Developing a privacy ontology for privacy control in context-aware systems

Ni Zhang, Chris Todd

Dept. of Electronic & Electrical Engineering, University College London

Abstract: This paper concerns personal privacy and privacy protection in context-aware ubiquitous computing environments. It proposes a privacy ontology solution to facilitate automated processes in privacy control. The development of the privacy ontology is an integrated part of our ongoing effort towards a privacy-respecting middleware solution for context-aware systems.

1. Introduction

Personal privacy protection has been a staple in ubiquitous computing conferences since 2000, which leads to a number of ameliorating solutions. However, much work has gone into investigating the design of privacy-preserving location sensing systems [1] and the integration of access control mechanisms into ubiquitous computing infrastructure [2]. These solutions addressed only a small subset of the privacy challenges faced by context-aware systems.

Context-aware computing is one ubiquitous computing paradigm that emphasizes taking advantages of contextual information (such as user location, activity, nearby people and devices, time of day, etc) to make decisions about how to dynamically provide services or adapt to meet user requirements. Under this circumstance, information that can be used to characterize privacy aspects of an individual is in a wide range and comes from various types of sources, and it is likely that individual privacy preferences towards the dynamic context-aware environment comprise a complex set of rules in response to various situations and changes over time. These make it challenging to provide adequate privacy protection therein. As a result of the difficulties, most current context-aware systems provide very little support for privacy, although researchers often note the importance of privacy and security in context-aware computing [3,4,5].

This paper proposes the use of ontology-based approach to model dynamic privacy preferences and rules. By representing privacy-related context information in a formal and unambiguous way, the privacy ontology servers as a shared model for exchanging privacy policies between users and context-aware environments, and among users in the environments. More importantly, we expect to take advantage of logic-based inference capability, which is inherent in ontology-based context models, to facilitate automated processes in privacy interaction between users and the context-aware system. Before describing the privacy ontology, we present a summary of literature survey on individual concerns over privacy and privacy protection in context-aware ubiquitous computing environments. It helps justify the need of the privacy ontology solution.

2. Individual privacy concerns in context-aware computing environments

A widely accepted definition of privacy is by Legal and policy scholar Alan F. Westin. He defined information privacy as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” [6]. Moving further from this general definition, we have attempted to qualify, within the scope of context-aware paradigm, the phrase *personal privacy,* by exploring individual concerns over privacy and privacy protection. Research prototypes and context-aware applications [1,7], as well as several different design guidelines for privacy-sensitive systems [5,6,8,9] have been examined. A brief summary of the literature review is presented as below.

On the one hand, largely similar to conventional computing systems, users in context-aware ubiquitous computing environments desire simple and appropriate levels of control over information disclosure, want feedback of information disclosure with respect to recipients, purposes and conditions, and have concerns over long-term retention of personal data and potential divulgence to third parties. In addition, according to [7], many people ask for system ability to override privacy needs in emergency situations.

On the other hand, there are two key privacy needs that have not been adequately addressed by researches in conventional computing systems and in ubiquitous computing. Context-aware paradigm requires a broad applicability of plausible deniability and ambiguous disclosure to avoid potentially embarrassing situations, undesired intrusions and unwanted social obligations. Plausible deniability refers to a situation that potential observers of information disclosure cannot determine whether a lack of disclosure was intentional. Mobile phone serves as a good example, in that if a person does not answer a call, it could be a technical reason (e.g. being outside of reach) or for social purposes (e.g. not wanting to talk to the caller right now) [9]. The system ability to allow disclosing ambiguous information is desired, as users' privacy preferences are often not black-and-white but rather involve different levels of accuracy or inaccuracy. The ambiguous disclosure is often applied in two ways, either abstracting away some details of information, or providing false information on purpose, such as using pseudonyms to hide a real identity.

Unfortunately, the literature review indicates limitations in approaches taken to date and it seems that personal privacy needs in dynamics context-aware environments, especially the plausible deniability and ambiguous disclosure, remain largely unsatisfied. Many existing approaches that work in conventional data management environments are inadequate to support personal privacy in context-aware paradigm. For instance, quite often users are allowed to express their privacy requirements only by filling in some forms with predefined layout and options. Such a fairly simple approach would not be useful where a user's willingness to share personal information may depend in part on the user location, recent and current activities, and may change over time.

Indeed, central to the privacy requirements in dynamic context-aware environments is about empowering people to choose information disclosure with the right people and services, in the right situations, and at the right level of detail, in addition to the ability to choose not to have information collected. Yet, the task to take full context-aware controls over how their personal information is shared can be overwhelming to users (due to sheer volume, especially at the sensor data level). The task might disrupt their ongoing activities, which defeat the basic goal to make context-aware environments unobtrusive. Demand for research efforts towards flexible mechanisms for relatively unobtrusive user participation in controlling the disclosure of their sensitive information (including getting notice, feedback, and explicit consent) is significant.

3. Privacy ontology

We have been working on a middleware solution that aims at addressing context-awareness and personal privacy protection all together. To cope with the concern that individuals' privacy preferences might change over time and in response to contexts, we have been introducing automated processes in privacy control (e.g. automatically computing and reasoning a individual's privacy preferences according to his initial settings). The automation mechanisms are characterized by the development of intelligent agent technologies [10] and the privacy ontology.

In particular, the privacy ontology servers as a shared information model for various components and parties involved in our architecture to have a common understanding about privacy rules while interacting with each other. Ontological information modeling technology is employed because it enables a formal description of concepts and their associated properties in a domain, and has an inherent strength in capturing relationships between concepts and properties. This can be used to reason over ontology descriptions as a means to support privacy check and matching.

The privacy ontology has been developing based on the terminology and policies specified in W3C's Platform for Privacy Preferences (P3P)[11], with the intention of benefiting from the substantial legal and social expertise that has been put into the development of the standards. The P3P standards provide a specification for stipulating privacy policies and allow the encoding of such policies into machine-readable XML. The P3P works with other preference languages such as A P3P Preference Exchange Language (APPEL) [12] to enable automated processes to read such policies and take actions on them. Although the P3P is initially an attempt to provide privacy mechanisms for Web community, an important part of the P3P Syntax played by the EXTENTSION element allows P3P policies to be adapted to ubiquitous computing environment.

In developing Privacy Ontology, we have adopted P3P terminology and created corresponding classes and properties. As illustrated in the Figure 1, a Privacy_Rule class is defined to represent privacy preferences set by users. Every privacy rule is expressed with two elements: Data (Data class) and Conditions (Condition class). The Conditions class contains all conditions under which a user is willing to disclosure data. According to the

P3P specification, the conditions can be classified based on various individual concerns including recipients of data, purposes of data collection, duration that data will be kept by recipients, a user's access privilege to his personal data once stored by recipients, and ways of handling disputes. The Privacy_Rule class has two properties: Data_is and Disclose_when, forming a triple expression that can effectively describe the relationships between privacy rule, data and disclosure conditions. Both properties Disclose_when and Data_is properties are allowed to have multiple values, since a set of data may have the same disclosure conditions.

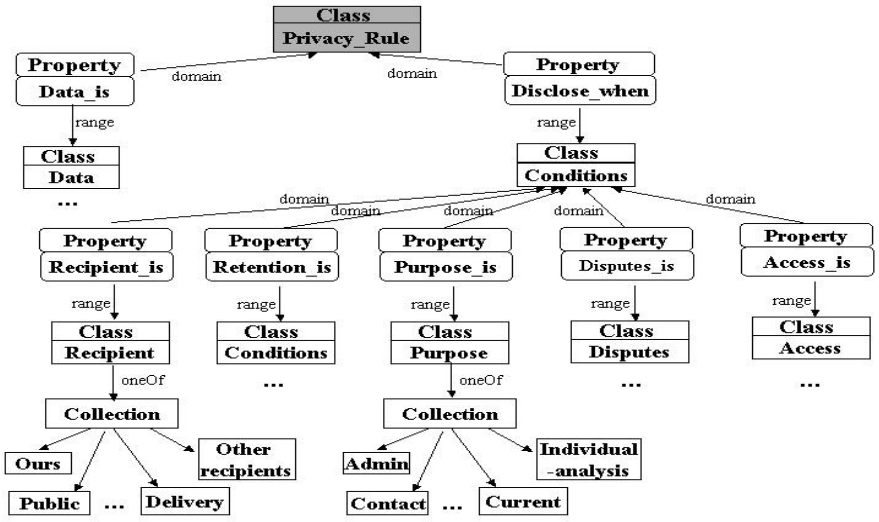

Fig. 1. A subset of the ontology specification of a privacy rule

The data element specified in the privacy ontology reuses most of the P3P base data scheme and represent typically personal sensitive information that is resorted to privacy protection, such as real identities, date of birth, home address, etc. Such information constructs a subset of the context information used in context-aware systems. Following the P3P specification, data schema is organized hierarchically by using a dotted notation, such as user.home-info.telecom.telephone. Using ontological modeling to capture the multiple-level hierarchy of P3P data scheme gets the advantage over other preference formulation methods employed by P3P, such as the commonly used APPEL With logic relationships embedded in the ontological modeling, our approach has a higher logic reasoning capability and better supports privacy check than the APPEL matching process. Take a user's telephone number for example, we assume that a data collector asks for a user's telephone number (user.home-info.telecom.telephone) while the user agrees to disclose all the home-information (user.home-info). Knowing all direct and indirect superclasses and subclasses, the ontology-based reasoning engine implanted in a intelligent privacy agent is able to tell that the data collector's collecting policy satisfies the user's privacy preferences, as the user.home-info.telecom.telephone is a subclass of user.home-info. Whereas in APPEL, such awareness of the class hierarchy does not exist, the user must specify a privacy rule exactly for the data user.homeinfo.telecom.telephone in order for privacy check to be successful.

4. Conclusion and future work

This paper has presented the motivation and approach to develop a privacy ontology for context-aware computing. The dyanmic natures of information in context-aware ubquitous computing environments have led to a trend in the context-aware research to embark on ontological information modeling approahces [13]. However, unlike many other context ontology efforts, which limited the use of ontology only to represent general context information (such as location, time, etc) and relationships between them, we have employed the ontological modeling approach to express privacy vocabulary and rules. By taking advantage of the real power of ontology as an enabler for logic-based inference and reasoning, our approach to the privacy ontology aims to facilitate automated processes in privacy control. Further work, among others, focuses on developing rule-based privacy mechanisms to employ the privacy ontology.

References

[1] Myles, G., Friay, A., and Davies, N., Preserving privacy in environments with location-based applications. IEEE Pervasive Computing, 2(1): 56-64, January -March 2003

[2] Hengartner, U., and Steenkiste, P., Access control to information in pervasive computing environments. In *9th Workshop on Hot Topics in Operating Systems*, Hawaii, May 2003.

[3] Maria R. Ebling, Guerney D. H. Hunt, and Hui Lei. Issues for context services for pervasive computing. In: *Proc. of the Workshop on Middleware for Mobile Computing 2001*, Heidelberg, Germany, November 2001.

[4] Satyanarayanan, M., Pervasive computing: Vision and challenges. *IEEE Personal Communications*, 8(4):10–17, August 2001.

[5] Langheinrich, M., Privacy by design— principles of privacy-aware ubiquitous systems. *In: Proc. of International Conference on Ubiquitous Computing* (UbiComp 2001), Atlanta, GA, USA, September 2001, volume 2201 of *Lecture Notes in Computer Science*, pp. 273–291. Springer-Verlag, 2001.

[6] Westin, A., (1967), *Privacy and Freedom*, Atheneum, New York

[7] Hong, J.I., and Landay, J.A.: An Architecture for Privacy Sensitive Ubiquitous Computing. In MobiSYS '04: *In. Proc. of the 2nd international conference on mobile systems, applications, and services*, pages 177–189. ACM Press, 2004. (2004)

[8] Ackerman, M.S., Darrell, T., and Weitzner, D.J.: Privacy in Context, Human-Computer Interaction, 2001, 16(2-4), pp. 167-176. (2001)

[9] Lederer, S., Hong, I., Dey, K. and Landay, A.: Personal Privacy Through Understanding and Action: Five Pitfalls for Designers, Personal and Ubiquitous Computing, Volume 8 Issue 6,November 2004 (2004)

[10] Zhang N., Todd, C. A Privacy Agent in Context-aware Ubiquitous Computing Environment, *Proc. of 10th IFIP Open Conference on Communications and Multimedia Security*, Springer, Lecture Notes in Computer Science (LNCS), October 2006, Crete, Greece (to appear).

[11] Cranor, L., Dobbs, B., Egelman, S., Hogben, G., and Schunter, M., The Platform for Privacy Preferences 1.1 (P3P1.1), http://www.w3.org/P3P/, July 2005

[12] Cranor, L., Langheinrich, M., and Marchiori, M., (2001) A P3P preference exchange language 1.0 (APPEL1.0). W3C Working Draft, April 2001, http://www.w3.org/TR/P3P-preferences

[13] Henricksen, K., Livingstone, S., and Indulska, J.: Towards a Hybrid Approach to Context Modeling, Reasoning and Interoperation, In *Proceedings of the 1st International Workshop on Advanced Context Modeling, Reasoning, and Management* in UbiComp'04, Nottingham, England, September 2004