Towards a Component based Privacy Protector Architecture

Amr Ali Eldin and René Wagenaar

Information and Communication Department
Faculty of Technology, Policy, and Management
Delft University of Technology
Telephone: +31 (15) 2781131
Fax: +31 (15) 2783741
E-mail: amre@ tbm.tudelft.nl

Abstract. The development of mobile communication technology and ubiquitous computing paradigm and the emergence of m-healthcare, m-business and m-education services have raised the urgency of dealing with personal information privacy threats. In this paper, we discuss the requirements, functionalities and roles needed to support privacy protection in context aware mobile information systems.

1 Introduction

Despite the huge benefits expected from ubiquitous or context aware computing in the fields of healthcare, business and education [5], it seems to be that context awareness adds new threats to individuals privacy. These threats exist due to the detection of personal sensitive information, such as location, preferences and activities, about individuals through sensors available anywhere and at any time [1]. Moreover, the possibilities of sharing users profiles, among different organizations without users consent and the ubiquitous linkage between individual identities and their context increase individuals' trace ability possibilities and hence threaten their privacy.

Organizations and service providers collect large amounts of personal information about individuals in order to deliver certain services to them; we see a conflict existing between personal information owners (individuals) and information collectors (service providers) regarding privacy control. This conflict is caused by the confrontation between service providers, aiming to collect more information about users in order to provide personalized services, and users requirements of controlling their privacy aspects.

In this research, we aim to develop a component based ICT architecture that resolves the mentioned conflict and gives users more control functionalities of their personal information by letting them to explicitly and permanently be able to provide their consent on the collection of their personal information in an autonomous and user friendly way.

2 Privacy Requirements of Mobile Information systems

In order to design privacy protector context aware mobile architectures, we enunciate the following requirements, based on the recent European Directives, and the US privacy guidelines, discussed in [1,2,3].

Notifying users of the way their information is being used by the collector and other third parties represents the basic requirement of privacy protection. This notification should let users know what information is being collected about them, which parties are using their information, in which purpose and how long it will be used. Privacy policies represent the way most web sites nowadays notify users about information practices. However, most these policies are so long that users do not read or understand them completely.

As a solution for this problem, the Platform for Privacy Preferences (P3P) [4], submitted by the World Wide Web Consortium (W3C), enables web sites to express their privacy policies in a machine-readable format that can be retrieved and interpreted by users browsers. It provides a mechanism to notify users of privacy policies before they submit their personal information. However, it does not provide a technical mechanism to enforce privacy protection and to make sure that organizations work according to their policies. Increasingly, it is not well adapted to the mobile environment due to the limited capabilities of mobile devices and the dynamic changing preferences of users. We see this requirement as a challenge for this environment. Thus, a new mechanism is required for such environments that can satisfy the n*otice* requirement and overcome those difficulties.

A second requirement, selectivity, states that users should be able to select among different options. The "take it or leave it" obligatory option does not represent a reasonable choice at all; users have only two options, whether to accept the way their information is being used and continue using that service or to decline and then not to continue the service. It would be more effective if the service providers give the users a number of options to choose from, that provide them a flexible way of controlling the way their information is being used.

After notifying users and allowing them to select among different choices, it is required that the user explicitly declare his/her acceptance for this type of usage. Most web sites ask for users consent, once and for all, directly after privacy policies reviewing by end users with the previously mentioned option: "take it or leave it", accept policy or reject policy. However, in a dynamic changing environment such as the mobile environment where users sensitive information can be collected, we believe that providing consent at the beginning only is not flexibly satisfactory for privacy protection. For example, a user might go to a private place where he would like not to be located. In this case, he would prefer to disallow his location detection. We see the need that users consent should always be requested before any collection of contextual information. Increasingly, this request for mobile users consent should be carried out in an autonomous, flexible and user-friendly way because in a dynamically changeable context aware environment, it can be expected that users be asked continuously to provide their consent.

Finally access rights control and security mechanisms are required to construct a shield that safeguards any privacy aware information system from surveillance and illegal access while stored and transmitted.

3 Roles and Functionalities

In order to achieve previously mentioned requirements, we see the following needed functionalities and roles of the proposed architecture: (See Fig. 1 & Fig. 2)

- **Policy Parser**

Policy parser would be responsible for providing user agents with the service provider policy that organizes how it deals with user information. In addition, it would format the policy practices to suit the user agent *device capabilities*. The service provider policy would represent the main component of the policy parser.

- **Consent Provider**

The user himself would maintain his/her consent. The user would configure his preferences and conditions of dealing with his personal information and keep them in

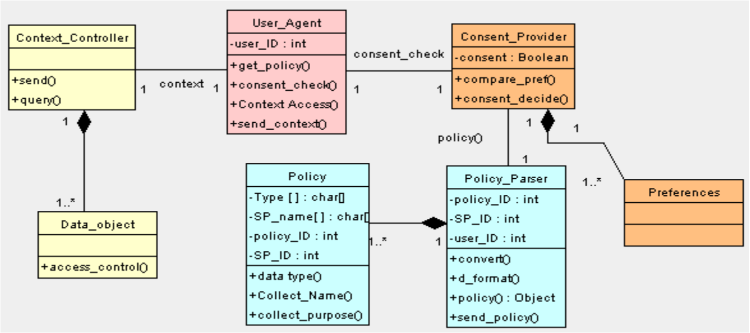

Fig. 1 Relationships & Functionalities

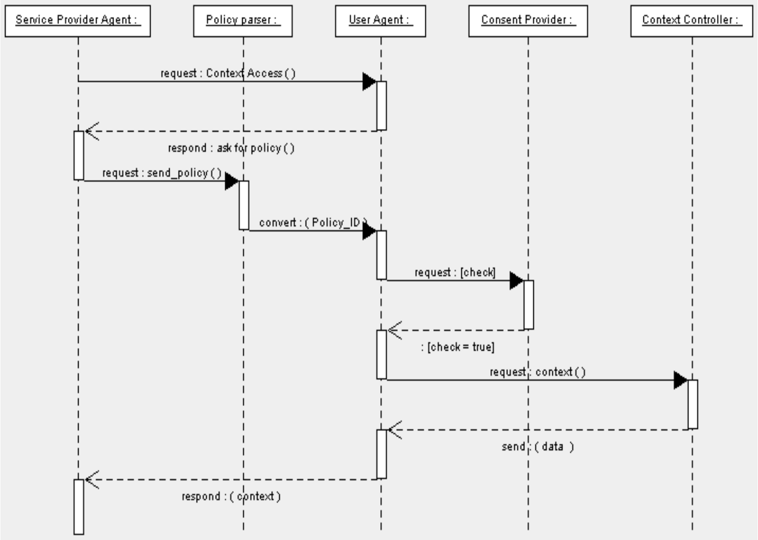

Fig. 2 Interactions Sequence Diagram

the preferences component. Then the consent provider would compare the policy practices of the incoming request for information with the stored preferences in order to decide whether to accept that way of dealing with the user's information. In addition, the user agent might negotiate with the service provider agent in order to *anoymize* or *pseudonymize* his data.

- **Context Controller**

Context controller component would play an important role. It would be responsible for controlling the collection of users contextual information in addition to controlling access privileges of users contextual information in order to restrict access to the users context. A number of issues would have to be considered such as how this control can be achieved and what privacy techniques can be used to establish this control.

Conclusion & Future work

Based on the above mentioned requirements of privacy control in context aware mobile information systems, we briefly discussed the required functionalities to fulfill these requirements together with components or building blocks needed of the proposed architecture. The design of the architecture components passes through different levels of abstraction because information hiding leads to more flexibility and simplicity in the design of complex systems. This research is in progress. In this paper, although focus has been given to supporting mobile users explicit consent rather than security; we enunciate that security functionalities to be included, in the future, in the design and implementation phases of the architecture as well. We will prototype the proposed components and emphasize how to provide users consent based on the policies practices and the stored preferences in an autonomous, flexible, and user-friendly way.

References

[1] Ackerman, A., et al: Privacy in context, HCI, 16, 2, (2001) 167 -179.

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

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

[4] P3P: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16th April (2002) Available at http://www.w3.org/TR/P3P.

[5] Samulowitz, M.: Designing a Hierarchy of User Models for Context-Aware Applications Workshop on 'Situated Interaction in Ubiquitous Computing' at CHI 2000 (2000)