2004

A Fuzzy Logic Based Approach to Support Users Self Control of Their Private Contextual Data Retrieval

Amr Ali Eldin
Delft University of Technology, amre@tbm.tudelft.nl

Rene Wagenaar
Delft University of Technology, renew@tbm.tudelft.nl

A FUZZY LOGIC BASED APPROACH TO SUPPORT USERS SELF-CONTROL OF THEIR PRIVATE CONTEXTUAL DATA RETRIEVAL

Eldin, Amr Ali[1], Jaffalan 5, Postbus 5015, 2600 GA, Delft. Delft University of Technology, The Netherlands. amre@tbm.tudelft.nl

Wagenaar, René, Jaffalan 5, Postbus 5015, 2600 GA, Delft. Delft University of Technology, The Netherlands. renew@tbm.tudelft.nl

Abstract

In context aware applications such as location based, m-health care, and m-business applications, it is expected that a huge amount of users context information will be collected, which threatens their privacy concerns. Users consent is a mandatory requirement of users privacy support. Increasingly, it seems clear that user consent decision implies the consideration of a number of factors. These factors vary in their impact on the user consent from one situation to another and from a user to another. In this paper, we propose a consent provider model that considers a number of factors influencing users consent, modeling their impact and evaluating their roles in the consent decision process based on fuzzy logic reasoning. Increasingly, we define a new data set called "contextual privacy attributes" which is associated with each user contextual data, and corresponds to influencing factors. We have prototyped the proposed consent provider model and integrated it into the real time UMTS mobile information and entertainment services (MIES) platform hosted at the university campus.

Keywords: Context aware information systems, privacy, information sharing, users consent, fuzzy logic.

[1] On leave from El-Mansoura University, El-Mansoura, Egypt.

1 INTRODUCTION[2]

One of the privacy requirements set by the European directive (2002) is to support users explicit consent for collecting their personal information. In a dynamically changing environment such as the mobile communications environment where users sensitive information can continuously be collected, we believe that users consent would always be of a dynamic nature and therefore should always be requested before any collection of contextual information. We assume that a dynamic consent decision will also need dynamic users preferences. In context aware environment, a user would have changing requirements in his/her privacy according to the changing situations and the impact of contextual information on him/her. Increasingly, this request for users consent should be carried out in an autonomous, flexible and user-friendly way. In P3P enabled systems, it is supposed that the user would configure his/her preferences and conditions of dealing with his/her personal information. Then the information practices of the incoming request would be compared to the stored preferences in order to get the users consent (P3P 2002). APPLE rules (2002) assumes three types of users consent: request, limited and block. The first one indicates that the user totally agrees to submit all the information needed by that information collector. While the second one prevents the information collector from getting identification information of the user such as device ID, the last type blocks any information transmission between the user and the information collector. Assuming that identification information represents the only required information not to be transmitted when an evaluation leads to doubts on the information collector trustworthiness adds more strictness to a flexible privacy solution. As a matter of fact, not only identification information represents private information, but other types of information could be private as well. Such as information that can lead to deduction of other private information, in particular information related to national security issues. APPEL (2002) rules, based on which users consent is developed, depend only on the information collector privacy policy and user preferences (Cranor 2002). The user has to manually choose among different preferences profiles or customary inserting his/her preferences. We enunciate that a user should be able to specify which confidentiality degree should be assigned to which information item so that a flexible evaluation could take place. However, when a user manually decides to share his/her contextual data based on matching results, he/she does some mental calculations before clicking the continue button or the cancel button. So, it can be deduced that the matching results represent only one, and not all of the factors that are needed for the user to make a consent decision. Two issues remain challenging yet: what are the factors affecting users consent decisions and how to effectively model the effect of these factors in the user consent decision process?

We assume that a flexible privacy approach should be a user centric one because users are the only ones capable of setting their own privacy preferences and also due to the changing demands of their privacy. However, we also assume that not all users know exactly what they need. Increasingly, most users will prefer more a user-friendly way, which reduces their interactions as much as possible and at the same time, satisfies their personal information privacy requirements. In (Ali Eldin & Wagenaar 2003), a number of functional components were proposed that could achieve user consent as one of the requirements of privacy supportive systems, discussed in (Ackerman 2001, Casal 2001 & Langheinrich 2001). The aim of this research is to develop a consent decision-making mechanism that fulfils the dynamic consent requirement by adopting dynamic user profiles with effective privacy preferences descriptions and intelligent decision-making. In this paper, we develop a user oriented approach that lets users have control capabilities of their contextual information and proposes a consent provider model that helps the users taking consent decisions based on a fuzzy reasoning engine. The paper has been structured as follows. Section 2 reviews some of the previous efforts in solving privacy issues. In

[2] This research is part of a larger program Uexperience, that is funded by the Ministery of Economic Affairs in cooperation with industry partners

section 3, we discuss the proposed consent decision-making approach. In section 4, we present the prototyping details, followed with the prototypes findings and Section 5 concludes the paper.

2 PRIVACY SUPPORT RELATED EFFORTS

There has been an intensive concern about privacy threats and ways of protecting users privacy in the literature. Although privacy-enhancing technologies (PET) are believed to help reducing privacy threats, they are still not effectively implemented (Huizenga et al. 2002). It can be seen that privacy threats arise from the linkage between users identity and their private information. Simply, it can be seen that breaking this link helps protecting users privacy. This could be achieved by either protecting users identities, by deterring identity capturing, or controlling private information perception. Most literature has given more concern for the first option of supporting users privacy. This approach assumes non-trustful information collectors and hence tries to either remove users identities as in most anonymous solutions (Chaum 1985, Camenisch & Herreweghen 2002) or to send virtual identities instead, known as pseudonyms (Lysynaskaya et al 1999). However, anonymization and pseudonimization cannot completely ensure privacy protection due to possibilities of leakage of some information that can be collected in subtle ways using traffic analyzers and therefore leading to identification of information sources (Rao & Rohatgi 2000). In addition, linking pseudonyms for different information collectors can lead to original identities inference (Hauser, & Kabatnik 2001, Hauser 2002).

The second option of supporting users privacy by controlling private information collection has been investigated via different ways. Controlling access to users information objects represents one of these ways. Another way is to reduce context information accuracy. However, this approach has its limitation on services that users can receive. A third way to control private information can be achieved by *data randomisation* before it is submitted and then collecting it back at the target. For instance, a hash function can be used to generate new random values of users attributes, and then those new values are stored instead of the original values. At the receiving party, original data can be deduced by applying a reverse hash function. However, when using this type of randomization of sensitive data, there is always a lack of accuracy because of hash collisions. Another approach of randomisation can be achieved while data is stored in databases by *database randomly partitioning* into unlinked encrypted partitions located on different sites that cannot release data separately, such that data is useless unless collected together at one server and decrypted via its owner (Clifton et al., 2002). *Hippocratic databases* have been introduced to support data encryption transmission and water marking (Agrawal & Kiernan 2002, Agrawal et al. 2002). However, the high complexity of such algorithms remains a main challenge to restricted computation devices such as mobile terminals (Lamparter & Westhoff, 2002). Physical security is also an option where access to private information can be restricted according to some physical locations (Langheinrich, 2001).

Rodden et al (2002) propose a minimal asymmetry approach to control personal location information. A trusted party keeps location information structured in such a way that other parties cannot have full access privileges until they have reached a service agreement. Moreover, user identities are replaced with pseudonyms when other parties collect the location information. It might be seen that the applicability of this approach is limited due to the intensive involvement of users in getting their pseudonyms and in giving their consent to information collectors. Further, privacy policies of information collectors, which are required in order to know how the information collectors will deal with users personal information, are not included in the users consent decision.

The Platform for Privacy Preferences (P3P), submitted by the World Wide Web Consortium (W3C), provides a mechanism to ensure that users can know about privacy policies before they submit their personal information but it does not provide a technical mechanism to enforce privacy protection and to make sure that organizations work according to their policies (P3P, 2002). However, there have been some efforts to extend P3P to the mobile environment. Langheinrich (2002) proposes a P3P based privacy aware system for ubiquitous environments. Nilsson et al (2001) have discussed how to implement the P3P

protocol in providing users with control over their location data and capabilities and preferences information (CPI). However, more work is required before the P3P protocol becomes widely applicable for the mobile environment due to its limitations in automating this expression and evaluation of privacy policies and users preferences by the limited capabilities of the context aware mobile devices, the dynamic changing context of users and the large number of context information collectors.

The assumption of non-trustful information collectors seems to be not realistic in daily life interactions especially in context aware systems where users information is being passively collected through a number of context sensors and delivered to a number of third parties. Not only users identity information but also contextual information with different degrees of confidentiality should be protected. Therefore, we think that controlling users contextual information perception is much more realistic. Controlling users contextual information perception implies taking decisions of whether to allow context entities to be collected by a certain party or not. This is known as user consent decisions. In addition, due to the dynamic nature of this environment, it will become imperative to have dynamic ways of expressing users privacy requirements. In this research, we develop a consent decision-making mechanism that fulfils the dynamic consent requirements by adopting dynamic user profiles with effective privacy preferences in order to facilitate the capability that users in a flexible way controls their context collection by other parties. Intelligent and autonomous decision-making is required in order to resolve the uncertainty attained due to the expected huge amount of information collectors and the shortage of users knowledge. In this paper, we focus on presenting an innovative mechanism that addresses the requirement of automating the decision-making process and to flexibly allow users to control their information collection.

3 TOWARDS CONSENT DECISION MAKING

3.1 Consent Decision Dependences

It seems clear that there are a number of factors upon which a user takes a decision on to share his/her information with others. These factors differ from one user to another in their roles and impact on users decisions. It is not the intention of this research to find out a full survey of factors that are affecting users consent decisions but to develop a way of modelling the impact of these factors and to effectively and flexibly implement this way of modelling. In this section, we focus on the most observable factors from plain reasoning.

3.1.1 Users trust of the information collector

Trust analysis and measurement have been of major interest in the literature (Gambetta 1988, Currall & Judge 1995, Glaeser et al. 2000). However, still users cognition of trust is not efficiently mapped onto physical measurements. For example: how to measure trust or how to define trust is still object of extensive study. Users trust in the information collector plays a major role in giving up or continuing with the service regardless his/her match results. For example, a user might choose to continue yahoo e-mail although yahoo might send some information to third parties just because she trusts that e-mail service. Trust also can refer to service quality or importance to the user, which might affect his/her decision on continuing the service, or not.

Increasingly, trust of an information collector can include a number of factors such as quality of service to the users, users need of the service, and users expectations of the information collector regarding their information collection.

3.1.2 Personal Information Confidentiality

It seems clear that personal information confidentiality largely determines whether users will give their consent, or not, to an information collector. Information confidentiality is driven by a number of

factors. Information value to a user can affect its confidentiality and hence its confidence. Increasingly, the culture itself may have different effects on personal information confidentiality. For example, a user salary, in the Netherlands, represents one of the most confidential information to him/her while in Sweden, salaries can be published online and the public will realize how much a user earns, just when he knows the type of work, she is doing. On the other hand, medical healthcare information varies in their confidentiality according to how much serious it is but not the culture. In addition, information confidentiality can vary according to user context. For example, user location information could be highly sensitive when the user is in a doubtful place rather than a normal one. However, if the same user is in another city or country away from his/her family or friends who know hem/her, she might not mind allowing a location-based service while she is in another doubtful place. Besides, confidential involvements of persons in some duties also represent relatively high confidentiality and should be kept private. Especially when such confidential information contains highly important political impact such as intelligence reports in case of wars legislation issues. Thus it could be concluded, that context confidentiality may affect users decision of the type of consent the user might give. Confidentiality depends on the type of collected information as well as context in which information is collected. In order to enable precise confidentiality based consent decisions, confidentiality should be crisply measured. Measuring confidentiality in itself is not an easy task since information confidentiality cannot be represented crisply. As a consequence, in this work, we assume confidentiality can be represented as a fuzzy concept, and hence we investigate the use of fuzzy technology in order to analyse and to take decisions based on it.

3.1.3 Users Interest in information sharing

The higher the user interest in information sharing or in other words, the higher the user willingness to share information is, the lower the possibility not to allow the sharing for any reason. For instance, a user interest or need for a service might be high enough that she gave up some of his/her private information. For example, some free programs install a lot of ad ware on a user's computer and most users allow that just because of their interest in those freeware programs. An example is Kazaa free media desktop, which installs in addition to itself other ad ware programs that could violate a person's privacy. We expect that the above mentioned two factors; users trust in the information collector and confidentiality of information will affect users interest in information sharing by increasing it or decreasing it.

3.1.4 Information Practices: asked and allowed

The above-mentioned factors represent a group of factor sets that cannot be crisply assigned values. In this subsection, another type of influence is considered. This type corresponds to the comparison between users allowed information practices, simply known as users preferences, and the asked information practices that are usually included in enterprises privacy policies. This comparison or evaluation reflects how much the information collector way of dealing with a user's information match with the user approved way of dealing with his/her information. In contrast to previously mentioned factors, this factor could be crisply measured, for instance by the number of hits obtained.

Privacy strictness varies from one user to another. It is not possible to generalize it or to have a common agreement on which data elements should be given away and which should not. In this context, each user defines how she thinks his/her personal information should be dealt with. However, optimal preferences that can lead to perfect representation of users privacy requirements still do not exist. There is still a lot to be done on defining preferences that match each user and that is efficient in describing their privacy needs. Increasingly, as information systems get more complex, and a lot of information collectors do exist with different types of information demands and different types of services, the process of managing these preferences gets higher in complexity as well. P3P (2002) and APPEL (2002) are considerable efforts in representing users preferences and matching them with information collector privacy policies. Based on this evaluation procedure, a user agent can summarize

the situation to the user and give hem/her the responsibility to decide whether to continue and the type of consent to give.

3.2 A Consent Provider Model (CPM)

In P3P (2002), information collectors practices are evaluated against users preferences and based on the evaluation, three types of users consent are obtained: request, limited and block. The P3P specification considers user's identification information, such as device ID, IP address and credit card details, as the only private information that needs to be protected. Hence, when the evaluation results show "*limit*", identification information is prevented by the user agent from submission to the information requester. We do believe that users private information differs from one user to another and cannot be defined in a general context or in advance. In addition, in context aware systems, it is expected that user context information confidentiality may depend on the situation where it is collected. For example, if a user is at work, he/she might not mind letting others to see his/her location, while if he/she is in some other place, the situation would be different. In addition, we expect a number of users self valued factors to influence their consent decisions. In this section, we propose a consent provider model that takes into consideration changing users preferences and automates the consent decision process based on the adoption of fuzzy logic techniques. The consent provider model consists of the following components (see figure 1):

3.2.1 Compare_Pref

In this step, users preferences on how their collected information should be used such as purpose of collection, retention of information and recipients of information are compared to information collectors' way of dealing with information, which is known as information practices. In this context, we define two groups of information practices: -

- Asked information practices

These are the information practices of the collector or the requester of the information. Usually, it's stored in the information collector privacy policy.

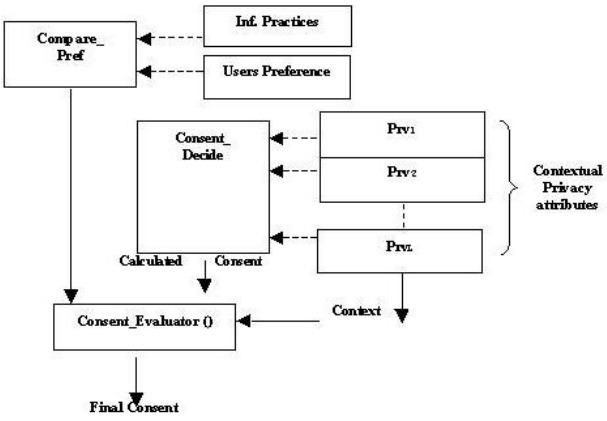


Figure 1 Consent Provider Model Composition

- Allowed Information Practices

This is also known as users preferences. It is stored in the user profile and is compared to the information collector privacy policy each time a user agent receives a request of information collection. The Compare_pref results will be fed to the Consent_Evaluator rules.

3.2.2 Contextual Privacy Attributes Data sets

In section 3.1, we explained a number of factors that affect users willingness to share information with others and we mentioned three of them. We define a new data set, called *contextual privacy attributes*, corresponding to these factors that are associated with users contextual information.

Definition

Let the requested context element set $Cx = \{Cx_1, Cx_2,\ldots,Cx_n\}$, which contains a number of context elements specified by the application domain, and let the abstract influencing factors set $Fac=\{fac_1,fac_2,\ldots,fac_m\}$. Then for each context element Cx_i exists a number "*L*" of privacy attributes $PrvAttr_{Cxi}$ corresponding to each factor set *Fac* such that $\Pr vAttr_{Cx_i} = \sum_{k=1}^{L} \Pr v_k(Cx_i)$.

For example, consider the case where influencing factors set $Fac = \{fac_1, fac_2, fac_3\}$. *Then privacy attributes set* $PrvAttr = \{Prv_1, Prv_2, Prv_3\}$

In this paper, we assume that the number of privacy attributes is always greater or equal to the number of influencing factors ($L >= m$). In addition, we assume that the users themselves will always be able to maintain these values because it is very critical in the consent decision process. Contextual privacy attributes are given values according to the reasoning used in analyzing and evaluating their effect on the associated context elements. Due to the difficulty in crisply defining such values, in this paper we adopt the use of fuzzy sets reasoning to implement them.

3.2.3 Consent Decide

In this step, a consent decision value is obtained based on contextual data privacy attributes. Due to the complexity and uncertainty in assigning values to these attributes and in deriving the rules that govern their impact for each user consent decisions, we adopt the use of fuzzy logic based reasoning in defining and representing these categories of information and in evaluating their impact on the user consent decisions (see figure 2).

Most of the industrially applied fuzzy inference systems (FIS) are based basically on Mamdani FIS (Mamdani, 1976) and Tagaki-Sugeno FIS (Tagaki and Sugeno, 1985). Mamdani inference system is one of the popular methodologies and is considered as one of the earliest fuzzy control systems. The main difference between Mamdani and Sugeno is that the Sugeno output membership functions are either linear or constant while the Mamdani outputs are considered fuzzy sets. The proposed approach calculates the output user consent from the input membership functions after applying the fuzzy rules using the Mamdani inference method.

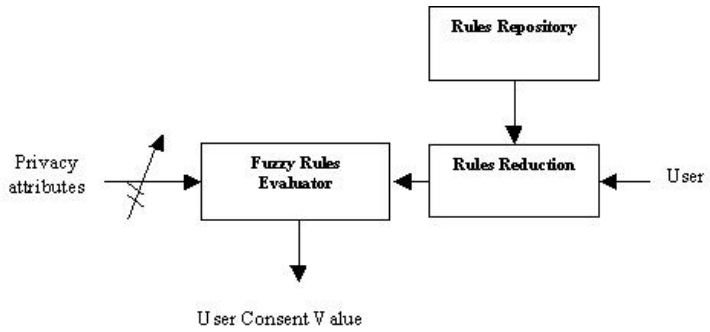


Figure 2 Consent _decide fuzzy rules

In the proposed fuzzy approach, rules are defined as "if then" blocks. Each privacy attribute and the output consent consist of three membership functions: {High, Medium and Low}. This produces a rule

space of 3^{L+1} entities (see figure 2). However, not all these rules are required, as some rules can be reduced after removing redundant ones. The reduction is done at the rule reduction component and it differs from one user to another. As a consequence of this reduction, the complexity of the model required to perform these rules is also reduced.

3.2.4 Consent Evaluator

The calculated consent value (*CalcCs*) from the consent decide component will vary from 1 to 10, and based on the calculated value, we expect three categories of consent values. If the calculated value is medium, this means that the consent decide rules could not define sharply the impact of the factors. In this case, we rely on the user on giving a definitive consent value for the system to continue its decision. Then, this entered value is stored in the user history for learning about the user and to make case based decisions in the future (see figure 3)

```
Function CnsEval // consent evaluator procedure
Input: Rc, Prv // Rc is requested context elements
Output: Fc//final consnet

Begin:

For each Rcc Do
        Calc Cs = Consent_Decide(Prv,Rcc); //calling Consent_Decide algorithm
        //using Comp_Pref and calculated consent for evaluation
        If Comp_Pref () and Calc Cs = High
                                                Fc= true;
        If Comp_Pref() and Calc Cs = Low
                                                Fc= False;
        If Comp_Pref () and Calc Cs = Medium
                                                Fc= user_response();
        Else
                                                Fc= false; // compare_pref is not valid
End
```

Figure 3 consent evaluator rules

4 PROTOTYPE TESTING

In this section, we introduce briefly the design of a simple prototype system in order to test the privacy consent model.

4.1 Prototype Details

The consent provider model has been implemented using server-based modules on a MySQl database hosted on an apache server. The *Consent_Decide* algorithm was coded in Matlab and C++ and compiled into a Win32 application. The consent evaluator and compare_pref procedures have been implemented as web server based applications using ASP and VB scripts. The consent provider model has been integrated into the MIES platform on a UMTS testbed in Delft University of Technology. MIES is an acronym for Mobile Information and Entertainment Services. The first prototype of MIES was developed and experimented by 12 conference visitors to the university campus. Users were connected to the UMTS network through a Nokia cell phone. Each user had a GPS enabled iPAQ with a Bluetooth wireless connection to the Nokia device. MIES offers GIS location based services and touristic information to campus visitors. It also enables users to locate and to contact each other. One of the designed services, a privacy aware finding people service was designed in such away that enables users to specify their allowed information practices and privacy attributes. Based on these attributes, the consent evaluation process was carried out on any coming request for users information. Finding people represents one of the services offered by MIES. We have designed this service to allow

users to search for other users of the MIES based on some criteria such as name, native language and research interests.

4.1.1 Context Information clusters

In this experiment, users context information has been defined into three clusters of information (see figure 4):

Personal information: this includes any information that's personal in nature such as name, date of birth, telephone numbers, address etc.

Professional Information: This includes information that's professional in nature such as job title, organization, work address, visiting address in delft, e-mail address, research interests, research fields, etc.

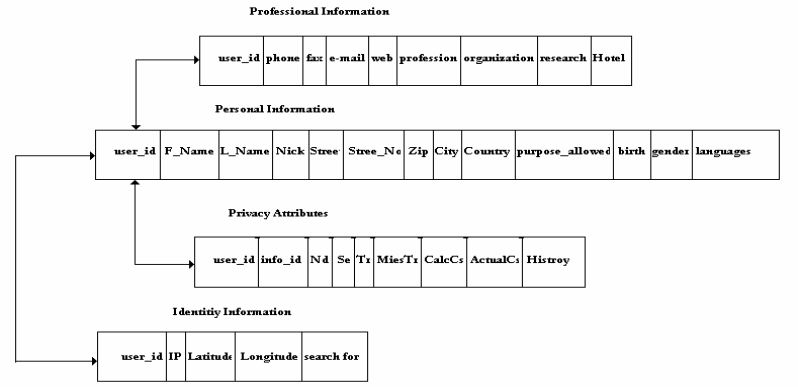


Figure 4 Context Information Clusters and Corresponding Privacy Attributes

Identification information: this includes information about users device IP addresses and users GPS location, This was obtained through the GPS device as latitude and longitude coordinates that could be easily transferred into certain locations within the university campus using a *TomTom* navigator.

4.1.2 Contextual Data Privacy attributes

Contextual data privacy attributes are directly related to factors that influence users' willingness to share their information with other users in the MIES. In section 3, we introduced the three most relevant factors based on literature and plain reasoning. With these factors, contextual data privacy attributes could be generated with values from 1 to 10. For the sake of simplicity, we consider only the factors mentioned in section 3 in deriving the corresponding privacy attributes. We derive three privacy attributes: *Nd*, *Se*, and *Tr* to refer to "*users interest in sharing*", "*confidentiality of the information*" and "*trust in the information collector*" respectively. Each user has three records of privacy attributes, one per each group of information. Each record contains values of the privacy attributes and corresponding calculated and actual consent values.

4.1.3 Getting Users Data

Users were asked to fill in two online web forms, the first one with their personal and professional information, while the second one asks about their privacy preferences. Then based on a developed PHP module, these preferences were then evaluated and converted onto a number of values, called privacy attributes, which are stored in a MySQL relational Database. Users identity information such as IP address was simultaneously recorded in the identity table. The GPS location was captured from a

GPS satellite by a GPS receiver connected to the iPAQ and the corresponding latitude and longitude coordinates were stored in the database as well with a 5 seconds refresh rate (see figure 5).

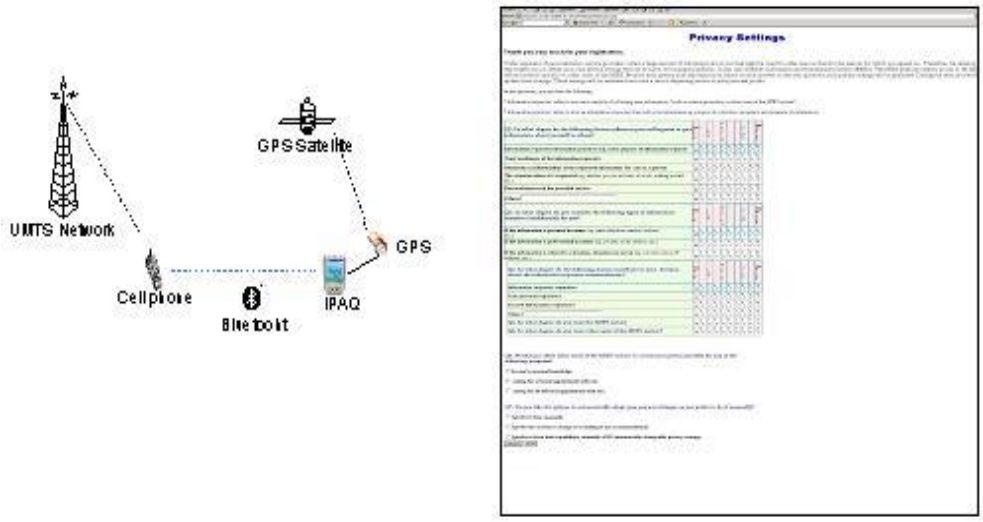


Figure 5 Getting users data

4.1.4 Information Practices Evaluation & Consent Decision Making

For the sake of simplicity, the only information practice variable was purpose of collection. We distinguish further three categories of purposes: -

- Personal Knowledge

Personal knowledge represents the default purpose of collection, and it means that the information collector collects the information for his/her own personal knowledge interest.

- Formal Appointments

Users are allowed to collect for the purpose of personal knowledge about the other user and at the same time are allowed to ask for professional appointments.

- Informal Appointments

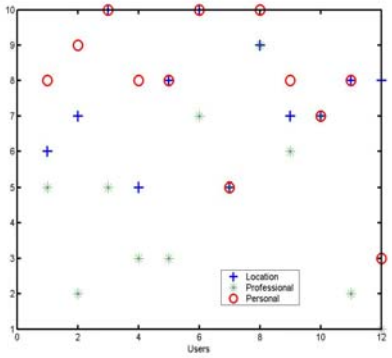
Users are allowed to ask for informal appointments such as coffee breaks, dinners etc.. The other two purposes are then by default allowed as well.

When a user requests to access a group of information of a certain user, his/her request passes through the *CnsEval procedure* (see appendix) which in turns decides whether to give access to the requesting user or not. Each group of information has a record in the database with all related privacy attributes and consent values. Before the *CnsEval procedure* is called, the attributes values are retrieved, and the *consent decider* component is activated. For the sake of simplicity, the consent decide fuzzy rules were implemented with *(DoS)=1*. The *CnsEval procedure* is called with both users purposes and the calculated consent value and then returns a Boolean value “true or false” corresponding to the user final consent.

4.2 Preliminary Results

There were 12 registered users to the MIES service most of them were foreign visitors to the university campus for the ESS03 conference that was held in Delft University of Technology in the period Oct. 22-25, 2003. Although most users recorded different privacy attribute values for the different groups of contextual information (see figure 6), the classification of users information into

three categories according to its confidentiality showed different consent values among only 4 users. Figure 7 shows the calculated consent values for the 12 users for each group of information. It can be seen from the figure that calculated consent was the highest in case of professional information for all users, while location was recorded to be of lower consent value than personal information in case of user 12 only. Most users have equal calculated consent values for both personal and location information. Due to the difference among users privacy attributes values, the corresponding calculated consent values were also considerably different especially in case of users 6 and 12.



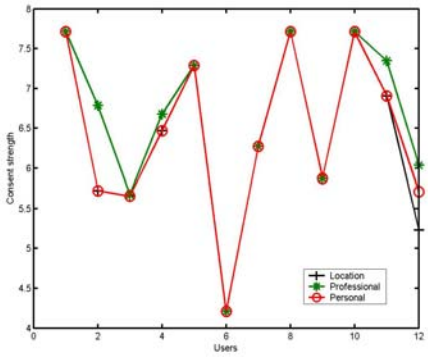


Figure 6 Users Privacy Attributes values *Figure 7 Calculated Consent values*

Due to the limited time period available for setting up the pilot test, we were not able to completely implement the consent evaluator algorithm. We could not ask users for their response when the calculated consent value appeared to lie within the medium value range, but we estimated users response according to the calculated consent value obtained. Hence, values above '5' were regarded as *approval* and the ones below '5' were regarded as *denial*. The implemented fuzzy algorithm used static rule space for all users, which do not reflect the dynamic nature of the environment. Therefore, in a further study we plan to implement a dynamic algorithm that can adapt its parameters and rules to each individual's interactions.

5 CONCLUSIONS AND DIRECTIONS

In this paper, we proposed an innovative mechanism that allows users to have control capabilities of their private contextual information collection in context aware environments. A new data set, called contextual privacy attributes, was proposed corresponding to individuals consent decisions influencing factors. For the sake of simplicity, we have considered only three factors: users interest in sharing their data, users trust of the data collector and users data confidentiality. We have proposed a consent provider model that is able to calculate a user consent decision value based on users preferences, information practices and contextual privacy attributes. The consent decider rules were implemented via fuzzy logic due to the ambiguity and uncertainty in sharply defining the privacy attributes values and impact on the final user consent. The proposed model has been implemented and integrated into the MIES platform, which works on the TU-Delft campus UMTS test bed. Initial results have shown the importance of effectively defining privacy settings that could represent users privacy requirements. In addition, most users asked for the combination of manually and automatically controlling of their privacy settings. Identification and personal information were recorded to be the most private contextual information categories. In the current MIES version, there was one implemented information practice: "*purpose of collection*". It is considered of importance to include other practices that constitute a privacy policy of an information collector in the evaluation process. In addition, we intend to consider the P3P specifications in the implementation of the *Comp_Pref*. The MIES services

were available for conference users; therefore, it was not possible to create a history of users interactions. We intend to proceed with and improve upon this work along two lines. The first is to design and implement a dynamic and learning model in the consent decide algorithm. The second line is on further investigation on the privacy-influencing factor set. Though finding out a complete list of contextual privacy factors is out of the scope of this paper, we do believe that this work could be improved and become more realistic and applicable if the influencing factors are more empirically tested for their impacts on users consent decisions. It came out that complete automatic control is not realistic due to users interest in manual involvements as well. We intend to adopt a manual and automatic mode where users' involvement is reduced to only cases where it is mandatory to resolve ambiguous consent values. As a consequence, the automatic learning mode can lead to higher level of user friendliness, in the sense of less interrupts for manual control, and flexibility which in turns enhances usability of the consent provider model.

References

Ackerman, A., et al (2001). Privacy in context, *HCI*, 16, 2, pp. 167-179.

Agrawal, Rakesh and Kiernan, Jerry (2002). Watermarking relational databases, *Proceedings of the 28th VLDB Conference*, Hong Kong, China.

Agrawal, Rakesh et al (2002). Hippocratic Databases *Proceedings of the 28th VLDB Conference*, Hong Kong, China.

Ali Eldin, Amr and Wagenaar, René (2003). Towards a Component based Privacy Protector Architecture in *the proceedings Short papers of the CAISE'03 15th International Conference on Advanced Information Systems Engineering*, Austria 18-20 June Pg 253-256.

APPEL (2002). A P3P Preferences Exchange Language 1.0. Available at http://www.w3.org/TR/P3P-preferences/

Casal, Carlos Rodríguez (2001). Privacy Protection For Location Based Mobile Services in Europe Vol(4), *Proceedings of the 5th World Multi-Conference on Systems, Cybernetics, and Informatics (SCI2001) Orlando, Florida USA.*

Chaum, David (1985). Security without Identification Card Computers to make Big Brother Obsolete *Communications of the ACM*, 28 (10): 1034-1044.

Camenisch, Jan; Herreweghen, Els Van (2002). Design and Implementation of Idemix Anonymous Credential System Technical Report, IBM Zurich Research Laboratory,

Clifton ,Chris et al (2002). Tools for Privacy Preserving Distributed Data Mining, *ACM SIGKDD Explorations 4(2)*

Cranor, L.F. (2002). Web Privacy with P3P, 1st edition, AT&T. ISBN: 0-596-00371-4

Currall, S.C. and Judge, T.A. (1995). Measuring Trust between Organizational Boundary Role Persons, *Organizational Behavior and Human Decision Processes, Vol.64(2), pp. 151170.*

European Directive (2002). Directive 2002/58/EC of the European Parliament and of the Concil of 12 July 2002, Available at: http://www.spamlaws.com/docs/2002-58-ec.pdf

Gambetta, D.G., Can we trust trust? in *D.G. Gambetta (Ed.), Trust, pp. 213-237, Basil Blackwell, New York, 1988.*

Available at: http://citeseer.nj.nec.com/gambetta88can.html

Glaeser, E. L., Laibson, D., Scheinkman, J. A., and Soutter, C. L. (2000). Measuring Trust. *Quarterly Journal of Economics. Vol.65, 2000, pp. 811-846.*

Hauser, Christian (2002). Privacy and Security in Location-Based Systems With Spatial Models *PAMPAS'02 Workshop on Requirements for Mobile Privacy and Security.*

Hauser, Christian and Kabatnik, Matthias (2001). Towards Privacy Support in a Global Location Service *Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001),* Paris.

Huizenga et al (2002). Security and Privacy Issues in Next Generation Mobile Networks and Services *PAMPAS'02 Workshop on Requirements for Mobile Privacy and Security.*

Lamparter, Brend and Westhoff, Dirk (2002). Security challenges in the future mobile Internet *PAMPAS'02 Workshop on Requirements for Mobile Privacy and Security.*

Langheinrich, Marc, 2001 Privacy by Design- Principles of Privacy-Aware Ubiquitous Systems *Proceedings of the 3rd International Conference on Ubiquitous Computing (Ubicomp2001),* Springer-Verlag LNCS 2201, pp. 273-291.

Langheinrich, Marc (2002). A Privacy Awareness System for Ubiquitous Computing Environments, In: G. Borriello, L.E. Holmquist (1999). *(Eds.): 4th International Conference on Ubiquitous Computing (UbiComp2002),* Springer-Verlag LNCS 2498, pp. 237-245.Lysynaskaya, Anna; Rivest, Ronald L. Pseudonym Systems in *Proceedings of the Sixth Annual Workshop on Selected Areas in Cryptography (SAC '99).*

Lysyanskaya et al (1999). *Pseudonym Systems* , in Proceedings of the Sixth Annual Workshop on Selected Areas in Cryptography (SAC '99) forthcoming in Springer-Verlag LNCS.

Mamdani, E.H. (1976). Advances in the Linguistic Synthesis of Fuzzy Controllers. *Journal of Man-Machine Studies, 8, 669-678.*

Nilsson, Mikael et al (2001). Privacy Enhancements in the Mobile Internet, *Proceedings of the IFIP WG 9.6/11.7 working conference on Security and Control of IT in Society*, Bratislava, 15 -16 June.

P3P (2002). The Platform for Privacy Preferences 1.0 (P3P1.0) Specification W3C Recommendation, http://www.w3.org/TR/2002/REC-P3P-20020416/

Rao, Josyla R. and Rohatgi, Pankaj (2000). Can Pseudonymity Really Guarantee Privacy, *Proceedings of the 9th USENIX Security Symposium*, Colorado, USA.

Rodden, Tom; Friday, Adrian; Muller Henk and Dix, Alan (2002). A Lightweight Approach to Managing Privacy in Location-Based Services, Technical Report Equator-02-058, University of Nottingham and Lancaster University and University of Bristol, October.

Tagaki, H. and Sugeno, M. (1985). fuzzy identification of Systems and its Application to Modelling and Control, *IEEE Transactions: systems, Man and Cybernets vol. 15, pp. 116-136.*