TU/e technische universiteit eindhoven

Perceived Privacy Handling in an Amigo Extended Home Environment Application

Abdullah Al Mahmud, Yeo Lee Chin

<ISBN nr. >

/ stan ackermans institute, center for technological design

Summary

Perceived privacy i.e., how users perceive that their privacy is handled by the system, is one of the key issues for the user acceptance of current ambient intelligent environment applications. This project was carried out in the context of the Amigo project, a large IST funded project in which 15 European organizations work together on the development of interoperable software architectures and applications for intelligent ambient home environments. Within the Amigo project, one of the tasks is dedicated to gain insights into how perceived privacy should be handled in an ambient intelligent networked home environment. Our project consisted of designing and building a functional prototype in which the system adapted to changes in the context of the user and the user's environment while accounting for the users control over their privacy.

A user-centered design approach was taken for which a subset of the Amigo extended home environment scenario was used. In this scenario, people can share experiences while they are located in two or more different places, for example, between two homes, or between a home and a hotel. A functional prototype was built in which photos could be shared between two locations. The Context Management Service and the User Modeling and Profiling Service from the Amigo project were integrated in the prototype. Our system added functionality by which people could set different privacy levels with regard to the content of the photos that could be shared, the precision of the actual location of people and other persons present in their environment. All these variables affect how and what people will share. Changes in the location of people were tracked by using sensors. A colored light system was used for presence notification. This prototype was developed in an iterative fashion, such that feedback from experts and end-users was generated and implemented in different phases of the project. Questionnaires and interview methodologies were used for the evaluation. Based on these results, recommendations for the Amigo software architecture and refinement of the developer's guidelines with regard to handling privacy in the user interface and in the middleware were made. A major conclusion was that privacy settings are very different for each individual, but that for most people having 3 levels is sufficient if they can control at least one of these.

Contents

List of Figures

List of Tables

1. Introduction

The major goal of an ambient intelligent environment is to seamlessly integrate technology for its users. The evolvement of a new form of invisible interaction was introduced to create extra comfort in people's lives. Since the technology is embedded in the environment, people are not aware that their information is tracked and disseminated. The continuous acquiring of context information of users raises a major privacy concern. Therefore, perceived privacy in an ambient intelligent environment is a crucial issue especially when people start to share their information outside of their homes. The question that arises is whether a user will accept this kind of technology or not. Users should be aware of, to whom and what information is acquired and shared by the system and there is a need for having control over the system that handles different information about them. In the Amigo-IST project, one of the goals is dedicated to gain insights into how perceived privacy should be handled in an ambient intelligent networked home environment.

The objective of this project is:
To design a context aware environment in which people share experiences while they are located in two or more different places (home, friend's home, hotel) and to use this system to investigate how people's perceived privacy can be protected when the context in one of their locations changes and threatens their privacy by dynamically adapting in the context to the new conditions.

In this project, the aim is to design and build a working prototype within Amigo context, in which it is based on a subset of the Amigo extended home environment application scenario. The prototype is privacy and context aware and is integrated with Amigo software modules. Then how this prototype handles end user's privacy in an extended home environment and how the system can dynamically adapt in the context where privacy is of utmost concern is investigated.

Amigo is a large European project for building interoperable middleware architecture for an ambient intelligent environment and taking care of a user's privacy. Amigo's open and interoperable middleware is able to connect electronic home appliances from one home to another home and build intelligent communication between homes. One of the focuses of the Amigo project is an extended home application. Extended home refers to two or more homes connected using embedded and computerized devices that allow two or more people in different homes to be connected. The advantages of an extended home is that it is time saving to control different devices in the house, even though the technology might be complicated for its users (Internet Home Alliances, 2002). The main reason behind an extended home application is that it can retain a social relationship between inhabitants of different homes and give them a feeling of emotionally being there.

In Amigo, privacy was initially proposed to be handled in the middleware service level. Each Amigo middleware service should implement a rule based privacy filter that will handle users' privacy preferences. It was found from field and conceptual studies that handling privacy in Amigo by using a filter on the middleware service level is not sufficient. It is important that in order to protect perceived privacy, there should be provision for direct control over the application. Therefore, perceived privacy should be handled at the application level too. From the previous study (Soute and Boland, 2006) it is found that an application can offer specific privacy-aware user interface. From their three user studies, the main finding was that perceived privacy should be handled at different levels in the Amigo architecture, including both Amigo middleware service level and Amigo application level.

The preferences of privacy are made according to the types of information being shared, the level of detail and with whom the information is shared. Furthermore, they proposed six design guidelines for developers.

The report is organized as follows. Chapter 2 describes the relevant background regarding privacy, context awareness and related works. Chapter 3 describes our approach. In chapter 4, the conceptual design is presented with some initial ideas and design rationales. Chapter 5 starts with the technical implementation of the system with a detailed explanation on the relation to Amigo services. In chapter 6, the evaluation results are presented. The discussion relating to the Amigo design guidelines and insights from the evaluation results are also presented in chapter 6. Chapter 7 shows the implemented design guidelines and refined design guidelines. Finally, chapter 8 presents conclusions.

This is a final year project done with two students from User-System Interaction, a two-year post-graduate program at the Eindhoven University of Technology (TU/e), the Netherlands.

2. Background

Summary

A literature review was conducted to know the state-of-the-art on the different aspects of the project, i.e. privacy, context awareness and its implication on ambient intelligent environment. Managing personal privacy in an ambient intelligent environment and adapting to the changes in the context are the major concerns within the Amigo project. Next to studying context and its sharing data consequences, the strength of context awareness has also been used to handle privacy itself. Besides, the early findings in the Amigo project were checked to understand and link what has been done so far (D1.1, 2005; Soute and Boland, 2006).

2.1. Context Awareness

Context awareness is an important matter in the current trends of computing. In mid 90's it was found that location aware computing and context-aware computing were seen as synonymous. Nevertheless, in reality, context can mean more than location, (Schimidt, 1999). Context can be any activity, location, and environmental change.

A context aware environment refers to an environment that is aware of the context in that environment and could react or adapt to different situations automatically. As human beings become mobile, they can be anywhere in the world, either at their own home, a hotel, or their friend's home, extended home environment thus plays an important role for people to be connected. Context aware communication system in extended home help family members to communicate with each other as if they are in the same place. In an ambient intelligent environment, the continuous gathering and processing of context information hinders people's privacy. Though there have been seen several efforts to preserve privacy in context aware environment, it would not be possible to perfectly preserve personal information (Langheinrich, 2001).

The solution given for preserving user's privacy is to give them more control and awareness about the information they are sharing. It is assumed that if people are in control of what they are sharing they might feel well to compromise with their privacy depending on the sensitivity of the shared information (Mayer and Rakotonirainy, 2003). However, they believe that privacy issues should be taken seriously for designing ambient intelligent system.

Among the several ways, Mayer and Rakotonirainy (2003) presented the way to handle privacy in the middleware level in context aware homes. They also mentioned that privacy management through a privacy manager in an application is very complicated. Users need to give the opportunity to explicitly define their privacy policies. Therefore, it is very important to investigate how to find an easy way for handling privacy policies for end users.

2.2. Management of Personal Privacy

Privacy, as a concept, is very fluid and dynamic and it is context and environment dependent (Palen et al., 2003; Patil et al., 2005). It is not only about anonymity or keeping personal information secret but also handling of every activity in one's own way. The vision of Mark Weiser (1999) is to seamlessly connect the environment invisibly. This vision cannot be fully accomplished if the users of the ambient intelligent environment do not have perceived control on what information is being shared and with whom. This clearly points to the

personal privacy of the user. Privacy is seen as the main obstacles in the acceptance of ambient intelligent application (Hong and Landay, 2004). Though it is very challenging to build application that is very much privacy sensitive, they have identified several high level requirements (end-user requirements and application developer requirements) for building privacy sensitive ambient intelligent applications. The key points are a. building a decentralized architecture b. control and feedback mechanism c. probable deniability and d. exceptions for emergencies.

There have been a number of efforts to handle privacy in ambient intelligent environments(Brodie et al., 2005; Yee, 2005; Zang and Todd, 2006) The work done by Lederer et al. (2003, 2004) is one of the key examples of this effort. They have built one user interface that provides appropriate control and feedback to protect their privacy. The goal was to share the right information with the right people at the right level. The prototype they built was a desktop interface which could help users to set their privacy preferences and overall an option for managing privacy for the end users. The context was represented as the sum of location, activity, companions and time. There was a log recording information about all inquires and disclosures. Users could navigate their log to help them understand what information is flowing and to whom. Moreover, they could configure their preferences in response to unfavorable disclosures. The same notion was addressed by Friedewald et al. (2007). They mentioned that people have a tendency to accept new technology without worrying much about privacy if they get sufficient benefits from them. For instance, people may use mobile phones and GPS though they have the risk of location tracking. However, they argued that the risks of privacy will be severe in the ambient intelligent environment and privacy preserving ambient intelligent system should be built rather than relying on users control over data. Though it is believed that privacy should be handled by making user more aware and giving them more control over their data. However, it is also true that control should not impose an extra burden for the users (Winters, 2004).

In our project, one of the requirements is to handle privacy in Amigo. To have an overview of different components of Amigo, the following section describes the Amigo architecture.

2.3. Overview of Amigo Architecture

Amigo architecture follows the service orientation paradigm. It consists of three components that build up Amigo server(s) and Amigo client(s) (see Figure 2.1). Platform and middleware resides in Amigo server. The server contains the functionality that is needed to facilitate an ambient in-house network. This includes solutions for context awareness, user profiling, multi-modal interfaces, etc. Applications and services are installed in an Amigo client and to be used by users. In this prototype, we focused on integrating a sharing application (which is one of the applications & services) with a subset of Amigo middleware services, the Context Management Service and the User Modeling and Profiling Service. As can be seen in Figure 2.1, Amigo handles more topics than we mentioned here. For detailed information about Amigo architecture, see D2.1 (2005).

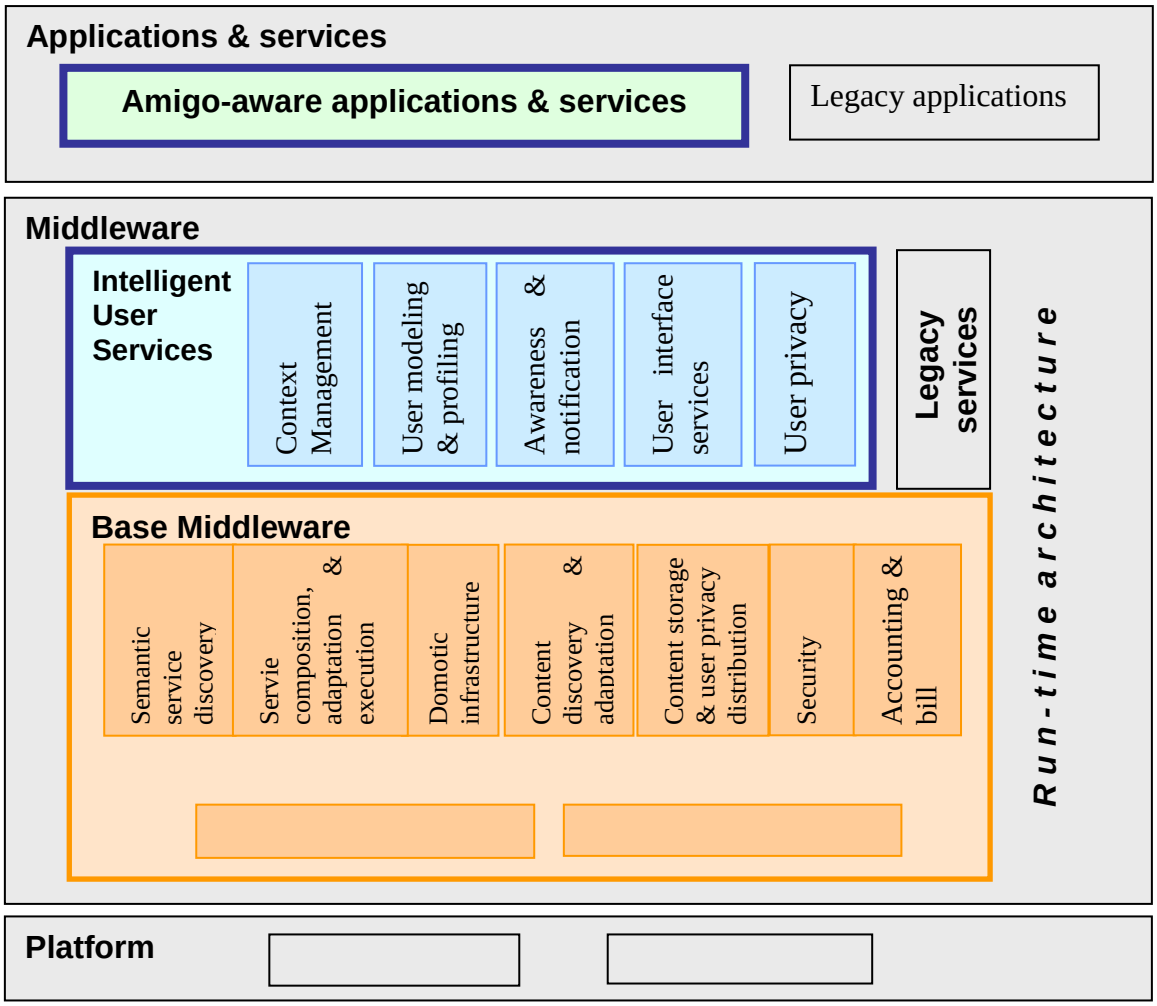

Figure 2-1: Amigo Architecture

2.4. Handling of Perceived Privacy in Amigo

All of the works mentioned above tried to find out a way to manage privacy in ambient intelligent environment though they did not really focus on how easy and viable it would be to model end user's privacy for easy management of different privacy preferences. In our approach, we had the base idea from those studies. In addition, we tried to build a way for easy management of privacy preference with a photo sharing application that will also be used as a universal application for home users. We also tried to represent context information in an intuitive way through light. This also helps to represent the privacy information more social and natural way to the users and not imposing any extra burden for the user.

Our way of handling perceived privacy is different from others. The above-mentioned systems were used solely for managing personal privacy without focusing on any real application. In our approach, privacy management module is embedded in an application that can be used for a variety of purposes. This means that privacy preference setting is a part of the application for the benefit of the user. This empowers users for using such an application for not only disclosing personal information but to handle different privacy preferences for different people in different situations. Finally our way of handling privacy addresses a perceived privacy model suitable for Amigo applications and as well as for other ambient intelligent applications.

In the context of Amigo project, perceived privacy has been defined as whether the users have perceived control over the shared information, that is, to whom and what extent personal information is shared or obfuscated with other people. We have design guidelines from Soute and Boland, (2006) based on the empirical data that is necessary for building a privacy aware ambient intelligent application. This work in the current project implements these guidelines for validating the early findings for protecting end user's privacy in an extended home environment.

3. Approach

To address perceived privacy in the context of Amigo project, a subset of the project's scenario was adapted to explicitly illuminate the perceived privacy problem. A user centred approach was taken in which this scenario was used to guide the design, development and implementation, and demonstration of the prototype. Figure 3.1 shows this approach as follows. The adapted scenarios, the design guidelines from the Soute and Boland (2006) and the Amigo user research results from (D1.1, 2005) were used as the starting points. Later on in several brainstorming session we developed the concept of our application. The conceptual design includes user interface concept, concept of sharing application, ideas for representing context information and finally the concept of privacy model, i.e. how to control data for end user's privacy. All the ideas for conceptual design were used to build a functional prototype. In building functional prototype phase, it consisted of developing a context-aware sharing application, developing a generic privacy interface, developing a sharing interface and finally integrating the context-aware sharing application with Amigo middleware services. The development of the prototype was done in an iterative manner by using the expert evaluation results. At the end, a user study was carried out with the prototype to get user feedback. Finally, the result of the user evaluation was incorporated to generate a modified set of generalized guidelines for designing Amigo privacy aware applications.

The scenario in this prototype was a subset of the Amigo extended home scenarios. The scenario describes different possible situations and events that could occur in the homes of people who have an operational 'Amigo' system. This scenario reflects typical activities of a family in their daily life. There were two scenes in the scenario which provide static and dynamic changes of context in an ambient intelligent home environment. The scenario will be explained in the next section.

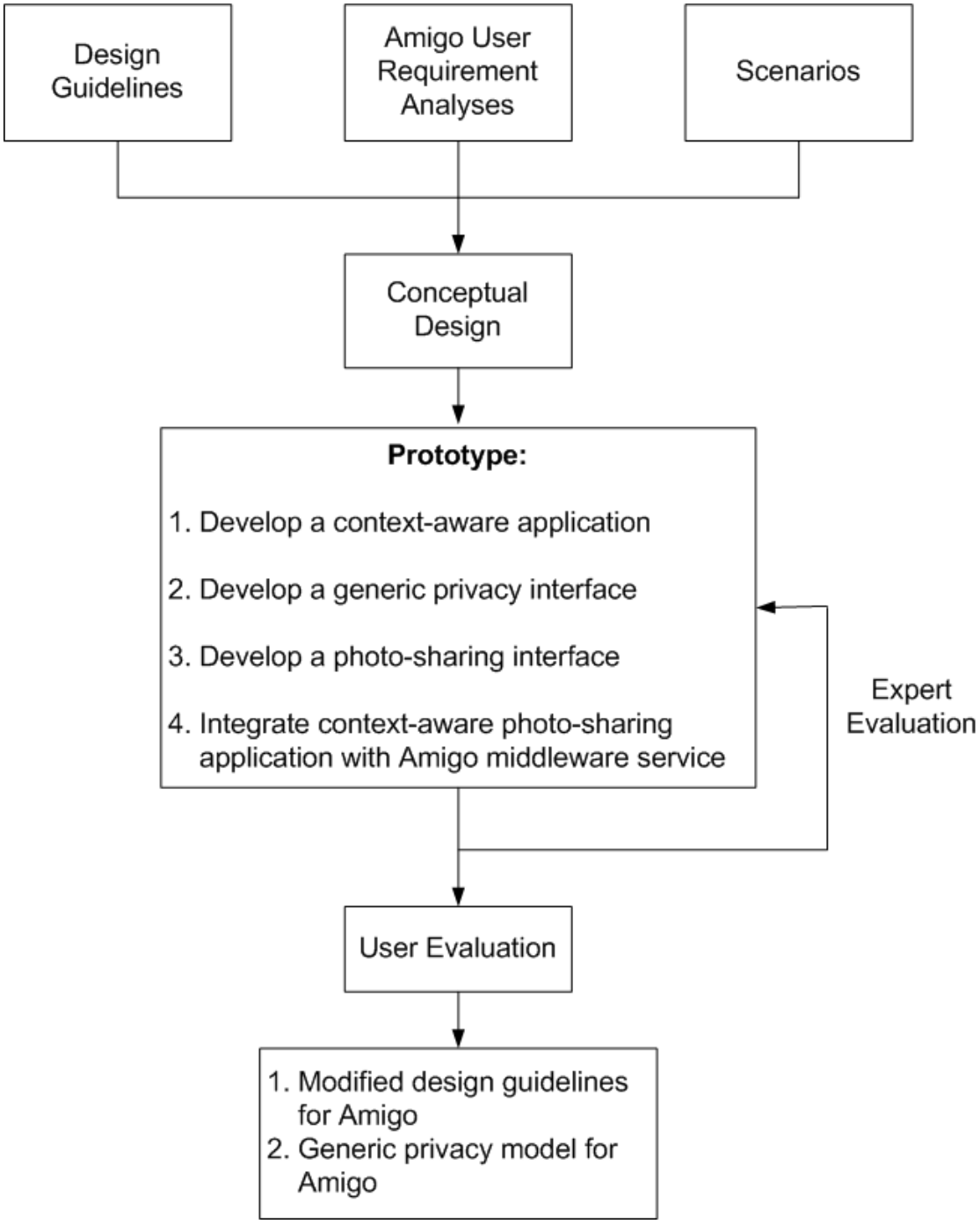

Figure 3-1: Workflow of the project

3.1. Scenario

The scenario is about a couple, Maria, and Jerry, and the system they used to communicate with each other, while they are physically separated. Maria and Jerry are married. They have one child, his name is Roberto. Jerry travels a lot for his work. Sometimes he is away for a month. Jerry and Maria like to use the new system they have to keep in touch with each other.

This system can be used from any display device that is connected to the Internet. By using the system, Maria and Jerry can be together, while they are at different locations. They can exchange information, share photos, play games, chat, share activities, feel each other's

presence and share their social context. They can do all these things at the same time, as if they are close together. Moreover, they can intuitively share their social context by using different light colors.

Maria and Jerry like to take photos of the special cocktails that they prepare. They like to talk about recipes and cocktails. But, they never talk about such things when Roberto is around. Maria has three different sets of new photos that she wants to upload to the system. The first set of photos is 10 years old. These are photos of her first marriage taken at the wedding day. She does not want anyone to see these photos. The second set of photos is recent photos of their visit to the zoo. She wants to look at these photos with Jerry and Roberto when they are together. The third set of photos shows the cocktails that she prepared a few days ago for their friends. She wants to look at these photos together with Jerry, but not with Roberto. Maria can tell the system these preferences. The system shows then the right photos with the right person at the right time.

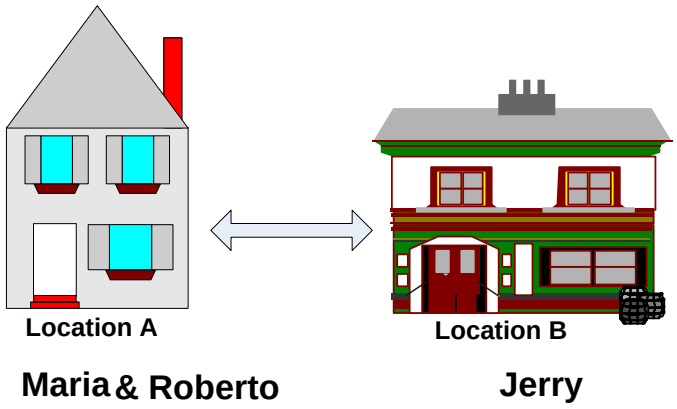

Figure 3-2: Maria and Roberto are in the same location

This month, Jerry is in the US for his work. Today is Sunday and both Maria and Jerry are free. Maria likes to be with Jerry and share the photos that she took a few days ago when some friends visited her. Roberto is with Maria, the second set of photos (zoo) is shown on the display device (see Figure 3.2).

Now it's time for Roberto to go to bed (see Figure 3.3). When Roberto has left the living room and he is in his bedroom, the photo set changes to the cocktail set on Maria's and Jerry's display. In addition, the color of the light in Jerry's room changes from pink to orange at the same time.

After being with Jerry for some more time, just to share each other's company, Maria leaves the session and logout from the system.

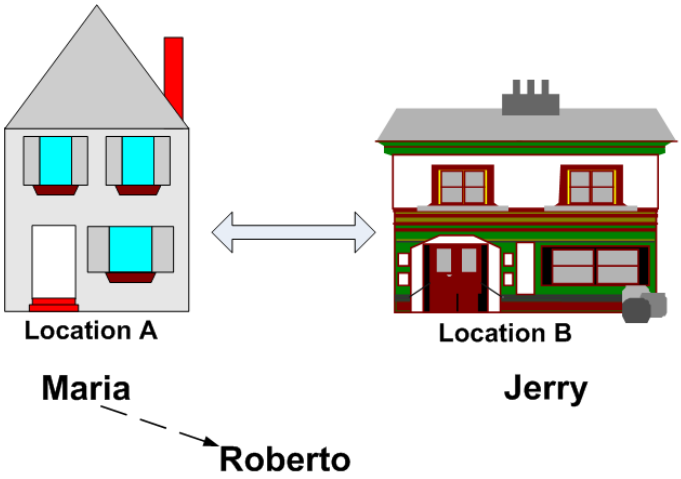

Figure 3-3: Roberto leaves the room

3.1.1. Technical description of the scenario

Assuming location A and location B are Amigo home A and Amigo home B, with a sharing application installed. The application could be installed in any display device like a television, a mobile phone, a computer or a PDA.

Maria is in location A and she wants to share photos with her husband, Jerry in location B. Maria logs in to her sharing application. The application shows her availability (for example, sleeping, eating, watching movie, busy) on the display device. At the same time, the light color of Jerry's room changes. Maria's availability, and the availability of Jerry, is checked by the intelligent system installed at both Amigo homes. Maria found that Jerry is available and initiates a sharing request. The system in location B informs Jerry about the request from Maria. Jerry accepts the request. A connection between the two locations is established. Sharing starts by showing Maria photos in slide show. At the same time, they can chat via text messaging or an audio/voice-chat service provided by the application.

Roberto, the son of Maria and Jerry leaves the room while Maria is sharing photos with Jerry. Amigo system recognizes the change and forwards the information to the application. The application checks Maria's privacy policy from her policy database to know how to react when her kid leaves the living room. In this case, Maria wants a different set of photos to be shown. The application reacts according to her privacy setting. At the same time, Amigo in Jerry's home notifies Jerry's application about the changes and the light colour in Jerry's room changes. The information represented by the colored light is understood by Jerry based on a social agreement between Jerry and Maria. At the end of the session, Maria ends the connection by saying goodbye to Jerry.

There are two scenes in the scenario, one is static situation and the other is dynamic situation. In a static situation, Roberto is together with Maria when she initiates the sharing request. When Roberto leaves the room, it reflects the dynamic situation in which context of Maria has changed. In both situations, Maria's privacy preferences should be handled by the application and the decision from the application should be context dependent.

4. Conceptual Design

Summary

In this chapter, we present the model we developed. Moreover, several possibilities of representation of context information is discussed. These ideas were hooked up with several Amigo services to create a privacy aware and context aware sharing application. The design rationale we had was two fold: one is for to intuitively present our privacy aspect to the user and the other one was to find an easy way of deploying our prototype with Amigo intelligent services. We have chosen a sharing application to be built to represent a more general sharing of context and content. The application will be used between two homes for sharing experiences. The application will be integrated with several Amigo intelligent services. Finally, a conceptual privacy framework will be presented that conveys the underlying design of our prototype.

4.1. Design Ideas

In several brainstorming sessions, the concept of the application was developed. The conceptual design includes initial concept about an application in an ambient intelligent environment, concept of user interface, concept of sharing information using the application, concept for representing context information and finally the concept of privacy model, i.e. how to control data for end user's privacy. All the ideas for conceptual design were used to build a functional prototype.

4.1.1. Initial ideas

The initial idea was to build a privacy aware and context aware application in an ambient intelligent environment (see Figure 4.1). The application is context and privacy aware, in which the context is retrieved from the environment and different control points are used to allow a user to control which piece of information he or she is sharing with his or her contacts and how the information is shared.

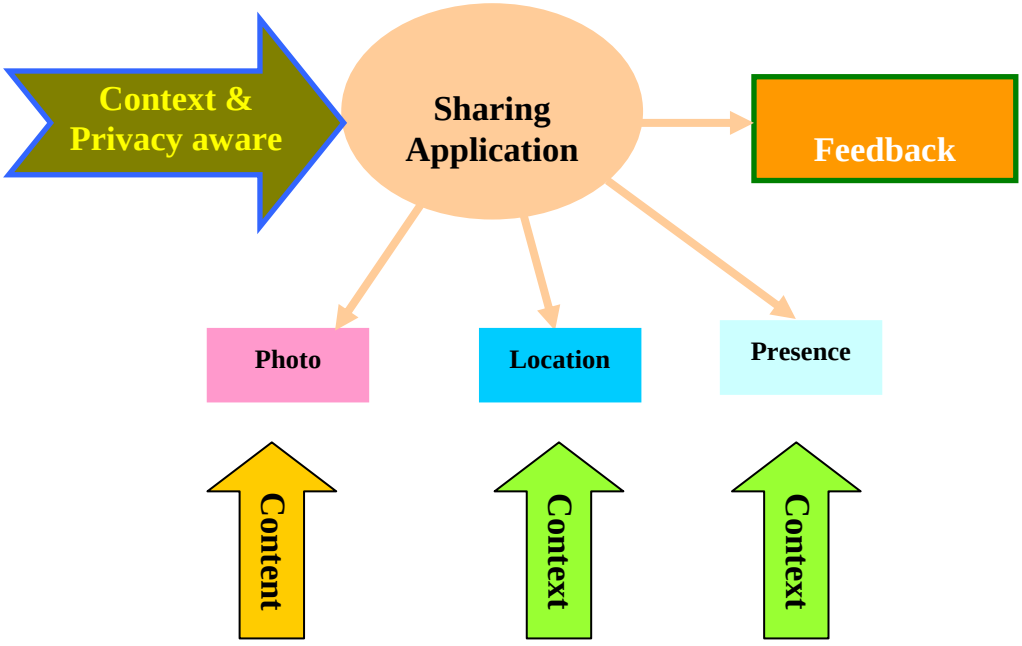

Figure 4-1: The conceptual diagram of the application

The application should allow a user to share information and activities with his contacts at other location. This information includes user's photos, user's location and user's presence. Feedback regarding to the content and context changes is represented by different icons and colored light in order to have at least two different ways of representation.

Based on the initial ideas, several components in an ambient intelligent environment were identified (see Figure 4.2). These components include the services, the applications, the control, the user and user's contacts. A service component has different pieces of software running in it. Their functions include collecting contextual information about the house and its inhabitants, like recognizing the person in the environment, knowing their activities, controlling security system in the environment etc. The contextual information is stored in the centralized database and can be used by an application. A control component allows a user to control the flow of data by setting his or her privacy preferences. A user's contacts can be a family member or a friend that interact with the user. The line with arrows shows the data flow from one component to another component. Several privacy decision points are stamped between different components to control the flow of data.

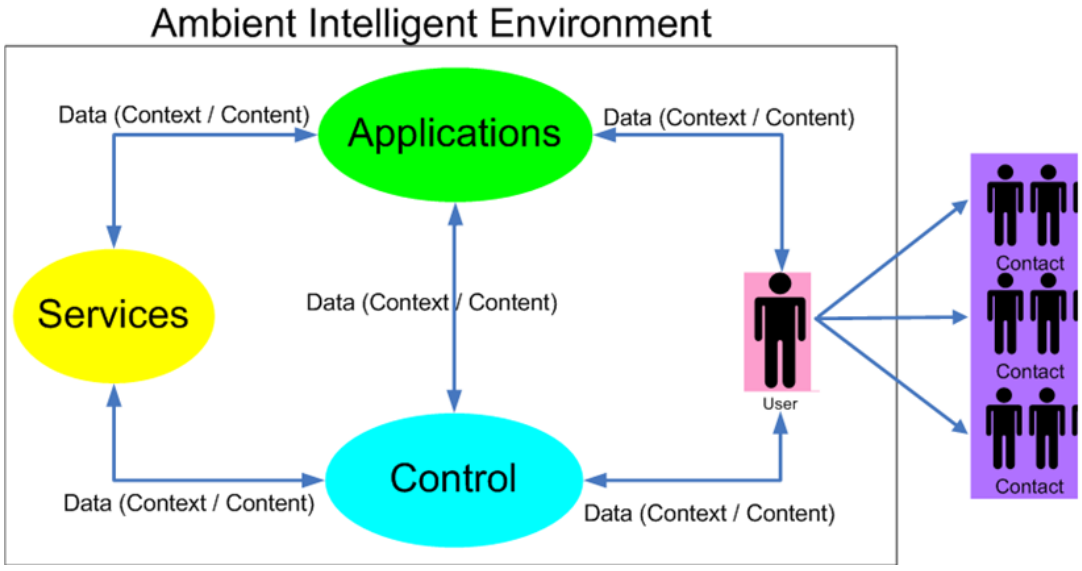

Figure 4-2: Components in an Ambient Intelligent Environment

Driven from the initial ideas, a sharing application, which allows two people to share photos, location and presence, was chosen. Besides that, an additional interface for a user to control the system by setting his privacy preferences was implemented. Finally, the sharing application reacts based on user privacy setting and is context dependent. Having several discussions with experts, a design decision was made. The decision was that the application will be designed by adding functionalities on top of an existing system. Towards this goal, an application named "Shared Activities" was chosen. It meets the capability of the design requirements and the design ideas. "Shared activities" was taken from Philips Research Innovation Lab (I-Lab). In "Shared Activities", photos could be shared between remote places by using TV as a display medium. The following section describes the unique interface used by this application and how it was adapted to the functional prototype.

4.1.2. Adapting PAT from I-Lab for prototype interface

Home entertainment system plays a vital role in our daily life. Almost every home has a Television (TV) for entertainment purpose. Philips Research Innovation Lab has built a sharing application, the "Shared activities", to make home entertainment easier and to control

the home appliances with one device i.e. TV. Shared activities are an application built with CE-HTML that has many different menu options. The navigation was designed according to the EasyLogic 3.0 standard (Oosterholt et al., 2006). This standard, which is based on a "Three-Feet-Interface", brings some unique requirements to our prototype. The principle of a "Three-Feet-Interface" is that a user should be able to control the interface by using a remote control while he is sitting comfortably on a couch. Due to this principle, the text displayed on the screen should be large enough to be seen. Besides, the way to navigate through the interface is limited to a few buttons on a remote control. Basically, the menu in EasyLogic standard is divided into two columns, left, and right. Left, right, up and down arrow keys are used to navigate through the menu. Four different buttons, red, green, yellow and blue are used for additional functions.

In order to have a standard and consistent interface between different Amigo demonstrators, we decided to build our application on top of the I-Lab application. The interface was extended for a privacy management interface where users can control the system by setting different privacy preferences. The original main menu from I-Lab has 5 different menus on the first screen. To keep thing simple and keep user focus, the main menu was reduced to only two main menus such as 'Television' and 'Sharing Application'. Each of them has several submenus. Besides following the unique requirements from EasyLogic standard, the interface was also designed based on Soute and Boland (2006) design guidelines. The detailed designed will be discussed in chapter 7. The following section describes the information being shared between two locations using this application.

4.1.3. Sharing information

In our application, presence, location and photo of a user are shared. Presence refers to user status, which is online, away, busy or offline. Location refers to where the person is located at certain time. According to Soute and Boland (2006) and Sheikh et al. (2006), we can present the user with a choice of level of detail in which the information can be shared. Different pieces of information can have different levels, for example, location has different precision levels, and these levels are "room", "building", "city", "known location", and "do not share". The example of this model is depicted in Figure 4.3.

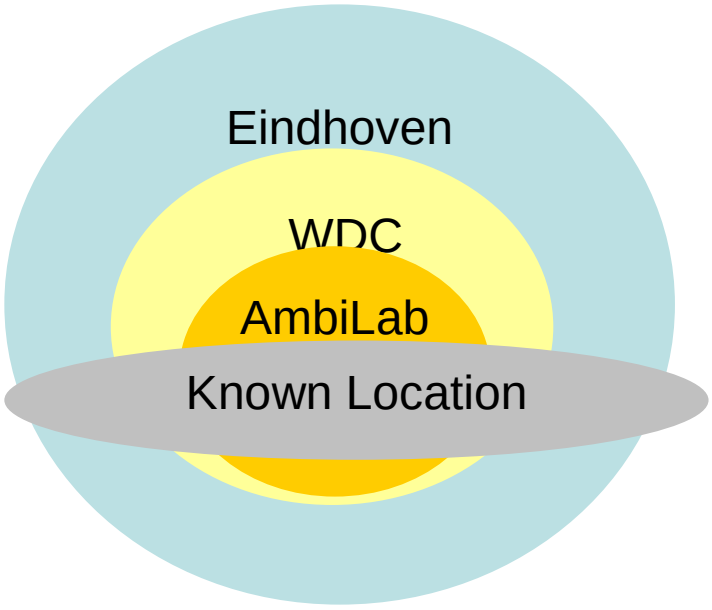

Figure 4-3: One example of different precision for location

Different precision levels provide a user the flexibility to choose which information is to be shared. Lederer et al. (2003) mentioned that in an ambient intelligent environment, it is important to have control over the precision of context information that will be disclosed to other people. Also according to the precision of the information, it depends on how much the real information is disclosed. Our selection of location preferences is similar with Lederer et al.'s (2003) ordinal precision level. However, they have used a level 'vague location' where we used 'known location', in which in our application, it can be used as custom location setting. We tried to keep the preferences setting simple for the user. Moreover, in our prototype, different precision level is shared according to the relationship with the person who is going to share.

Regarding the question of control, the users can set preferences (who will see what and when). The application will react according to the preferences setting. The preferences setting for a specific person will be configured by the owner of the application who has the central control of the application.

4.1.4. Representing context information

Representing context information in an intuitive way is important. We tried to represent the context information by icons, colored text and colored light. We showed photo-sharing application by a photo icon, presence status by colored text and presence and activities by colored light. Light source can be one of the ways to represent context information without interrupting someone explicitly. This can on the one hand help to exchange information between two parties according to prior agreement and on the other hand provide sufficient feedback for the application user.

We have tailored the representation for the lucidity of our application. For our prototype we have used 4 different colors (see Table 4.1) to represent different situation of the context. The first two are whether some one is logged into the photo sharing application or not. If someone is not logged in the color of the light will be black and as soon as someone logs in the light color will be green. The color of the light changes to pink when the photo is sharing between parents. If the kids leave the room, the light will change its color to orange. This also gives the other person feedback that the context changes i.e. the kids leave the room. The color is the social agreement between the two parties. Information modeled in Table 4.1 is in fact a compound context since it combines activities with status and location of a user.

Table 4.1: Representing different context with different colors of light

Information	Representation
Not logged in	Black
Logged in	Green
Sharing photos while kid is present	Pink
Sharing photos while kid is not present	Orange

4.2. Amigo Intelligent Services

As mentioned before, the prototype is built within Amigo context. This means that the prototype is built within an ambient intelligent environment. In this environment, contextual information is retrieved from the technology embedded somewhere in the environment. In Amigo, each technology is controlled by a service running in an Amigo server. Context Management Service (CMS) is one of the services. CMS is used to track location of a user and store the location in the server. The idea in the prototype is to integrate the sharing

application with this service to obtain user location. Furthermore, another service in Amigo, the User Modelling and Profiling Service (UMPS) is used to store user profile and to create reasoning based on the interaction of a user with his context and feedback. Our idea was to use the basic facilities provided by UMPS and extend its usage to store user privacy preferences setting.

4.3. Privacy Model: A Conceptual Privacy Framework

Our concept as explained in previous sections helps us to design a generic privacy model in an ambient intelligent environment. In short, the privacy model can be represented by different combinations of the components in an ambient intelligent environment as shown in Figure 4.4

Figure 4-4: Privacy Model

Our model is based on services, application, control, users, and user's contacts. The setting (which is how the application reacts) is context dependent (see Table 4.2). For instance, if Maria [user] is at her room [context] and using a sharing application [applications], and her husband Jerry is alone at another location [contacts] and also logged in to an application, then use setting A- share photos. Setting A – share photo is a setting preset by Maria using privacy preferences setting interface.

Table 4.2: An example of applying privacy model in an Amigo home

Services (Context)	Applications	Control	Users	Contacts	Setting (Context dependant)	
					Context	**Enforced Privacy Policies**
At room At home Not at home	Sharing Application - - Photo	Interface for privacy preferences setting	Any user	User's contacts -- Friends Family Colleagues	Person A at home	Setting A- Share
					Person B at home	Setting B- Don't disturb
					Person B is alone	Setting C- Accept sharing request
						Setting D- Don't share

The intended system will work according to the following mechanism. We assume that all the needed services like CMS and UMPS are installed in two homes and call these homes the Amigo homes. The application that will be intermediary for all services is the sharing application. Sharing application is an application that allows users at different location to share information and activities, provided that they are Amigo home users. A user can control the application by setting his privacy preferences from application privacy management interface. For privacy reason, a user needs a personal identification number (PIN) in order to use the application. The basic flow of the mechanism in one Amigo home is showed in Figure

4.5. Bear in mind that the services are already embedded in the home and their information can be accessed and used by the application.

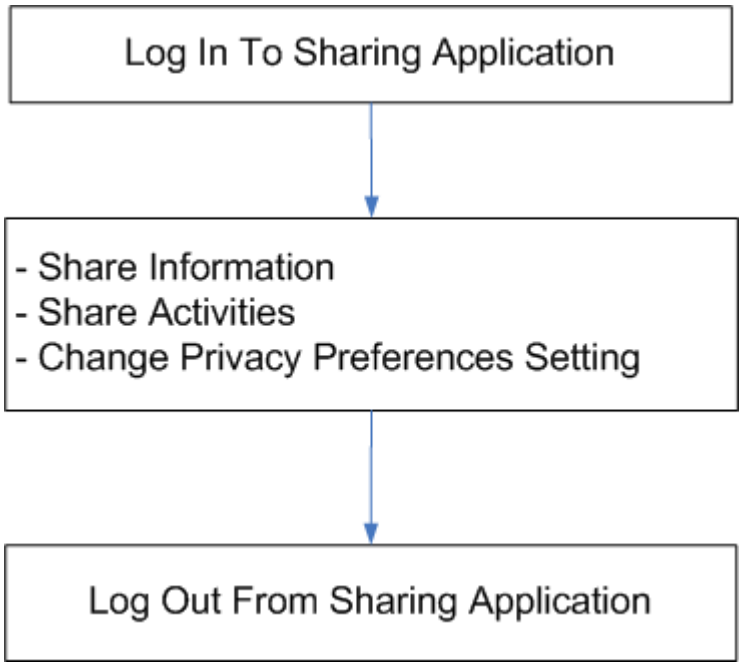

Figure 4-5: Basic flow of the sharing application

The services in the homes are activated in three different stages such as upon login, after login and log out. Once the user logs in to the application by selecting his or her name and pin, the application first authenticates the user's password by communicating with UMPS. If the pin is valid, the user can start using the application to share information and activities with his contacts. The information being shared are user location, user presence and user photos. The activities being shared are browsing photos together. A lighting service will set the room light according to privacy setting and will change dynamically if the context of the user is changed. When the user initiates a request to his or her contact to share an activity, for example, to share photos, the contact will receive a notification. If the contact accepts the request, the photo sharing session is started. A list of photos from the user is displayed on the screen; the photos are arranged in private and public categories. Only photos in the public are to be shared. The photo sharing session can be ended at any time during the sharing session. A user can modify his or her privacy preferences at anytime after login to the sharing application, for example, with whom he or she wants to share the photos with; which location precision level to be shared with his or her contacts. The application takes care of privacy setting of the user. To end the sharing application, a user logs out from the application. For a detailed flow of the application, two sequence diagrams were drawn (see Appendix C). Figure C.1 shows a sequence diagram to login to the application. Figure C.2 shows a sequence diagram when a sharing request is initiated and photos are being shared.

5. Technical Implementation

Summary

In this chapter, the architecture of the prototype and the inner working of this architecture are explained. Furthermore, details about different components in the architecture, which includes Amigo server, Amigo client and the network to connect different homes are described. All these components are running by using the Amigo framework. Finally, we present some technical limitations that we encountered while building the application.

5.1. Abstract Application Architecture

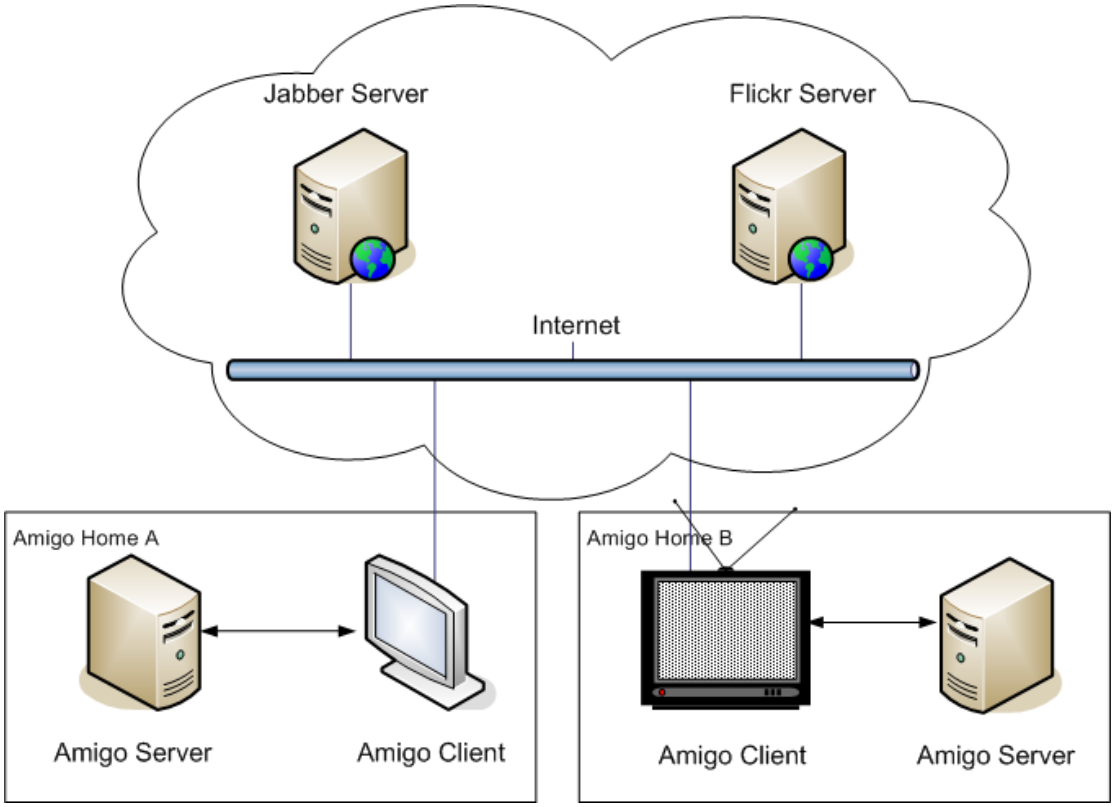

Figure 5-1: Abstract application architecture with two Amigo homes

Assuming that different services and applications are installed in two different homes and call them Amigo homes. There are many ways to connect the homes, Figure 5.1 shows the way we chose to connect these two homes in an abstract view. Typically, in our setup, there are three main components in each Amigo Home, the Amigo server, the Amigo client and the Internet. The server consists of different services running in the home. It acts as a centralized database that stores contextual information about the home and its inhabitants. The client can be any display device that is connected to Amigo server and the Internet. An application is installed in an Amigo client. One Amigo client can have more than one application running in it. Context information is shared between two Amigo homes through an application and the Internet. A user is given control over which information is to be shared. Jabber server is used to store user's contacts information. Flickr Server is used to store user's photos. Several privacy decision points are stamped at different locations to control data flow from one component to another component. The abstract view of this application was used to guide the

design of the prototype. The following section shows a closer look at the detailed application architecture.

5.2. Application Architecture

Privacy is important when information is shared. In the prototype, information is shared between Amigo server (Amigo Intelligent User Services), Amigo client (Applications) and between different homes. Before information is passed from one component to another, it will first go through a privacy decision point. Privacy Decision Point (PDP) I is used to control the information that is being shared between Amigo server and Amigo client. PDP II and PDP III are used to control the information that is being shared between different applications across different homes. Figure 5.2 shows the application architecture with PDP located at different stamp points.

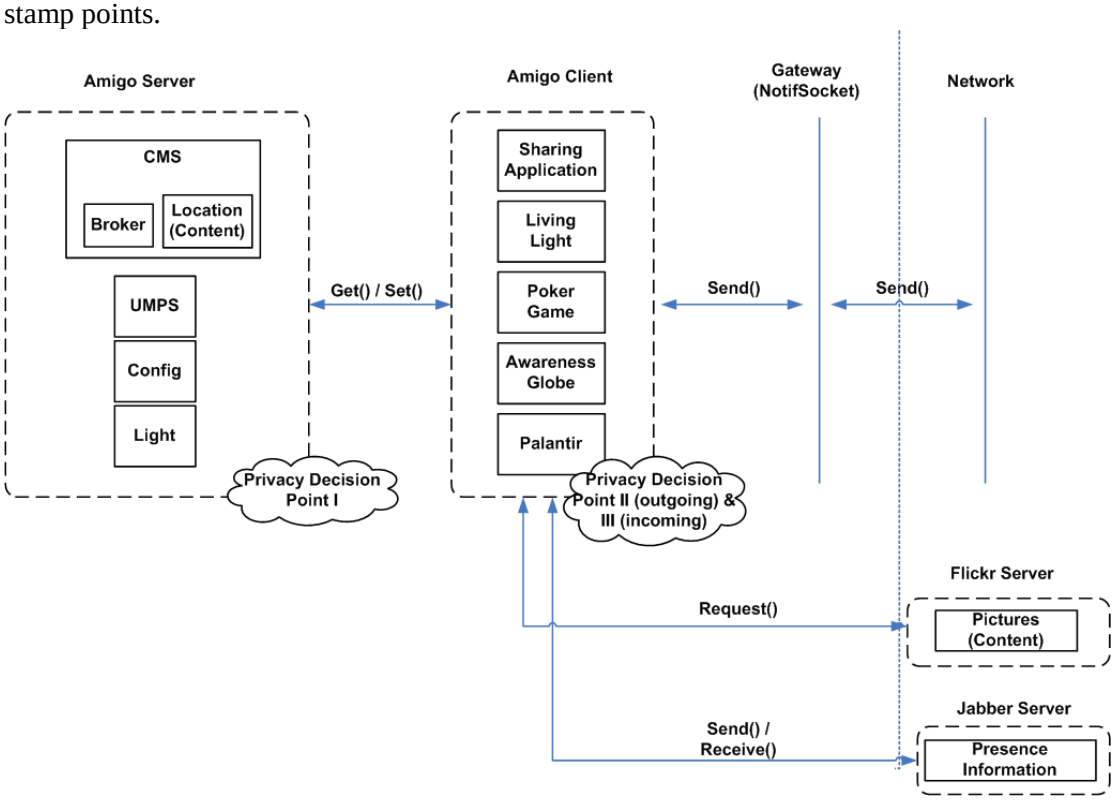

Figure 5-2: Application architecture

PDP is a piece of rule-based software that reacts based on user privacy preferences. User preferences are stored in UMPS using XML format. Once a requester requests a piece of information, the software will check user's privacy preferences. The information that passes the rules is sent to the requester.

Besides different PDPs, the application architecture shows the three main components in the prototype:

i) Amigo Server
ii) Amigo Client
iii) Network

Amigo Server consists of different services running in an Amigo home. Different services provide different types of information to the client. Client consists of different Amigo

intelligent applications that can be used in an Amigo home. Network is used to allow more than one home to be connected. In the prototype demo, an Internet connection is used to establish the connection between two computers. Each computer is connected to a television. The following sections describe all the components of the architecture and how does PDP is enforced.

5.3. Amigo Server

There are a few services running in an Amigo server that includes Configuration Service (CS), User Modelling and Profiling Service (UMPS) and Context Management Service (CMS). New services can always be installed. In this prototype, these services are used to provide contextual information about the home and its inhabitants.

5.3.1. Configuration service

Configuration service stores data about Amigo home in general, this includes the home ID, the users in the home, the applications installed in the home, and each user accessibility for an application. An example of the database in Maria's home is shown in Table 5.1.

Table 5.1: Data in configuration service

Amigo_Home_Application_Table

HomeID	Application
MariaAmigoHome	PhotoSharing
MariaAmigoHome	PokerGame
MariaAmigoHome	AwarenessGlobe
MariaAmigoHome	Ambulance

Amigo_Home_User_Table

HomeID	UserID
MariaAmigoHome	Maria@privacydemo.amigo.net
MariaAmigoHome	Jerry@privacydemo.amigo.net
MariaAmigoHome	Roberto@privacydemo.amigo.net

Amigo_User_Application_Table

UserID	Application
Maria@privacydemo.amigo.net	PhotoSharing
Maria@privacydemo.amigo.net	PokerGame
Maria@privacydemo.amigo.net	AwarenessGlobe
Maria@privacydemo.amigo.net	Ambulance
Jerry@privacydemo.amigo.net	PhotoSharing
Jerry@privacydemo.amigo.net	AwarenessGlobe
Jerry@privacydemo.amigo.net	Ambulance
Roberto@privacydemo.amigo.net	PhotoSharing
Roberto@privacydemo.amigo.net	Ambulance

'Amigo Home Application Table' stores the information about Maria's home ID and the applications she installed. 'Amigo Home User Table' stores the information about users in Maria's home. 'Amigo User Application Table' stores the information about user

accessibility for an application. When an application is started, PDP I is enforced to provide a list of users who can use the application and only allow these users to use it. One example is that when PhotoSharing is started, if Maria's name is on the table, then show her name on the menu.

NOTE: For the time being, the users who can access the application are hard coded in the program.

5.3.2. User modelling and Profiling Service

In this prototype, User Modelling and Profiling Service (UMPS) is used to store user profile and privacy preferences. The profile is stored in XML format. Table 5.2 shows Maria's personal identification number (PIN) stored in UMPS. From this table Maria's pin is '8888'. A user pin is stored under 'PersonalDetails' and the key id used is 'Pin'. pin is needed when a user attempts to login to the application. When a user login to an application, PDP I is enforced. If a user entered correct pin, then only further action can be performed.

Table 5.2: Maria's Password in UMPS

```
<PersonalDetails>
        <key id =”Pin”>
                <valueset>
                        <value type =”string”>8888</value>
                        <rating>1000</rating>
                        <justification>Explicit</justification>
                </valueset>
        </key>
</PersonalDetails>
```

User privacy preferences are used to control which piece of data is to be shared between homes. Table 5.3 shows an example of a XML format for storing Maria's privacy preference for location. This example shows to whom the data owner wants to share his or her location and in which precision level. The data falls under 'preferences' for privacy preferences. The data to be stored is location, and the key id for the data is 'locationsharingprivacylevel'. The location is labeled in different levels, each level is assigned one integer value to indicate its corresponding level, for example, 4 is for 'share my room location'. For detail of the associated level and its description, refer to Table 5.4. The value for parameter id is the name of the contact in which the data owner wants this piece of information to be shared with, in this example it is Jerry. In short, this example shows that Maria wants to share her room location with Jerry. All three PDPs are enforced for this purpose.

Table 5.3: An example for location privacy preference

```
<Preferences>
        <PrivacyPrefs>
                <LocationSharing>
                        <key id=”LocationSharingPrivacyLevel”>
                                <valueset>
                                        <value type =”4”>Share my room location</value>
                                        <rating>1000</rating>
                                        <justification>Explicit</justification>
                                        <parameter id=”UserId”>
                                                <value>jerry</value>
                                        </parameter>
                                </valueset>
                        </key>
                </LocationSharing>
        </PrivacyPrefs>
</Preferences>
```

In this prototype, UMPS is used to store user's privacy preferences about location and photo. For each privacy setting, the information is labeled in different levels. In the case where the information is to be shared with other people, different level will then be assigned to different people based on user's preferences. This implies that having different levels, it allows a user to have control over which information is to be shared and to protect user's privacy. For example, in our prototype, a user can share his or her location with other people. The location information provides from Amigo service is labeled in three different levels, from the exact location of the user, to the building where the user is, and to the city where the user is located at that moment. Maria, a user of the application, can choose to share her exact location with her husband Jerry and at the same time choose to share her city location with her friend, Paul, in the USA. This preference setting is stored in UMPS, and when she is sharing her location information using the application, PDP II is enforced to determine the dissemination of the context information.

5.3.3. Context Management Service

Context Management Service (CMS) provides information about location of the user. It is connected to a sensing device (Sensite Solutions, 2005b) for detecting wireless tags (Sensite Solutions, 2005a). The range of detection is 300m in line of sight. Whenever a user carries the tag in the home, his or her presence is detected by the service. Once a user has logged in to the application, PDP II is enforced to determine the dissemination of the context information. The information is labeled in different levels (see Table 5.4). We have adapted the location context source that was provided by Amigo for this purpose. Note that the level starts with 2 as level 0 is reserved for not sharing any information about the location and level 1 is reserved for sharing 'known location' with others. The labeling is based on our data model as depicted in Figure 4.3.

Table 5.4: Location information and their meaning

Location information from CMS	Meaning
2	City location
3	Area (building) location
4	Exact (room) location

5.4. Amigo Client

Our application is installed in an Amigo client. The application enables users from different locations to communicate. By using the application, users can exchange information, share activities, play games, chat, feel each other's presence and share their social context. The main functions in this application are sharing information and activity in two or more Amigo homes. In order for this to work taking into account of the privacy issues, several functions are implemented:

1) Login / logout from the application
2) Sharing information – presence context, location and application status
3) Sharing activity – share photos with people at other location
4) Setting privacy preferences

5.4.1. Login to the application

The application is installed in a CE-HTML enabled television. Because a television is a public device that can be used by every family member, while the data is privacy and sensitive, a user needs to use a pin in order to login and use the application. Once an application is turned on, names of the users that can use the application appear on the main menu in the television. A user starts the application by choosing his or her name on the menu. A dialog box will pop up to prompt the user to enter his or her pin. Once the user has entered a pin, the application will verify the pin. A user is logged in to the application if he or she has entered a correct pin.

5.4.2. Sharing information

A user can share different piece of information with different people that are located anywhere in the world at the same time. He or she has the freedom to choose which information he or she wants to share and with whom he or she wants to share the information with from the privacy preferences interface in the application. The three sources of where the information comes from are, i) information provided by Amigo service, for example, the location of the user ii) information provided by an application, for example, the status of the application, i.e. on or off iii) information provided by the user, i for example, the availability, i.e. online, busy, away or offline. Default setting is assigned to a new user. The user can modify his or her privacy settings from the privacy preferences interface. PDP is enforced to make sure that the application will react according to the privacy setting and user context. User can see the feedback from the application interface. Moreover, different color of light is used to represent different status of the user, i.e. online/offline/sharing photos. For this purpose, we have embedded a living light into our application.

5.4.3. Sharing activity – share photos with people at other location

A user can share photos with his or her contacts by using the application. Before sharing can be happened, the photos should be uploaded to a server. Each photo that is uploaded to the server is tagged with different tag ID. This again follows our data precision model as depicted in Figure 4.3. The ID can be 'private', 'public' or anything else depending on the need of the user. Once a user invites a contact to share his or her photos, PDP II is enforced to select the appropriate set of photos for sharing. The selection is based on user photo privacy preferences, taking into account of the tag ID of the photos, the presence and location of the user. The set of photos can change accordingly when the context of the user changes.

5.4.4. Privacy preferences setting

A user can set his or her application and location privacy preferences using the interfaces from the application. For application privacy, a user chooses whether to share his or her application with someone or not. This implies that if a user agrees to share his or her application with X, only then X can share the application with him or her. For location privacy, a user chooses whether to share his or her location with someone or not, and furthermore he or she can choose which location level he or she wants to share with that person.

5.5. Network

Network allows more than one home to be connected with each other. In this prototype, the application communicates with each other via a Jabber server(Jabber Software Foundation, 2006). Flickr server is used to store the photos.

Jabber Server is used to exchange messages and user availability between two Amigo homes almost in real time. The Extensible Messaging and Presence Protocol (XMPP) is used to allow this happen. The types of messages exchanged include user's location information and user application status, and user availability shows user current status, i.e. online, away, busy or offline. Besides that, Jabber Server is also used for initialization of a photo sharing request and establishing the connection between the two homes.

In order for a user to share his or her photos using the application, the photos have to be manually uploaded and stored in a server. Flickr server is used. Each photo should be tagged to indicate the 'privacy level' of that photo. For example, if a photo is tagged as 'parents', it means that this photo is to be shared with parents only.

5.6. Technical Limitations

The interoperability of the Amigo architecture helps to build and integrate other application very easily. The intelligent user services that were running at Amigo homes have some limitations. Some of the key limitations are explained below

5.6.1. CMS

Delay in sensing the latest location of a badge is due to a few technical reasons. One of them is that there is a five seconds interval for a sensor to detect a badge. When a badge has changed its location, it takes few seconds before the sensor retrieves the latest information. The interval can be reset, however, lifetime of the battery in the badge is shortening dramatically if the interval is shortened.

5.6.2. UMPS

There are three different ways to enter input to UMPS, i) UMPS client -- command prompt ii) UMPS GUI interface iii) UMPS web services interface. UMPS client and web services store their data in Microsoft Access, while UMPS GUI interface store its data in XML file. Due to the differences, UMPS client and web services are used as the media to enter value in UMPS.

5.6.3. Flickr Server

The photos for each user in this application are pre-loaded to flickr server manually. In this prototype, two different groups of photos are uploaded, i.e. photos tagged as 'parents' and photos tagged as 'parents and kids'. Photos tagged as 'parents' are to be shared when no kids

are around, while photos tagged as ‘parents and kids’ are to be shared when there are kids around. By using flickr web interface, a photo can be tagged as “public” or “private”. However, when calling method ‘flickr.photosets.getPhotos’ from Flickr Application Programming Interface (API), only photos tagged as “public” can be accessed and be displayed, even though the argument “privacy filter” is used. In order to solve this limitation, the description for each photo is being disguised as a ‘tag’ for that photo. For photo that is supposed to be tagged as ‘parents’, the description for that photo would be ‘parents’; the same apply for other tags. In this way, while retrieving a photo from flickr using “flickr.photos.getInfo”, our application will first check the description of that photo before determining which photo is to be shared between the two users.

5.6.4. Jabber server

Multiple requests create problem, in which if one person request for some actions while the other person is not online, the jabber servers stores those request and creates problem when it is started again.

If a user tries to login while jabber server is off, the socket for the connection request is lost, there is no notification about the failure of the connection. The consequence from this is that a user has to wait infinitely for the connection in our application.

6. User evaluation

Summary

We built a context aware photo sharing application and it was integrated with several Amigo services. The design guidelines from the earlier studies were incorporated in the prototype. Finally, the prototype was evaluated with several participants. Participants were explained a scenario and was shown different functionalities of the prototype. The main finding was that people understand the concept of the privacy aware application and they believe that it can preserve their privacy. Users have control over the system through privacy setting with different levels of context and content sharing. Users understand the levels of location sharing and 3 levels of location sharing are fine for them as long as they can control one of these levels.

6.1. Objective

The prototype was evaluated with a range of objectives. We used to operate user feedback with regard to:

1. Do people understand such an application?
2. Do people understand the concept of sharing locations?
3. Do people understand the use of light to represent context information?
4. Do people understand the privacy setting of the application?

6.2. Method

6.2.1. Participants

There were 5 pairs of participants in the user study. Participants were recruited from Philips Research Europe, Eindhoven. They had mixed background-technical and non-technical. All the participants were familiar with Internet technology.

6.2.2. Procedure

The testing session was approximately 1 hour. Each session was separated into three parts. First part was moving through the scenario, the second part was the demonstration of the prototype and the last part was filling in questionnaire and interviewing. The interview session was video taped for further analyses.

Participants were welcomed and they filled in the consent form. In each session, there were two people. One of researchers was acting as Maria and the other one as Jerry. The session started with the scenario that we described in chapter 3.

At the end of the story, participants were shown an example of how to change location information. Participants were given an overview of the functionalities of the prototype. One of the functions of the system was that it detects who are in the house and where they are. That is, the system can detect the location of people. This implies that the system selects the appropriate set of photos for sharing based on the presence and location of people and can change these sets accordingly when the context of the user changes. In the same way, the system selects the color of the light and changes this when the context of the user(s) changes. The choice and meaning of the color is based on a social agreement between the participating

users. After the demonstration of the prototype the participants were asked to discuss together and fill in the questionnaire (see appendix A).

6.2.3. Environment

The prototype was set up in the Ambi-lab here at Philips Research. Two display devices were used to show the participants what is happening in Maria and Jerry's location. The test room was organized in such as way that it would represent tow homes

6.2.4. Materials

The figure 6.1 shows the DMX light and its associated hardware used in our prototype. The tag we have used with the doll to represent Roberto is shown in figure 6.2. The actual setup of the prototype is shown in figure 6.3

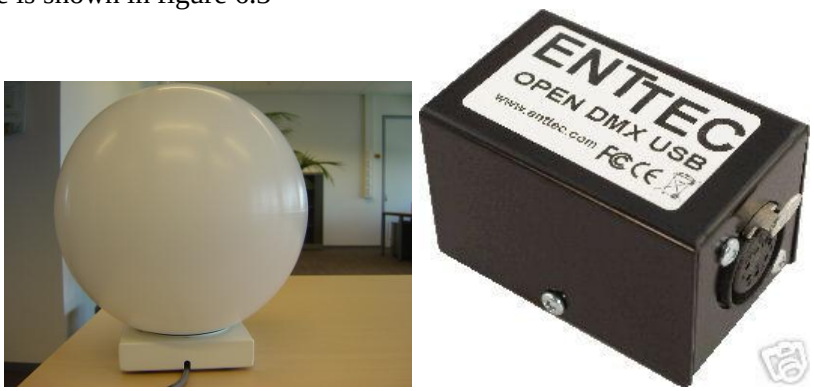

Figure 6-1: DMX light used in our prototype and its associated hardware

Figure 6-2: The tag (left) embedded in the Pooh (right) to represent Roberto

Figure 6-3: Set up of the prototype in Ambi-Lab at Philips Research

6.3. Results

Overall, we observed that the participants understood the context of our evaluation. They also comprehend the scenario, the functionality of the system. This might imply that consequently the implementation was understood as well. We try to argue for the aforementioned comments, based on the results from the questionnaires, interviews and videos.

6.3.1. Salient features

- **Do users understand such an application?**

Control over the system. The main feature of the system is that it is possible to set different privacy settings for different users. Therefore, it is possible to get control over the system.

Different levels of sharing. Users have the preferences to set different sharing for different people. This was done via the interface where they can choose whether to share or not share. The sharing option extends over different people, hereby providing a person dependent privacy setting. Moreover, the option for sharing location gave them the more freedom to choose. The can set different precision level: share city location, building location, room location and finally the known location.

Feedback. The system reacts based on the privacy setting by adapting the context of the user.. The direct feedback is shown via several means. The first one is log in and log out function. As soon as the user logs into the system the system provides feedback by showing the text of different color, for example green when online, red if someone is offline. The second feedback from the system is the content change due to the change of context. In our prototype different set of photos are shown according to where Roberto is located. Finally, the light color changes according to change of context.

Context awareness. The system provides context awareness for each user. In the prototype, the system reacts to the situation when Roberto is in the same room with. On the other hand the use of the colored light helps to figure out what is happening with the context in the other home.

The above-mentioned features clearly pointed to the requirements of building privacy aware application that were mentioned in Soute and Boland (2006). However, participants reported some shortcomings of the application that are discussed below.

Complexity. Participants reported that configuration of the system and usage would be complex. It is worth noting that the interaction with the display device was done via a remote control. So it may seem that the operation of such a system is complex. On the other hand it gives a very simple and intuitive way of interaction and the familiarity of the devices though the application.

Forgetting the preference setting. It is very obvious that users may forget different privacy setting for different users. However, the system saves all the current settings and when users log in again they can see the application is responding to the previously set setting. This actually gives users flexibility to set preferences every time. Participants gave feedback that sometimes it is not a good idea to use the previous setting as the default one since the preference might have changed for the specific person. We believe that there is a need for a default value to safeguard privacy with minimal functionalities.

Cheating. All the users reported that user might cheat with the system. This is true in that sense that a user may try to fake the system to let other people know that he is not at a specific place tough he is there. It also implies that people believe in technology but not the users who will use the technology. On the other hand, during the user evaluation it came out that some people really want to cheat with the system. One suggestion was to add an override function with the system.

6.3.2. Sharing location

- **Do users understand the concept of sharing locations?**

The users reported that they could share their location from the preference setting of the application and they saw the feedback on the screen. However, participants reported that there were some drawbacks in sharing different locations for different people. The major points are discussed below:

Social implications. In our implementation, we have given 4 different levels of location sharing. If someone shares higher level with friend X and lower level with friend Y this may offend person X if somehow X comes to know that he or she was given a different level than Y. One participant said, "*If someone does not share the lower level precision does it mean that he or she is very rude"?* Therefore, it is clear that sharing different precision of location information is a difficult issue both for the person who shares and for the person with whom the information is shared. We believe that sharing something is dependent on the relationship. In home-to-home networking, the implemented context aware system will be used between very limited number of people and with intimate people. The sharing will be dependent on the level of intimate relation.

Having received feedback regarding the social implications in location sharing we also got some advice from users about what could be improved in the precision of the sharing or if more levels could be beneficial.

Customize levels. All of the users were asking for a level where they can customize their own location setting. Since our setting was dependent on a specific scenario and to avoid complexity of the implementation we had only four levels of sharing. In our prototype we had one known level for location that was kept for customization that is either user can set some location agreed upon with the person or they can customize the location setting for other people. However, users were asking for more levels for instance, region, country, levels of activity etc. We believe that, the custom level could be used for more choice of location setting it could help in fulfilling users need. This finding also validate earlier findings presented by Soute and Boland (2006)

6.3.3. Sharing context information with a light

- **Do people understand the use of a light to represent context information?**

During the experiment participants understood the use of colored light in the application though they had a mixed reaction regarding the color of the light.

Passive notification. The use of light in the home environment gives a passive notification about what the other person is doing. The system works even the display device is not on. The only requirement is to have the Amigo system on. In the prototype when some one logs into the system from one home, the light of the other home turns green. By passive notification the system informs the user about any event without bothering them through the ambient environment.

Coded interpretation. The color of the light is used as coded interpretation between the people who are sharing information. Therefore, only limited number of people may know what the color means. This can help a user to share private information in an unobtrusive and more social way.

Though the use of light is intuitive in our application it had some drawbacks with regard to privacy, which was pointed out by the participants.

Limited in expression. The first and foremost drawback reported was that one light couldn't represent the states of many people. The feedback was bearing in mind the there might be many people at home and for each person there might be nee of more lights. Due to the advancement of lighting technology, it is possible to user more lights and the combination of different light types.. Even the tiles of different light color with different animation are available at Philips research. On the other hand, if one person has a different relationship it might be confusing and people can easily forget what does the different color mean and they could also forget the agreement with different people. The solution is to make some associations when defining their relationship with people via the light.

6.3.4. Trust in Amigo and privacy protection

- **Do people understand the privacy setting of the application?**

People understood the different privacy settings for different users and that the application responded to a previously set setting. To get the reaction from people we asked them to rate the system on the following questions shown in table 6.1. There were 7-point Likert scale

questions, where 1 means they did not agree at all and 7 means they agreed with statement very much. The means of the ratings were shown within the bracket.

Table 6.1: Mean ratings, on a scale from 1(not at all) to 7(very much)

Question	Mean rating
Trust in Amigo	5
Amigo will help in maintaining social relationship	4.5
Amigo will protect privacy	4.3

Figure 6-4: Snapshots from two interview sessions

The results from the rating questions shows that the Amigo application has potential in maintaining social relationships and people trust it and they believe that Amigo has the ability to protect their privacy.

6.4. Discussion

In this section, we will summarize the main points that came out from the user evaluation. The discussion will revolve around trust, privacy, disclosure of personal information and representation of context information. The discussion will be based on our experience with the project and the relevant literature in this field.

People appreciated the system and the concept of presenting the possibility of building a privacy aware application. Their appreciation can be found from one of the participant's quotes: *"The system is really cool and works perfectly"*. The major issues are discussed here with regards to existing findings.

6.4.1. Trust

It was evident that people trust the system. If they know the capability of the system that is system can retain their privacy they will believe it. One participant said, *"If I know the capability of the system I will trust it rather I will have less trust on the people who will be using it "*.

The system will be trustworthy if it takes a conservative decision. Again, this also establishes that in the functionality of the system there should be hard privacy rules that are the default cases. The default value of the privacy should be very rigid. Usually in our prototype once users have set some preferences for privacy, the next time this setting will be used as the

default value. However, from the evaluation it became clear that people do not want to let others know the same setting for the next time.

The Amigo system is very intelligent and this also raises a concern for some users. For instance if someone is in Amsterdam does the system will correct him or her or the system will follow the user's request (the other person requesting for specific information). Here the participants were pointing out that the system should not identify by itself rather follow the instructions set by the user and take intelligent actions based on the users preset preferences. If the other party knows the capability of the system, they might be suspicious of the person why he or she is not online. The other person will expect the exact location of the system.

One participant said, *"Just one button ora defaultoption that no information will be revealed".*
Participants wanted to have one central control or setting from where they can control the application so that it does not reveal information. If such a situation happens which possibly hinders their piracy they can protect it via central control. The issue of lack of control popped up in the qualitative interview with the participants. One participant mentioned, "*Its great that the system is operating automatically. But you are delegating everything to the system so there is lack of control since the systemis is doing everything automatically".* Another participant said, *'Can you trust the system that it is sufficiently aware of the context to adapt itself to the right setting'?* Since we used RFID tag in our prototype and due to its slight delay in sensing with regards to new user locations participants had the perception that the system may be not sensing it properly. However, the delay was due to the tag itself. This has led to questions for users whether they can really trust such a system that can adapt to the context that was changing.

6.4.2. System autonomy and privacy

There should be a balance in what the system can do and what people will do with the system. If the system is always accurate users cannot cheat. One participant said, '*you should be able to define what you wan't. The system cannot identify itself*.

During the interview session, the issue that was revolving many times was the setting of different privacy preferences and changing it. People might infer something when they see someone is changing his levels/locations. This eventually may complicate the social relationship. One participant mentioned, *"For a particular friend if you change your setting people will infer something- as if I want to hide something"*.

For some people level may have different meanings. When you change it to a more precise level, do we need to keep the high-level information as well? One user stated, "*People don't need to know that you have set some kind of privacy setting for them*". Another user said "*If someone is at home it (Amigo system) should recognize and do not share them. If I really want to show, I can override-there should be some manual control. I need to trust the system that it will not embarrass me: no automatic embarrassing situation/decision will not be taken by the system*".

This also supports earlier results from Soute and Boland (2006) that automatic location detection is accepted by the people as long as they have the feeling of being control over them. From their results, it is found that, *"People prefer to share information at the lowest level of detail that is appropriate but they desire to add noise (e.g. by lying) for social acceptability.*

Participants reported that having different levels makes relationship complex, however, they agreed that it is truly a matter of relationship and situation when someone want to know or let others know exact location. They reported that for family settings no need to know exact location. For medical care application, it (Amigo system) needs to know the exact location. For instance, in emergency condition the application could work.

6.4.3. Privacy vs. trust

It became clear from the comments of the users that there is close relationship between privacy and trust. If people can trust the system that it will preserve privacy the way they want they will rely on the system. Overall, the trustworthiness of the system depends on its decision-making according to user's preferences. Since in an ambient intelligent environment it is necessary to disclose information, which is eventually necessary to build trust relation with human and technology. It is really important to identify minimum disclosure of information that is necessary to build sufficient trust to accomplish some task for the user (Bhargava, 2006). In our prototype, it was crucial to know how much information about the inhabitants of one home to be disclosed to other people to build a sufficient trust level for the people in extended home. It is still hard to say anything explicitly or measure how much information to be disclosed needs proper investigation. We believe it is a matter of situation and relationship when and how the application will be used. This eventually will help end users to use system like Amigo that it will preserve their privacy and the trust with such a system will be higher. Even for the context aware part of the application, if it is really context aware and follow the privacy rules of the user, it might be perceived as trustworthy by the user.

6.4.4. Representing context information

Representing context information by colored light has some limitation. People cannot remember the coded representation of many relationships. One participant said, *'after 20 color I will forget'- not too many color'*. We tested the prototype with one light. Participants wanted to have more lights each indicating one person; that will give them a kind of sense that how many people are in a room. As appreciated by the users, we proposed to use of color light to share ambience and to represent the very personal and intimate way of sharing information. Even the urgency of the information can be represented by light. Though it was not implemented in our prototype, the urgency can be shown by the intensity and using deep color of the light. Overall, the use of light in Amigo like application could benefit for users to share experience in a very intimate and private way.

6.4.5. Preferences for disclosures

The disclosure of personal information /context information had different precisions in our application. It was evident that people wanted to have control over the different precision levels and particularly they asked or a custom precision level for location information. In our application people tried to adjust the precision depending on the need and urgency of the situation. Sometimes they really wanted to hide their actual location keeping in mind that hiding will give them more flexibility about their privacy. The open question put in the Lederer et al's study that giving different levels of precision to different people is socially acceptable or not. It came out from our evaluation that different precision level might make the social relation complex and the probable social clash. However, we believe that the usage of the application in a home setting will not really create any problem. We have focused in our prototype on spatial precision that is where someone is located currently. For instance, it can be either in a building or in a specific room in the building.

7. Refined User Interface Design Guidelines

Summary

In this chapter we explain the interface that we built following the design guidelines proposed by (Soute and Boland, 2006). We tried to adapt these guidelines and implemented them in our prototype. The original interface we used to extend and build our concept was not built keeping in mind the privacy of the end user. However, we found it good enough to deploy our concept for building an application that can preserve privacy of the end users. The design guidelines proposed by Soute and Boland (2006) are given below:

1. Provide proper security and inform users of security measures
2. Provide control on several levels
3. Present users with a choice of level of detail in which the information should be shared
4. Provide clear feedback over shared information
5. Never automatically share information without user consent
6. Avoid using automatic intervention to maintain user privacy

Finally we propose some refined guidelines that are necessary for the developers to build context-aware privacy safe application.

7.1. Implemented design guidelines

The implemented design guidelines will be explained using relevant snapshot of the interface that we built.

1: Provide proper security and inform users of security measures

Figure 7-1: Snapshot of the screen: Enter PIN

Our prototype can be used for different members of the family. For security reasons, we have added PIN for each user (see Figure 7.1). This security is important in the sense that each user preferences are associated with his or her own identity. People might not be able to view others personal setting without his or her consent.

2: Provide control on several levels

Figure 7-2: Snapshot of the screen: Preferences Setting

The prototype provides control over the privacy settings on several levels to protect users privacy. The control is implemented by allowing user to set different privacy preferences from the interface. By using the interface, users have several options for sharing. There are three submenus under preferences setting (see Figure 7.2), they are 'Sharing Application Setting', 'Location Preference Setting' and 'Photo Preference Setting'. Users have control on each of these, for instance, under 'Sharing Application Setting'; the user can choose to whom he or she wants to share the application. Besides setting different privacy preferences, a user can deny or accept a request when there is an incoming request (see Figure 7.3).

Figure 7-3: Accept or deny invitation

3: Present the user with a choice of level of detail in which the information should be shared

This guideline says that each type of information can be shared in several levels of detail and it should be possible for the user to adapt the level of detail to the context in which the information is shared. One example is the location information, in this prototype, the user can share different levels of his or her location with other people. This example is illustrated in Figure 7.4. From Figure 7.4, it is clear that user has different options to disclose his or her location information. He or she can either let other people know the exact location or more higher-level location information depending on their preference and the relation with the people.

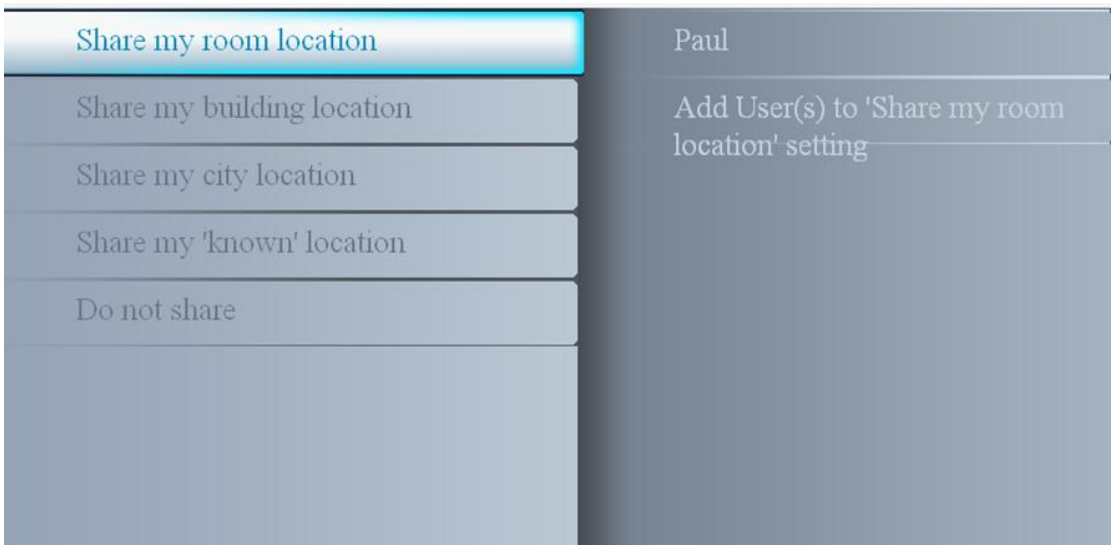

Figure 7-4: Location Preference Setting

4: Provide clear feedback over shared information

It is important to know what information is shared while sharing some information to other people. It is equally important to know how exactly the information is presented to other person.

In our prototype, we have made the information shared to the other party visible on the same screen consistent with the menu style. This shows what the person is sharing, with whom and the level of detail.

Figure 7-5: Snapshot of the screen: Feedback

For instance, from figure 7.5, Maria is online (indicated by the green font), she has her photo sharing application on and is sharing her building location with Jerry. At the same time, Jerry is online, has his photo sharing application on and is sharing his city location with Maria (note that because Maria's name is highlighted, it is understood that the information is shared

between Maria and Jerry). Moreover, Jerry is the current user of the application while Maria is his contact. The feedback is real-time and consistent with the user interface style guide of the EasyLogic.

5: Ask for user consent before sharing information

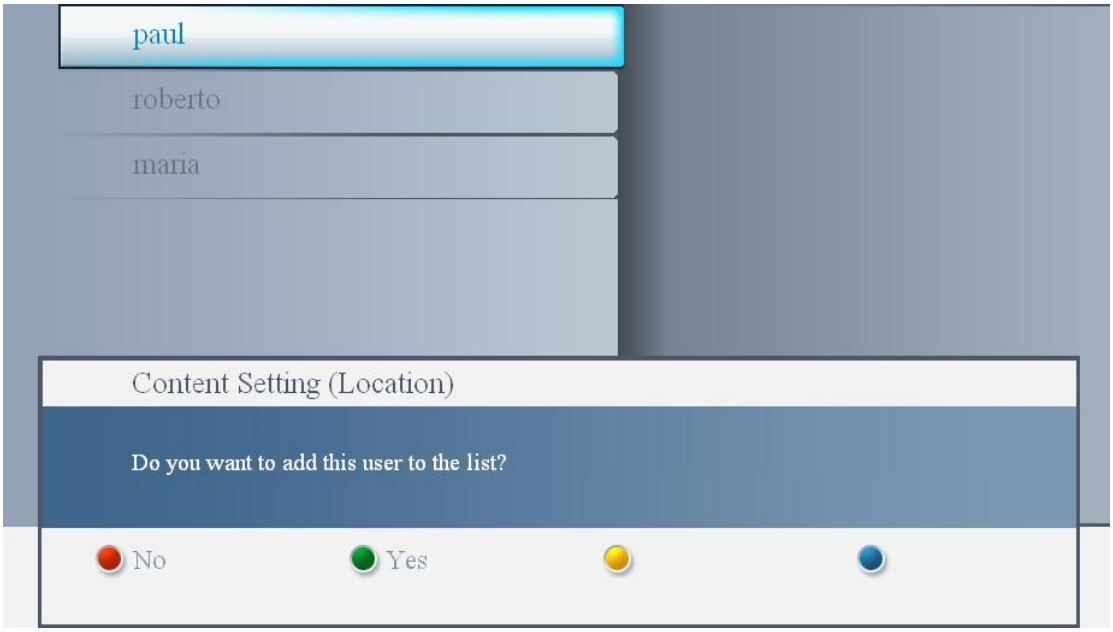

Figure 7-6: Adding User for Sharing Information

The guideline was intended for requesting user's consent while adding someone to the shared list. In our prototype, we have implemented the confirmation message whether someone will be added in the shared list or not. By having this confirmation message, the user can think twice who the person he is adding.

6: Avoid using automatic intervention to maintain user privacy

The 6th guideline was not implemented in our prototype and it will be discussed in the following section.

7.2. Privacy and Design Guidelines

Privacy is not just a set of static rules, rather very dynamic in nature. Therefore, we believe that the solution that we presented is not an absolute one. We also believe it is not possible to perverse end user's privacy in a generic manner. Our effort is a step towards handling of perceived privacy in Amigo intelligent extended home environment. We also propose some of the design guidelines for building privacy safe context-aware application.

7.3. Notes on building privacy interface

As mentioned before we have chosen an existing application for building our prototype. The existing application and its interface was not tested for its suitability for the end user. This also pointed out by our users while we evaluated the prototype. In particular, the menu of the application was text based which sometimes confused the user. The prototype was deployed on a display device like TV and the user interaction was like a person interacting with his TV

by a remote controller. The distance from the display device also created problem for the users. We also mentioned that our main idea was not to evaluate the usability of the interface rather the privacy aspects associated with this application. However, during the evaluation we gained insights about the usability of such an interface. From the early expert evaluation, we also received feedback that the interface was not suitable for end-user to easily understand and interact with it. It would need to be designed more user-cantered way to make it usable the end-user.

From our experience we would like to add that the interface for setting privacy preferences need to be easily configurable for the end-user. There should have a balance between the social context and technological means of building interface for the usability of the privacy interface. As there is a wise saying that 'good privacy leads to bad usability' so it is important to build application that will be able to protect privacy and on the other hand usable for the users in terms of configurability and the general usage.

Here we have rewritten some of the design guidelines that can be seen as an extension of the previous guidelines mentioned in (Soute and Boland, 2006). These extended guidelines are based on the social context i.e. focus here is on the perceived social privacy.

Original guideline 1: ***Provide proper security and inform users of security measure***

Modified guideline: **Provide usable security and inform users of security measure**

The original guideline emphasizes on the data encryption for protecting user information and informs the end user of the security risks. In terms of the Amigo the prototype used in the extended home environment, we think that this kind of security measures does not need to show every time to the end user since it will make an unnecessary burden for them. As confirmed by the result of our user study that user once needs to know the capability of the system- what it can do and later they trust on it.
With the term usable, we refer to more intuitive way of providing security for the users that will be easily remembered. Our prototype was built for the home users and we assumed that the application would be used for different users residing at home. The concept of pin code was introduced here to provide security for different users. However, we got feedback that people might forget the pin code easily. Therefore, there is a need for usable security for the user. To solve the problem of forgetting pin code, biometric measurements can be used but still it should be used in the application in a very intuitive fashion.

Original guideline 3: ***Provide users with a choice of level of detail in which the information should be shared***

Modified guideline: Provide users with automatic and /or manual choice of level of detail in which the information should be shared.

It is important to disclose different level of information to different people for preserving privacy as well as maintaining relationship for the user. Our prototype also had 4 levels of locations to be disclosed for different people. The three levels were pre-chosen by the user according to his preferences and the fourth one is the more vague i.e., known location that can be manually set i.e. a customized level. The prototype that we built of course was a scenario

specific but users showed their interest to have customized levels in such an application. Since the application is intelligent and context aware, it should know in advance the users' preferences that can be chosen from the set of options for sharing locations that is different precision levels for locations. Moreover, when the actual locations is out of those set location or even when the location of the user changes more options needed for the user. A customized precision level could help in this regard.

Original guideline 4: ***Provide clear feedback over shared information***

Modified guideline: Provide clear feedback over shared information by audio, video, text or images or in combination of any of these.

This realization came out when we were building our prototype iteratively. We showed the shared information like location context, activity context and the application usages in one panel of the interface that was being shared to the other party. From the evaluation of our prototype it came out that the images of the photo sharing application was not clear to some of the users. We realized that it would be helpful for the user to give the feedback by other means for instance audio, video or text whatever is appropriate for specific application. During the interview participants added that the audio is important in such an application though we did not have any audio.

We also would like to focus the term *clear feedback* as content wise (i.e., what kind of information, with whom and what level of detail) and form the user's side it should be easily understandable.

Original guideline 6: ***Avoid using automatic intervention to maintain user privacy.***

Modified guideline: **Avoid using automatic intervention to maintain user privacy unless and until it is not preset or preconfigured by the user.**

The sixth design guidelines mentioned by Soute and Boland (2006) was 'avoid using automatic intervention to maintain user privacy'. The implication was not to stop sharing information automatically without the consent of the user. Since in our scenario, the photo sharing application is context aware it will react according to the preset user preferences. If for instance someone enters into Maria's room then the photo sharing will be switched to another mode and the change of context will be shown by colour light. However, here the sharing is not stopped but still the sharing changes from one mode to another mode without explicitly taking any consent from the user. In fine, we would like to say that if the system is context aware and the user reconfigures the privacy preferences then automatic intervention is not a threat for user privacy as long as the system works according to the preset privacy rules.

Finally, we would like to say that the guidelines are not panacea. It is recommended to follow the guidelines to build privacy-preserving interface for Amigo. However, there might be some other elements that might come up while these guidelines will be used in different applications used for different purposes.

8. Conclusions

We followed the design guidelines and built the application according to the initial scenario. Light was used to represent contextual information about people at another location. However, there was only one light used in this prototype, only one person can use the light. Therefore the concept is not fully representing the actual scenario. This prototype can be extended by using two lights to show contextual information about two people.

The designed privacy model was used for a person to control which piece of information to be shared and with whom by setting different privacy preferences. And the piece of information is shared with other people in another location by using an application. Once the information reaches another location, it will be shared as it is without taking into account the other user's context. For example, Maria wants to share her photo with her parents but not with her parent's friends. By using this privacy model, Maria can share her photo with her parents, but there is no way to inform the parents that she does not want this photo to be seen by parents' friends. The privacy model can be extended to allow the parents to know about Maria's privacy preferences. This can be done by including Maria privacy preferences while she is sharing her photo with her parents, and the control point in the parents' house can react according to parent's context and Maria's privacy preferences.

In the scenario, simplified version was implemented to keep thing simple and focus. Only two people are sharing information and activities. And only two categories of photos are being shared. In real life, the scenario can be more complicated. We believe that the designed privacy model can handle more complex real life scenarios as long as a strict default setting is incorporated.

The main focus in this prototype was to study how people's perceived privacy is handled in an extended home environment. The usability and correctness of the words used in the interface was not the focus. However, it is equally important for the user to actively exercise the privacy concerns and overall the acceptance of an Amigo likes system. The user will accept the real interaction with Amigo like privacy safe application when it will meet the expectation of its users.

The inclusion of color light in the prototype was appreciated. It can implicitly represent the intimate information and thus could be a nice choice to intuitively share contextual information.

The prototype can be extended to include more functions, for example, add or delete contacts, and upload photos and organize those photos manually by the user. Additional interface to allow a user to control the sharing of the photos can be useful. Moreover, we did not touch all the components in real Amigo architecture. For example, we did not take into account about the data security, in which the data might be stolen or lost during a sharing session. Security component could be used to tackle this issue.

Implementation of the prototype and the integration with Amigo services was not complex as Amigo architecture is based on service orientation architecture. Initially Amigo was an in home network, but in an extended home environment where more than one home can be connected, Amigo server which resides in the home can be moved to the internet to be a comprehensive server. In this case, several homes can be connected together through Amigo server.

The evaluation of the prototype was exploratory where we investigated whether people understand this application and the different privacy aspects. Still it needs to identify how such a system will be used in a real life setting. The complexity of the setting of different preferences needs to be investigated as well. The real prototype can be installed in separate homes and a diary study can be done to find out the unanswered question from our evaluation. However, we believe that the implication of different privacy aspects could be different in real setting depending on the person who will use the system and how much he or she is comfortable with technology.

Refined design guidelines for building privacy safe context aware applications were proposed based on previous design guidelines and the evaluation results. A major conclusion was that privacy settings are very different for each individual, but that for most people having 3 levels is sufficient if they can control at least one of these.

Question remains that whether people will understand the different privacy policies. Are users familiar with the privacy jargon? From the technical point of view, what happens if there is any collision with the different privacy policies of different users? Does it really make things complicated? Building and deploying large-scale prototype can answer these questions. A useable privacy interface is crucial for the end-user to use the application.

Acknowledgements

First, we would like to thank Maddy D. Janse for letting us to work in this interesting project. Her insightful and critical comments and her engagement in the project helped us to shape our ideas. Without her helpful involvement, the accomplishment of this project would not be possible.

Our utmost gratitude to Peter Vink who was co-supervising our project. His patience and time for our project was very helpful.

We also would like to thank Peter Lambooij, Dietwig Lowet, and Leo Rozendaal for their helping hands and letting us using their codes for the implementation of the prototype.

Thanks also goes to our TU/e mentor Jun Hu for his helpful comments in the several phases of the project.

A special mention to all the participants who took part in our user study and gave us useful feedback.

References

1. Bhargava, B. (2006). Innovative Ideas for Privacy Research. Proceedings of the 17th International Conference on database and Expert Systems Applications (DEXA'06).

2. Boland, H., and Soute, I. (2006). Perceived privacy in ambient intelligent environments, Technical note TN-2006-00774.

3. Brodie C., karat, Clare-Marie., John., Feng J.(2005). Usable Security and Privacy: A case study of developing Privacy management Tools. Symposium on Usable Privacy and Security (SOUPS) 2005, Pittsburg, PA, USA.

4. D1.1, A. D.(2005). Amigo user research results. Number IST-004182 Amigo.

5. D2.1, (2005). Specification of the Amigo Abstract Middleware Architecture. Number IST-004182 Amigo.

6. Friedewald, M.., Vildjiounaite, E.., Punie, Y., Wright, D. privacy, identity and Security in ambient intelligence: A scenario Analysis. Telematics and Informatics 24(1): 15-29 (2007)

7. Hong, J. I. and Landay, J. A. (2004). An Architecture for Privacy-Sensitive Ubiquitous Computing, MobiSys 2004, Boston, Massachusetts, USA.

8. Internet home alliance (2002). White paper-The US Connected Home market. Internet Home Alliance.

9. Jaber Software Foundation (1996-2006). Jabber protocol. http://www.jabber.org

10. Langheinrich, M.(2001). Privacy by design-Principles of Privacy-aware ubiquitous systems. In S. Shafer G.D. Abowd, B,Brumitt, editor, Ubicomp 2001: Ubiquitous Computing: Third International Conference, volume 2201, pages 273. Springer Berlin Heidelberg.

11. Lederer, S., Hong, J.I., Jiang, X., Dey, A.K., Landay, J.A., Mankoff, J(2003). Towards Privacy for Ubiquitous Computing, Technical Report UCB-CSD-03-1283, Computer Science Division, University of California, Berkeley.

12. Lederer, S., Hong, I., Dey, A. K. and Landly., A.(2004) Personal privacy through understanding and action: five pitfalls for the designers. Personal and Ubiquitous Computing., 8(6):440-454.

13. Lederer, S., Beckmann, C., Dey, A., and Mankoff, J. (2003) Managing Personal Information Disclosure in Ubiquitous Computing Environments. IRB-TR-03-05, June 2003.

14. Lederer, S., Mankoff, J., and Dey, A. (2003). Who Wants to Know What When? Privacy Preferences Determinants in Ubiquitous Computing, CHI 2003, April 5-10, USA.

15. Meyer, S., and Rakotonirainy., A(2003). A Survey of Research on Context-Aware Homes, Workshop on Wearable, Invisible, Context-Aware, Ambient, Pervasive and Ubiquitous Computing. Conferences in Research and Practice in Information Technology, Vol. 21.

16. Oosterholt, R., Roberts, G., Putten, J. van der., Brouwer, A., Peeten, J., Neervoort, P., Kohar, H.(2006). EasyLogic 3.0 for TV centric products. The UI category Standard for Remote Controlled Large Screen Devices. Published by Philips Design.

17. Palen, L. and Dourish, P. (2003). Unpacking "Privacy" for a networked world. In Proceedings of CHI 2003. pp.129-136, 2003.

18. Patil, S., and Lai, J. (2005). Who gets to Know What When: Configuring Privacy Permissions in an Awareness Application, CHI 2005, April 2-7, 2005, Portland, Oregon, USA.

19. Sensite Solutions (2005a). Product Leaflet Logisphere BN208 Intelligent Tag. http://www.sensite-solutions.com/.

20. Sensite Solutions (2005b). Product Leaflet Logisphere HBL100 Wireless Network Controller. http://www.sensite-solutions.com/.

21. Schmidt, A., Beigl, M., and Gellersen, Hans-W. (1999), There is More Context than Location, In: *Computers & Graphics Journal*, Elsevier, Volume 23, No.6, pp 893-902.

22. Sheikh, K., Wegdam, M., and van Sinderen, M.(2006). Enforcement of Dynamic Privacy Policies in Distributed Context-aware Homes. Adjunct Proceedings of the 4th International Conference on Pervasive Computing, Dubline, Ireland, Published by Australian Computer Society(OCG): Vienna, Vol. 207, pp. 227-230

23. Weiser, M. (1991). "The Computer for the 21st Century", *Scientific American*, September, 1991, pp. 94-104.

24. Winters, N. (2004). Personal privacy and popular ubiquitous technology. Proceedings of Ubiconf 2004, April 19th, Gresham College, London.

25. Yee, G. (2005). Using Privacy Policies to Protect Privacy in UBICOMP. Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)

Appendix A

Test questionnaire

Dear participant,

Thank you for your participation. Please answer the following questions according to the system you have just shown. There is not right and wrong answer. You are free to express what you think.

1. What are the 4 most salient features (possibilities) of this system? List below

    a. _____

    b. _____

    c. _____

    d. _____

2. List 4 advantages of such a system

    a. _____

    b. _____

    c. _____

    d. _____

3. List 4 disadvantages of such a system

    a. _____

    b. _____

    c. _____

d. _____

4. Maria and Jerry can know where they are, in which room, which houses etc.
    a. List 4 advantages
        i. _____
        ii. _____
        iii. _____
        iv. _____
    b. List 4 disadvantages
        i. _____
        ii. _____
        iii. _____
        iv. _____
    c. List 4 missing levels
        i. _____
        ii. _____
        iii. _____
        iv. _____
5. Do you think the application is responding to the newly set location?
    - ❑ Yes
    - ❑ No
6. List 4 advantages using light to show your context.
    a. _____

b. _____

c. _____

d. _____

7. List 4 disadvantages using light to show context

a. _____

b. _____

c. _____

d. _____

8. Can you think of other things that you can do with light? Try to give three examples:

I. _____

II. _____

III. _____

Please circle the appropriate number:

9. Do you trust that Amigo will protect your intimate information (your availability for instance online, offline do not disturb etc, your environment etc)?

Not at all 1 2 3 4 5 6 7 Very much

10. Do you believe that Amigo will be helpful for maintaining your social relations?

Not at all 1 2 3 4 5 6 7 Very much

11. Do you believe that Amigo will protect your privacy?

Not at all 1 2 3 4 5 6 7 Very much

12. Amigo shows changes in your social context and adapts to it. In which situation is this desirable?

    a. Keep sharing photos while you are not at home

    b. Showing your presence while you are not at home

    c. Informing your partner while you are alone or not

    d. Sharing your fridge content

    e. Other _____

Comments:

Appendix B

Raw data from the participants

What are the 4 most salient features (possibilities) of this system?

-Location information

-Easy way of content sharing

-Lots of privacy levels

-Easy to use in the living room. -No PC needed

-Recognizing where I am

-Logging in and logging out

-Changing display depending on who comes to into room.

-Changing references for what --location info is shown to others

-The possibility to get information anywhere

-The possibility to stay in private (location)

-Share info depending on who is present

-Set different requirements for different people

-Users have the privacy of location information

-Users can choose the preference of the pictures

-The system can change the settings depending on who is in the system

-The colors of the light give the information about who is in the system

-Communication anywhere

-Communicate different types of information

-Share photo

-Login to the system

-Change preferences

-Context awareness

-Availability (only need a networked device with display units

-Control (you control when the others see about you.

-Potential: many applications can benefit from the above three points

-Bringing separated people virtually together

-Keeping in touch

-Medium for sharing life events

-Communication

List 4 advantages of such a system:

-Communicate with friends all over the world

-Privacy levels for different people

-Indicates unobtrusively if another person is online

-Allows to share content whenever the other person is.(as lon as he has an internet connection)

-Provides the option to share certain pictures only in certain conditions

-Detects the situation/condition

-Different levels of location sharing

-Can see Picture and location at the same time

-Can see when a person comes online

-Can seed secret message (light colors)

-Can be alerted to change in your own context

-Easily share of content

-Privacy is protected

-Person can choose not to disclose info: non-intrusive

-Different setting for different people

-Provides context awareness for each user

-Provides communication info according to user relations

-Share information (no only about photo)

-Community/sharing is easier when apart

-No need to configure or check what you are sharing since its context sensitive

-You can use many devices; not tied to one particular device; its more freedom

-Extended connectedness of users

-Global managing system for a) house control b) family's media library

-Controlled transparency / visibility to others

-Simple manipulations composed with communication through PC

-Concentration on special group, such as family members.

-More comfortable when using remote controller

List 4 disadvantages of such a system:

-You forget to change privacy setting then everybody can see where you are.

-Detection of a third person like Roberto only works in the Amigo home, not in a hotel

-May be I would like to share that 'I am online with e few people (e.g. with Jerry but not with other friends in this particular case.

-Can I share content with people who can then copy it and share with a third person.

-Have to wait for sometime to come online

-Cannot lie about your location

-Helps to lie to other people about what you are discussing (bad)

-You may not want a person to know at a given time/moment where your are, but the setting may allow that

-The meanings of the light's color are not very easy to remember

-Requires context-aware equipment/devices in order to use it/its feel potential

-Privacy? Cheating?

-Did not observe the light

-Complexity: because of the possibilities configuration and usages are not simple

-If more than one person on a room using one device you can only log in as 1 user- so u need one device per user for some application.

-Might feel controlled

-Mistake in sharing can influence sensitive life areas

-Intimacy can be broken, info disclosed

-User should rely on system in important life questions

-I feel it is still dangerous to put marriage pictures in the system

-Privacy problems with sharing locations

Maria and Jerry can know where they are, in which room, which houses etc.

a. List 4 advantages

-No login needed if system knows who is in the room.

-Different level of detail for different people.

-Can give details from the location (e.g. I should not cal now)

-Saves asking question: where are you

-Save saying things like: I am not on the train etc.

-It's easy for them to tell what they are doing

-Parents can keep track of kids

-They can know each other's information in detail

-Ability to help incase someone needs it.

-Free and safe

-Know each other

-The can get better idea of others: context availability

-Keeping in touch

-Synchronization of events, plans

-Closure

-Good for children and married persons who may need to be taken care of.

b. List 4 disadvantages

-Privacy

-Creates obligation for a person to set his location to a level of detail that normally reflects the relation.

-Creates a slight feeling of being tracked/monitored

-Makes it stupid to say where you are or ask where a person is

-Cannot lie about where you are(this is a easy way to star conversation)

-If I don't show someone my 'room' am I very rude?

-Privacy concerns

-Sometimes people want to keep some privacy. So these information my be too much

-Sometimes people maybe don't want certain person on his contact list to know that they are online

-Ability to help incase someone needs it.

-Sometimes people maybe don't want certain person on his contact list to know that they are online

-Trust

-Sharing a higher level with someone shows that you don't trust them- you don't want them to know. They could be offended

-Might feel observed

-Controlled

-Too close

-No intimacy, private life

-If you are not living in a palace, not necessary to know in which room

c. List 4 missing levels

-Country

-In the car

-On the bike

-Levels that imply a certain level of availability, e.g., at work, in a meeting

-A 'lie' (e.g. say I am somewhere that I cannot)

-General level e.g. at home, at university

-Familiar terms like kitchen

-Blurry levels like 'shopping' driving from x to y.

-A level which doesn't allow one to know where the other is but without the explicit "don't show" option

-Workplace

-Activity related locations

-For a friend in a different country you would need to specify the country and region; for a friend in the same town you don't need that

(room level) in regards to home.

-Work / home / swimming pool / somewhere in the city → My frequent places, that I want to make visible + somewhere else

-Users should be able to set his locations

-Levels depend on the person you are sharing them with

-If the system has GPS, then people cannot hide themselves

-Fixed levels can be difficulties to determine when getting too precise

Do you think the application is responding to the newly set location?

- Yes (10)
- Yes [but pointers because if I change from room to building during session other person still knows].

List 4 advantages using light to show your context.

-Easy to understand for everybody

-Without turning on device u can know who is online.

-Unobtrusive

-Doesn't require the device to be on

-Can represent enough context state (a color=state)

-Coded interpretation (only the people know the meaning)

-Easy

-Intuitive

-Visibility

-Not that clear, coz we don't know where is the light

-Quickly identifiable

-Many different contexts can be identifiable

-Passive notification

-No need for a screen or complicated device is all rooms if you want to be informed using light.

-Non-irritative in the evening

-Customizable

-Not visible to others

-Fashion

-Easy to notice

-And how strong the light will be

-And how strong the light will be.

List 4 disadvantages using light to show context

-Light turns on while you are sleeping.

-3 different colors are better than 20 colors: easy to remember

-I won't see if someone was online etc while I was out of room.

-Activate bright light may be considered energy waste during daytime.

-When I am sleeping, I don't want the light to go on when someone comes online.

-One light cannot represent the states of many people.

-Changes the lighting of the room

-Others know that something has happened

-I will forget what it means [even if they don't know what it means]

-People may not agree on the meaning of the color and they may forget the meaning

-Many relationship/light might be confusing

-Not easy to see if the user in a big room or in a very bright room.

-Cultural differences for colors and their contradictions/meanings

-Colour-blind people may have disadvantage-handicapped

-Visible by anyone in the room (Privacy)

-You have to remember what the color/intensity means

-Not so appropriate during day time

-Restricted to a specific place in house

-Might look silly to other people

-Not involved

-No efficient to have a lamp only for sharing context

-Limited in what it can express.

-Not very specific

Can you think of other things that you can do with light? Try to give three examples:

-Not too much, see answer 7b

-Provide light

-The contact can be shown with blinking light

-Each person in one end may be represented by a light unit

-Don't use one light but a whole room lighting effect

-Information indicator

-Send 'light messages' – smiles / kisses

-Expressing emotions via light set up (like living light)

-Set the colors by myself

-It can be a multi-color lamp for example when Roberto is not around, it can display many colors or family colors

Amigo shows changes in your social context and adapts to it. In which situation is this desirable?

-Informing your partner while you are alone or not [needs to have a override option] (4)

-Other:

-Showing your partner/social context that you are not available for a chat when Amigo can infer that (e.g., I am sleeping, not home, studying then I cannot chat

-Sharing your fridge content (4)

-Other: Contacting other friends when some friends come to visit you

-Showing your presence while you are not at home (4)

-Other: Sharing your current activity would be useful. (i.e. Listening to music)

-Also it could be used to share important dates or your schedule with friends and family, making it easier to organize things (calendar function with different levels of detail for people and privacy)

-Keep sharing photos while you are not at home (5)

Appendix C

Sequence diagrams

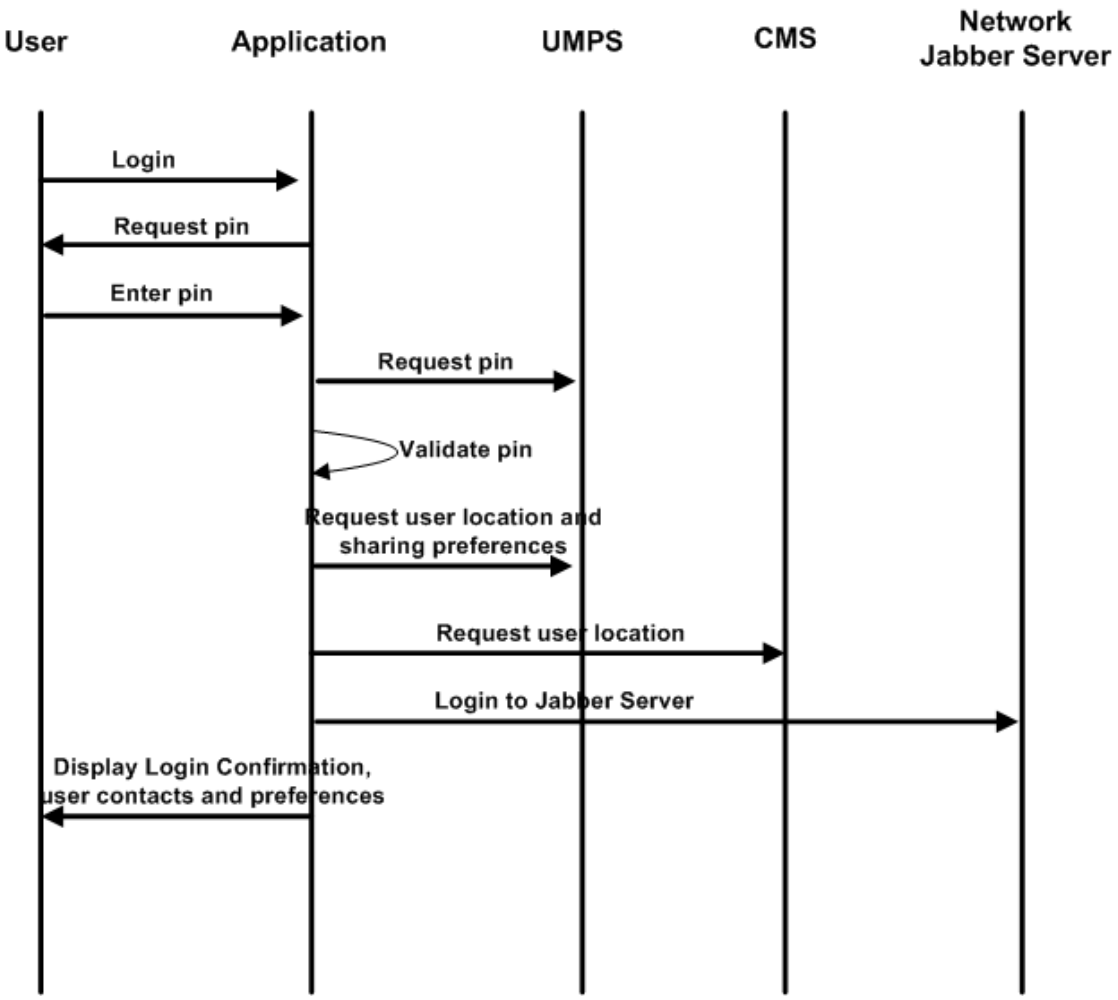

Figure C.1: Sequence diagram for login to the application

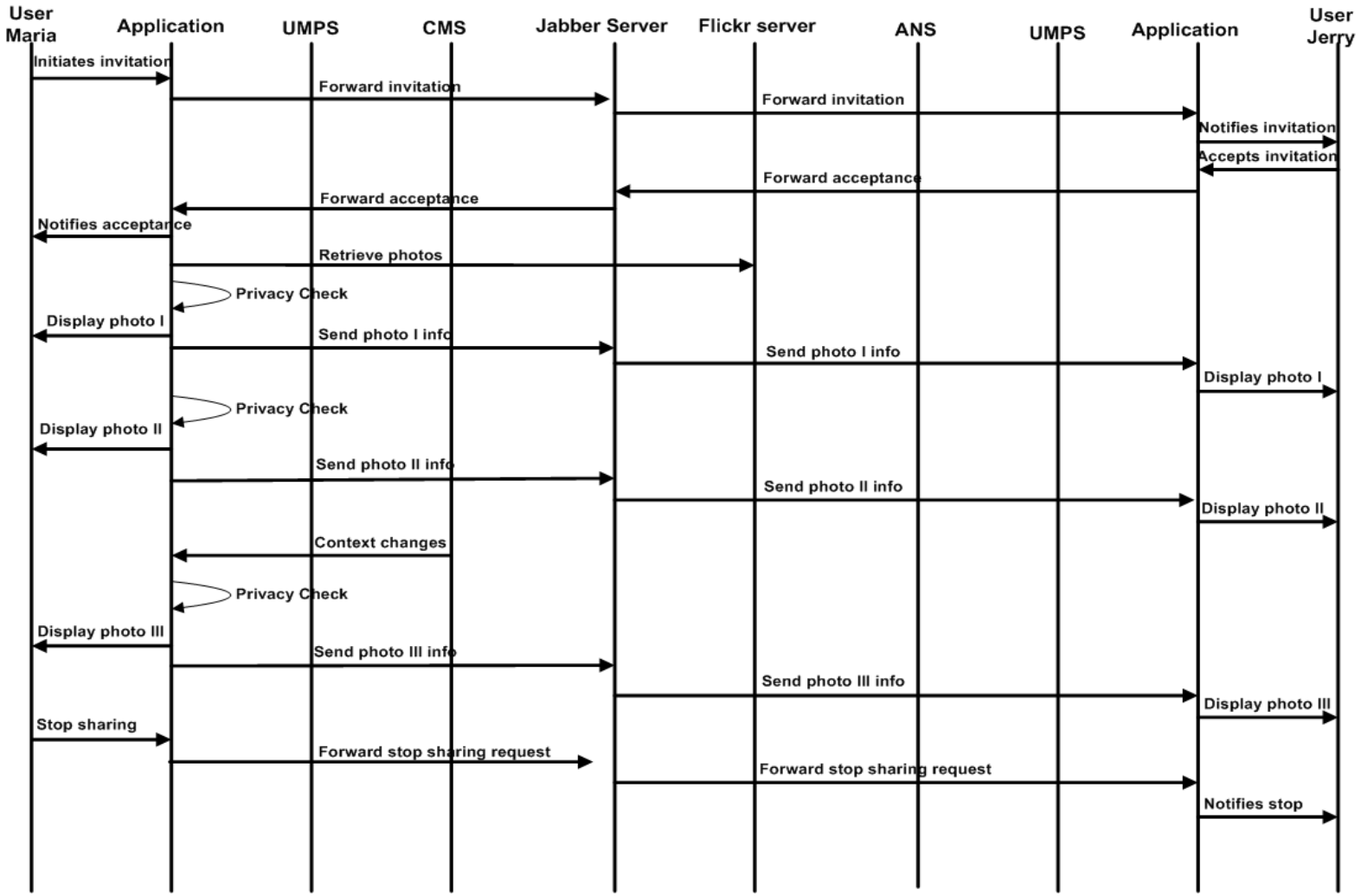

Figure C.2: Sequence diagram of photo sharing mechanism between two homes