A Trust-Based Approach to Control Privacy Exposure in Ubiquitous Computing Environments

Pho Duc Giang[1], Le Xuan Hung[1], Riaz Ahmed Shaikh[1], Yonil Zhung[1], Sungyoung Lee[1], Young-Koo Lee[1] and Heejo Lee[2]
[1]Computer Engineering Department, Kyung Hee University, Korea,
[2]Computer Science and Engineering Department, Korea University, Korea.
{pdgiang, lxhung, riaz, zhungs, sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr, heejo@korea.ac.kr

***Abstract*—In Ubiquitous Computing environments, service servers play a central role of actively providing information about a person to help people determine whether he is available for contact or not. A tradeoff exists in these systems: the more sources of data and the higher fidelity in those sources which can improve people's decision, the more privacy reduction. Alternatively, there is generally no a priori trust relationship among entities interacting in pervasive computing environments which makes it essential to establish trust from scratch. This task becomes extremely challenging when it is simultaneously necessary to protect the privacy of the users involved. In this paper, we first show how trust evaluation process of the user's system can be based on previous interactions and peer recommendations. A solution then relied on trust to control privacy disclosure is proposed that depends on pre-defined privacy policy. Several tuning parameters and options are suggested so that end-users can customize to meet the security and privacy requirement of a ubiquitous system.**

I. INTRODUCTION

Despite the existence of controversies about long-term technology prediction, there seems to be a strong consensus that new technologies should be focused on the user, improving the quality of life and adapting to the individual. Future technologies will provide context-aware services and will introduce new levels of personal safety. Personalization and ubiquitous access to information and communication will be essential. Additionally, with an increasing number of wireless devices and access technologies available, end-users will be able to access their space in anywhere and at anytime.

Unfortunately, the flexibility of the environment comes at a cost – higher security risks, vulnerabilities, and privacy disclosures. The traditional association with a network provider may not exist, replaced by a far more vague connection with a number of unknown entities, network nodes and service providers. In these situations, people commonly use a wide range of information sources to maintain awareness of another person or service provider and to determine their availability. For example, people may make decisions based on a combination of a person's current activity, location, behavior, and the state of her local environment (the state of the office door, lights, PCs, or desks). Therefore, it seems likely that by increasing the range and detail of data related to somebody, people will be able to better understand her condition. However, a tradeoff between awareness and privacy needs to be considered: more sources of information and more detail also mean that privacy is reduced, and few people are willing to let detailed information about them be sent out as a broadcast through an application server.

In this paper, we introduce the idea of using trust to provide finer-grained control over the exposure of personal information, thus helping to manage the privacy tradeoff. By giving different amounts of data to different types of people, our service servers deployed in the ubiquitous environment could increase disclosure without compromising privacy. It is clear that our willingness to let others gather information about us is strongly related to who they are and what their relationship is to us. To determine whether someone is trusted or not and how much private-sensitive data should release to her, we first rely on two different evaluation factors: peer recommendation, and time-based past interaction history to calculate the trust value. After that, based on the trust estimation process, we assign one of the three possible states: trusted, public, or distrusted (blocked) to the requester. By applying pre-defined trust-based privacy policies, we can administer and disseminate appropriate personal data to the partner.

The remaining paper is organized as follows. We briefly overview related work in Section 2. Next, in Section 3, we present the proposed method. Finally, in Section 4, conclusions and future work are drawn.

II. RELATED WORK

In the privacy literature for ubiquitous computing environment, attribute certificates (X.509 [1], SPKI [2])

1-4244-1326-5/07/$25.00/©2007 IEEE

generally do not protect the privacy of holders that can be identified and traced each time they show a certificate. Privacy-preserving (e.g. anonymous and/or untraceable) attribute certificates are proposed in some works that rely on blind signatures [3], or pseudonyms [4]. Establishing and verifying trust relationships is a common issue of pervasive spaces. Mechanisms to deal with trust are mainly based on rewards/penalties [5] or on reputation [6]. However, privacy is not taken into account in those approaches. Davis and Gutwin [7] have considered using relationship to provide finer-grained control over the disclosure of information. They conducted a survey that asked people what amount of data that they would disclose to different relationship types. From that point, they planned to build a working prototype, allowing people to differentiate disclosure by relationship. Nevertheless, the scope and the size of the survey are rather small so the results still need more time to verify. Up to now, research has focused mainly on propagation and composition of privacy preservation model while paying less attention to how privacy information is actually controlled when a user decides to disclose her data.

III. Our Methodology

In this section, we propose a privacy protection scheme based on the concept of trust with peer recommendation and past interaction history, and the trust-based privacy policy to guarantee that users' privacy sensitive data will not be delivered in a wrong way to a wrongdoer. There are two different stages in our solution: i) we estimate the trust value for each request coming from an entity; ii) we exploit the trust-based privacy policy to make decision how much private data should release to the guest. All these two phases can be performed automatically. We aimed to develop a system that required minimal ongoing user involvement. In particular, we did not want users to have to repeatedly evaluate the acceptability of a request for private information. Instead, we wanted to push a query's acceptance or rejection to the system itself and only bring a query to user's attention if they had not established a policy to handle it. Moreover, we believe user privacy should be protected by default; as a consequence, the system architecture lets a user elect to share certain information rather than protect specific information.

A. Trust Evaluation

In ubiquitous community, the production of trust is relied on several cues. For example, we tend to trust or distrust potential partners based on their past interactions. We also ask our already trusted principals (e.g. buddy, spouse, supervisor, colleague, secretary, etc, in reality) about their prior experiences with the new prospect uncommon before. The process of the user's system *P* to evaluate the trust value of any principal *Q* is shown in Fig. 1.

B. Time-Based Past Interaction History

Past Interaction History is an entity's previous transaction knowledge to certain principal. As a matter of fact, past interaction history is usually recorded in log files on the subjects' systems that keep track of all actions relational participants took with the system. Since the log file is configured to keep monitoring events for a specified amount of time, it is reasonable for us to apply trust evaluation based on the temporal factor.

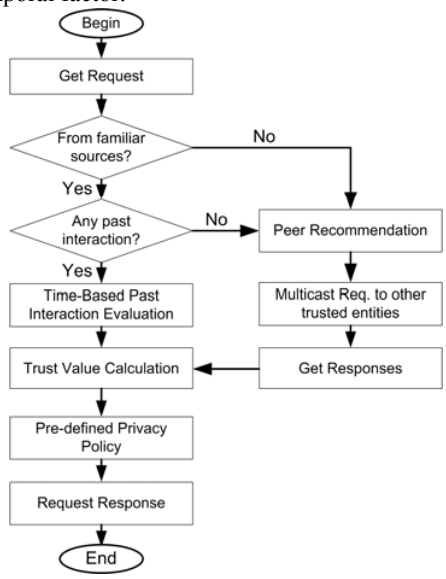

Fig. 1. Flow Chart of Trust Evaluation

We can generally define successful and unsuccessful interactions between a principal Q and an application P established on the past behaviors in which an unsuccessful interaction means that the principal did not get the outcome as it expected. Nevertheless, the nature of an interaction might reflect more than just successful and unsuccessful status. For instance, a principal might obtain the result completely contrary to the expectations whereas another one might gain a better effect. Moreover, the outcome of an interaction might be different in the view of the two principals. Due to the complexity of modeling this transition, we restrict our proposed scheme to the two statuses: successful and unsuccessful.

Let us define SI_t as the number of successful past interactions and UI_t as the number of unsuccessful interactions of the system at time *t*. Now, the trust value of *Q* as calculated by a system *P* is defined as follows:

$$T_{P,Q} = 100\left[\frac{SI_t}{SI_t+UI_t}\right]\left[1-\frac{1}{Ae^{(\alpha SI_t-\beta UI_t)}}\right]$$

Where α, β, and A are adjustable positive constants in the system and can be tuned if necessary.

The expression $\left[1-\frac{1}{Ae^{(\alpha SI_t-\beta UI_t)}}\right]$ approaches '1' quickly with an increase in the number of Successful Interactions and/or a decrease in the number of Unsuccessful Interactions within certain period of time. Notice that our choice of the above expression is for the smooth property of the exponential function and ease of calculation. It turns out that $T_{P,Q} = 0$ if $(\alpha SI_t - \beta UI_t) < 0$. In other words, the trust value of principal *Q*

is equal to 0 if its number of Unsuccessful Interactions is greater than the number of Successful Interactions with the system P. The factor $\left[\frac{SI_t}{SI_t+UI_t}\right]$ indicates the percentage of successful interactions in the whole communication session. We actually exploit the time-based sliding window mechanism [8] to estimate the percentage of successful communications.

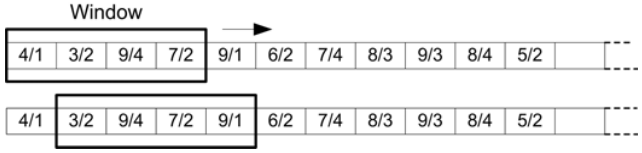

Fig. 2. Time-Based Sliding Window Mechanism

A sliding window is a variable-duration window that allows the system to compute different principals' trust value relied on successful interactions in a specified number of timing units. Note that the window size could be changed depending on the user's configuration. In Fig. 2, the current window length is presumably configured as a 4-unit sliding window. During the first timing interaction unit, the number of successful and unsuccessful communication was 4 and 1 respectively. Once a unit of time passes, the window slides one time unit from left to right, eliminating the previous interactions in the first unit from the trust calculation. Hence, very old past history information will not be involved in working out a trust evaluation as time goes by. Under the simple example shown in Fig. 2 with α = 1, β = 2, and A = 1,

$$T_{P,Q} = 100\left[\frac{23}{(23+9)}\right]\left[1-\frac{1}{e^{(1.23-2.9)}}\right] = 100\frac{23}{32}\left[1-\frac{1}{e^{5}}\right] \approx$$

≈ 70 (points) for the first interval. However, $T_{P,Q}$ will be changed in the next interaction interval since the number of successful and unsuccessful interactions are 9 and 1 which are different from the previous ones:

$$T_{P,Q} = \quad 100\left[\frac{28}{(28+9)}\right]\left[1-\frac{1}{e^{(1.28-2.9)}}\right] = 100\frac{28}{37}\left[1-\frac{1}{e^{10}}\right] \approx$$

≈ 76 (points).

C. Peer Recommendation

Peer Recommendation factor is required when the system has no or not enough information about a principal. Obviously, if there exists certain peer having more interactions with this principal, his suggestion should be likely logical and important for assessing the trust value.

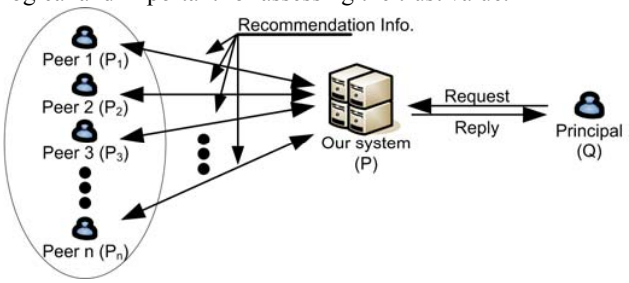

Fig. 3. A Peer Recommendation Scenario

Following the flow chart indicated in Fig. 1, suppose that the system was not familiar with this kind of request before so our system P has to ask other peers in the environment for their suggestions. In this situation, the system will send multicast a request for comments about the new principal Q to its confident community. We denote the time stamp between a principal Q and the system P as $\tau_{P,Q}$ and τ is the time at which Q decides to interact with P. Suppose n is the number of principals currently active in the environment. Let $P_1, P_2, \ldots, P_n$ represent the principals in the space. We also say that principals with high trust values will not send false recommendations. Moreover, let Δτ denote the threshold time interval. Under those assumptions, and Fig. 3, the trust value for the requesting principal Q is defined as follows:

$$T_{P,Q} = \frac{\eta_1 T_{P,P_1} T_{P_1,Q} + \eta_2 T_{P,P_2} T_{P_2,Q} + \eta_3 T_{P,P_3} T_{P_3,Q} + \ldots + \eta_n T_{P,P_n} T_{P_n,Q}}{100 \cdot n} \quad (n \neq 0)$$

$$\Leftrightarrow T_{P,Q} = \frac{\sum_{i=1}^{n} \eta_i T_{P,P_i} T_{P_i,Q}}{100 \cdot n} \quad (n \neq 0)$$

Where $\eta_i = Be^{\theta\frac{\Delta\tau_{P_i,Q}}{\Delta\tau}} \in (0,1]$, with $\Delta\tau_{P_i,Q} = \tau_{P_i,Q} - \tau$. B and θ are adaptable positive constants which can be chosen apart to guarantee that $\eta_i \leq 1$. For example, we select θ = 1. To establish $\eta_i \leq 1$, B must be picked out such that B ∈ $(0, \frac{1}{e^{\frac{\Delta\tau_{P_i,Q}}{\Delta\tau}}}]$. Since $\Delta\tau_{P_i,Q} \leq \Delta\tau$, we have $B_{max} \approx 0.46$.

Obviously, $T_{P,Q}$ = 0 if n = 0. In other words, peer recommendation will not be involved in trust evaluation process if there is no peer in the space. Besides, notice that η_i swiftly approaches '1' with increase in the argument $\Delta\tau_{P_i,Q}$. This means that very old and short experiences of peers with the principal in a period of time Δτ should have less weight in trust estimation over the new and long ones. Fig. 4 shows that the value of η_i increases quickly if $\Delta\tau_{P_i,Q}$ augments gradually within 100 timing units. After finishing the trust evaluation phase, we move towards the second phase in order to decide how much personal data will deliver to the principal (Fig. 1).

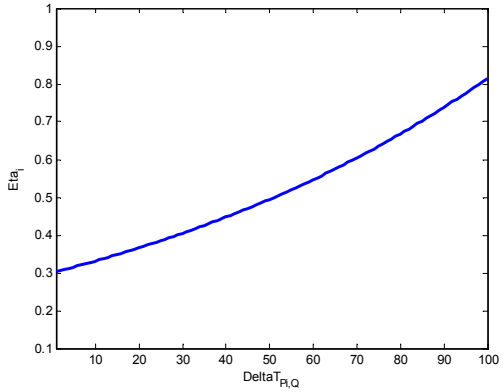

Fig. 4. η_i against $\Delta T_{Pi,Q}$ with θ = 1 and B = 0.3

D. Trust-Based Privacy Policy Management

We design a Privacy Policy module to describe the constraints such that the user's data is treated in the manner that she would expect, in the sense of being in accordance with her privacy policy. Once a principal's trust level was quantized by our system, it will be considered as one of three pre-defined states: Trusted, Public or Distrusted with the support of a trust-privacy mapping function $M_P(x)$ as follows:

$$M_P(x) = \begin{cases} \text{Trusted} & , 100 - c_2 \le x \le 100 \\ \text{Public} & , 50 - c_1 \le x < 100 - c_2 \\ \text{Distrusted} & , 0 \le x < 50 - c_1 \end{cases}$$

Where c_1 and c_2 are adjustable positive constants and can be tuned separately. Respecting this component, we propose 2 different parts, Zone Customization and Privacy Policy Establishment, that help users manage their personal data at the user interface level properly and effectively.

E. Zone Customization

Inside this sub-module, we develop 3 special zones correlative to 3 distinctive states of a principal *Q*. Then, we also recommend 3 different privacy control levels for each Trusted & Public Zone. Concerning that point, Public Zone's and Trusted Zone's sliders are used to adjust c_1 and c_2 value in the trust-privacy mapping function respectively. We suggest the following trust-based boundaries for control privacy disclosure:

TABLE I
TRUST-BASED ZONE RANGES WITH 3 DIFFERENT RESPECTIVE LEVELS OF TRUST

Zone / Level	Trusted Zone	Public Zone	Distrusted Zone
High ($c_1 = c_2 = 24$)	[96, 100]	[46, 95]	[0, 45]
Medium ($c_1 = c_2 = 14$)	[86, 100]	[36, 85]	[0, 35]
Low ($c_1 = c_2 = 4$)	[76, 100]	[26, 75]	[0, 25]

F. Privacy Policy Establishment

Whenever the system *P* receives a request from certain principal *Q* desiring to query your personal information, it will have to decide whether to place that entity in the Trusted Zone, Public Zone, or Blocked Zone. Placing certain principal in the Trusted Zone enables you to share your privacy-sensitive information and other resources to that principal. Principals you know and get high trust values based on our trust evaluation model should go in the Trusted Zone. Also, placing certain principal in sensitive information to that requester and protects you from the security risks associated with resource sharing. Principals with medium trust values should go in the Public Zone. In the meanwhile, Blocked or Distrusted Zone contains requesters that you do not want to contact with.

TABLE II
THE CONTENT OF AN ENTRY IN A DYNAMIC UPDATED PRIVACY POLICY

Name	Source (ID/ IP Address / Site)	Trust Value (points)	Zone	Comment
Family's PCs	220.68.80.23	100	Trusted	Family
Ms Kim's Laptop	163.180.100.5	86	Trusted	Professor Lee's secretary
Giang's Notebook	192.168.100.8	50	Public	Professor Lee's student
Unknown	Unknown	0	Distrusted	Stranger

IV. CONCLUSION AND FUTURE WORKS

The aim of this paper is to contribute to the development of a strict discipline for designing privacy control mechanisms in ubiquitous environments. In this study, we introduce a trust-based approach to control privacy disclosure by taking uncertainty of trust into account with a precise computation model. Additionally, we apply customizable privacy policy to efficiently handle malicious principals. As a future work we are going to build up the proposed trust evaluation and privacy policy modules that put our findings into practice, allowing people to differentiate exposure their personal information by trust estimation.

ACKNOWLEDGMENT

This work was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2006-C1090-0602-0002).

REFERENCES

[1] S.Mendes, "A new approach to the x.509 framework: Allowing a blogbal authentication infrastructure without a global trust model," Proceedings of NDSS 95, 1995.

[2] C. Ellison, "Spki certificate theory," Internet Request for Comments: 2693, 1999.

[3] D. Chaum and R.L. Rivest, "Blind Signatures for Untraceable Payments," Advances in Cryptology, Proceedings of Crypto 82, pp. 199-203, 1982.

[4] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation," LNCS 2045, 2001.

[5] M. Jakobsson, J. P. Hubaux, and L. Buttyan, "A Micro-Payment Scheme Encouraging Collaboration in Multi-hop Cellular Networks," Financial Cryptography, January 2003.

[6] P. Michiardi and R. Molva, "Core: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," IFIP - Communication and Multimedia Security Conference 2002.

[7] S. Davis and C. Gutwin, "Using Relationship to Control Disclosure in Awareness Servers," Proceedings of the 2005 Conference on Graphics Interface, May 09-11, 2005, Victoria, British Colombia.

[8] Riaz Ahmed Shaikh et al., "Intrusion Tolerant Group-based Trust Management Scheme for Wireless Sensor Networks", submitted for publication.