D-018

Evaluating Risks for Card-style Identity Management

Ding xiaochen †
Dingxiaochen@toki.waseda.jp

Mizuho Iwaihara†
Iwaihara@waseda.jp

Abstract: Card-style identity management systems have been developed to help users control their digital identities stored at different identity providers. However, current card-style identity management systems are lack of the ability to evaluate the risk of user's identities, which may resultantly cause enormous financial or privacy loss to user. So it is necessary to assist users by presenting the risk of every identity when the identities are to be released to the service providers. In this paper, a risk evaluation model based on privacy attribute ontology is proposed to enhance the privacy of card-style identity management systems.

1 . Introduction

With the rapid growth of Internet, web services have become one of the most important applications in the network, where users can do shopping, play games, make friends, and even work. Before enjoying these services provided by service providers (SP), some basic personal information of users, such as name, e-mail, address is required for authentication. How to manage this information effectively and safely becomes a serious problem for the users. In order to solve the problem, card-style identity management systems like Microsoft Windows CardSpace[1], Higgins identity management system[2] have been developed, which can help users manage their private identity attribute from their own perspective. In these systems user's digital identities are represented by virtual information card which contains information of user's identity and card. However, these systems are all focusing on protecting transmission safety and interoperable structure between existing identity management systems, less work is poured into evaluating risks of user's identity attributes. When users need to release an identity to the service provider, they have to evaluate the potential risks caused by this release themselves. But it would be hard for a common user without professional knowledge to decide which identity attribute is of high risk or low risk. Carelessly sending these identity attributes to the service providers will cause some personality damage or financial damage to the users. According to the JNSA's report on information security incident[3], in 2008 there are 7.23 million victims suffered from information leakage accidents, the total compensation for damages are more than 236 million dollars in Japan. In this paper, a risk evaluation model based on privacy attribute ontology is proposed to enhance the privacy of card-style identity management systems. We believe that by presenting the risk of every attribute to the users in the card-style identity management systems, users can control their digital identity more safety and easily.

† Graduate School of Information, Production and System, Waseda University

2 . Risk Evaluation

First, let us see a simple scenario to show risk issues in the card-style identity management systems. Fictious.com is an online-game service provider. Bob is a user of a card-style identity management system. Fictious.com requests several attributes for registration and it accepts both managed card issued by identity providers and self-issued card issued by user himself. The card-style identity management system automatically chooses two information cards satisfying the request as follow:

Requested attributes: first name, last name, email.

> *Card name: Student card*
> *Card type: Managed*
> *Issued by: Waseda Univ*
> *Attributes: student number, first name, last name, email, address, department.*

> *Card name: Game card*
> *Card type: Self-issued*
> *Issued by: Bob*
> *Attributes: first name, last name, email, mobile phone number, date of birth, gender, web page.*

Bob now could send either card to the service provider. From the privacy perspective, "email" in the student card has higher sensitivity than the one in the Game card, because university email is a very important attribute which is often used to login university's system and receive some important messages. If Bob chooses to send the student card rather than Game card, he will take a higher risk. If the risk of every attribute is presented clearly, it will be much easier for Bob to make his decision: send, not send or which to send.

2.1 Risk Values

To solve this privacy problem, in this paper we use risk values to represent the risk of every attribute which is a numerical scale of 1 to 5, where 1 is the least severe and 5 is the most severe. This is a very obvious way to tell user how much risks he/she will undertake if some specific attributes are chosen to be sent. Two kinds of risk value are defined; one is personality risk value which is a risk value indicating the potential personality damage to the user. Another is financial risk value indicating the potential damage to the user. Every attribute in the identity management system owns these two risk values.

2.2 Privacy attribute ontology

A concept of privacy attribute ontology (PAO) built on the OWL web languages has been proposed [4]. In this paper we use PAO-based method to solve the risk evaluation problem in the card-style identity management system. Fig.1 shows a basic PAO, which contains composite classes, single classes, and risk values.

In PAO, a class represents a basic concept, like name and email. A composite class consists of a number of component classes. Each class has two risk values, personality risk value and financial risk value.

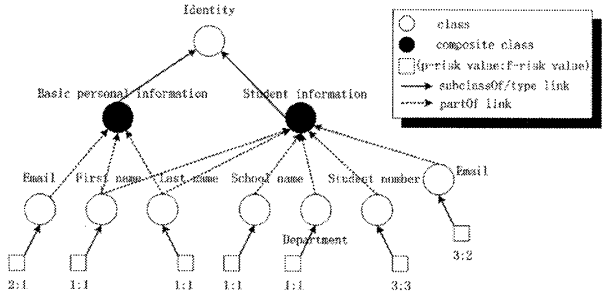

Fig.1 Privacy attribute ontology

In order to construct PAO, we use requested privacy attributes from 8 different service providers. These privacy attributes are well categorized according to the structure of PAO. JNSA proposed a simple-EP diagram in [3] to measure the emotional distress and economic loss when a privacy attribute is released. We extended this simple-EP diagram to (1-5) level and use the extended simple-EP diagram to decide the personality risk value and financial risk. Fig.2 is a PAO constructed by us.

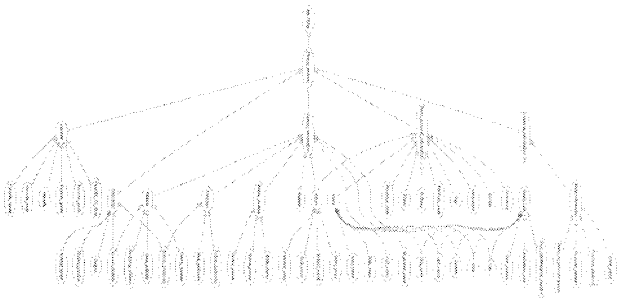

Fig.2 Privacy attribute ontology

2.3 Privacy attribute ontology matching algorithm

In this section we explain how to evaluate risk for privacy attribute in a card-style identity management system, utilizing PAO. First we will introduce the concept of semantic similarity and how to calculate the SimilarityScore.

Definition 1: *Let τ be a value threshold of similarity, a1 and a2 are two privacy attributes. We say that a1 and a2 are semantically similar if SimilarityScore(a1,a2) $\geq \tau$.*

$$SimilarityScore(a1,a2) = w1 * JaroWinkler(a1,a2) + w2 * Wordnet\ Similarity(a1,a2) \quad (1)$$

Here w1 and w2 are two weight factors. JaroWinkler and WordNet similarity are two methods to calculate structure similarity and semantic similarity between two words.

The basic idea to evaluate the risk for an information card is if attributes in the information card can be matched with a semantically similar class in the PAO, then this attribute can inherit the risk values form its semantically similar class. So the problem becomes a matching problem between PAO and information card. We consider the following two stage approach: Firstly, do matching between composite classes of PAO and name of information card, and then choose the pair which has the highest similarity score. If the name of a composite class is more semantically similar to the name of information card, we believe there will be more possibility that we can find similar attributes to the information card in the component classes of the composite class. Based on this belief, the main purpose in this step is to find the most matched composite class so that it may contain attributes we wanted. Secondly, do matching between each component class which belongs to the composite class that found in the first step and each attribute in the information card. Then use the Hungarian method to solve a weighted bipartite matching problem. The following shows the proposed matching algorithm. Compare to [4] the proposed method can reduce the matching times.

Input: Information card c and PAO
Output: Evaluated privacy attributes
Method:

1. For each composite class D in PAO and card name B of an inforamtion card c, caculate similarity score(D,B).
1.1 According to the result of step 1, find a matching (D',B) which has the higheset similarity score.
2. For each component class C of D' and each attribute A in c, caculate similarity score(C,A).
2.2 Slove weighted bipartite matching.

Fig.3 Algorithm: Two statge PAO matching

2.4 Presenting Risk values

Through applying the proposed matching algorithm to each information card, the risk of attribute can be evaluated. When the user needs to send an information card to the service provider, the card-style identity management system could present risk values of each attribute in this card and if the user knows the risk he/she will take if sending this card, he/she could make a safer decision. The example in the beginning of Section2 can be solved by our method, where the user will see sending Game card will take less risk than the student card because email in Game card has a personality risk value of 2, while the one in the student card has a higher personality risk value of 3.

3 . Conclusion and Future works

In this paper we proposed a risk evaluation method based on privacy attribute ontology for card-style identity management system. Our proposed method can automatically infer risk values to each privacy attribute in the information card and through presenting risk values to users when some attributes need to be released to service providers, we believe users could make more precise and reliable decisions. Our future work includes improving the current matching algorithm in the card-style identity management systems and developing a CardSpace compatible system to implement our proposed methods.

References

[1] Microsoft Developer Network (MSDN) CardSpace page, http://msdn.microsoft.com/CardSpace

[2] Higgins Open Source Identity Framework, http://eclipse.org/higgins/

[3] Japan Network Security Association, Information Security Incident Surveys (2008).

[4] Mizuho Iwaihara, Kohei Murakami, Gail-Joon Ahn, and Masatoshi Yoshikawa: Risk Evaluation for Personal Identity Management Based on Privacy Attribute Ontology. In: ER 2008, LNCS 5231, pp.183-198, 2008.