Trust Based Privacy Protection Method in Pervasive Computing

Feng Gao¹, Jingsha He² and Shunan Ma¹
¹College of Computer Science and Technology, ²School of Software Engineering
Beijing University of Technology, Beijing 100124, China
maple0371@emails.bjut.edu.cn, jhe@bjut.edu.cn, mashunan@emails.bjut.edu.cn

Abstract - In pervasive computing environments, resources and services are usually provided by a variety of different suppliers with multiple computing devices and from heterogeneous networks. Accordingly, various privacy protection methods with lots of privacy policies were used. Before some meaningful interaction starts or services offers, a certain level of trust must be established, this trust establishment and communication process may involve privacy information exchange. Consequently, a method for integrate the privacy protection methods and deal with privacy and trust tradeoff is necessary. In this paper, we propose a novel trust based privacy protection method by using a three levels trust based privacy protection model (TPPM). Our main contributions include: (1) TPPM can integrate the various privacy protection methods and specify privacy policies; (2) TPPM can automatic make privacy disclose decision with achieving the goal of less privacy information loss and more trust gain during the trust establishment and the interaction process; (3) our method can be used in kinds of applications scenarios flexibly. Simulation results and analysis show our method can accomplish privacy preserving and fast trust establishment well.

Index Terms - privacy protection; trust; pervasive computing; ontology; privacy loss entropy; trust gain entropy

I. INTRODUCTION

Weiser [1] described a vision for twenty-first-century computing in which he used the term “ubiquitous computing” and later termed as “pervasive computing.” Pervasive computing envisions an environment in which we are surrounded by many embedded computer devices. Those computing devices provide us with a mobile, spontaneous and dynamic way to enjoy various resources and service which give us tremendous freedom and convenience without aware of them.

As the saying goes every coin has two sides, pervasive computing will exacerbate the privacy problem. Unless privacy is adequately protected, the progress of pervasive computing will be slowed down or derailed altogether, even places people in a monitored environment that mass computing will be slowed down or derailed altogether, even places people in a monitored environment that mass monitors (embedded devices) surrounded with. In pervasive computing environment (PCE), resources and services are usually provided by variety of different suppliers with multiple computing devices and from heterogeneous networks. Accordingly various methods with lots of policies were used to protect privacy. It therefore becomes necessary and important to study the mechanism to integrate privacy protection methods and specify privacy policies.

In PCE, entities (or devices) which make connections and interactions may know little about each other or without prior knowledge at the beginning of communication. Therefore, in many cases, before any meaningful interaction starts or services offers, a certain level of trust must be established. During the trust establishment process, an entity may request some information from other entities that probably involves privacy, which implies some privacy loss for the entities. Therefore, it is clearly that study effective privacy quantification and trust-privacy tradeoff mechanism are very necessary for privacy protection in pervasive computing environment.

Taking these in mind, in this paper, we propose a novel trust based privacy protection method by using a three levels privacy protection model (TPPM). Our motivation is supply a privacy protection method which can be used in PCE with privacy protection methods integration, privacy polices specification and balancing privacy loss and trust gain during the interaction.

The rest of this paper is organized as follows. In the following section, we briefly discuss some related work. In Section III, we exhaustive describe PPTM level by level. In Section IV, we introduce a novel privacy protection method by using TPPM. After that we do some simulations to analyze the performance of the TPPM in Section V. Finally, we conclude this paper in Section VI in which we also discuss some future work.

II. RELATED WORK

Access control which grants access permissions to an authorized user has become an important factor to ensure the security in PCE [2-4]. Automated trust negotiation (ATN) is a new approach to access control and authentication in open, flexible systems, especially in PCE [5], also some researches has been done for privacy preserving in ATN [6-8]. Though the access control methods and ATN can ensure the privacy information not be accessed from the unauthorized entities, some open issues still need to be addressed. In PCE, the user may be
willing to sacrifice some privacy to enjoy some services; consequently, how much privacy can the entities afford to lose in order to getting some services seem as an important issue.

Entropy has been used to mathematically model the minimization of privacy loss [9-12]. In the discussion of privacy-trust tradeoff issue in distributed system, privacy is quantified by categorizing its importance used in trust evaluation [13]. Since trust and privacy are context-dependent, privacy may require that different trust evidence be used to make the decision as to how to deal with different application scenarios. Unified trust values or a simple trust rank is insufficient for making privacy disclose decision.

Initially, ontology was introduced as a method for “explicit specification of a conceptualization” [14], now, ontology widely used in computing domain to solve the issues of information classification, information integration, policy description and so on [15-17].

III. TRUST BASED PRIVACY PROTECTION MODEL

In this section, we will introduce a trust based privacy protection model (TPPM) that includes the aggregation and abstract level, the privacy loss and trust gain quantification level, and the decision level. The architecture of TPPM is illustrated in Fig.1.

A. Aggregation and Abstract Level

Aggregation and abstract level is in the bottom of TPPM, it adopts ontology method to aggregate various privacy policies which are used in different privacy protection methods, and it also abstracts the privacy policies by the semantic way to create privacy policy ontology and privacy information ontology.

Definition 1. Trust evidence is the information which can offer trust for the communication parties. Tokens submitted and certificates exchanged during the authentication process or communication, and any history records of interaction etc all can be considered as the trust evidence. In our aggregate and abstract approach, we consider trust evidence as an attribute of the privacy ontology.

Privacy policy ontology describes the category of privacy policies. Privacy policies are abstracted as privacy policy ontology with the attribute of trust evidence that is described as a policy in which “trust value” is an attribute named trust evidence that is higher level is always enforced at the low levels. Also as illustrated in Fig. 2, if Policy 1 adds a new attribute, say Trust evidence 3. Trust evidence 3 must be included when Policy 1.2 is enforced.

Privacy ontology describes the privacy information category with its attributes named trust evidence that is needed for privacy disclosure. The privacy ontology is illustrated in Fig.3 in which P1 represents class 1 of privacy information and P1.1 represents a subclass of P1 having the inherited function from P1.

Property 1. (Inheritance Property): A child has the inheritance relationship with its parent. As illustrated in Fig.2, if Policy 1 calls for the Trust evidence 5, Policy 1.1 and Policy 1.2 will inherit this demand.

Property 2. (Mandatory Property): The policy of a higher level is always enforced at the low levels. Also as illustrated in Fig. 2, if Policy 1 adds a new attribute, say Trust evidence 3, Trust evidence 3 must be included when Policy 1.2 is enforced.

Privacy ontology describes the privacy information category with its attributes named trust evidence that is needed for privacy disclosure. The privacy ontology is illustrated in Fig.3 in which P1 represents class 1 of privacy information and P1.1 represents a subclass of P1 having the inherited function from P1.

Property 3. (Default Property): An upper-class’ default policy is inherited and enforced by a subclass if and only if the child doesn’t have the corresponding policy. In Fig. 2, if the constraint of Policy 1.1’s conflicts with that of Policy 1’s, Policy 1.1 won’t inherit Policy 1’s constraint.

Property 4. (Conflict Avoiding Property): During the aggregate process, if two piece of privacy polices are conflicted, deal with that as follows. Suppose that policy A controls the privacy information \( P_A \{ p_1, p_2, ..., p_m \} \) and needs trust evidences \( r_{A} \{ t_1, t_2, ..., t_k \} \), while policy B controls the privacy information \( P_B \{ p_1, p_2, ..., p_n \} \) needs trust evidences \( r_{B} \{ t_1, t_2, ..., t_j \} \). If \( \exists p_j : (p_j \in P_A) \lor (p_j \in P_B) \) let policy A controls \( p_j \) and delete \( p_j \) from \( P_B \{ p_1, p_2, ..., p_n \} \).

Figure 1. Architecture of TPPM
B. Privacy Loss and Trust Gain Quantification Level

With privacy policy ontology and privacy ontology created in the aggregation and abstract level, we can quantify privacy loss and trust gain during trust establishment and interaction process based-on information theory conveniently.

Definition 2. We denote the trust that the interaction counterpart should be achieved when disclosing one piece of privacy as $T_b$, the trust that the counterpart has already been achieved before the privacy disclosure as $T_a$ and the counterpart's trust variation for the entity after the disclosure of privacy as $T_c$.

Definition 3. Conditional probability $p_1 = \text{prob}(T_a | T_b)$ denotes the probability of achieving $T_a$ under condition $T_b$.

Definition 4. Conditional probability $p_2 = \text{prob}(T_c | T_b)$ denotes the probability of achieving $T_c$ under condition $T_b$.

Definition 5. Set $T_{\{e_1, e_2, \ldots, e_n\}}$ denotes the trust evidences that are needed when disclosing one piece of privacy information.

Definition 6. Entropy is a quantitative measure of information content and uncertainty over a probability distribution.

Assume that entity A needs entity B to achieve trust level $T_a$ before disclosing to it a piece of privacy and A currently trusts B at level $T_b$. And $P_1 = \text{prob}(T_a | T_b)$ is the probability of entity B achieving $T_a$ under condition $T_b$. Then let’s consider two situations:

If $T_b ≥ T_a$, then $p_1 = 1$ and $\log p_1 = 0$. We considered this situation as no privacy information loss.

If $T_b < T_a$, it means that would lead to privacy information loss when the information is disclosed.

Under the second situation above, disclosing the privacy needs some trust evidences, $P_U = \text{prob}(T_a | T_b)$ represent the $i^{th}$ trust evidence’s conditional probability when disclosing the privacy information. Let $p_1, p_2, \ldots, p_n$ denote the original values of conditional probability $p_U$. Then

$$P_U = \frac{p_1}{p_1 + p_2 + \ldots + p_n}, \quad (k = p_1 + p_2 + \ldots + p_n) \quad (1)$$

We use entropy $H_1$ to denote privacy information loss:

$$H_1 = -k \left( \sum_{i=1}^{n} p_i \log p_i \right) \quad (\sum_{i=1}^{n} p_i = 1, k = p_1 + p_2 + \ldots + p_n) \quad (2)$$

Entropy $H_1$ expresses average information loss when disclosing a piece of privacy. A bigger $p_i$ indicates less privacy information loss and a higher probability of achieving $T_a$ with $T_b$.

Privacy disclosure can lead to change to trust levels. We use $P_{2i} = \text{prob}(T_{ci} | T_b)$ to represent the conditional probability of $i^{th}$ trust evidence’s trust gain variation when this piece of privacy is disclosed. Let $p_1, p_2, \ldots, p_n$ denote the original values of conditional probability $P_{2i}$, we preprocess the conditional probability as follows:

$$P_{2i} = \frac{p_i}{p_1 + p_2 + \ldots + p_n}, \quad (g = p_1' + p_2' + \ldots + p_n') \quad (3)$$

We use entropy $H_2$ to denote trust gain:

$$H_2 = -\left( \sum_{i=1}^{n} P_{2i} \log P_{2i} \right)$$

$$\left( \sum_{i=1}^{n} P_{2i} = 1, g = p_1' + p_2' + \ldots + p_n' \right) \quad (4)$$

Entropy $H_2$ expresses average trust gain by disclosing a piece of privacy. A bigger $p_2$ indicates more trust gain since it indicates low uncertainty for gain $T_c$ which means more trust gain when disclosing a piece of privacy.

In PCE, in many cases before any meaningful interactions start, a certain level of trust must be established. Intuitonally, the entities may want to lose less privacy to achieve the desired trust. On the other hand, entities want to disclose privacy information to gain more trust in the trust establishment process. We use $H$ to represent the relationship between privacy information loss $H_1$ and trust gain $H_2$ as expressed below:

$$H = \alpha H_1 + \beta H_2 \quad (\alpha + \beta = 1) \quad (5)$$
C. Decision Level

The decision level is on the top of the privacy protection model that gives privacy discloser decision automatic that based on the two lower levels. This decision level obeys four basic rules during the decision process.

Rule 1. (Default Rule): If the interaction entity’s trust satisfied the constraints of the trust evidences, disclose this privacy information.

The default parameter is \( a = \beta = 0.5 \) that to balance privacy and trust in the privacy loss and trust gain quantification level.

Rule 2. (Granularity Control Rule): If the \( L_i \) level privacy information of privacy ontology does not satisfied privacy disclosure demand by privacy policy while \( L_j (j < i) \) level privacy information satisfied, iff there should be disclose some privacy or the interaction will be ended (the user want to continue the interaction), allow disclose \( L_j \) level privacy information.

Rule 3. (Minimum Privacy Rule):

(1) If both level \( L_i \) and level \( L_j (j < i) \) privacy information of privacy ontology satisfied privacy disclosure demand by privacy policy, and only one piece of privacy information should be disclosed, deny \( L_i \) level privacy information disclosed.

(2) If some privacy information satisfied the demand of privacy policies and not all of privacy information should be disclosed, disclose the privacy information which privacy loss entropy is less.

(3) If the requested privacy information does not satisfied privacy policies and it must disclose some privacy information, disclose privacy with privacy loss entropy descending order step by step.

Rule 4. (Parameter Selection Rule): If the user need to trade privacy for trust, i.e., to sacrifice privacy in order to achieve a certain level of trust, adjust the parameter as \( a < \beta \). If the priority of interaction is to protect privacy, adjust the parameter as \( a > \beta \).

Rule 5. (Priority Rule): The priority of decision rule is default rule, granularity rule, and minimum privacy rule. The priority of minimum rule is (1), (2) and (3). If the privacy disclosure decision under rule 1, rule 2 and rule 3 can not satisfied the interaction demand, user rule 4 to change parameters in order to achieve the interaction.

IV. PRIVACY PROTECTION METHOD

In PCE, use our trust based privacy protection method can protect privacy effectively also with fast trust establishment. We abstract the user and the service provider (or interaction entity) as privacy owner and privacy requester respectively. The process of our trust based privacy protection method is as follows.

Step 1: The privacy requestor send privacy access request to the privacy owner;

Step 2: The privacy owner check the trust evidences that needed for access privacy information by the TPPM.

Step 3: The TPPM check privacy ontology and then notify the trust evidences that needed for privacy accessing to the privacy requestor;

Step 4: The privacy requestor submit some trust evidences to the privacy owner;

Step 5: The trust model do the trust evaluation based on the submitted trust evidences, and then transfer the trust evaluation result to TPPM;

Step 6: The TPPM make privacy disclosure decision based on trust evaluation result.

In fact, the process of negotiation between the trust evidences request and submission is complex, we simply illustrate this flow in Fig.4. After trust evidences negotiation, our TPPM will give the decision of privacy disclosure.

Figure 3. Process of Privacy Protection Method

V. SIMULATION RESULTS AND ANALYSIS

In this section we will do some simulations to analyze the performance and the effect of privacy protection by using our method.

We simulate our trust based privacy protection method by using TPPM in Location Based Service application scenario. In LBS application, the information that submitted and the query action may contain privacy. We consider both the information submitted and the query action which contain privacy as a piece of privacy information to understandable. In simulations, we compare the TPPM’s performance of privacy protection.
(described by privacy loss entropy) and trust establishment (described by trust gain entropy) to recently trust based privacy protection researches [11-13] (we record this as DPEP in simulations) that disclosure privacy under the same trust level with equally probability.

The following assumptions have been made during the simulations. The disclosure of one piece of privacy information requires 3 trust evidences. The disclosure of privacy information is randomly chosen from privacy information set. The conditional probability is computed based on the Bayes net in which we use the random number between 0 and 1 as the value of conditional probability in the simulation. There are 10 pieces of privacy information in privacy information set.

Table I.

<table>
<thead>
<tr>
<th>Selecting</th>
<th>Privacy Loss Entropy</th>
<th>Trust Gain Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min</td>
<td>Ave</td>
</tr>
<tr>
<td>1 from 10</td>
<td>0.08</td>
<td>0.16</td>
</tr>
<tr>
<td>3 from 10</td>
<td>0.43</td>
<td>0.64</td>
</tr>
<tr>
<td>5 from 10</td>
<td>0.76</td>
<td>1.05</td>
</tr>
<tr>
<td>7 from 10</td>
<td>1.10</td>
<td>1.34</td>
</tr>
</tbody>
</table>

Table 1 illustrates four cases of privacy loss entropy and trust gain entropy compare the extreme situation of TPPM (disclose privacy information with minimum privacy entropy and disclose privacy information with most trust gaining) to randomly choosing privacy information for disclosure with running 50 rounds.

We can see that in the extreme situation, in order to protect privacy strictly TPPM can always choose the privacy information with minimum privacy entropy to disclose. In the other extreme situation that to achieve trust establishment fast, TPPM can disclose privacy information with most trust gaining. We can conclude that TPPM can achieve the goal of protect privacy strictly or fast establish trust with privacy preserving, and it has better performance compare to DPEP. In addition, this situation has a premise that this privacy discloser does not violate the decision rules of TPPM.

Then we analyze the normal situations. In case 1, we choose the parameter $\alpha = \beta = 0.5$ to balance privacy and trust in TPPM that compare privacy loss entropy and trust gain entropy to DPEP. The x-axis denotes the count of privacy disclose choice, e.g. "1" denotes selecting 1 piece of privacy from 10, "2" denotes selecting 2 pieces of privacy from 10 etc. We record privacy loss entropy and trust gain entropy in y-axis respectively which illustrated in Fig. 5. We can see that TPPM’s privacy loss entropy is less than DPEP which means better privacy preserving, and TPPM’s trust gain entropy is more than DPEP which means more trust gain by doing privacy disclosure decision.

Then we analyze the situation of the TPPM’s parameter selection. In case 2, we simulate the scenario that trade privacy for trust, i.e., to sacrifice privacy in order to achieve a certain level of trust. So we choose the parameter $\alpha = 0.4, \beta = 0.6$ and $\alpha = 0.3, \beta = 0.7$ respectively. The x-axis denotes the count of privacy disclose choice while the y-axis denotes privacy loss entropy and trust gain entropy respectively in Fig.6. We can see that, the bigger $\beta$ the more privacy loss and more trust gain.

Case 3 simulates the scenario that the priority is to protect privacy, so we choose the parameter $\alpha = 0.6, \beta = 0.4$ and $\alpha = 0.7, \beta = 0.3$ respectively. The x-axis still denotes the count of privacy disclose choice while the y-axis denotes privacy loss entropy and trust gain entropy respectively in Fig.7. It is clear that the bigger $\alpha$ the less privacy loss, and with bigger $\alpha$ the trust gain is less.

Figure 5. Comparison of TPPM to DPEP
Consequently, we can conclude that our TPPM has better performance in privacy protection and trust establishment compare to recently trust based privacy protection researches [11-13] that disclosure privacy under the same trust level with equally probability. And with parameters adjustment, TPPM can achieve privacy preserving and fast trust establishment well.

VI. CONCLUSION

Pervasive computing give us tremendous freedom and convenience without aware of the computing devices. Unless privacy is adequately protected in pervasive computing environment, it may places people in a monitored environment that mass monitors (embedded devices) surrounded with. In this paper, we proposed a trust based privacy protection method by using a three level trust based privacy protection model (TPPM). This model adopts ontology method to create privacy policy ontology and privacy ontology aiming at integrates privacy protection methods and specifies privacy polices. TPPM applies entropy computing mechanism to quantify privacy loss and trust gain before privacy disclose with the goal of balance privacy loss and trust gain during the interaction. It can make privacy disclose decision automatic with achieving privacy protection and fast trust establishment. Then we do some simulations to analyze the performance of TPPM. According to the simulation results and analysis, we can conclude that the trust based privacy protection method can achieve privacy preserving and trust establishing well.

In the future, we will further refine our method through implementation and applications. And we will analyze the complexity and cost of our method; refine our method to balance privacy preservation and its additional cost.

REFERENCES


Feng Gao received her B.S. degree in e-business engineering from PLA Information Engineering University in 2007. She is currently working towards the Ph.D. degree with the School of Computer Science and Technology, Beijing University of Technology. Her research interests include network security, privacy protection and trust etc.

Jingsha He is a Professor of the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. He received his doctorate from the University of Maryland at College Park in 1990. Prior to joining BJUT in 2003, he worked for IBM, MCI Communications and Fujitsu Laboratories engaging in R&D of advanced networking and computer security. His interests include methods and techniques that can improve the security and performance of the Internet.

Shunan Ma is a Ph.D candidate in the College of Computer Science and Technology at Beijing University of Technology, Beijing, China. She received her B.S. degree in Qufu Normal University in 2004 and M.S. degree in Jiangnan University in 2007, respectively. Her research interests include network security and distributed network technology.