problem with this approach is that of determining the role of the user at any time. One could either require that the user indicate to the system whenever he/she changes role or one could set up rules by which the system can deduce the role for itself. In some cases this is straightforward (e.g. if the user is at some specific location then he/she is in work mode – or home mode). However, it is not always as simple as this.

This approach has been adopted in the first phase of Daidalos.

C. *Multiple Virtual identities*

In this third approach the notion of virtual identity is separated from that of the role of the user. In this case by providing a set of virtual identities for the user to use, he/she is able to limit the knowledge any particular subsystem can acquire about him/her.

From the previous section it will be obvious that this does raise significant problems with regard to determining the role of the user and building up and using the preferences associated with that role without having the virtual identity as a key to access it.

This is the basic idea that is planned to be used in the second phase of Daidalos. At this stage it is clear that some way needs to be provided to allow the Personalization module to obtain this information although no final decision has been taken on how this will be achieved.

Again the effects on security and privacy should be to enhance these by making it very difficult, if not impossible, for a service to access information on a user's context or preferences unless that service is specifically entitled to do so.

VI. Conclusion

This paper describes the effects of different strategies for handling user identity on personalization and security in the case of personalized redirection in a wireless pervasive computing environment. The first system, PRCD, is a basic system for experimenting with personalized redirection and adopts the simplest approach, namely one in which each user has a single global identity. The system has been fully implemented and evaluated by a group of users with different levels of expertise. While this approach is the simplest to implement, it offers least flexibility and, potentially, least security.

The second system, Daidalos, is a pervasive service platform (PSP) that sits on top of a service provisioning platform (SPP) to provide a powerful adaptive system, which takes care of the user's needs with minimal user intervention. The basic functionality (including personalized redirection) has been implemented in stand-alone fashion and demonstrated in December 2004. Since then the focus has been on integration, and a fully integrated version of the system will be demonstrated in December 2005. This is based on multiple identities based on roles as outlined in section 3.2. The second phase of this project is expected to start in January 2006 and run to December 2008, and this will focus on virtual identities that are separated from roles as described in section 3.3.

The effects on personalization and security are described in the paper. What is clear is that there is a balance between personalization and privacy and security. If one is to provide a system with the maximum privacy, it is at the expense of the user's convenience with regard to personalization. On the other hand, if one provides more support to the user for the accumulation of user preferences and hence simpler personalization, this does weaken the overall privacy and security.

Acknowledgment

The authors thank all our colleagues in the Daidalos project developing the pervasive system. Y. Yang thanks the ORS and Heriot-Watt University for support of the work on PRCD. Apart from funding the Daidalos project, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that it is fit for any particular purpose. The user thereof uses the information at his sole risk and liability.

References

[1] M. Weiser, "The computer for the 21st century," *Scientific American*, vol. 265(3), pp. 94-104, 1991.

[2] J. Sun, "Mobile ad hoc networking: an essential technology for pervasive computing," in *Proc. Int Conf on Info-tech & Info-net*, Beijing, China, 2001, pp. 316-321.

[3] A. Zaslavsky, "Adaptability and interfaces: key to efficient pervasive computing," in *NSF Workshop on Context-Aware Mobile Database Management*, Providence, Rhode Island, 2002, pp. 24-25.

[4] M. Handte, C. Becker, and K. Rothermel, "Peer-based Automatic Configuration of Pervasive Applications," in *Proc. IEEE Int. Conf on Pervasive Services 2005 (ICPS'05)*, Santorini, July 2005, pp. 249-260.

[5] M. H. Williams, I. Roussaki, M. Strimpakou, Y. Yang, L. MacKinnon, R. Dewar, N. Milyaev, C. Pils, and M. Anagnostou, "Context Awareness and Personalisation in the Daidalos Pervasive Environment," in *Proc. IEEE Int. Conf. on Pervasive Services 2005 (ICPS '05)*, Santorini, July 2005, pp. 98-107.

[6] M. H. Williams, Y. Yang, L. MacKinnon, R. Dewar, and N. Milyaev, "Personalised Redirection of Communication in a Pervasive System," in *Proc. 12th IEEE Int. Conf. on Telecommunications*, Cape Town, May 2005.

[7] B. Farshchian, J. Zoric, L. Mehrmann, A. Cawsey, H. Williams, P. Robertson, and C. Hauser, "Developing Pervasive Services for Future Telecommunication Networks," in *Proc. WWW/Internet 2004*, Madrid, Spain, October 2004, pp. 977-982.

[8] J. Clarke, S. Butler, C. Hauser, M. Neubauer, P. Robertson, I. Orazem, A. Jerman Blazic, H. Williams, and Y. Yang, "Security and Privacy in a Pervasive World," in *Proc. Eurescom Summit 2005: Ubiquitous Services and Applications*, Heidelberg, April 2005, pp. 315-322..

[9] R. Liscano, I. Roger, Y. Qinxin, and A-H. Suhayya, "Integrating multi-modal messages across heterogeneous networks," in *Proc IEEE ICT*, June 1997.

[10] H. J. Wang, B. Raman, C. Chuah, R. Biswas, R. Gummadi, B. Hohlt, X. Hong, E. Kiciman, Z. Mao, J. S. Shih, L. Subramanian, B. Y. Zhao, A. D. Joseph, and R. H. Katz, "ICEBERG: An Internet-core network architecture for integrated communications," *IEEE Personal Communications Magazine*, 2000.

[11] N. Anerousis, R. Gopalakrishnan, et al., "The TOPS architecture for signalling, directory services and transport for packet telephony," in *Proc. 8th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSS-DAV)*, Cambridge, UK, 1998, pp. 41-53.

[12] B. Thai, R. Wan, A. Seneviratne, and T. Rakotoarivelo, "Integrated personal mobility architecture: a complete personal mobility solution," *Mobile Networks and Applications*, vol. 8(1), pp. 27-36, 2003.

[13] M. Roussopoulos, P. Maniatis, E. Swierk, K. Lai, G. Appenzeller, and M. Baker, "Person-level routing in the mobile people architecture," in *Proc. USENIX Symposium on Internet Technologies and Systems*, Boulder, Colorado, 11-14 October, 1999, pp. 165-176.

[14] A. D. Stefano and C. Santoro, "NetChaser: Agent support for personal mobility," *IEEE Internet Computing*, pp. 74-79, March-April 2000.

[15] Y.Yang and M. H. Williams, "Adaptation of Content in Personalized Redirection of Communication," *International Journal of Business Data Communications and Networking*, vol. 1(4), pp. 51-63, 2005.

[16] M.H. Williams, Y. Yang, N. Taylor, S. McBurney and E. Papadopoulou, "Personalized Dynamic Composition of Services and Resources in a Wireless Pervasive Computing Environment," in *Proc. International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, 2006.