Toward Trust-based Privacy Protection in Consumer Communication

Fei Xu[1,2], Jingsha He[1*], Jing Xu[1] and Yuqiang Zhang[1]

[1]*Beijing University of Technology, Beijing 100124, China*
[2]*China Academy of Sciences, Beijing 100093, China*
xfei@emails.bjut.edu.cn, jhe@bjut.edu.cn

Abstract

In consumer communications, entities, i.e., users, hand-held devices, etc., that connect to or interact with each other may know little about each other or without any prior knowledge. Therefore, in many applications, before a serious interaction begins, certain level of trust must be established between the interacting entities, which may require that some information that may contain privacy about the entities be exchanged between the entities. Thus, privacy protection and trust establishment are inter-related issues that should be properly balanced to ensure both smooth communication and proper privacy protection. In this paper, we focus on trust based privacy protection in consumer communications by elaborating on three key issues: (1) quantification of privacy, (2) characterization of the relationship between privacy and trust, and (3) influence of trust on privacy protection. With trust based privacy protection, prior to an interaction, entities can set their privacy preferences conveniently and, during the interaction, they can choose their policies freely such as specifying whether privacy protection takes a higher priority than trust establishment, or vice versa. Our analysis and simulation experiment show that through using proper privacy protection patterns, trust based privacy protection can satisfy diverse privacy protection requirements in consumer communications.

Keywords: *security; privacy protection; trust; information theory*

1. Introduction

The rapid development of networking and communications technologies has made it more convenient for consumers to interact with each other to exchange information and to share digital contents, making privacy protection one of the primary concerns in network security. In consumer communications, the entities that connect to or interact with each other may know very little about each other or without any prior knowledge at the beginning of an interaction. In many cases, before a meaningful interaction begins, a certain level of trust must be established between the communicating entities to ensure the success of the interaction. Consequently, trust can be considered as an integral part of security and used as a primary security mechanism to make access decisions in the exchange of information and provision of services.

During the process of trust establishment, an entity may request some information that may contain some privacy from one or more other entities, leading to the loss of privacy to the requesting entity. Meanwhile, the exchange of such information can help

* The corresponding author (email: jhe@bjut.edu.cn).

establishing trust between the entities. Intuitionally, trust and privacy can be treated as a pair of interlinked concepts with some conflicting properties. That is, information may contain some privacy about an entity, but, on the other hand, can help the communicating entities establish trust to make successful interactions possible.

Although some privacy-enhancing technologies and privacy protection methods have been proposed for privacy preservation during trust establishment in the past, these methods are designed more for privacy protection and may thus adversely affect trust establishment. On the other hand, some methods have been proposed for balancing privacy and trust or for trading privacy for trust in certain applications. However, in these privacy-trust balance/tradeoff methods, an entity may disclose some privacy to a communicating entity in exchange for some trust from the entity without considering the actual patterns of interaction that may directly incur privacy loss. There has not been much work in which both privacy protection and trust establishment are considered in consumer communications.

Trust can be defined in many different ways with the main characteristics of being asymmetric, subjective and context-dependent. The main characteristics of privacy are also diverse, subjective and context-dependent. Since they share some common characteristics and both privacy and trust have long been familiar concepts in human interactions, in this paper, we explore the relationship between privacy protection and trust establishment as the basis for the development of an effective privacy protection mechanism to achieve both privacy protection and trust establishment goals.

The rest of this paper is organized as follows. In Section 2, we review some related work. In Section 3, we discuss some key issues in trust-based privacy protection. First, we propose a privacy quantification method based on multiple decision factors that include user preferences, context constraints, trust on communicating entities and privacy interaction history and feedbacks. Second, we study the relationship between privacy and trust and propose a function to describe such relationship. Third, we describe the influence of trust on privacy protection patterns. In Section 4, we present the application of our analysis result on trust based privacy protection. Finally, we conclude this paper in Section 5.

2. Related Work

Privacy protection and trust establishment have received a great deal of attention in network security research [1, 2]. Auto trust negotiation (ATN) framework was proposed as a solution for interactions between entities in open network environments. Accordingly, privacy preservation in the process of trust negotiation has been considered as a serious issue. Li, *et al*., proposed a heuristic and context-aware algorithm for the identification of the optimal chain by using context-related knowledge to minimize the disclosure of sensitive information [3]. Squicciarini, *et al*., proposed a set of privacy-preserving features for inclusion in any trust negotiation system [4]. Bhargav, *et al*., discussed the significance of federated identity management system for the protection of user information that takes into consideration automated trust negotiation techniques [5]. Lee and Winslett proposed algorithms that can be used in trust negotiation with minimal overhead and proven security and privacy properties [6].

The above work is aimed at protecting privacy in trust establishment. However, in order to start a meaningful interaction, some privacy information still needs to be disclosed. Consequently, some work has been done in which privacy is used to trade for trust in certain application scenarios [7]. A design and implementation of a P2P data sharing protocol with privacy and performance tradeoff was also described [8].

Although in the above work, privacy can be traded for trust or performance in some

applications, unnecessary privacy loss may occur without considering interaction patterns. A study on the relationship between interaction patterns and privacy preservation was not well done [9].

3. Trust-based privacy protection

To develop an effective method on privacy protection based on trust in network interactions, we consider the following key issues: privacy quantification, relationship between privacy and trust and influence of trust to privacy protection patterns.

3.1. Privacy quantification

Privacy is a concept that combines law, sociology and psychology, so the dimension of privacy includes multiple decision factors. Therefore, all the factors should be considered in privacy quantification. Major decision factors in privacy quantification include four attributes: user preferences, context constraints, trust on communicating entities, privacy interaction history and feedback of privacy interaction.

(1) User preferences: Typical user preferences that can be set by a user entity should at least include type of privacy information, type of service and objectives of interaction. The user can define privacy preferences in terms of the type of each service. For example, the user can specify that credit card information be disclosed only for online shopping, but not for any other types of service. For ease of illustration, we list below eleven types of services:

- Email;
- Online shopping;
- Banking;
- Social networking;
- Forums and user-generated contents;
- News and information;
- Instant messaging;
- Downloadable data;
- Online games;
- Health related information;
- E-government and e-learning.

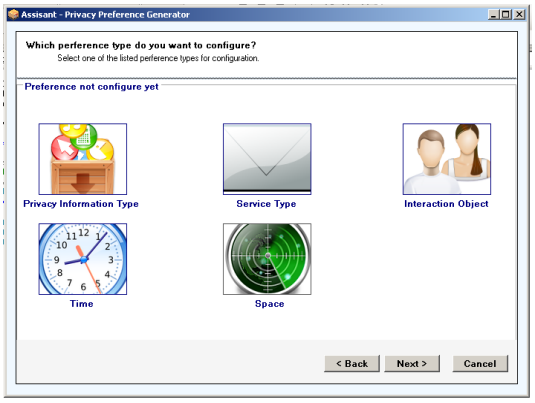
The user can also specify privacy preferences for special interactions. For instance, Alice can set “deny” to her classmate Bob’s request to access certain privacy information about her or set “permit” the interaction only when her trust on Bob has achieved 0.8 within the scale of 0 to 1.

(2) Context constraints: Usually, context constraints can be both temporal and spatial. Since privacy is context-dependent, it means that a privacy disclosure decision may not always be the same in different temporal and spatial scenarios.

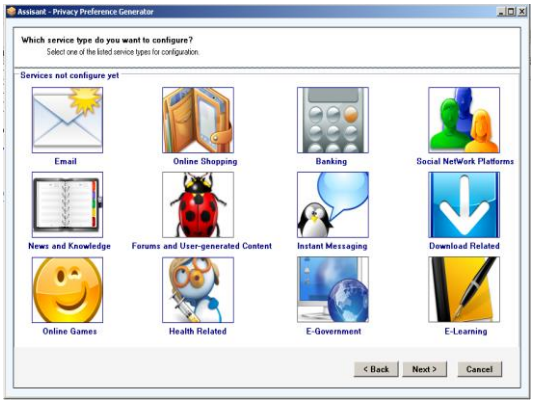
(3) Trust on communicating entities: In consumer communications, an entity may interact with a variety of other entities. Intuitively, an entity's privacy disclosure decision is related to the trust on the communicating entity to some extent. Theoretically, however, trust can be viewed as a probability of a trusted entity doing something that would benefit the trusting entity. Consequently, trust allows an entity to make some decisions.

(4) Privacy interaction history and feedbacks: If two communicating entities have exchanged some privacy information before and thus satisfied with each other, they are probably more than willing to exchange some more privacy according to psychological studies. Therefore, after the entities have exchanged some privacy, there should be a feedback function regarding whether one entity has disclosed the other entity's privacy without proper consent. So the privacy interaction history and feedbacks should also be considered in privacy quantification.

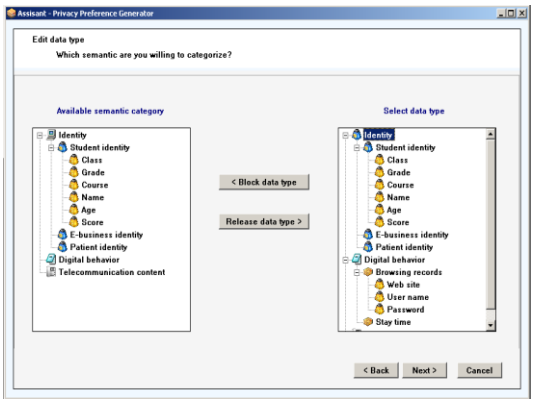
Figure 1 shows an exmple of an interface for users to set up privacy preferences.



(a) Main menu.



(b) Type of service setting.



(c) Privacy information

Figure 1. An exmple of an interface for setting user privacy preferences

Based on the above analysis, we propose a privacy quantification method based on the afore-mentioned decision factors and use entropy to derive the weight for each of the decision factors.

Let x_i and x_j be the privacy information owner and the privacy information requester, respectively. Let p denote the privacy information rank that a requester can get. We define a privacy quantitative function G that includes M decision factors $Y_m(x_i, x_j)$ ($1 \le m \le M$) each of which has its weight v_m defined as follows:

$$G(x_i, x_j, p) = \sum_{m=1}^{M} v_m Y_m(x_i, x_j) \tag{1}$$

where weight v_m satisfies the following condition:

$$\sum_{m=1}^{M} V_m = 1, (0 \le v_m \le M) \tag{2}$$

Privacy information rank p is determined by the result of function G. The larger the value of G is, the higher the sensitive rank p that a requester can get.

Let H be the information entropy for a decision factor which can be computed using the following formula:

$$H(Y_m(x_i, x_j)) = -Y_m(x_i, x_j) \log^{Y_m(x_i, x_j)} - (1 - Y_m(x_i, x_j)) \log^{Y_m(x_i, x_j)} \tag{3}$$

3.2. Relationship between privacy and trust

We consider both the content and the action that can provide some information as one piece of information during communications. Therefore, a piece of information may contain some privacy while offering some trust for the communicating entity.

In different networks or applications, trust and privacy may have different relationships. Here, we use function F(p,t) to describe the relationship between privacy and trust in network interactions.

(1) F(p,t)=Fpmin(p,t),(p<t)/t: This function is used to determine the minimum amount of privacy that an entity should disclose in order to achieve a desired level of trust in which condition (p<t)/t means that trust is constant while privacy that an entity elects to disclose is variable. The priority here is privacy protection. To use this function, privacy should be quantified and the minimum set of privacy information should be selected and disclosed to the communicating entity in order to achieve the desired level of trust by the communicating entity.

(2) F(p,t)=Ftmax(p,t),(t<p)/t: This function is used to determine the highest level of trust that an entity can get by disclosing some privacy in which condition (t<p)/t means that privacy that an entity elects to disclose is constant while trust is variable. The priority here is trust establishment. To use this function, privacy loss and trust gain must be evaluated for the privacy disclosure set and the privacy that can gain more trust should be selected and disclosed to the communicating entity.

(3) F(p,t)=Ftmin(p,t),(p<t)/p: This function is used to determine the minimum level of trust that an entity should grant to a communicating entity after a certain amount of privacy has been disclosed by the entity. The goal is to protect system security of the entity in that the communicating entity should not be granted too much trust to avoid excessive access authority. As we have pointed out, information not only contains privacy, but also helps trust establishment and many trust establishment methods have adopted the scenarios of interaction as one of the trust evaluation elements. In this function, condition (t<p)/t means that privacy that the entity has disclosed is constant while trust is variable. The priority here is privacy protection.

(4) F(p,t)=Fp-t(p,t),(t<p)/p: This function is used to denote privacy feedbacks to trust establishment after some interactions. If an entity has failed to protect a communicating entity's privacy as promised, *e.g.*, disclosing the privacy to a third party without proper consent, such privacy violation would cause the entity's trust to be degraded by the other entity. In this function, condition (t<p)/p means that privacy that the entity has disclosed is constant while trust is variable. The priority here is to adjust the level of trust with the goal of privacy protection.

A good privacy-trust relationship can increase the rate of successful interactions and consequently the level of satisfaction of the communicating entities. Equipped with the above four functions, an entity can freely choose its interaction policy and priority, *e.g.*, privacy protection over establishment, or vice versa. Obviously, the key point in utilizing the privacy-trust relationship during interactions is to resolve the issue of quantifying privacy loss and trust gain.

As we have described before, privacy quantification should consider multiple decision factors. We can thus quantify privacy information, which measures the sensitivity of privacy, based on the quantification method described in the previous section. Furthermore, we need to study the quantification of privacy loss and trust gain.

The way of computing trust gain is based on a trust model in which we can define a trust benefit function $B(t_i)$ and associate it with a trust level t_i. Then, trust gain G can be calculated using the following formula:

$$\begin{aligned} &Trust\_gain \\ &= G(new\_trust\_level, old\_trust\_level) \\ &= B(new\_trust\_level) - B(old\_trust\_level) \end{aligned} \tag{4}$$

Let x_i and x_j be the owner and the requester of privacy information, respectively, p be the privacy information rank that the privacy requester can get, and q be the privacy information rank for which the privacy requester asks. We define a privacy rank function $PR(p)$ for each privacy rank. Then, privacy loss L can be calculated using the following formula:

$$\begin{aligned} &\Pr ivacy\_loss \\ &= L(requester\_p\_rank, request\_p\_rank) \\ &= PR(q) - PR(\mathrm{p}) \end{aligned} \tag{5}$$

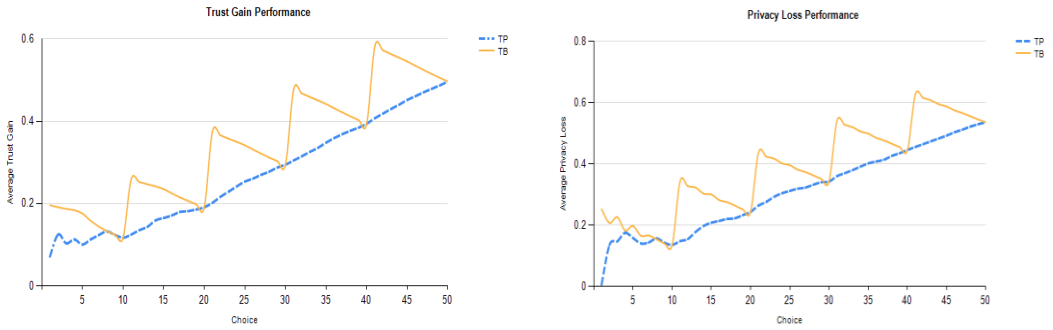
As we have pointed out, a piece of information may contain some privacy but, on the other hand, can help trust establishment between communicating entities. So we construct an information list that contains the pieces of information that entities may exchange in interactions along with "trust gain" and "privacy loss" for each piece of information computed using our quantification method. The total number of pieces of information in the list is, say, 50 and both the trust gain and the privacy losses vary between 0 and 1.

Table 1 shows the information list in which pieces of information are arranged in an ascending order with respect to trust gain.

Table 1. Information list

No.	Content	Trust gain	Privacy loss
1	Email	0.2	0.3
2	Tel	0.7	0.8
….	….	….	….
50	Address	0.8	0.9

In one scenario, we analyze the performance of trust establishment using the privacy-trust relationship. In this case, the priority is trust establishment. We compare our trust-based privacy protection method (T_B) to the trust-privacy tradeoff method (T_P) proposed by Deghaili et al. [10] in which the dynamic nature of the relationship between trust and privacy is not considered so that privacy is disclosed under the same trust level with equal probability. Our simulation results are shown in Figure 2 (a, b) in which the x-axes denote the terms of information that the interactive entity requires and the y-axes denote the average trust gain, *i.e.*, sum(trust gain)/terms, and the average privacy loss, *i.e.*, sum(privacy loss)/terms, respectively. We can see from the figures that T_B has a better performance in trust gain than T_P but T_B causes more privacy loss than that T_P. We can thus conclude that T_B can better meet the requirement on trust establishment.



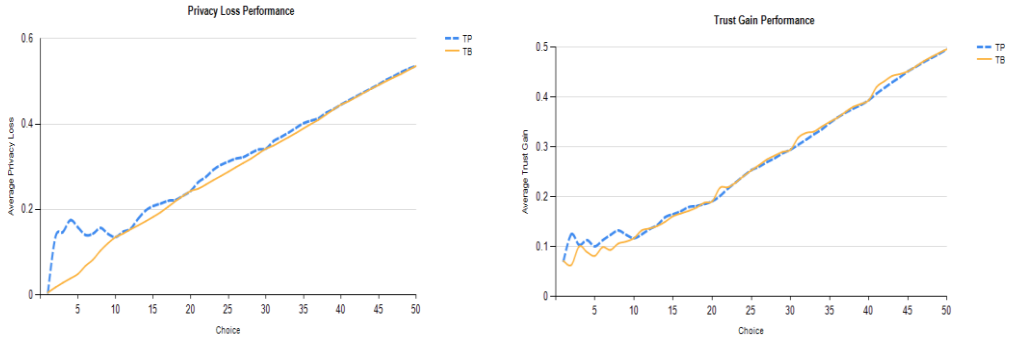
(a) (b)

Figure 2. Simulation results for the case in which trust establishment has a higher priority than privacy protection

In the other scenario, we analyze the performance of privacy protection by comparing T_B to T_P in network interactions. In this case, the priority is privacy protection. Our simulation results are shown in Figure 3 (a, b) in which the x-axes denote the terms of information that the interactive entity requires and the y-axes denote the average trust gain and the average privacy loss, respectively. We can see from the figures that T_B incurs less privacy loss than T_P while the trust gain is comparable. We can thus conclude that T_B has a better performance in privacy preservation.

3.3. Influence of trust on privacy protection patterns

During network interactions, trust could be closely related to privacy protection patterns. Trust among communicating entities affects the way in which the entities interact with each other as well as the complexity of the interactions. If the entities have a higher level of trust on each other, they can use less complex privacy protection patterns. In general, the higher the trust that an entity has on another, the less complex the privacy protection patterns can be.



(a) (b)

Figure 3. Simulation results for the case in which privacy protection has a higher priority than trust establishment

In consumer communications, the way in which an entity discloses information that contains privacy to others can be categorized into three classes from the viewpoint of privacy protection patterns: direct mode, confusing mode and indirect mode.

(1) Direct mode. In this mode, an entity discloses its privacy information directly to another interactive entity. For example, a user may be asked to provide his/her email address during registration with an e-business site. This is a direct mode for the user to disclose his/her privacy information, *i.e.*, the email address, to the site. This mode has the lowest complexity of interaction which occurs when the information owner has a high level of trust on the information requester.

(2) Confusing mode. In this mode, privacy information is disclosed with some ambiguity. For example, in a data publication application, before data are published, something may be done on the original data in order to protect privacy of the data owner. This mode can be applied when the information owner has a medium level of trust on the information requester.

(3) Indirect mode. In this mode, the information owner may need some help from a trusted third party in order to complete the interactions. This mode incurs the highest level of complexity of interactions which can occur when the information owner has a low level of trust on the information requester.

Let IP=$\{ip_1, ip_2, \ldots, ip_n\}$ ($n \geq 1$) denote the set of privacy protection patterns in which ip_1 denotes the pattern for the direct mode and ip_n denotes one for the indirect mode. An element $ip_r \in IP$ (where $2 \leq r \leq n-1$) denotes a privacy protection pattern for the confusing mode and such elements are arranged in an ascending order of complexity from the viewpoint of interactions.

In trust evaluation, trust T (where $0 \leq T \leq 1$) can be divided into m (where $m \geq 1$) levels. Assuming that there are n privacy protection patterns $\{ip_1, ip_2, \ldots, ip_n\}$ in the set IP of privacy protection patterns, IP can also be divided into m subsets. A mapping $M: T \rightarrow P=\{ip_1, ip_2, \ldots, ip_l\}$ (where $l \geq 1$) is a function for determining the corresponding subset of privacy protection patterns that an entity can choose from given that an interactive entity's trust level is $t \in T$. The subset of privacy protection patterns from which an entity can choose is based on the level of trust on the other communicating entity.

We now use the location based service (LBS) as an example to explain the influence of trust on privacy protection patterns. This example reflects the current development in which an increasing number of communication devices (*e.g.*, mobile phones, PDAs, *etc.*) have been loaded with software that offer the positioning capabilities, *e.g.*, GPS. Users can make location-dependent queries, such as "finding the nearest hospital", that can be answered by an LBS like Google Maps. However, this type of services can result in the disclosure of privacy about individuals, *e.g.*, health conditions, lifestyle, *etc*.

Assuming that there is a user A and an LBS provider B, before A uses the service offered by B, A should assess the trustworthiness of B. A can then assume three trust levels on B, *e.g.*., high, medium and low, and the corresponding privacy protection pattern subsets can be $\{ip_1\}$, $\{ip_2, ip_3\}$ and $\{ip_4\}$, respectively.

ip_1: direct mode in which A provides his/her location information to B directly.

ip_2: confusing mode in which A adds some location-irrelevant information in his/her location information before providing the information to B.

ip_3: confusing mode in which A uses a spatio-temporal cloaking method to further make his/her location less clear before providing the information to B.

ip_4: indirect mode in which A uses an encryption algorithm to encrypt his/her location before providing the information to B.

If A trusts B at level "high", A would use privacy protection pattern ip_1 in which the location information will be provided directly to B. If A trusts B at level "medium", A would select ip_2 or ip_3 according to specific application scenarios and negotiate a privacy protection pattern with B. If A trusts B at level "low", A would use privacy protection pattern ip_4 in which the location information will be encrypted before being provided to B.

We now evaluate and compare the performance of our trust based privacy protection method (TPM) with the privacy-aware access control method (AP) [11] in terms of privacy preservation and interaction successful rate. In the comparison, we use the data sets from the real-life CENSUS data downloaded from site http://www.ipums.org. Table 2 contains a summary of the attributes in the CENSUS data.

Table 2. Summary of the attributes in CENSUS

Attribute	Number of distinct values
Age	78
Gender	2
Education	17
Marital	6
Race	9
Work-class	8
Country	83
Occupation	50
Salary-class	50

Figures 4 and 5 contain the corresponding experiment results from which we can see that, by taking into consideration of the influence of trust on privacy protection patterns, our method can achieve a higher rate on interaction success with a comparable rate of privacy disclosure in network interactions.

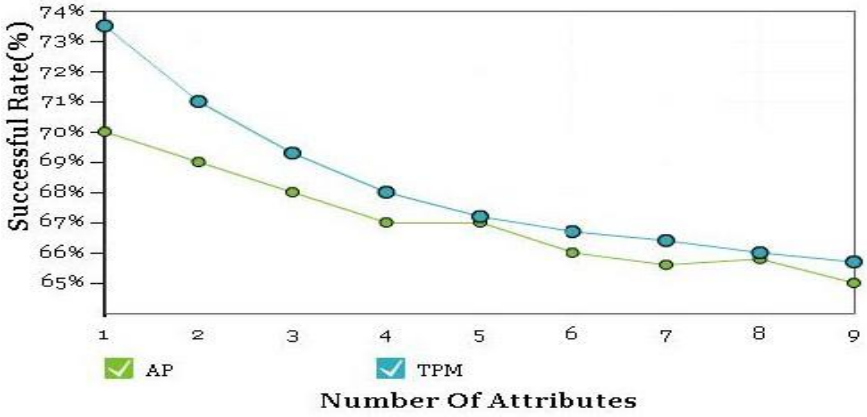


Figure 4. Rate of interaction success

Figure 5. Rate of privacy disclosure

4. Application of trust-based privacy protection

We now present a framework on the application of our trust based privacy protection method in network interactions, which is shown in Figure 6.

At the low layer of the framework, a user can set his/her privacy preferences. Then, the system quantifies privacy information by considering multiple descision factors such as context constraints. At the middle layer, based on the analysis on the relationship between privacy and trust and according to privacy loss quantification and trust gain quantification, the user can decide his/her interaction policy, *i.e.*, setting the priority on protection privacy or on trust establshment. At the top layer, the user can choose privacy protection patterns acoording to trust on another communicating user through a mapping function from trust to privacy protection patterns.

Consequently, with trust baesed privacy protection in consumer communicationss, users can set their privacy preferences conveniently and, during interactions, they can choose their interaction policy freely. Users can also choose the interation policy by deciding the priority

on privacy protection or on trust establishment, thereby satisfying diverse requirements on privacy protection which is often subjective. According to our simulation results, trust based privacy protection can satsitfy different privacy protection requirements and improve the success rate of interactions.

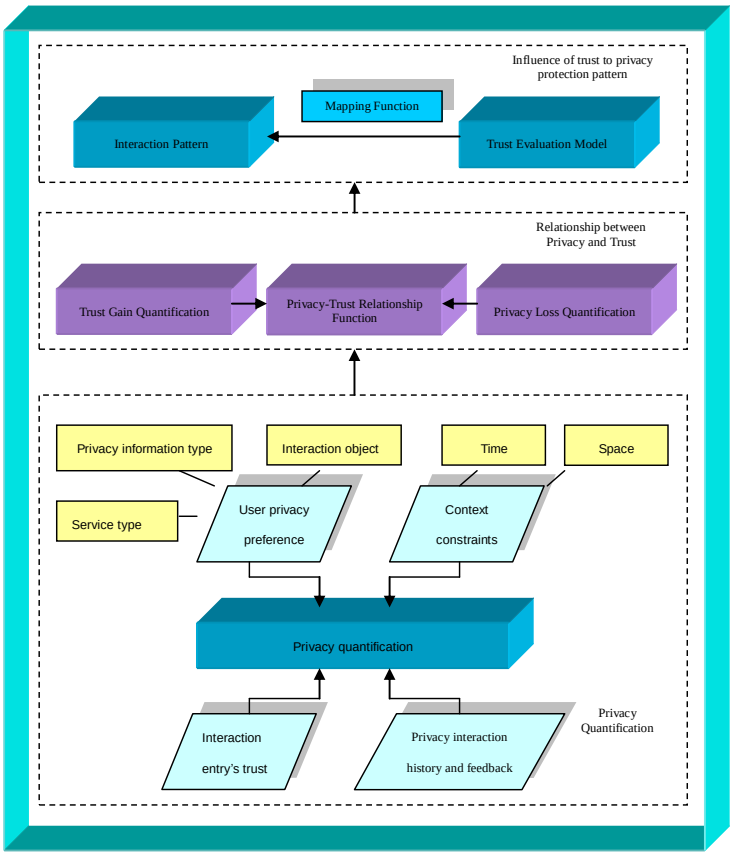


Figure 6. Application of trust based privacy protection

5. Conclusion

In this paper, we studied there key issues in trust based privacy protection. First, we proposed a multiple decision factor based privacy quanfitification method in which factors such as user preferences, context constraints, trust on interaction entities, and privacy interaction history and feedbacks are considered. Then we studied the relationship between privacy and trust in which we proposed a function to describe such relationship. Third, we studied the influence of trust on privacy protection patterns and compared our method to another comparable method.

Based on our analysis and simulation resluts in this paper, we can conlude that trust based privacy protection can satsitfy diverse privacy protection requirements while improving the sucess rate of interactions, which offers a promising approach to resolving security and privacy issues in consumer communications.

Acknowledgments

The work in this paper has been supported by funding from National Natural Science Foundation of China (61272500) and from Beijing Education Commission Science and Technology Fund (KM201010005027).

References

[1] J. Grant, "The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards, IEEE Internet Computing, vol. 12, no. 6, **(2011)**.
[2] T. Hashem and L. Kulik, "Don't Trust Anyone: Privacy Protection for Location-based Services". Pervasive and Mobile Computing, vol. 7, no. 1, **(2011)**.
[3] J. Li, D. Zhang, J. Huai and J. Xu, "Context-aware Trust Negotiation in Peer-to-Peer Service Collaborations", Peer-to-Peer Networking and Applications, vol. 2, no. 2, **(2009)**.
[4] A. Squicciarini, E. Bertino, E. Ferrari, F. Paci and B. Thuraisingham, "PP-trust-X: A System for Privacy Preserving Trust Negotiations", ACM Trans. Information and System Security, vol. 10, no. 3, **(2007)**.
[5] A. Bhargav, A. Squicciarini and E. Bertino, "Trust Negotiation in Identity Management", IEEE Security and Privacy, vol. 5, no. 2, **(2007)**.
[6] A. Lee and M. Winslett, "Enforcing Safety and Consistency Constraints in Policy-based Authorization Systems", ACM Trans. Information and System Security, vol. 12, no. 8, **(2008)**.
[7] G. Bella, R. Giustolisi and S. Riccobene, "Enforcing Privacy in E-commerce by Balancing Anonymity and Trust", Computers and Security, vol. 30, no. 8, **(2011)**.
[8] T. Isdal, M. Piatek, A. Krishnamurthy and T. Anderson, "Privacy-Preserving P2P Data Sharing with OneSwarm", Proceedings of SIGCOMM 2010, New Delhi, India, **(2010)** August 30-September 3.
[9] S. Pearson and Y. Shen, "Context-Aware Privacy Design Pattern Selection", HP Laboratories Technical Report, Hewlett Packard Laboratories, USA, vol. 74, **(2010)**.
[10] R. Deghaili, A. Chehab and A. Kayssi, "Trust-Privacy Tradeoffs in Distributed Systems", Proceedings of the 2008 International Conference on Innovations in Information Technology, Al Ain, United Arab Emirates, **(2008)** December 16-18.
[11] M. Li, X. Sun, H. Wang, Y. Zhang and J. Zhang, "Privacy-aware Access Control with Trust Management in Web Service", World Wide Web, vol. 14, no. 4, **(2011)**.

Authors

Fei Xu received her Ph.D. degree in Computer Science and Technology from Beijing Unibersity of Technology in China. She is now a member of the research staff in the Institute of Information Engineering (IIE) at China Academy of Sciences in China. Her research at IIE has led to theoretical and technical improvement in information security, including the detection and analysis of data leakage, information control, network security evaluation and security situation awareness in large-scale networks. Dr. Xu has published several papers in scholarly journals and international conferences in the above research areas.

Jingsha He received his B.S. degree in Computer Science from Xi'an Jiaotong University in China and his M.S. and Ph.D. degrees in Computer Engineering from University of Maryland at College Park in USA. He is now a professor in the School of Software Engineering at Beijing University of Technology in China and has published over 170 research papers in scholarly journals and international conferences and received nearly 30 patents in the United States and in China. Prof. He's research interests mainly include information security, network measurement, and wireless ad hoc, mesh and sensor network security.

Jing Xu received her M.S. degree in Computer Scienec and Technology from Beijing University of Technology in China in 2011 and is currently pursuing her doctoral degree at the same university. Her major research interests include information security, privacy protection and wireless sensor network security in which she has published several papers in scholarly journals and international conferences.

Yuqiang Zhang is currently a Ph.D. candidate in the College of Computer Science at Beijing University of Technology in Beijing, China. His major research fouses on information security and wireless sensor network security. He has participated in several projects and published several technical papers in the above research areas.