Multi-Determiner Protection of Private Data in Pervasive Computing Environments

Anis Yousefi[†], Rasool Jalili[††], Mahdi Niamanesh[†††]

Network Security Center, Department of Computer Engineering,
Sharif University of Technology, Tehran, Iran[*]

Summary
Protection of private data is one of the most challenging issues threatening the success of Pervasive Computing (PC). Regarding the principles of privacy and the vision of pervasive computing, one of the most troublesome problems is how to provide people's control of their data while not distract them to a great extent. A suitable approach for protecting people's private data in PC environments should consider the intention of all influential entities (data determiners), and invisibly gain their consent by applying their desired preferences. In extension of the current approaches which consider a single set of preference rules for a private data item when deciding about its disclosure, we propose dealing with different preferences of all involved determiners in a distributed manner. In this paper we investigate possible determiners of private data and propose a set of required meta-data as well as a multi-determiner protection procedure to protect private data with regard to the preferences of its determiners. Moreover, we propose the DELEGATION behavior as a determiner's response to a request instead of ACCEPT or REJECT. We demonstrate the efficiency of the suggested procedure and present a prototype implementation of a multi-determiner architecture to realize the protection procedure.

Key words:
Data Privacy, Pervasive Computing, Multi-Determiner Private Data.

Introduction

Privacy has a long evolving history. That every individual should have full protection in her/his personal affairs and private data is a principle as old as the common law; but the definition, nature, and extent of such protection have been renewed from time to time [1]. The term *Informational self-determination* was first used in the context of a German constitutional ruling related to personal information collected during the 1983 census [2]. It reflects Westin's description of data privacy: *"The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."* [3]. This basic right warrants the capacity of individuals to determine in principle the disclosure and use of their personal data.

Protection of private data varies from denying any access to information to defining more flexible rules which control the disclosure of data [4]. Each data item may be assigned to one or more entities, called owners, which are authorized to manipulate or disclose it or determine its function and use [5]. An approach for privacy protection incorporates self-control policy-based systems, which serve as proxies, applying owner's data disclosure policy known as privacy preferences. Preferences reflect the intention of the person to whom the data relates, regarding the level and conditions of disclosing that data. Current policy-based privacy protection systems are based on a platform to gain the consent of data owner by evaluating her/his privacy preferences against data usage promises of Requesters (i.e. privacy policy) [6, 7].

Progressively, as heterogeneous information systems with different privacy rules are interconnected, more technical control and logging mechanisms will be required to reconcile, enforce, and monitor privacy policy rules and laws, to ensure accountability of information use. Pervasive computing with the promise of anywhere, anytime access to critical programs and data, introduces a difficult challenge to overcome the problem of privacy protection while maintaining the goals of minimal user distraction and invisibility. The invisible nature of pervasive computing makes it difficult to see where information is flowing and how it is being used. A simple action like entering of a person into a smart place may reveal a considerable amount of her/his private data without her/his consent or even awareness of data collection. Mechanisms such as location tracking, smart spaces, and use of surrogates which continuously monitor user actions complicates the privacy protection problem. Indeed, the potential for serious loss of privacy may deter knowledgeable users from using a pervasive computing system [8, 9].

[*] This research was partially supported by ITRC, # 500/8478

Manuscript received December 5, 2006.
Manuscript revised December 25, 2006.

Increasing relationships and interactions among individuals in pervasive computing environments (PCEs) inspires the idea of multi-determiner private data. The great amount of private data in PCEs may be related to and ruled by multiple entities; each ruler or determiner may be the data owner or any other entity authorized to affect the decision of data disclosure. In order to clarify the concept of multi-determiner data, consider a typical smart laboratory in a pervasive hospital in which patients personal data and research-related data are under the control of patients, laboratory managers, related physicians, and hospital rules. Any decision about disclosure of such data is based on the preferences of all these determiners. We can recognize three types of determiners namely: *data owners*, *data deputies*, and *environment*. Data owners are individuals (such as patients, managers and physicians) having the primary responsibility for determining rules of data disclosure. The owners may delegate their responsibility to any trusted individuals called deputies. Environment may also influence the disclosure decision.

There are two probable approaches to deal with data disclosure rules defined by multiple determiners of it. In the first approach, a meta-preference representing a de-conflicted version of preferences may be created before and used throughout the evaluation process. This approach, however, imposes a high cost of conflict resolution to the system. An alternative approach, which is presented in this paper, deals with different sets of determiners preferences rules in the execution time and based on the coming data request.

In this paper we investigate the necessity of dealing with different determiners and the requirements of multi-determiner protection of private data. We propose an applicable procedure to runtime management of decision making process and convergence of choices in the presence of multiple determiners. We analyze the efficiency and applicability of the solution by offering a graph-based representation of the process. A prototype implementation of our multi-determiner protection system is also presented.

The rest of this paper is organized as follows. In the next section, we presented a simple scenario to indicate the necessity of multi-determiner data protection and investigated the categories of determiners. In section 3 the required fundamentals for realizing such protection is proposed, including the ownership information file, the operators, and the new way of responding a request, namely the DELEGATION behavior. Using these meta-data, a conflict-free deadlock-free protection procedure is proposed in section 4 and its efficiency is evaluated. In section 5, an architecture for a multi-determiner protection system is devised and its implementation is consequently demonstrated. In section 6 we present a discussion of some related approaches and our extension to them. Finally, conclusions and future work are given in section 7.

2. Multi-Determiner Private Data

In this section, three categories of entities which are authorized to determine rules of data disclosure are investigated. To clarify the issue, a smart hospital in PCE is illustrated.

2.1 The Smart Hospital Scenario

Consider a laboratory in a hospital which is full of smart devices. Patients are instrumented with vital-sign monitors and with a means of determining their location. Physicians and nurses have wireless PDAs, also instrumented with a means of determining their location. The managers of this laboratory are Prof. Mead and Prof. Butler who conduct some medical researches on groups of volunteer patients. They track experiments through their hand-held devices wherever they are.

There are two types of private data in this scenario which has to be protected against unauthorized access, namely: *patients health-related data* and *experimental data*. Laboratory privacy protection system (LPPS) is responsible for controlling the disclosure of such data. Suppose a journalist tries to access the current condition and results of an experiment by connecting to the laboratory information system (LIS). Upon receiving his request, LIS calls the LPPS to evaluate the situation and make the right decision. Based on a set of rules, LPPS should refer to privacy preferences of Prof. Mead and Prof. Butler as primary determiners in deciding about laboratory's private data (data owners). Prof. Mead's preference file indicates that he agrees to disclose any item of experimental data for non-commercial purposes. However, Prof. Butler has more strict rules. He prefers to delegate the responsibility of decision making in case the requester is about to publish the experimental data. Dr. Brown and Dr. Lee are two professionals assigned by Prof. Butler to further investigate the situation and decide properly. So, LPPS seeks the preferences of these deputies to fulfill their goal. Based on the preferences of these four determiners, and rules of the laboratory, LPPS allow or forbids the journalist to access the requested data.

2.2 Private Data Determiners

Current privacy protection systems support a single set of preferences rules usually pertinent to data owner's desires or representing meta-preferences of a group. They assume that the only one who can determine the rules of data disclosure is its owner (or meta-owner in general). However, actual process of privacy decision making may depend on the distributed rule-sets, defined by multiple determiners of a datum. Moreover, these approaches can not model scenarios in which a data owner appoints or consults others to decide about her/his private datum. To address these issues, we first investigate different authorized determiners of private data. The determiners can be categorized into these three classes: Data Owners, Data Deputies, and the Environment.

2.2.1 Private Data Owners

Owner of a private data is an individual or organization who has the main responsibility and authority over the data. Owners of private data are the indisputable determiners of it. They are the only authorized entities to assign data disclosure rules (privacy preferences) and can authorize other individuals to determine these rules. Private data in PCEs may have multiple owners. For example, in the smart laboratory scenario, managers of the laboratory, Prof. Mead, and Prof. Butler, are owners of laboratory private data controlling its privacy; in the other words, each professor has the right to determine her/his own preferences to control the disclosure of the data.

2.2.2 Private Data Deputies

By delegating the responsibility of decision making, data owner allows another individual namely the deputy, to decide about the disclosure of her/his data. Therefore, the protection system refers to the preferences of deputy to make the decision. In our scenario, Dr. Brown and Dr. Lee are deputies to decide about publishing the experimental data.

2.2.3 Environment

The environment in which data request takes place may enforce special rules regarding the disclosure of private data. Due to the fact that every location in PCEs may require some private data in exchange of providing some services and my force some rules regarding private data disclosure, there is no other choice except either accepting these rules or being blocked against these services. So the environment can be regarded as a potential determiner in the process of data protection. In the hospital scenario, there may be special rules in each laboratory room which impose the disclosure of private data to a specific group of requesters in definite situations. For example, the hospital may have special rules which enforce disclosure of experimental data to Prof. Gabel, head of the hospital.

2.3 Requirements of a multi-determiner privacy protection system

Multi-determiner protection of private data refers to the process of finding the decision of each determiner about hiding or disclosing private data and combining them to reach a common opinion. Since multi-determiner private data are governed by multiple entities, a protection mechanism should be devised to gain the consent of each determiner in order to disclose the data; therefore, it is required to clarify the answer of two questions for the protection system:

- Who are the primary determiners of the requested data?
- Who are the deputies of the data?
- How to converge on a shared decision among the determiners?

The answer to these two questions makes the bottom layer of the protection process. The proposed mechanism to cover these questions requires a set of assisting meta-data as well as a suitable management algorithm which are explained in the next section.

3. Fundamental Elements of a Multi-Determiner Privacy Protection System

The concept of multi-determiner protection of private data can be added to a variety of privacy protection systems which tend to work in environments having shared private data which are controlled by multiple determiners. In this section, we propose a set of meta-data to satisfy the requirements of a multi-determiner privacy protection system.

3.1 System Meta-Data

Indicating determiners of a multi-determiner data and the mechanism of converging on a shared choice is a major step in designing the multi-determiner privacy protection system. The following set of metadata can be added to the current policy-based solutions of privacy to satisfy this requirement.

3.1.1 Ownership Information

Protection of private data is primarily based on the preference rules defined by its owners. Therefore, the first step towards protecting a private data is identifying its owners and evaluating their preferences. There may be a number of approaches to overcome this problem. We propose using a kind of meta-data which we call *ownership information* to provide information about owners of each private data item. This information includes data owners identity, and a reference to their preferences file. Ownership information files can be maintained in a database and retrieved in the time of evaluating a data request, to indicate the controlling process.

3.1.2 Organizing Operators

Each determiner may have a different attitude in deciding about hiding or disclosing a data item in a given condition and this may lead to a conflict between determiners choices. However, reaching the final decision requires converging on a choice by establishing a proper conflict resolution mechanism. It helps the system to recognize how to deal with possible disagreements.

For this reason, we propose a number of operators which help conflict resolution by showing the organization of determiners in deciding about a specific request. We introduce three types of operators namely ALL, MAJORITY, and ONE.

ALL is used when consent of all determiners is required to accept or reject a data request. In this case, if all determiners agree/disagree to disclose a requested data, the request is accepted/rejected. However, if there is no consensus among determiners, the request is rejected.

MAJORITY states that most of the determiners should agree to accept or reject a data request. This agreement indicates the final decision.

And, ONE is used when one of the determiners is sufficient for making the final decision. The determiners will be asked in order; if one of them made a decision, the final decision is achieved. But if the decision could not be obtained from a determiner for any reasons, privacy protection system tries to get the decision of the next determiner in the list.

3.1.3 Behaviors

Behaviors indicate the activity taken upon successful matching of a rule in a determiner's preferences. Our system supports three behaviors and three rule types corresponding to each behavior. The behaviors are described as follows:

- ACCEPT: this behavior shows that the request for private data is accepted and the system will send out the requested data to the requester.
- REJECT: this behavior shows that the request is not accepted and the requester will be blocked from accessing the requested data.
- DELEGATE: in addition to the common ACCEPT and REJECT behaviors considered in the current protection approaches, we propose the DELEGATION behavior to deal with the situations in which a determiner desires to delegate the responsibility of decision making to others, named deputies. The deputies list and their organization are indicated in the body of the DELEGATION type rule.

3.2 Data Protection Rules

Data protection rules are required to control the disclosure of data. These rules include privacy preferences of determiners and environment rules. Evaluation of such rules informs the privacy protection system about the intention of determiners regarding the disclosure of their private data.

3.2.1 Privacy Preferences

Preferences are rules assigned by each determiner of private data to show the circumstances in which s/he agrees to disclose her/his data. These rules are used by the privacy protection system to automatically decide based on the desires of the determiners. Since protection of private data greatly depends on the preferences rules, it is important to devise a suitable structure that allows determiners to define any desired rules. The preferences language presented in this paper is an XML-based structure which describes rules of ACCEPT, REJECT, and DELEGATE type. The BNF representation of the language is as follows:

```
ruleset     = '<RULESET>'
                1..* rule
                otherwise
              '</RULESET>'
rule        = '<RULE behavior="' behavior '">'
                data_group
                request_group
                policy_parameters
                contextual_condition
                [deputies]
              '</RULE>'
otherwise   = '<otherwise behavior="' behavior '"/>'
```

The behavior property of *<RULE>* (described in the previous section) determines the type of the rule that is the behavior of the system in the presence of particular conditions.

Having many types of private data and a large number of data requesters in pervasive computing, it is a good idea to permit determiners to define desired rules based on data categories instead of a specific data item. The number of rules will decrease considerably in this way and the complexity of specifying and controlling them will be consequently reduced. Each rule describes the determiner's preferences to disclose a special category of private data to a specific group of requesters. The rule contains the preferred values of policy parameters that should be matched with the information available in requester's privacy policy. It also describes the contextual situation in which the rule will be fired.

Rules of user preferences are being evaluated orderly from top to bottom. When a rule is fired the evaluation will end and therefore the system does not face a conflicting rule. The priority of a rule is determined by its precedence in the rule sequence. If neither of the rules is applicable, a default rule is fired (otherwise) which is a rule without any specified conditions and simply shows the behavior that should be applied whenever no other rule is selected.

3.2.2 Environment Rules

Environment rules are composed of a number of rules provided by the environment which influence the decision of determiners. A typical environment rule states that *which group of determiners should disclose which category of their private data to which requester groups under which circumstances*.

Respecting such rules is one of the advantages of our work. It makes the interaction between data owners and environment services easier.

3.3 Data protection information

Data protection information refers to the information needed to evaluate the data protection rules. This information may be relevant to data usage promises of requester specified in her/his privacy policy, contextual information provided by context manager, or the organization of user groups and data categories defined by data determiners.

3.3.1 Privacy Policy

P3P [14] is a standard protocol, providing a mechanism for Web sites to specify their privacy practices (privacy policy) in a machine-readable format. In our solution, we suggest using P3P standard to define requester's privacy policy in order to take advantage of its widely accepted use, availability of supportive tools [17], and its extensibility.

To increase the expressiveness of P3P policies, we suggest adding an extension to its *retention* element to indicate the quality of data maintenance, which is an important factor for a determiner when deciding about disclosure of data. The *<RETENTION-TYPE>* extension is as follows:

```
'<EXTENSION optional="yes">'
    '<RETENTION-TYPE>'
        retention type
    '</RETENTION-TYPE>'
'</EXTENSION>'
retention type = encrypted
```

3.3.2 Contextual Information

Contextual information is a kind of meta-data that is related to items (e.g. individuals, events, etc). In our work we refer to context as the circumstances that influence the decision of determiners. Some examples would be time of the request, location of the requester, and the situation of environment and its involved entities. In general, condition of determiners, requesters, and environment are determining factors in deciding about data disclosure. For example, in the smart hospital scenario, Prof. Mead may want to prevent the monitors in the patient's room from showing the patients health related data whenever an external visitor is in the room.

3.3.3 Knowledge of Data Categories and User Groups

It is not applicable for a determiner to define her/his preferences for each specific item of data or each requester one by one. Data categories and user grouping information

help defining the protection rules in a group-based manner. This kind of information determines the organization of private data and their possible requesters and will be used at the time of evaluating determiners preferences file.

4. Multi-Determiner Protection Procedure

In this section, the process of managing multiple determiners in answering a specific request is discussed. And the conflict resolution and delegation management algorithms are presented.

4.1 Multi-Ownership and Delegation Management Algorithm

Protection of multi-determiner private data requires proper management of multiple owners and the delegation scenario in answering a data request. The management algorithm initiates by indicating primary determiners of the data and continues along with evaluating each determiner's preferences. The algorithm is based on a graph representation of the delegation scenario called the delegation graph:

G (V, E) = the delegation graph
En ∈ Set of Determiner Entities
Op ∈ {ALL, MAJORITY, ONE, NULL}
visited ∈ {True, False}
behavior ∈ {ACCEPT, REJECT, DELEGATE, NULL}
$V \subseteq En \times Op \times visited \times behavior$
$E \subseteq V \times V$

The graph represents the authorized owners and deputies of a datum in the context of a specific request. Each node stands for a determiner, with the behavior her/his preferences file suggests for the current context. *(NULL, op, True, NULL)* represents notation of the starting node which tends to show the organization of owners by *op*. Every node with a *(en, op, True, Delegate)* style shows a delegation from en determiner to some deputies organized as *op*. Every node with a style of *(en, NULL, True, bhvr)* presents a determiner who has accepted or rejected the request and her/his selected behavior is determined by *bhvr*.

The management algorithm starts by evaluating the ownership information file which indicates the owners and their organization as specified by the organizing operator. This information is used to make the primary delegation graph. The process then continues by examining each node that is evaluating each owner's preferences file. If the owner's selected behavior is ACCEPT or REJECT, the result is assigned to the behavior parameter. However, if it is DELEGATE, preferences of the deputies should be investigated. Therefore, the execution thread adds a new set of nodes to the primary delegation graph and starts the evaluation process on this new set. The overall management process is done in a depth first style so that the ACCEPT or REJECT decision of each determiner is achieved before moving to its sibling. Completing the evaluation of all the children of a given node, the organizing operator is applied by the parent node and the final decision is achieved.

We can consider each node as an evaluator which evaluates the preferences of a determiner and assigns the result to the *behavior* variable. When the execution thread reaches a new node, it returns the behavior variable to the parent node (the delegator) if it has been evaluated, or asks the node to calculate it otherwise.

The visited parameter determines whether the node has evaluated the preferences and specified the behavior. A visited node do not met twice in the above algorithm. If the execution thread reaches a previously met node, it returns the behavior specified in behavior parameter without evaluating the preferences file one more time. This will reduce the overall time of the algorithm. The average time required for answering a specific request is equal to the number of visited nodes (determiners) multiplied by the average time required for processing each node, that is evaluating a preferences file. Assuming *n* as the number of visited determiners, the order of algorithm is *O(n)*.

Figure 1 illustrates the delegation graph which is created during the evaluation of the journalist's request, presented in the smart hospital scenario.

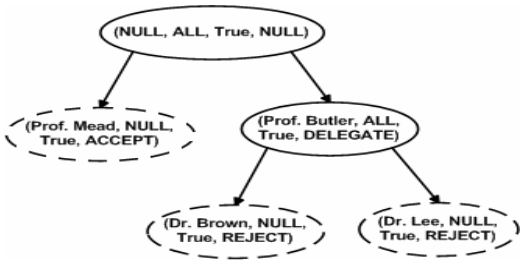

Fig. 1 Delegation Graph Sample.

4.2 Deadlock Resolution

One problem of the described algorithm could be a possible situation in which a loop occurs in the delegation scenario. Assume a chain of delegations in which last deputy is the first; this image shows a dependency

between decisions of different deputies that prevents the system from reaching a final ACCEPT or REJECT result. Our delegation management algorithm presents a simple solution to overcome this problem.

When the execution thread reaches a node which has been visited before, it returns the answer specified in the answer field if it is ACCEPT or REJECT; but if the answer is DELEGATE, a loop have been detected and is resolved by returning default answer of the node. This answer can be specified by adding a *default−answer* field to each node of the graph. The answer can be specified from an additional property of the preferences rules, called the *default−behavior*.

This approach reflects what an individual usually does in real world situations. S/He may ask others to decide on behalf of her/him or help her/him made a proper decision. But in the case nobody can make a suitable decision, s/he should decide anyway.

There are many alternative solutions to overcome this problem in general. A programmer can choose between these approaches while implementing the framework depending on the target environment. For example, another solution would be simply rejecting the request in such situations. This resolution is helpful in protecting highly sensitive private data. In this way the privacy of data will not be jeopardized by a false disclosure.

4.3 Conflict Resolution

In this section, the conflict resolution scheme of the multi-determiner privacy protection system is explained. There are three kinds of conflicts among data protection rules:

- Conflicts between environment rules and preferences of the determiner.
- Conflicts between two or more determiners.
- Conflicts between the rules defined in a determiner's preferences file.

The first category of conflicts is resolved by assigning a priority between environment and determiners. As discussed before, environment rules are often dominant. So our protection procedure begins with the evaluation of these rules and if they don't limit determiners to do a specific activity, it continues with evaluating determiners preferences. Evaluating determiners may raise the second type of conflicts which are resolved with the help of organizing operators, explained before. In addition, conflicts in a determiner's preferences rules are resolved by the traditional conflict resolution approaches. For example, the newest policy may be dominant, or the most specific rule may be preferred.

5. Prototype Implementation

To realize the multi-determiner protection of private data, we developed a multi determiner protection system for PCEs. The architecture and prototype implementation of this system are demonstrated in this section.

5.1 Architecture of the Multi-Determiner Protection System

Our multi-determiner protection system is based on the architecture shown in Figure 2. Once an entity requests a data item, the *Request Manager* asks the *Data Interface* to retrieve it. Whenever the requested data is private, the requester must submit the privacy policy along with her/his request. The *Request Manager* sends the request and its policy to *Privacy Protector*. This component is responsible for recognizing owners of the data and evaluating their preferences against privacy policy and contextual information. Combining the results of evaluating the preferences, final decision can be made. If the environment encloses an environment policy, it should also be regarded in decision making process. Final decision would be either accepting or rejecting the request.

The *privacy protector* component depicted in Figure 2 is composed of a number of components which support the multi-determiner nature of our system. For this purpose, it has a *multi-determiner manager* component responsible for the management of multi-ownership and delegation, *environment manager* accountable for evaluating the regulations of the environment and *preferences manager* which evaluates each determiner's preferences against privacy policy of the requester and contextual information.

5.2 Implementation Results

To demonstrate the feasibility and usefulness of our approach we have implemented the main components of the presented framework. This implementation is not meant to work in a real environment; instead, it is a prototype implementation done to realize how our

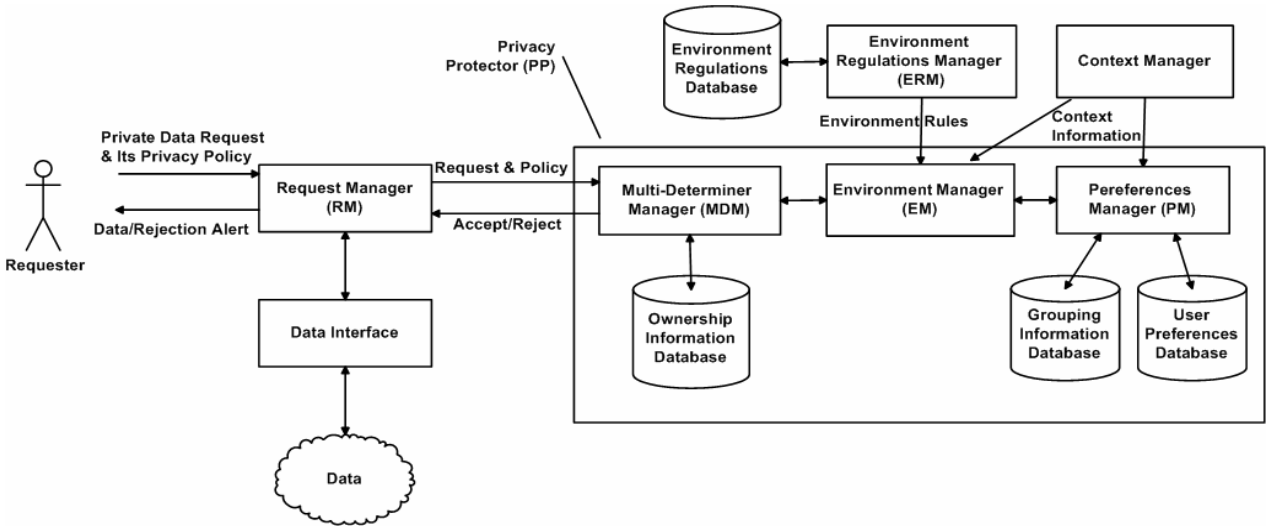

Fig. 2 Multi-Determiner Privacy Protection System Architecture

architecture is responding to what will happen in real data protection scenarios and can be touched slightly to make an operational application devoted to the target environment. It is obvious that to make this implementation answer the requirements of a perfect privacy protection system in a PCE, one should add more details to the presented implementation. Figure 3 shows a screen capture of the interface of the implementation which can be used either to define privacy related meta-data, or to check out the matching process upon receiving a request.

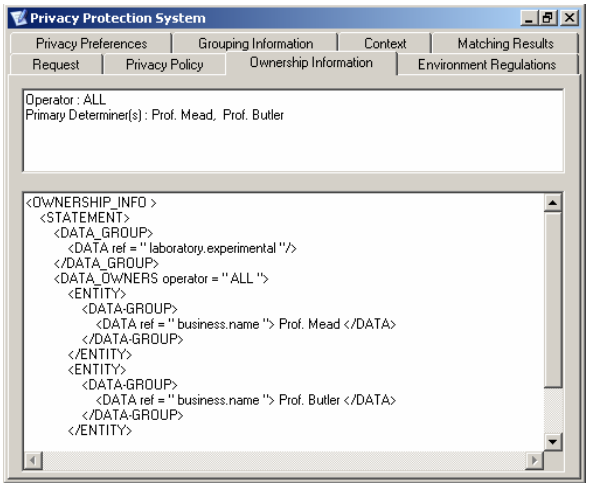

Fig. 3 Screen Capture of the Privacy Protection System

6. Related Work and Discussion

As privacy threats increase by ever increasing integration of new technologies into our lives, various computer-based techniques emerge for privacy protection. Files, emails, and other private records can be encrypted. Anonymity and pseudonymity tools are used to prevent users actions from being linked to their identity while interacting with their favorite services [10]. In addition, there are filters and noise introducing mechanisms to decrease the accuracy of private data which leads to reduce privacy threats [11]. Privacy issues of specific applications, environments, and also specific kinds of data are investigated and numerous privacy preserving platforms are presented. Privacy preserving mobile applications [12], privacy aspects of RFID systems [13], and location privacy [10] are examples of such research.

P3P1.0 and 1.1 [14] provide a syntax for specifying privacy policies and a mechanism for associating policies with Web resources. However, they do not specify how the user preferences can be expressed and be matched with a policy file. A P3P Preference Exchange Language (APPEL) developed by W3C is a language for describing user preferences which can be interpreted by P3P agents and consequently compared to sites P3P policies [15]. Based on the APPEL language, there are a number of privacy protection software applications, such as AT&T Privacy Bird [16] and P3P toolkit by Joint Research Center [17]. For example, AT&T's Bird is a client-side software which enables a user to configure her/his basic privacy preferences on her/his own machine. The user preferences are expressed in an APPEL rule-set, which is compared with the policies of the visiting Web site.

In 2002, a privacy awareness system (PawS) for pervasive computing was developed by W3C's researcher, Marc Langheinrich, which allows data collectors to both announce and implement data usage policies, as well as providing data subjects (owners, in our literature) with

technical means to keep track of their personal information as it is stored, used, and possibly removed from the system [18]. Supporting various types of data, as well as diversity of requesters from users to applications in PCEs, are some advantages of PawS. In addition, Privacy proxies, policy-based data access through PawDB, privacy announcement mechanisms such as Jini-integrated policy links, privacy beacons to announce the privacy policies of explicit and implicit data collections, keeping track of all data collections by users personal privacy assistant, and automatically enabling or disabling optional PCE services based on the users preferences, are advantages of PawS as a privacy protection system for PCEs.

In 2005, Hong et. al. designed a plug-in service for the middleware in pervasive computing and implemented a simple application called ”find-a-friend” to manage the inquiries about the location information of friends in a manner that preserves the privacy of users based on context-aware evaluation of their preferences [19].

Our system extends the concept of determiner in existing policy-based privacy protection approaches by introducing the idea of multi-determinacy in assigning protection rules and deciding about a private data. Therefore, it could be a proper companion for current protection systems such as PawS and the middleware privacy protection system, by introducing an efficient mechanism to context-aware protection of multi-determiner private data in PCEs while utilizing the benefits of such systems like protecting the privacy of context information, policy-based access to private data repositories, or the use of privacy beacons.

7. Conclusions and Future Work

In this paper, we proposed the idea of multi determiner protection of private data in PCEs. We discussed different aspects of multi-determinacy and possible determiner categories. We introduced the case of protecting multi-owner private data in which each owner is a determiner, delegation of authority to deputies, and applying environmental regulations in which the environment influences the decision about the disclosure of individuals private data. We also proposed a proper algorithm to manage protection of private data in the presence of multiple determiners and presented the necessary meta-data to realize the multi-determiner protection process. Besides, we presented our conflict resolution scheme to resolve possible conflicts among determiners. Finally, we implemented a prototype system to show the applicability of our solution to multi-determinacy problem.

Considering the positive results, our future investigation is to create our fully functional privacy protection system which allows examining of the approach with complex, real-world, pervasive computing scenarios. In such a framework, one of the main focuses would be conflict detection and resolution strategies. Improving semantic concepts in our system to simplify the interaction between users is in our list of further research.

References

[1] Warren, S., Brandeis, L.: The right to privacy. Harvard Law Review 4(5) (1890), p. 193–220
[2] Iachello, G.: Privacy and Proportionality. Phd thesis, Georgia Institute of Technology (2006)
[3] Westin, A.F.: Privacy and Freedom. Atheneum, New York NY (1967)
[4] Langheinrich, M.: Privacy by design—principles of privacy-aware ubiquitous systems. In: Proc. Third International Conference on Ubiquitous Computing (UbiComp), Springer-Verlag (2001)
[5] State of California Department of Consumer Affairs: Recommended Practices on Notice of Security Breach Involving Personal Information. (2006)
[6] Brodie, C., Karat, C., Karat, J., Feng, J.: Usable security and privacy: A case study of developing privacy management tools. In: Proc. Symposium on Usable Privacy and Security (SOUPS’05), ACM Press (2005)
[7] Price, B., Adam, K., Nuseibeh, B.: Keeping ubiquitous computing to yourself: a practical model for user control of privacy. International Journal of Human-Computer Studies 63(1-2) (2005) 228–253
[8] Satyanarayanan, M.: Pervasive computing: Vision and challenges. In: Proc. IEEE Personal Communication. (2001)
[9] Adam, K., Price, B., Richards, M., Nuseibeh, B.: A privacy preference model for pervasive computing. In: Proc. First European onference on Mobile Government, Brighton, UK (2005)
[10] Beresford, A., Stajano, F.: Location privacy in pervasive computing. In: Proc. IEEE Pervasive Computing 2003 (PERCOM’03), IEEE Press (2003)
[11] Alarcon, R.A., Guerrero, L.A., Pino, J.A.: Temporal blurring : A privacy model for oms users. In: International conference on user modeling. Volume vol. 3538 of Lecture notes in computer science., Springer (2002) 417–422
[12] Klein, B., Miller, T., Zilles, S.: Security issues for pervasive personalized communication systems. In: Proc. 2nd International Conference on Security in Pervasive Computing. Lecture Notes on Computer Science, Heidelberg, Springer-Verlag (2005)
[13] Garfinkel, S., Juels, A., Pappu, R.: Privacy: An overview of problems and proposed solutions. In: Proc. IEEE Security and Privacy. (2005)
[14] W3C: The Platform for Privacy Preferences 1.0 specification (P3P1.0), http://www.w3.org/tr/p3p. (2002) W3C Recommendation 16 April 2002.
[15] W3C: A P3P Preferences Exchange Language 1.0 (APPEL 1.0). (2002) W3C Working Draft 15 April 2002.
[16] Byers, S., Cranor, L., Kormann, D., McDaniel, P.: Searching for privacy: Design and implementation of a p3p-

enabled search engine. In: Proc.Workshop on Privacy Enhancing Technologies (PET2004), Toronto, Canada (2004)
[17] JRC: JRC P3P Resource Centre Code Downloads, http://p3p.jrc.it/licenceterms.php?download=toolkit. (2004)
[18] Langheinrich, M.: A privacy awareness system for ubiquitous computing environments. In: Proc. Ubicomp 2002, Goteberg, Sweden (2002)
[19] Hong, D., Y.M., Shen, V.Y.: Dynamic privacy management: a plug-in service for the middleware in pervasive computing. In: Proc. Mobile-HCI'05, Salzburg, Austria (2005)

Anis Yousefi received her B.Sc. degree in Software Engineering from Iran University of Science & Technology, Tehran, Iran in 2004. She is currently a M.Sc. student at Sharif University of Technology, Tehran, Iran. Her research interests are Pervasive Computing, Semantic Web, and Information Security and Privacy.

Rasool Jalili received his Ph.D. in Computer Science from The University of Sydney, Australia in 1995. He joined the Department of Computer Engineering, Sharif University of Technology, Tehran, Iran, as an assistant professor. His research interests are Distributed Systems and Information Security.

Mahdi Niamanesh received his B.Sc. and M.Sc. degrees in Computer Engineering from Sharif University of Technology, Tehran, Iran in 1999 and 2001, respectively. He is currently a Ph.D. student at Sharif University of Technology, Tehran, Iran. His research interests are Dynamic Reconfigurable Protocol Stacks and Pervasive Computing.