Journal of Universal Computer Science, vol. 12, no. 3 (2006), 252-269
submitted: 30/10/05, accepted: 15/1/06, appeared: 28/3/06 © J.UCS

Quality of Privacy (QoP) for the Design of Ubiquitous Healthcare Applications

Mónica Tentori, Jesús Favela
(Department of Computer Science, CICESE, Ensenada, B.C. México
{mtentori, favela}@cicese.mx)

Victor M. González
(Department of Informatics, University of California at Irvine, USA
vmgyg@ics.uci.edu)

Abstract: Privacy is a complex social process that will persist in one form or another as a fundamental feature of the substrate into which ubiquitous computing (ubicomp) is threaded. Hospitals are natural candidates for the deployment of ubicomp technology while at the same time face significant privacy requirements. To better understand the privacy issues related to the use of ubicomp we place our efforts in understanding the contextual information relevant to privacy and how its interplay shapes the perception of privacy in a hospital. The results indicate that hospital workers tend to manage privacy by assessing the value of the services provided by a ubicomp application and the amount of privacy they are willing to concede. For ubicomp applications to better deal with this issue we introduce the concept of Quality of Privacy (QoP) which allows balancing this trade-off in a similar way as that of Quality of Service (QoS) does for networking applications. We propose an architecture that allows designers to identify different levels of QoP based on the user's context. Finally, we identify the main privacy risks of a location-aware application and we extend its architecture exemplifying the use of QoP to manage those risks.

Keywords: quality of Privacy, ubiquitous computing, privacy-aware computing, ubiquitous healthcare
Categories: K.4.1, H.5.2

1 Introduction

Ubiquitous computing will surround users with a comfortable and convenient information environment that merges physical and computational infrastructures into an integrated habitat [25]. Context-awareness will allow this habitat to take on the responsibility of serving users, by tailoring itself to their preferences as well as performing tasks and group activities according to the nature of the physical space. Thus, the more an application is aware of the user's context, the better it can adapt itself to assist him. Paradoxically, the more an application knows the user the greater the threat to his privacy [6]. Consequently, the use of ubiquitous computing brings some risks, being the potential invasion of privacy among the most important ones.

Because user's demands and expectation for privacy are context dependent, [5; 17], we decided to base our efforts on understanding the contextual variables that shape the perception of privacy in a particular setting: hospital work. Although previous studies have addressed the impact of privacy in ubicomp, hospitals are of

particular interest because they are appropriate settings for the deployment of this technology [3], while, at the same time, raising important issues related to privacy. Our work is framed within other efforts aiming to design and deploy ubicomp solutions supporting hospital work [7; 14]. These efforts are a step forward in the direction of providing accurate and timely information to hospital staff in support of adequate decision-making [7; 15]. Despite the benefits of ubicomp in healthcare envisioned by those applications and the fact that the importance of privacy has been highlighted, there have been fewer attempts to understand the privacy concerns of medical workers, how those concerns affect their practices, and how they are affected by the introduction of ubicomp technologies. The problem is that developers currently have little support in designing software and in creating interactions that are effective in helping end-users manage their privacy [8].

Despite this, design of ubiquitous systems for hospital settings have, in general, overlooked privacy issues, because of this, cases of users' distrust and abandonment of potentially useful ubiquitous applications in a hospital have been reported [21]. For instance, by being invisible, these technologies facilitate the collection and use of information about individuals without their knowledge. Thus, a cost, in the form of privacy, might need to be paid to benefit from ubicomp. The risks are high: even a few privacy violations could lead to user distrust and abandonment of ubicomp and to lost opportunities to use the technology to improve their activities [9].A clear example of users' distrust and abandonment of potentially useful ubiquitous applications in a hospital is the nurses' rejection to use of a location-estimation system in the medical center of Castro Valley, California [18].

Based on this, we want to explore the contextual variables that shape hospital workers' perception of privacy. The understanding of how people react to privacy threats will help us identify the contextual variables that influence end-user's privacy needs and propose mechanisms to adequately manage them by incorporating privacy concerns in the design of ubicomp.

The rest of the paper is organizes as follows: We first present in section 2 the results of a case study conducted to identify the contextual information which shapes hospital workers' perception of privacy, discussing how this perception in their everyday practices is affected with the introduction of ubicomp technologies. In Section 3, we present the use of Quality of Privacy and an architecture to manage QoP in ubicomp. Section 4 illustrates the use of our architecture by extending a location-aware application. In Section 5 we discuss previous research related to privacy in ubicomp, and how it compares to our work. Finally, Section 6 presents our conclusions and directions for future work.

2 A case study in hospital work

For a period of three months we conducted a workplace study at a public hospital. This study helped us assess some of the privacy issues hospital workers face on their everyday practice, how they deal with it, and the way it influences their decision making. In addition, a workshop evaluation helped us understand how hospital worker's perception of privacy changes by the foreseeing use of ubicomp technologies. Next, we briefly describe the results of the case study, more detailed information is described in [24].

2.1 Methodology

The study at the hospital started with a period of systematic observations where we shadowed three medical interns, two nurses, and two physicians throughout their morning, afternoon, and night shifts. Each person was observed for a period of three working days. Our observations in the hospital helped us identify specific instances where privacy was compromised, or decisions were made taking privacy issues into consideration. We used this information to generate two sets of scenarios, one based on current practices, and other where the use of ubicomp is considered We conducted ten interviews with five hospital workers and discussed typical scenarios of usage with them, to get a sense of whether they found the proposed ubicomp systems supporting their work and if the scenarios made apparent privacy concerns. As a result of those interviews we derived a new set of four ubicomp scenarios that were both useful for medical work but rose privacy concerns for hospital workers. Each scenario was defined to explore both, the benefit of the ubicomp application supporting medical work and its impact on the privacy of those using it.

We presented the four scenarios to 27 medical interns in a workshop evaluation. The participants were asked to situate themselves in a specific role within the scenario. After each scenario, they were asked to complete a survey with 7 Likert-scale assertions for each scenario, to evaluate the threats raised by the technology to their privacy. Finally, we applied these findings to identify the contextual information used to regulate and manage privacy using a ubicomp application.

2.2 Privacy management

From our observational data we identified a set of privacy concerns that emerged during the enactment of work of those individuals that we observed. These concerns center around the individuals themselves, the information they manage, and the people they interact with. In general, we noticed that the perception of the importance of each concern can be affected by the particular circumstances experienced by people. We observed that medical personnel often act with little concern for privacy in order to cope with specific circumstances or to facilitate their work. For instance, despite that the medical record is an official document that, according to the rules, cannot be removed from a particular area of the hospital; sometimes the medical interns move these documents to other areas to facilitate the study of a case. This situation is generally with the knowledge and even the encouragement of attending physicians as they see it as a way for interns to take full responsibility of a case and to help them improve their decision making.

2.3 Ubicomp scenarios that raise privacy concerns

With the results of the interviews, we defined four scenarios that integrate one or more of the ubicomp services that have been proposed in support for healthcare and other working environments. Table 1 indicates the different ubicomp services that were included in each of the four scenarios we selected.

SCENARIOS Ubicomp services	1	2	3	4
Displaying information from a personal device			√	
Monitoring people's location			√	√
Locating services			√	
Context-based notifications and reminders	√		√	√
Data transfer between heterogeneous devices		√		
Tracking people's movements				√
Audio/video capture of people's activities		√		√
Memory aid		√		
Identify people with similar needs/interests			√	

Table 1: Ubicomp services used in the grounded-scenarios

The first scenario illustrates how an intern requests laboratory studies and receives context-aware notifications of the availability of the results through a handheld. The second scenario shows how photographs of the intern's activities, taken while performing a surgical procedure, can help her as memory aid when she is interrupted by an emergency, and later on needs to resume the task. The third scenario shows how colleagues collaborate discussing a clinical case through heterogeneous devices. Finally, the fourth scenario illustrates how a supervisor can find out if a given procedure has been performed, by looking at where the intern was throughout the day and looking at pictures of him taken at different times during his shift. We next describe scenarios 3 and 4 to illustrate some of the technology proposed for, and privacy issues raised by, the scenarios.

2.3.1 Scenario 3: Physicians Collaborating through Heterogeneous Devices

While Dr. Garcia is evaluating the patient in bed 234, her PDA alerts her that a new message has arrived. Her handheld displays a hospital floor map indicating her that the X-ray results of patient in bed 225 are available. Before Dr. Garcia visits this patient, she approaches the nearest public display that detects the physician' s presence and provides her with a personalized view of the Hospital Information System. In particular, it shows a personalized calendar application and a floor map highlighting recent additions to clinical records of patients she is in charge of, messages addressed to her, and the services most relevant to her current work activities. While she is analyzing the information, she notices in the map, that Dr. Díaz, the traumatologist assigned to this patient, is walking down the corridor in the next floor. By selecting the icon representing Dr. Díaz she can invite him to join a collaborative session. Dr. Díaz receives a message indicating that the cardiologist would like to discuss a case with him and specifying the location of the nearest display available where he can visualize information related to the case. He accepts the invitation and moves to the nearest display. When the display recognizes his presence it shares the running applications like the floor map, the calendar, and the instant messenger with Dr. García. Dr. García display from his PDA information relevant to the case. Both doctors decide to record the discussion to store it for later

reference. They can now browse the patient's medical record and analyze the X-ray image to make the clinical decision. As Dr. Díaz is interested in analyzing the treatment more carefully, he decides to store the taped discussion in his PDA to consult it later.

This scenario has a few privacy implications since the physicians are aware of each other's location and availability, also, one of them is using a large display in a semi-public area with sensitive information, and the clinical discussion is being stored. On the other hand, the scenario illustrates how the technology can address the actual need for collaboration in clinical decision making.

2.3.2 Scenario 4: Medical Supervising through the Floor Map

Mrs. Diaz, a head nurse, wants to know if an intern made a clinical procedure to the patient in bed 222. She approaches a semi-public display where she selects the name of the intern in charge of the patient. Then a window showing a map of the area pops-up. The window includes a widget that represents a Timeline and can be used to scroll through time with the map in the window displaying the location of the intern (see Figure 1). The map shows that the intern entered room 239 and spent a few minutes there. Mrs. Diaz stops the Timeline to find the intern's activities in this room. The display shows the electronic medical record related to the patient in room 239 and photographs of the intern's activities taken at the time the procedure was made. Trough the timeline Mrs. Diaz notices that the intern entered the Internal Medicine office. Trough the photographs displayed, she realizes that the intern was chatting with Rita, another intern, until Dr. Perez arrives to the office; and then the three discuss a clinical case. Following the activities of the intern throughout the day she realizes that the procedure wasn't made, and assigns it to another intern.

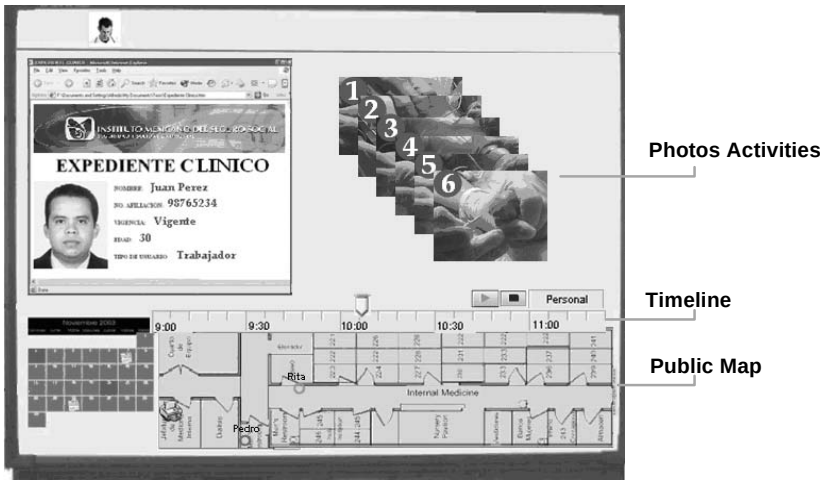

Figure 1: With the timeline tool a supervisor can follow the location and activities performed by medical interns

This scenario has serious privacy implications since the nurse (and potentially other supervisors) can track the location of the intern throughout the day, including

photos of the intern's activities. We included such scenario because it was considered useful by hospital staff' who actually supervise the interns' activities. A head nurse made the following comment during an interview when a preliminary version of the scenario was shown to her: *"I find this system really helpful because I can evaluate through the photos if my staff follows the norm, besides these photos could be used as study reference"*. In addition, although the people interviewed were not at first concerned of their colleagues being aware of their current location, they were not foreseeing the privacy risks raised by the capture of this information and its potential use to track their location for a period of time and infer their activities as illustrated in the scenario.

2.4 Contextual information

Two sets of contextual information were identified differing in the role they play in preserving privacy. The first set is defined as *contextual elements.* This refers to the parameters that the user wants to protect while using a ubicomp environment and they are perceived qualitatively. These parameters can be regulated at different levels by the technology satisfying the need for privacy as perceived by the user. On the other hand, we identified the *contextual variables* that prompt the user to protect his privacy while using a ubicomp application. We define the *contextual variables* as triggers that will condition the need for privacy using a ubicomp application. The interplay of those elements will ensure a certain level of privacy perceived by the user and regulated by the technology.

In accordance with previous studies [14], location, identity, and time are important factors in assessing privacy concerns. Similar results were obtained in our own study. For example, related to the location, a medical intern made the following comment during an interview: "*… when you have time off you might also have pending tasks, and if you're in the break room or in the dinning room I'll would be concerned if my location is being shared; because this information could be used to get a sense of the amount of work that I've done, or I haven't because I was in my lunch break"*. In this case, for instance, if a medical intern is in the bathroom or the dinning room, he wouldn't want to be disturbed or he might not want others to know how much time they spent in this particular location. In addition, when they're in these places, they in general, wouldn't require access to a patient's medical records. In this case, they would rather have the system know only their general location, for instance the fact that they are in a given floor, or within the hospital. In addition to these variables, we found activity, access, and persistence as being highly relevant context when assessing privacy risks.

Based on our findings we propose that a ubicomp application should take into account contextual information to adapt its behavior in order to preserve end-user privacy. Our aim with this is to help designers and users support a spectrum of trust levels and privacy needs in order to create privacy aware applications for ubicomp.

3 Privacy Aware Computing

There is a trade-off between the amount of privacy a user is willing to concede and the value of the services that can be provided by a ubiquitous application. For

instance, if a physician doesn't want to be easily located she can login into the hospital information system sharing only her role as a physician, and not her identity. In this case, she might not be able to access the records of her patients, but still be able to access services such as the hospital's digital library. Similarly, users should be able to control the precision with which their location is made available to others, based on contextual variables such as the identity of the receiver. For instance, a physician can choose to share his detailed location with fellow doctors, but other staff, medical interns, for instance, will only know if he is in the same floor or in the hospital. In the above examples, the physician requests the level of privacy he expects when joining the ubiquitous environment and based on contextual information the environment adapts in order to preserve privacy. To define and manage, at the users and system level, the amount of privacy one is willing to concede, we introduce the concept of Quality of Privacy (QoP). This comes from an analogy with that of Quality of Service (QoS), well known in computer networks [12].

3.1 Quality of Privacy (QoP)

Quality of Service (QoS) is a broad term used to describe the overall experience a user or application will receive over a network [13]. For example, suppose that two physicians are discussing an X-ray image of a patient trough video conferencing. In this case, the network has to provide high quality video showing both the X-ray image and the video of the physicians. If network congestion is experienced the quality of the services might be degraded. In that case the network would implement a QoS setting that for instance, would reduce the quality of the video but will preserve the X-ray image quality as much as possible. Quality of Service is implemented by allowing the user to demand a specific performance from the network in order to reserve resources for certain services. In the example, the physicians might want to preserve the quality of the X-ray image over that of the video, so the users can demand certain QoS to the application. In this case the users' needs are expressed qualitatively, based on their perception (i.e. high, medium or low quality). For instance, in case of congestion they might specific a QoS that set a low quality of the video. On the other hand, the network uses parameters that are expressed quantitatively, such as bandwidth or jitter.

A similar trade-off is presented between the services offered by a ubiquitous environment and the cost that the users' might need to pay in regard to privacy. Similarly, privacy can be considered at two levels: the qualitative perception of the user and the quantitative parameters managed by the technology. To cope with this we introduce the concept of Quality of Privacy (QoP) following the analogy with QoS. We characterize the level of QoP based on five contextual elements which we discussed in Section 2. Based on this, a user can demand a certain level of QoP to the ubiquitous environment using a qualitative measure (i.e., logging into the system as an anonymous user). On the one hand, the perception of anonymity will be mapped by the system to certain values of one or more contextual elements. In this case, the ubiquitous application must adapt its behavior considering the user's context in order to satisfy the level of QoP, that both, the application and the user have agreed upon. The level of QoP demanded from the user will depend on contextual variables and the degree of privacy desired while using the ubiquitous application. On the other hand, the information that the user is willing to share with the system determines the

services the environment is willing to provide her. Consequently, to represent different levels of QoP and manage user and technology views of QoP we designed an ontology in which the values associated to each contextual element will depend on the application's logic and the nature of the ubiquitous environment.

3.2 An ontology to manage QoP

The ontology allows us to balance the privacy trade-off enforcing privacy conditions demanded by users and enforced by the ubicomp environment. This ontology uses the Event-Condition-Action (ECA) model [14]. We use XML to express privacy configurations based on this ontology. The ontology we designed includes three components: (1) an *event* describing the need to execute an action, and it is characterized by the five contextual variables: location, identity, time, activity and artifacts, which change dynamically while the user's context varies; (2) a *condition* defining rules that must be enforced to determine which action might need to be executed and; (3) an *action* containing a set of functions that may be executed to enforce or relax privacy policies. In this case the actions might be executed *interactively,* when a user explicitly executes an action; or *passively*, when the environment reacts based the user's context.

Table 2 shows an example of an ontology used to regulate QoP. It shows, how the level of detail of the information shared decreases as the QoP increases. This example shows the values corresponding to the design of a context-aware hospital application. Similarly, a context-aware tour guide won't need to define the identity by roles or the location by rooms, In this case it might be better to use age groups for the identity and geographic position for location.

Location	Identity	Access	Activity	Persistance
X, Y position	Name	Free	Available	Indefinite
Room	Role	With confirmation	Busy	Months
Floor	Anonymous	Denied	Unavailable	Days

Table 2: Contextual elements to regulate privacy using a certain level of QoP

3.3 An architecture for privacy-aware computing

Privacy mechanisms must be triggered when the information is captured [11], as well as when the information is being requested [16]. This has suggested us to regulate privacy both in the side of the user (client) as well as in that of the environment (server). Figure 2 shows our proposed agent-based architecture for privacy-aware computing, that extends the SALSA agent-based framework reported in [22].

In this architecture, a broker handles the communication between all services using an extension of the agent communication language, itself based on the Extensible Messaging and Presence Protocol XMPP which incorporates the ECA model to preserve users' privacy. This protocol includes privacy related information based on the ontology presented above, in order to manage QoP provisions. A Context-aware filter running on the client (c-filter) allows the user to set his preferred level of QoP. In this case, when the user joins the ubicomp environment, or the user's context changes, the desired level of QoP is negotiated between the user and the

broker. Similarly, when an application requires information about the user, a context-aware filter in the server (s-filter) negotiates the QoP set by the user and shares this information with the client's applications maintaining the QoP set by the user.

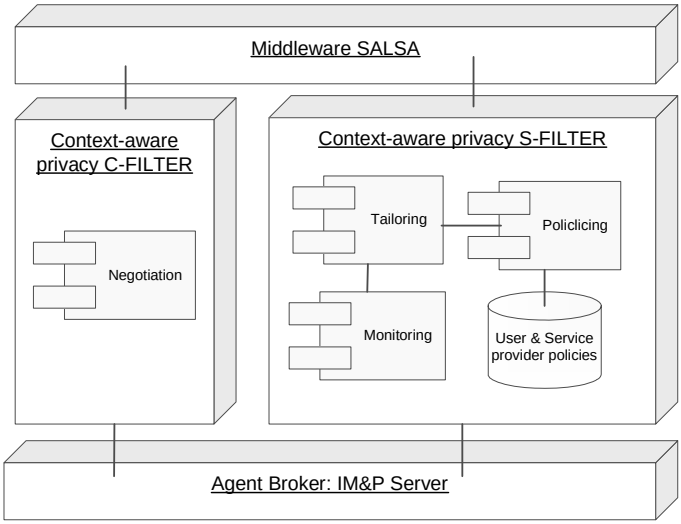

Figure 2: An architecture for privacy-aware computing

3.3.1 Broker

An *Agent Broker* handles communication between agents, which represent users, services and devices. Information is communicated through XML messages. To implement this service we have used the Jabber open-source instant messaging server (www.jabber.org) and extended its Extensible Messaging and Presence Protocol XMPP. This server also stores the state of people and agents and notifies their changes to other agents subscribed to them.

3.3.2 Context-aware privacy c-filter

This agent controls the information shared by the user with the ubicomp environment acting as a filter between the user and the broker. It uses a module *negotiation* which allows reaching an agreed level of QoP between the user and the ubicomp environment. For example, if a user decides to join the ubicomp environment with certain level of QoP this filter adapts the user's information to be shared with the broker. In addition, after the negotiation, this agent must inform the result of the contract to the broker.

3.3.3 Context-aware privacy s-filter

This agent controls the information shared by the broker and the other agents who represent users, services and devices, respecting the level of QoP demanded by the user and the policies specified by the agents. Each time an agent requires information of the users connected to the system, this filter evaluates the need of privacy and

based on this evaluation decides to admit or reject the request. If the request is accepted users' policies must be applied adapting the users' information. Four modules compose this agent. The *monitoring* module monitors the contextual elements to determine the level of QoP desired at a certain moment. After some conditions are met the *policing* module ensures that all parties adhere to the level of QoP. Through the *user and services repository* the policing module obtains the policies specified by the user and compares then with the requested information. After that, the users' information used by the ubiquitous environment is updated in the *access behavior repository*. Finally, the *tailoring* module adapts the information in order to preserve the level of QoP demanded.

3.3.4 A protocol to deal with privacy

The SALSA development framework provides an expressive language that enables the exchange of different kinds of objects between agents (such as actions, perceived information, or simple messages), between agents and users (such as the user's profile and events generated by the user's actions), and between agents and services (such as the service's state). These objects are encoded using XML (eXtensible Markup Language). Thus, SALSA provides developers an API that facilitates the composition, sending, and receiving of messages between agents. We extend this protocol with mechanisms that allow programmers to specify the ontology to manage privacy depending on the nature of the application. For instance, the method sendXMLcommand(xmlContent, agentID) is used by an agent to request another agent to execute a specific action. When it is invoked, the method will form an XML message by adding the tags that specify the kind of message and to whom it is addressed as illustrated in Figure 3.

```
<message to='map-a@server_jabber' from='pd-a@server_jabber'
id='acl_message'>
    <x xmlns='x: acl_message'>
       <command>
           <content>
              <event>
                 <location></location>
                 <time><time>
                 <activity></activity>
                 <state></state>
              </event>
              <condition>
                  <QoP></QoP>
              </condition>
              <action>
                   <adaptation userID=garcia@server_jabb/>
              </action>
           </content>
       </command>
     </x>
</message>
```

Contextual variables to be met in order to preserve privacy

Contract agreed by the application and the user

Method to be executed by the agent

Figure 3: XML message sent by the privacy s-filter agent to a user agent, requesting the adaptation of the information preserving a desire QoP

The message incorporates the event/condition/action paradigm to preserve users' privacy. Then, it will add the content of the message which is contained in xmlContent. This variable specifies the action or method to be executed by the agentID.

4 The Location-aware Migration Component

To illustrate how the proposed architecture can be used in the design of privacy-aware applications we re-designed a location-aware migration component reported in [2]. This component allows users to seamlessly transfer information to any device in the vicinity, such as a PDA, a PC or a public display, from a handheld computer. To provide this functionality we designed and implemented a migration component that allows the transfer of information between diverse heterogeneous devices. The information to be transferred includes digital files and URLs, while the source and target devices could include PDAs, PCs and public displays. The command is activated from the file system by using a selection in the option menu that is visualized with the right-click. In the PDA the user needs to hold the stylus for a few seconds over the file he wants to transfer, for the option to appear. In figure 4, we can observe the result of such action. The file transfer component can also be triggered from another application that whishes to invoke this service. For instance, URL's can be transferred by directly clicking on the URL in the Web browser and selecting the device to which the information will be transferred.

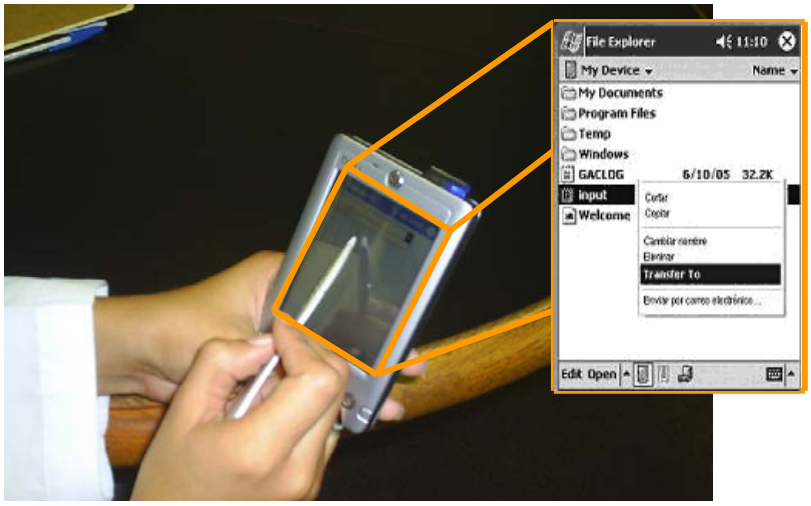

Figure 4: Screen that illustrates the selection of the file to be transfer from the PDA

Once the options menu appears, the user needs to select the *Transfer To…* option. When selecting this option, the list of devices present in the vicinity is displayed. These are the possible target devices to which the information can be transferred. The information migration takes place when the user chooses the target device. Once the

information has been transferred, a notification is sent to the source device and the file is opened by an application in the target device, according to its filetype.

Privacy is an important issue in the use of large public displays [23]. For this reason we placed special emphasis on protecting the users' privacy by allowing the control of the information and providing feedback about how it's used [5]. Within the context of this application, we identified that the persistence of the information, the identity of the sender and how the information is displayed must be managed to protect privacy. For example, during a meeting, a user might need to transfer a document from his PDA to a public display. In this case, he would like to share the information with the participants until the meeting ends and he might not want to automatically display the information for privacy concerns. For this, when a user transfers information to a public display he will expect the system to erase his information once the meeting is finished. In our approach, the system allows the users to specify privacy policies to manage the persistence of the information shared and how the information will be displayed. In addition of these policies, the system provides feedback informing the privileges that a particular file/url has. For instance, the privacy bar can show how much time the file can be displayed or stored. In both cases, the user could be able to change their policies based on his needs.

Also, because presence is privacy-sensitive information, the protocol for presence information must be able to protect the data from possible threats, such as eavesdropping, corruption, tamper and replay attacks. To protect the communication confidentiality we used the methods proposed in [20], which enable the sender to sign and/or encrypt an instant message sent to a specific recipient, sign and/or encrypt presence information that is directed to a specific user, and sign and/or encrypt any arbitrary message directed to a specific user. To achieve this, our clients must manage Stanza Security ensuring confidentiality and integrity of transmitted XMPP stanzas between endpoints according to [10]. To do this, a payload XML structure is created, which contains the full stanza to be secured, into OpenPGP [19] format. An example of a paylod signed presence stanza is illustrated in Figure 5.

```
<presence to='map-a@server_jabber' from='pd-a@server_jabber'>
  <status>Online</status>
  <x xmlns='x:QoP' QoP='id'/>
  <x xmlns='jabber:x:signed'>
     QA/AwUBOjU5dnol3d88qZ77EQI2JACfRngLJ045brNnaCX78ykKNUZaTIoA
     oPHI2uJxPMGR73EBIvEpcv0LRSy+=45f8
  </x>
</presence>
```

Figure 5: A signed presence stanza

Figure 6 shows the elements of the migration component, which include the source device, the target device, the resource to be sent and, the component that carries out the transfer of the information and, if required, adapts the information based on the nature of the target device. The component is implemented with four agents. The *Source Proxy agent* represents the information to be transferred by the user to another device. Besides, it includes the mechanisms required to transfer the information, as well as the permissions granted by the source device to the

information being sent. The *Information Adaptation agent* adjusts the information based on the characteristics of the target device and the specifications defined by the source device. In this case, for instance, medical images being moved to a PDA might be reduced in size before being transferred. Finally, the *Target Proxy agent* represents: characteristics (capabilities, type of applications, etc.) of the device that receives the information; the device itself which will decide whether to accept or reject the transfer request; and the actions to be performed with the information received, which could include, storing or opening the file with a specific application.

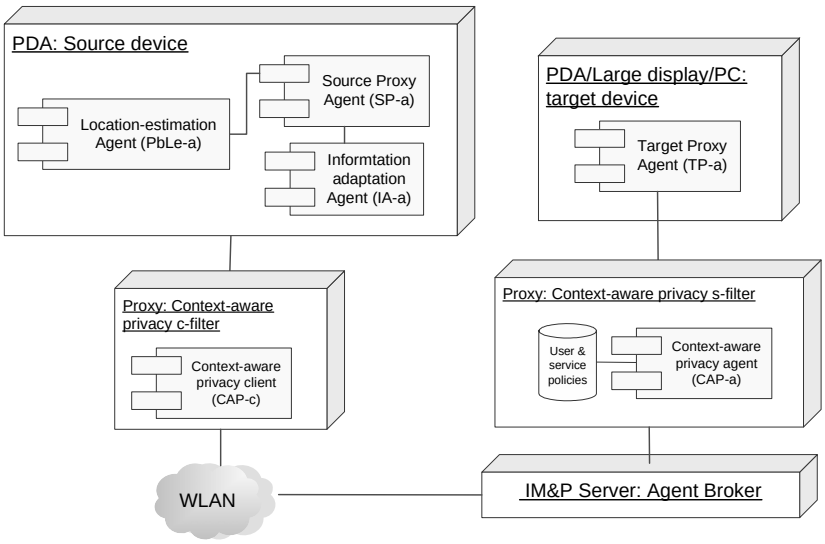

Figure 6: Architecture of the location-aware migration component preserving the user's privacy conditions

In order to preserve privacy we add a layer between the broker and the migration component. The additions to the architecture are included in two proxies' nodes which represent the filters in the server and client side discussed in Section 3. Each one includes one new agent component that communicates with each other and with other components through the Agent Broker. This has allowed for a seamless integration of the new components, since only minor modifications were required to other components. The *context-aware privacy c-client* acts as a proxy between the user and the ubicomp environment. It incorporates an interface to adequately manage the negotiation of privacy. And the *context-aware privacy s-agent* acts as a proxy between users and agents in the environment and the broker. All information requests for a service in the ubicomp environment go trough this agent, which monitors the environment to determine whether conditions are such that the system must adapt its behavior in order to preserve privacy. It makes use of a users and provider policies repository to maintain the privacy configuration specified by the users or services.

4.1 Sample application

Figure 7 illustrates how the system's components interact to support the following scenario.

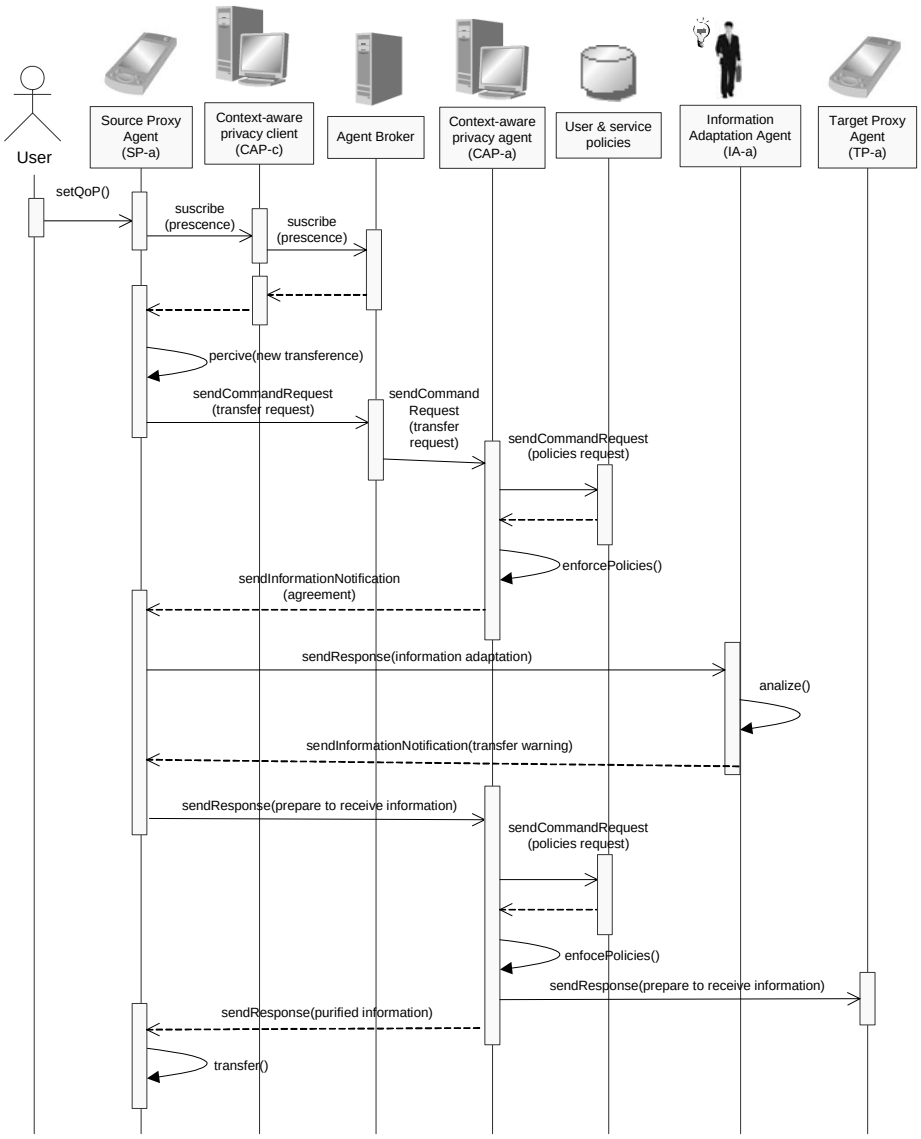

Figure 7: The sequence diagram illustrates the negotiation of QoP to use a service provided by the ubicomp application

Everyday, at the internal medicine office, the medical interns meet with the attending physician to discuss the status of their patients. They help each other by

discussing the diagnosis as well as future treatments for the patients. The physicians decide to discuss the case of the patient in bed 226 who is not responding to treatment as expected. They present on the public display the information related to the patient, such as X-Ray results and the medical record.

During the meeting the physicians might want to share articles, working papers, presentations and different kind of documents relevant to the discussion. In this case, the physicians might need to protect the privacy of the information shared by controlling the persistence and the way in which it is displayed. While the physicians discuss the case of the patient in bed 226, Dr. Garcia, the attending physician, wants to display a recent article he considers relevant to the current discussion. Using the migration component, Dr. García selects the article that he wants to share with the group but he wants to keep it public only during the meeting and he doesn't want to involuntarily display the article. In this case, he chooses a certain level of QoP specifying the time of persistence and the display mode. The context-aware privacy c-filter receives this information and adapts the information of the user based on the privacy ontology for the system. This agent sends the user's presence to the broker specifying the contract between the ubicomp environment and the user as a certain level of QoP. The agent broker notifies to all the devices in the vicinity and those that agree with such conditions are displayed on Dr. Garcia' PDA. By selecting the icon that represents the public display, Dr. Garcia decides to transfer the article from his PDA to the public display. The context-aware privacy s-filter compares Dr. Garcia' QoP with the policies announced by the agents that represent the devices in the vicinity. In this case, the public display accepts the QoP demanded by the user and doesn't display automatically the article.

5 Related work discussion

Privacy has been identified as an important issue in the ubicomp literature. Most of the work in this area has focused on field studies aimed at better understanding the privacy issues faced by ubicomp users, and providing frameworks and design proposals to address the risks of privacy raised by ubicomp technologies.

Adams [1], conducted an empirical investigation into the individual's perception of privacy in environments outfitted with audio/video capture equipment. She found that the subjects' perceptions of privacy in these environments depend on the interrelation of the identity, the information receiver and the use given to that information, as well as its sensitivity. In addition to these variables, we found the content of the information, the location of its storage, and its persistence as being highly relevant. On the other hand, information privacy is not the only issue which needs to be protected; we found that the activity of the information's owner is also significant. Thus, privacy can be managed if we attend to the context in which the entities interact, and in particular pay attention to the contextual variables found to be of major concern to the users.

The Principle of Minimum Asymmetry introduced by Jiang *et al.* seeks to minimize the imbalance between the people about whom information is being collected, and the systems and people that collect and use that information [9]. In our study we obtained evidence of this asymmetry in the hospital setting and that this

asymmetry is more evident in hierarchical relations, as the one between medical interns and their supervisors.

Beckwith [4] reports on an ethnographic study he conducted in an eldercare facility with a sensor-rich environment that monitors the locations and activities of residents and staff. A key finding was that different stakeholders can have drastically different perceptions of the invasiveness of a technology, its potential for abuse, and even its purpose. In this case the design of the system must be flexible enough to support different perceptions. Even though that study was made in a hospital environment it was not focused on the practices of hospital workers'; in addition, it only evaluated the perception on privacy related to the ubicomp services available in the specific environment where the study took place. Our study explores different services proposed in ubicomp and deals with how hospital workers' perception of privacy during their everyday practices changes with the introduction of ubicomp technologies in such environment.

The privacy awareness system (pawS) for ubiquitous computing environments allows data collectors to both announce and implement data usage policies, as well as providing data subjects with technical means to keep track of their personal information as it is stored, used, and possibly removed from the system [12]. The limitation of the pawS' approach is that the privacy protection is only managed when the capturing is taking place, once the information is shared with the system the user's only can track its use. Meanwhile, Myles *et. al.* [16] developed a system that gives users fine-grained control over the release of their location information. This system protects the information shared, once an application has requested it. In this case validators determine whether the information requested can be released and, if so, whether it should impose any special constraints (such as reducing the accuracy of the location's data). In this case the information is protected once it is in the system, so, in contrast with pawS information which a user's hasn't agreed to share is stored and managed. In our design we consider both issues, by adding filters in both sides in which the information is managed (on the client as well on the server). Thus, we guarantee that the user shares the minimum of information necessary, as well as how it is shared.

6 Conclusions

In this paper, we propose mechanisms to deal with privacy in ubiquitous computing environments. Our efforts include a workplace study conducted in a hospital to identify the contextual variables and its role in privacy management. Based on how hospital workers use context to shape their privacy, we inform how an adequate management of contextual information will allow designers to deal with privacy concerns in the design of ubicomp. To cope with this, we introduce the concept of Quality of Privacy (QoP) which can be used to develop privacy-aware computing systems that balance the trade-off between the amount of privacy a user is willing to concede and the value of the services that can be provided by the application, in a similar fashion as Quality of Service (QoS) does in computer networking. We describe an architecture that considers the users' context to satisfy the level of QoP that both, the application and the user have agreed upon. We exemplified our proposal extending a location-aware migration component which presented several privacy

risks that were addressed during its re-design. We plan to analyze the privacy implication in several ubicomp services and apply the concept of QoP to cope with the risks identified. Furthermore, we want to improve our proposals to help designers reduce the privacy trade-off. Finally, we plan to deploy a privacy application at hospital to explore the implications of using privacy-aware tools in everyday work.

Acknowledments

We thank the personnel at IMSS General Hospital, in particular Simitrio Rojas and Julia Mora and to Professor Marcela Rodriguez who provided helpful comments on this work. This work was funded by UCMEXUS under contracts Conacyt-CN-02-60 and Conacyt-U- 40799, and through scholarships provided to Victor M. González, and Mónica Tentori.

References

[1] Adams, A. 2000. "Multimedia Information Changes the Whole Privacy Ballgame". *In Proc. of the Computer, Fredom and Privacy*. Toronto, Ontario Abril 4-7, 2000 ACM Press. pp.1-8.

[2] Amaya, I., J. Favela, and M. Rodriguez. 2005. "Componentes de software para el desarrollo de ambientes de cómputo ubicuo". *In Proc. of the Ubiquitous Computing and Ambient Intelligence*. Granada, Spain September, 14-16 Editorial Thompson. pp. 173-180.

[3] Bardram, J. 2004. "Applications of ContextAware Computing in Hospital Work - Examples and Design Principles". *In Proc. of the ACM Symp. on Applied Computing*. Nicosia, Cyprus March, 14-17 ACM Press. pp. 1574-1579.

[4] Beckwith, R. 2004 "Designing for Ubiquity: The Perception of Privacy." *IEEE Pervasive*. 2(2): 40-46.

[5] Bellotti, V. and A. Sellen. 1993. "Design for Privacy in Ubiquitous Computing Environments". *In Proc. of the European Conference of Computer Supported Cooperative Work*. Milan, Italy September, 13-17 Kluwer Academic Publishers. pp. 77-92.

[6] Brown, P.J. and J.F. Gareth. *Context-awareness and privacy: an inevitable clash?*, in *Department of Computer Science*. 2004, University of Exeter: Exter, United Kingdom, pp. 20.

[7] Collins, J. 2004 "RFID Cabinet Manages Medicine". *RFID Journal.* 1081(1): 10-22.

[8] Hong, J.I. and J.A. Landay. 2004. "An Architecture for Privacy-Sensitive Ubiquitous Computing". In *Proc. of the Mobile Systems, Applications and Services*. Boston, Massachusetts Junio 6-9, 2004 ACM SIGCHI. pp. 177 - 189.

[9] Jiang, X. and J.A. Landay. 2004 "Modeling Privacy Control in Context-Aware Systems". *In IEEE Pervasing Computing*. 1(3): 59-63

[10] Karneges, J. *JEP-01xx: Stanza Security*. 1999.

[11] Langheinrich, M. 2001. "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems". *In Proc. of the Ubicomp*. Atlanta, GA September,30 - October, 2 Springer-Verlag LNCS. pp. 273-291.

[12] Langheinrich, M. 2002. "A Privacy Awareness System for Ubiquitous Computing Environments". *In Proc. of the Ubicomp*. Göteborg, Sweden Septiembre 29 a Octubre 1, 2002 Springer-Verlag LNCS. p. 8.

[13] Lawrence, T.F. 1999 "Quality of Service (QoS) A Model for Information". *IEEE Fourth International Workshop on Object-Oriented Real-Time Dependable Systems*. 4(6): 180-183.

[14] Lederer, S., J. Mankoff, and A.K. Dey. 2003. "Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing". *In Proc. of the Conference on Human Factors in Computing Systems*. Fourt Lauderdale, Florida Abril 5-10, 2003 ACM SIGCHI. pp. 724-725.

[15] Munoz, M.A., M. Rodriguez, J. Favela, A.I. Martinez-Garcia, and V.M. Gonzalez. 2003 "Context-Aware Mobile Communication in Hospitals." *IEEE Computer*. 36(8): 38-46.

[16] Myles, G., A. Friday, and N. Davies. 2003 "Preserving Privacy in Environments with Location-Based Applications". *IEEE Pervasive computer*. 2(1): 56-64.

[17] Palen, L. and P. Dourish. 2003. "Unpacking 'privacy' for a networked world." *In Proc. of the Conference on Human Factors in Computing Systems*. Vienna, Austria April, 24-29. ACM SIGCHI. 129-136.

[18] Reang, P. 2002. "Dozens of nurses in Castro Valley balk at wearing locators". *In Proc. of the The Mercury News*. San Jose, CA September, 6. p. 4-4.

[19] RFC2440. *OpenPGP Message Format*. 1998. Available at: http://www.faqs.org/rfcs/rfc2440.html

[20] RFC3923. *End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol(XMPP)*. 2004. Available at: http://www.xmpp.org/specs/rfc3923.html

[21] Rice, K. 2002 "Nurse Tracking Systems: Do the Benefits to Nurse Managers Outweigh Risks to Nurses' Privacy?: Writing for the CON Position." *MCN, American Journal of Maternal Child Nursing*. 27(2): 73 - 73.

[22] Rodriguez, M., J. Favela, A. Preciado, and A. Vizcaino. 2005 "Agent-based Ambient Intelligence for Healthcare". *AI Communications*. 18(3): 10-16.

[23] Tan, D.S. and M. Czerwinski. 2003. "Information Voyeurism: Social Impact of Physically Large Displays on Information Privacy". *In Proc. of the Conference on Human Factors in Computing Systems*. Lauderdale, Florida April, 5-10 ACM SIGCHI. 748-749.

[24] Tentori, M., J. Favela, and V. González. 2005. "Designing for Privacy in Ubiquitous Computing Environments." In *Proc. of the Ubiquitous Computing and Ambient Intelligence*. Granada, Spain September, 14-16 Editorial Thompson. pp. 27-35.

[25] Weiser, M. 1998 "The future of ubiquitous computing on campus". *Communications of the ACM*. 1: 41-42.