Obtaining P3P Privacy Policies for Composite Services

Yi Sun, Zhiqiu Huang, and Changbo Ke

College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu 210016, China

Correspondence should be addressed to Yi Sun; sunyiyily@126.com

Received 12 January 2014; Revised 22 June 2014; Accepted 26 June 2014; Published 13 July 2014

Academic Editor: Jesualdo Tomás Fernandez-Breis

Copyright © 2014 Yi Sun et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of web services technology, web services have changed from single to composite services. Privacy protection in composite services is becoming an important issue. P3P (platform for privacy preferences) is a privacy policy language which was designed for single web services. It enables service providers to express how they will deal with the privacy information of service consumers. In order to solve the problem that P3P cannot be applied to composite services directly, we propose a method to obtain P3P privacy policies for composite services. In this method, we present the definitions of Purpose, Recipient, and Retention elements as well as Optional and Required attributes for P3P policies of composite services. We also provide an instantiation to illustrate the feasibility of the method.

1. Introduction

Nowadays Internet has become one of the major ways for people to get services. More and more people are accustomed to using web services. And with the development of web services technology, web services have changed from single to composite services. Web service composition is an approach to build new composite services by combining existing services. It not only reuses existing web services to improve the efficiency of service development, but also satisfies service consumers’ multifunctional demands. However, whether services are single or composite, service consumers’ privacy information is inevitably collected by service providers. And it is hard for service consumers to control the disclosure of their privacy information. In order to prevent the privacy information from being misused, service providers are requested to publish their privacy policies. Based on the privacy policies published by service providers, service consumers are able to know what service providers will do with their privacy information.

P3P (platform for privacy preferences) [1] was released by World Wide Web Consortium (W3C) in April 2002. It provides a standard and machine-understandable privacy policy. W3C also designs APPEL (A P3P Preference Exchange Language) [2] which allows service consumers to specify their privacy preferences. A P3P user agent can compare the P3P policies of service providers with the privacy preferences of service consumers. The comparison results enable the service consumers to decide whether to use the services or not. Since P3P was originally designed for single services, it cannot be applied for composite services directly. A composite service may consist of several independent web services which are called member services. All these member services have their own P3P policies which may specify different privacy practices of the same private data. How to isolate these discrepancies is one challenge. How to obtain the P3P policy for a composite service consisting of several services is another challenge.

In this paper, we firstly present the definitions of Purpose, Recipient, and Retention elements as well as Optional and Required attributes for P3P policies of composite services. Secondly, based on these definitions, we obtain P3P privacy policies for composite services. Finally, we provide an instantiation to illustrate how to obtain a P3P privacy policy of a composite service concretely.

The rest of this paper is organized as follows. Section 2 describes the syntax of P3P privacy policy. Section 3 proposes a method to obtain P3P privacy policies for composite services by defining the Purpose, Recipient, and Retention elements as well as the Optional and Required attributes for P3P policies of composite services. A case study is presented to prove the feasibility of the method in Section 4. Related work is discussed in Section 5. Section 6 concludes the paper.
2. P3P Syntax

P3P privacy policies inform service consumers how service providers will deal with their privacy information. The overall structure of a P3P policy is shown in Algorithm 1. A P3P privacy policy is described by a Policy consisting of an Entity element, an Access element, a Disputes-Group element, zero or more Extension elements, and one or more Statement elements. Entity gives a precise description of the legal entity making the representation of the privacy practices. Access indicates whether the site provides access to various kinds of information. Dispute-Group describes dispute resolution procedures that may be followed for disputes about a service’s privacy practices.

Statement is the core of P3P privacy policy. It describes how a website collects and uses the private data of service consumers. Statement comprises Purpose, Recipient, Retention, and Data-Group elements. Purpose states for what purpose the private data of service consumers may be used. It has six predefined values such as current, admin, and develop. Recipient describes to whom the private data of service consumers will be exposed. Retention states how long the private data of service consumers will be retained by service providers. Data-Group contains a list of private data (Data element) of service consumers which may be collected by service providers and data categories (Categories element). Moreover, Data, Purpose, and Recipient are either optional or mandatory by taking an optional attribute called Optional for the former and Required for the latter two. The value of Optional is either no (default value) when the data must be collected or yes when the data is optional. The value of Required can be always (default value), opt-out, or opt-in. Always means the purpose/recipient is always needed. Opt-out means the data may be used for the purpose/may be distributed to the recipient unless the user requests that it not be used in this way. Opt-in means the data may be used for the purpose/may be distributed to the recipient only when the user affirmatively requests this use. Algorithm 2 shows an example P3P policy from http://www.walmart.com/ [3].

3. P3P Policies in Composite Services

Web service composition uses web services, no matter single or composite, as fundamental elements to create new services. It not only reuses existing services but also improves the efficiency of service development. The application of service composition is supported by many techniques, such as BPEL [4] and WSDL [5]. BPEL specifies the internal business process of a composite service. WSDL describes the interfaces of member services. Through these interfaces, member services can be invoked. At present there are many existing approaches to service composition, some of which are abstract methods and some of which aim to be industry standards [6–9].

P3P is one of the structured privacy policy languages widely used in the world today [10, 11]. It specifies how service providers will deal with the privacy information of service consumers. However, P3P cannot be applied for composite services directly because it was originally designed for single services. There is a need to research on P3P privacy policies for composite services. Statement element states the way service providers will handle the privacy information of service consumers, which is a top concern to service consumers. Therefore, the main emphasis of our research on P3P privacy policies for composite services is the Statement element. And in a Statement, the major elements are Data, Purpose, Recipient, and Retention.

As a composite service consists of several member services, the service providers of these member services have their own P3P policies that may specify different privacy practices of the same private data. For example, a composite service called Service A is constituted of three single services, and the P3P privacy policies of these services are called Policy1, Policy2, and Policy3 as shown in Algorithm 3. From Algorithms 3, 4, and 5 the Retention value of #user.name in Policy1 is indefinitely which means the data is retained for an indeterminate period of time while the Retention value of #user.name in Policy2 is stated-purpose which means the data is retained to meet the stated purpose. The Purpose value of #user.name in Policy1 is current while the Purpose value of #user.name in Policy2 is current and telemarketing. The Recipient value of #user.home-info in Policy3 is ours and unrelated while the Recipient value of #user.home-info in Policy3 is ours and same. In addition, the Optional value of #user.name in Policy1 is no which means the data must be collected while the Optional value of #user.name in Policy1 is yes which means the data is optional. Then what are the Purpose, Recipient, and Retention values of #user.name and #user.home-info in the P3P policy of Service A? What are the Optional values of #user.name

Algorithm 1: The P3P policy structure and an example P3P policy from http://www.walmart.com/ (the structure of P3P privacy policy).

```
Policy[Entity, Access, Disputes-Group, Statement(s) {Purpose [Required], Recipient [Required], Retention, Data-Group{ Data [Optional] [Categories]}}]
```

Algorithm 2: The P3P policy structure and an example P3P policy from http://www.walmart.com/ (a P3P policy from walmart.com).
privacy policies of member services are denoted by \( P \), noted as \( P_1, P_2, \ldots, P_n \). The set of Purpose values of the Data element in privacy policy of composite service is denoted by \( P_{CS} \)
\[
P_{CS} = P_1 \cup P_2 \cup \cdots \cup P_n. \]

According to Definition 1, we can get the sets of Purpose values of Data elements in privacy policy of Service \( A \):
\[
P_{A, \text{user.name}} = P_{1, \text{user.name}} \cup P_{2, \text{user.name}} \cup P_{3, \text{user.name}} = \{\text{current}\} \cup \{\text{current, telemarketing}\} \cup \emptyset
\]
\[
P_{A, \text{user.home-info}} = P_{1, \text{user.home-info}} \cup P_{2, \text{user.home-info}} \cup P_{3, \text{user.home-info}}
\]
\[
= \emptyset \cup \{\text{current, telemarketing}\} \cup \{\text{telemarketing}\}
\]
\[
= \{\text{current, telemarketing}\}. \tag{1}
\]

3.2. Recipient Definition. In a P3P privacy policy, Recipient element has six predefined values which are ours, delivery, same, other-recipient, unrelated, and public. Ours refers to the service provider and/or a third party that processes data only on behalf of the service provider for the completion of the stated purposes. Delivery refers to legal entities performing delivery services that may use data for purposes other than completion of the stated purpose. Same represents legal entities that use the data on their own behalf under equitable practices. Other-recipient represents legal entities that are constrained by and accountable to the original service provider but may use the data in a way not specified in the service provider’s practices. Unrelated represents legal entities whose data usage practices are not known by the original service provider. Public refers to public fora. In addition to ours and public, the other four predefined values represent a set of recipients, respectively. These recipients have been known explicitly by service providers. Therefore, delivery, same, other-recipient, and unrelated denote, respectively, the set of delivery services possibly following different practices, the set of legal entities following equitable practices, the set of legal entities following different practices, and the set of legal entities whose data usage practices are not known. We define the six predefined values of Recipient element in privacy policies of composite services as follows.

Definition 2. A composite service consists of \( n \) member services. If Recipient values of a Data element in privacy policies of member services include ours, the Recipient values of the Data element in privacy policy of composite service include ours as well.

Definition 3. A composite service consists of \( n \) member services. The sets of delivery values of a Data element in privacy policies of member services are noted as delivery\( \gamma_{S_1} \), delivery\( \gamma_{S_2} \),
Table 1: Recipient values of Data elements in Service A.

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Policy1</th>
<th>Policy2</th>
<th>Policy3</th>
<th>Policy4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our#user.name</td>
<td>Including</td>
<td>Including</td>
<td>Not including</td>
<td>Including</td>
</tr>
<tr>
<td>Delivery#user.name</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Same#user.name</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other-recipient#user.name</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unrelated#user.name</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Public#user.name</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Policy1</th>
<th>Policy2</th>
<th>Policy3</th>
<th>Policy4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our#user.home-info</td>
<td>Not including</td>
<td>Including</td>
<td>Including</td>
<td>Including</td>
</tr>
<tr>
<td>Delivery#user.home-info</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Same#user.home-info</td>
<td>0</td>
<td>0</td>
<td>SameCS#user.home-info</td>
<td>SameCS#user.home-info</td>
</tr>
<tr>
<td>Other-recipient#user.home-info</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unrelated#user.home-info</td>
<td>0</td>
<td>Unrelated#user.home-info</td>
<td>0</td>
<td>Unrelated#user.home-info</td>
</tr>
<tr>
<td>Public#user.home-info</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
</tr>
</tbody>
</table>

..., delivery\(S_n\). The set of delivery values of the Data element in privacy policy of composite service is denoted as delivery\(_{CS}\), delivery\(_{CS} = delivery\(_{S_1}\) \cup delivery\(_{S_2}\) \cup \cdots \cup delivery\(_{S_n}\).

If a Data element is not included in privacy policy of a member service or Recipient values of the Data element in privacy policy of a member service do not include delivery, the set of delivery values in the service's privacy policy is set to be an empty set.

Definition 4. A composite service consists of \(n\) member services. The sets of same values of a Data element in privacy policies of member services are noted as same\(_{S_1}\), same\(_{S_2}\), \ldots, same\(_{S_n}\). The set of same values of the Data element in privacy policy of composite service is denoted as same\(_{CS}\), same\(_{CS} = same\(_{S_1}\) \cup same\(_{S_2}\) \cup \cdots \cup same\(_{S_n}\).

If a Data element is not included in privacy policy of a member service or Recipient values of the Data element in privacy policy of a member service do not include same, the set of same values in the service's privacy policy is set to be an empty set.

Definition 5. A composite service consists of \(n\) member services. The sets of other-recipient values of a Data element in privacy policies of member services are noted as other-recipient\(_{S_1}\), other-recipient\(_{S_2}\), \ldots, other-recipient\(_{S_n}\). The set of other-recipient values of the Data element in privacy policy of composite service is denoted as other-recipient\(_{CS}\), other-recipient\(_{CS} = other-recipient\(_{S_1}\) \cup other-recipient\(_{S_2}\) \cup \cdots \cup other-recipient\(_{S_n}\).

If a Data element is not included in privacy policy of a member service or Recipient values of the Data element in privacy policy of a member service do not include other-recipient, the set of other-recipient values in the service's privacy policy is set to be an empty set.

Definition 6. A composite service consists of \(n\) member services. The sets of unrelated values of a Data element in privacy policies of member services are noted as unrelated\(_{S_1}\), unrelated\(_{S_2}\), \ldots, unrelated\(_{S_n}\). The set of unrelated values of the Data element in privacy policy of composite service is denoted as unrelated\(_{CS}\), unrelated\(_{CS} = unrelated\(_{S_1}\) \cup unrelated\(_{S_2}\) \cup \cdots \cup unrelated\(_{S_n}\).

If a Data element is not included in privacy policy of a member service or Recipient values of the Data element in privacy policy of a member service do not include unrelated, the set of unrelated values in the service's privacy policy is set to be an empty set.

3.3. Retention Definition. In P3P privacy policies, Retention element has five predefined values which are no-retention, stated-purpose, legal-requirement, business-practices, and indefinitely. No-retention means information is not retained for more than a brief period of time necessary to make use of it during the course of a single online interaction. Stated-purpose means information is retained to meet the stated purpose. Legal-requirement means information is retained to meet a stated purpose, but the retention period is longer because of a legal requirement or liability. Business-practices indicates information is retained under a service provider's stated business practices. Indefinitely indicates information is retained for an indeterminate period of time. When the Retention value is stated-purpose, legal-requirement, or business-practices, service providers will give the specific destruction time. If the Retention value is no-retention, we set the retention time to be zero noted as 0. And if the Retention value is indefinitely, we set the retention time to be infinity noted as \(\infty\). We choose the longest retention time of a Data.
element in the privacy policies of member services as the retention time of the Data element in privacy policy of composite service. Moreover, we use specific time instead of stated-purpose, legal-requirement, and business-practices to represent Retention values in the privacy policies of composite services. And if a Data element is not included in privacy policy of a member service, we set the Retention value of the Data element in the service’s privacy policy to be null.

**Definition 8.** A composite service consists of n member services. The specific time corresponding to the Retention values of a Data element in privacy policies of member services is denoted by \( T \), noted as \( T_{S_1}, T_{S_2}, \ldots, T_{S_n} \). The Retention value of the Data element in privacy policy of composite service is denoted by \( T_{CS} \). If \( 0 < \max\{T_{S_1}, T_{S_2}, \ldots, T_{S_n}\} < \infty \), \( T_{CS} = \max\{T_{S_1}, T_{S_2}, \ldots, T_{S_n}\} \). If \( \max\{T_{S_1}, T_{S_2}, \ldots, T_{S_n}\} = 0 \), \( T_{CS} = \) no-retention. If \( \max\{T_{S_1}, T_{S_2}, \ldots, T_{S_n}\} = \infty \), \( T_{CS} = \) indefinitely.

The Retention values of #user.name and #user.home-info in privacy policies of member services are shown in Table 2. According to Definition 8, we can get Retention values of Data elements in privacy policy of Service A as follows:

\[
T_{A, user.name} = \max\{T_{1, user.name}, T_{2, user.name}, T_{3, user.name}\} = \infty = \text{indefinitely,}
\]

\[
T_{A, user.home-info} = \max\{T_{1, user.home-info}, T_{2, user.home-info}, T_{3, user.home-info}\} = \infty = \text{indefinitely.}
\]

(2)

3.4. Attributes Definition. In a P3P privacy policy, Data, Purpose, and Recipient elements can take an optional attribute called Optional for the former and Required for the latter two. The Optional value is either no when the data is needed or yes when the data is optional. And if the Optional value of data is not explicitly specified, the Optional value of the data will take the default value (no). The Required value for Purpose elements can be always, opt-in, or opt-out. Always means the purpose is always required. Opt-in means data may be distributed to the recipient only when the user affirmatively requests this use. Opt-out means data may be distributed to the recipient unless the user requests that it not be used in this way. And if the Required value of a recipient is not explicitly specified, the Required value of the recipient will take the default value (Always). We define the values of Optional and Required attributes in privacy policies of composite services as follows.

**Definition 9.** A composite service consists of n member services. The Optional values of a Data element in privacy policies of member services are denoted by \( O \), noted as \( O_{S_1}, O_{S_2}, \ldots, O_{S_n} \). The Optional value of the Data element in privacy policy of composite service is denoted by \( O_{CS} \). If one of \( O_{S_1}, O_{S_2}, \ldots, O_{S_n} \) is no, then \( O_{CS} \) is no; otherwise \( O_{CS} \) is yes.

If a Data element is not included in privacy policy of a member service, the Optional value of the Data element in the service’s privacy policy is set to be null.

**Definition 10.** A composite service consists of n member services. The Required values of a Purpose value in privacy policies of member services are denoted by Req. not as Req_{\text{opt-in}}, Req_{\text{opt-out}}, Req_{\text{always}}. The Required value of the Purpose value in privacy policy of composite service is denoted by Req_{CS}. If one of \( Req_{S_1}, Req_{S_2}, \ldots, Req_{S_n} \) is always, then \( Req_{CS} \) is always. If all of \( Req_{S_1}, Req_{S_2}, \ldots, Req_{S_n} \) are opt-in, then \( Req_{CS} \) is opt-in. Otherwise \( Req_{CS} \) is opt-out.

If a Purpose value is not included in privacy policy of a member service, the Optional value of the Purpose value in the service’s privacy policy is set to be null.

**Definition 11.** A composite service consists of n member services. If a Recipient value is ours or public, the Required value of the Recipient value in privacy policy of composite service is the same as the value in privacy policies of member services.

If a Recipient value is not included in privacy policies of member services, the Required value of the Recipient value in privacy policy of composite service is set to be null.

**Definition 12.** A composite service consists of n member services. The Required value of public in privacy policies of member services is denoted by Red, noted as Red_{\text{opt-in}}, Red_{\text{opt-out}}, Red_{\text{always}}. The Required value of public in privacy policy of composite service is denoted by Red_{CS}. If one of \( Red_{S_1}, Red_{S_2}, \ldots, Red_{S_n} \) is always, then \( Red_{CS} \) is always. If all of \( Red_{S_1}, Red_{S_2}, \ldots, Red_{S_n} \) are opt-in, then \( Red_{CS} \) is opt-in. Otherwise \( Red_{CS} \) is opt-out.

If public is not included in privacy policy of a member service, the Required value of public in the service’s privacy policy is set to be null.

According to Definition 9, we can get Optional values of Data elements in privacy policy of Service A as shown in Table 3. The Optional value of #user.name in privacy policy of Service A is no. The Optional value of #user.home-info in privacy policy of Service A is no.

According to Definition 10, we can get Required values of Purpose values in privacy policy of Service A as shown in Table 4. The Required values of Purpose values in privacy policy of Service A are all always.
According to Definitions 11–12, we can get Required values of Recipient values in privacy policy of Service A as shown in Table 5. The Required value of same\_user.home-info in privacy policy of Service A is always. The Required value of unrelated\_user.home-info in privacy policy of Service A is opt-out.

By Definitions 1–12, we have got the Purpose values, Recipient values, Retention values, and Optional values of Data elements in Service A as well as the Required values of Purpose and Recipient elements. On the basis of the semantic associations of Purpose, Recipient, Retention, and Data elements, we can obtain the P3P privacy policy for Service A as shown in Algorithm 6.

### 4. Case Study

Consider an online travel broker service named Travel-Broker. The TravelBroker service consists of FlightBooking, HotelReservation, and Payment services. People can book plane tickets, reserve hotel rooms, and pay online through TravelBroker. The P3P privacy policies of FlightBooking service, HotelReservation service, and Payment service are called Policy\_1, Policy\_2, and Policy\_3, respectively, as shown in Algorithms 7, 8, and 9. Next we will show how to obtain P3P privacy policy for TravelBroker.

According to Definition 1, we can get the sets of Purpose values of Data elements in privacy policy of TravelBroker:

\[
P_{\text{CS, user.IDCardNo}} = P_{\text{1, user.IDCardNo}} \cup P_{\text{2, user.IDCardNo}} \\
\quad \quad \cup P_{\text{3, user.IDCardNo}} \\
= \{\text{current}\} \cup \{\text{current}\} \cup \emptyset = \{\text{current}\},
\]

\[
P_{\text{CS, user.Name}} = P_{\text{1, user.Name}} \cup P_{\text{2, user.Name}} \\
\quad \quad \cup P_{\text{3, user.Name}} \\
= \{\text{current, contact}\} \cup \{\text{current, contact}\} \\
\quad \quad \cup \{\text{current}\} = \{\text{current, contact}\},
\]

According to Definition 9, we can get Optional values of Data elements in privacy policy of TravelBroker as shown in Table 8. The Optional value of #user.IDCardNo in privacy policy of TravelBroker is no. The Optional value of #user.Name in privacy policy of TravelBroker is no. The Optional value of #user.Mobile in privacy policy of TravelBroker is no. The Optional value of #user.BankCardNo in privacy policy of TravelBroker is no.

\[
P_{\text{CS, user_MOBILE, BankCardNo}} = P_{\text{1, user.Mobile}} \cup P_{\text{2, user.Mobile}} \\
\quad \quad \cup P_{\text{3, user.Mobile}} \\
= \{\text{current, contact}\} \cup \{\text{current, contact}\} \\
\quad \quad \cup \{\text{current}\} = \{\text{current}\}.
\]

\[
P_{\text{CS, user.IDCardNo}} = P_{\text{1, user.IDCardNo}} \cup P_{\text{2, user.IDCardNo}} \\
\quad \quad \cup P_{\text{3, user.IDCardNo}} \\
= \{\text{current}\} \cup \{\text{current}\} \cup \emptyset = \{\text{current}\},
\]

\[
P_{\text{CS, user.Name}} = P_{\text{1, user.Name}} \cup P_{\text{2, user.Name}} \\
\quad \quad \cup P_{\text{3, user.Name}} \\
= \{\text{current, contact}\} \cup \{\text{current, contact}\} \\
\quad \quad \cup \{\text{current}\} = \{\text{current, contact}\},
\]
The Scientific World Journal

Algorithm 6: P3P privacy policy for Service A.

Table 6: Recipient values of Data elements in TravelBroker.

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Policy1</th>
<th>Policy2</th>
<th>Policy3</th>
<th>Policy4</th>
<th>PolicyCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oursuser.IDCardNo</td>
<td>Including</td>
<td>Including</td>
<td>Not including</td>
<td>Including</td>
<td></td>
</tr>
<tr>
<td>Deliveryuser.IDCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sameuser.IDCardNo</td>
<td>Sameuser.Name</td>
<td>0</td>
<td>0</td>
<td>Sameuser.Name</td>
<td></td>
</tr>
<tr>
<td>Other-recipientuser.IDCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Unrelateduser.IDCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Publicuser.IDCardNo</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not</td>
<td></td>
</tr>
<tr>
<td>Oursuser.Name</td>
<td>Including</td>
<td>Including</td>
<td>Including</td>
<td>Including</td>
<td></td>
</tr>
<tr>
<td>Deliveryuser.Name</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sameuser.Name</td>
<td>Sameuser.Name</td>
<td>0</td>
<td>0</td>
<td>Sameuser.Name</td>
<td></td>
</tr>
<tr>
<td>Other-recipientuser.Name</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Unrelateduser.Name</td>
<td>0</td>
<td>Unrelated2user.Name</td>
<td>0</td>
<td>Unrelated2user.Name</td>
<td></td>
</tr>
<tr>
<td>Publicuser.Name</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not</td>
<td></td>
</tr>
<tr>
<td>Oursuser.Mobile</td>
<td>Including</td>
<td>Including</td>
<td>Including</td>
<td>Including</td>
<td></td>
</tr>
<tr>
<td>Deliveryuser.Mobile</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sameuser.Mobile</td>
<td>Sameuser.Mobile</td>
<td>0</td>
<td>0</td>
<td>Sameuser.Mobile</td>
<td></td>
</tr>
<tr>
<td>Other-recipientuser.Mobile</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Unrelateduser.Mobile</td>
<td>0</td>
<td>Unrelated2user.Mobile</td>
<td>0</td>
<td>Unrelated2user.Mobile</td>
<td></td>
</tr>
<tr>
<td>Publicuser.Mobile</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not</td>
<td></td>
</tr>
<tr>
<td>Oursuser.BankCardNo</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not</td>
<td></td>
</tr>
<tr>
<td>Deliveryuser.BankCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sameuser.BankCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Other-recipientuser.BankCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Unrelateduser.BankCardNo</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Publicuser.BankCardNo</td>
<td>Not including</td>
<td>Not including</td>
<td>Not including</td>
<td>Not</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Retention values of Data elements in FlightBooking, HotelReservation, and Payment services.

<table>
<thead>
<tr>
<th>Retention</th>
<th>Policy1</th>
<th>Policy2</th>
<th>Policy3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuser.IDCardNo</td>
<td>1 month</td>
<td>20 days</td>
<td>Null</td>
</tr>
<tr>
<td>Tuser.Name</td>
<td>1 month</td>
<td>∞</td>
<td>2 months</td>
</tr>
<tr>
<td>Tuser.Mobile</td>
<td>1 month</td>
<td>∞</td>
<td>2 months</td>
</tr>
<tr>
<td>Tuser.BankCardNo</td>
<td>Null</td>
<td>Null</td>
<td>1 month</td>
</tr>
</tbody>
</table>

Table 8: Optional values of Data elements in TravelBroker.

<table>
<thead>
<tr>
<th>Data</th>
<th>Policy1</th>
<th>Policy2</th>
<th>Policy3</th>
<th>PolicyCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>User.IDCardNo</td>
<td>No</td>
<td>No</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>User.Name</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>User.Mobile</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User.BankCardNo</td>
<td>Null</td>
<td>Null</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

According to Definition 10, we can get Required values of Purpose values in privacy policy of TravelBroker as shown in Table 9. The Required value of current in privacy policy of TravelBroker is always. The Required value of contact in privacy policy of TravelBroker is opt-out.

According to Definitions 11–12, we can get Required values of Recipient values in privacy policy of TravelBroker as shown in Table 10. The Required value of same1user.Name in privacy policy of TravelBroker is always. The Required value of unrelated2user.Name in privacy policy of TravelBroker is opt-out. The Required value of same1user.Mobile in privacy
Algorithm 7: P3P policies of FlightBooking service, HotelReservation service, and Payment service (P3P policy of FlightBooking service).

```
Policy₁(\{Entity(#business.name): FlightBooking, \ldots\},
  \{Purpose: (current),
  \quad \text{Recipient: (ours),}
  \quad \text{Retention: (legal-requirement),}
  \quad \text{Data: (#user.IDCardNo)}\})
```

Algorithm 8: P3P policies of FlightBooking service, HotelReservation service, and Payment service (P3P policy of HotelReservation service).

```
Policy₂(\{Entity(#business.name): HotelReservation, \ldots\},
  \{Purpose: (current),
  \quad \text{Recipient: (ours),}
  \quad \text{Retention: (legal-requirement),}
  \quad \text{Data: (#user.IDCardNo)}\})
```

Table 9: Required values of Purpose values in TravelBroker.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Policy₁</th>
<th>Policy₂</th>
<th>Policy₃</th>
<th>Policy₄</th>
<th>Policy₅</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td>Opt-out</td>
<td>Opt-in</td>
<td>Null</td>
<td>Opt-out</td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Required values of Recipient values in TravelBroker.

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Policy₁</th>
<th>Policy₂</th>
<th>Policy₃</th>
<th>Policy₄</th>
<th>Policy₅</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same₁.user.Name</td>
<td>Always</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Always</td>
</tr>
<tr>
<td>Unrelated₂.user.Name</td>
<td>Null</td>
<td>Opt-out</td>
<td>Null</td>
<td>Opt-out</td>
<td></td>
</tr>
<tr>
<td>Same₂.user.Mobile</td>
<td>Always</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Always</td>
</tr>
<tr>
<td>Unrelated₂.user.Mobile</td>
<td>Null</td>
<td>Opt-out</td>
<td>Null</td>
<td>Opt-out</td>
<td></td>
</tr>
</tbody>
</table>

policy of TravelBroker is always. The Required value of unrelated₂.user.Mobile in privacy policy of TravelBroker is opt-out.

By Definitions 1–12, we have got the Purpose values, Recipient values, Retention values, and Optional values of Data elements in TravelBroker as well as the Required values of Purpose and Recipient element. On the basis of the semantic associations of Purpose, Recipient, Retention, and Data elements, we can obtain the P3P privacy policy for TravelBroker as shown in Algorithm 10.

5. Related Work

When people enjoy the convenient, efficient, and flexible services on the Internet, their privacy information is inevitably collected by service providers. References [12, 13] assessed the risks of privacy abuse by game theory. The conclusion was that service providers tended to seek for undue interests by misusing and exposing users’ privacy information. In order to prevent users’ privacy information from being abused, service providers are asked to publish their privacy policies on their websites. P3P privacy policy has been used by more and more websites. By July 2003, 30% of the top 100 websites had used P3P. And 23% of the top 500 websites had used P3P [14].

Some scholars have researched on the semantics for P3P privacy policy and the relationships among several P3P privacy policies. The work from Hogben expressed P3P privacy policy formally by an OWL ontology [15]. This work had been written to the W3C Working Group Note. Yu et al. proposed data-centric formal semantics for P3P policies, which precisely and intuitively modeled the relationships between different components of P3P statements [16]. Agrawal et al. enunciated key privacy principles for privacy-aware database systems and proposed a strawman design for the database systems using purpose-centric base [17]. Boontawee Suntisrivarnaporn and Khurat proposed semantics for P3P employing a data-purpose centric relational table [18]. They used an OWL ontology to systematically and precisely describe P3P privacy policy. In our previous work, we put forward data-recipient centric formal semantics for P3P policies, which supported the semantic conflict detection of P3P [19]. May et al. proposed two flexible policy relations derived from bisimulation in process calculi [20]. They illustrated the relations using examples from P3P. Nikolaos Papanikolau et al. presented an approach to check for refinement between policies [21]. They automatically generated CSP models from P3P policies and then performed various tests using the FDR model checker.

With the wide application of web service composition, the protection of users’ privacy information in composite services attracts more and more attention. However, there are only a few scholars studying the application of P3P privacy policies in web service composition. Khurat et al. enhanced P3P to be able to support composite services, proposed a formal semantic for P3P employing a data-purpose centric relational table, and defined combining methods to obtain privacy policies of composite services [22]. However, due to the syntax of P3P being extended, P3P privacy policies of composite services generated by such methods could not be directly used to match with users’ privacy preferences. Our proposed method does not change the syntax of P3P. P3P privacy policies of composite services obtained by our method can match with users’ privacy preferences directly. Michele Chinosi and Trombetta checked whether a BpeX-represented business process was compliant with a P3P privacy policy by introducing a data model for BPMN and a corresponding XML-based representation called BpeX [23]. Li et al. proposed a graph-transformation based framework to check whether an internal business process adhered to the organizations’ P3P privacy policies [24]. Both [23, 24] applied
P3P privacy policies in web service composition by business processes. However, they did not propose methods to obtain P3P privacy policies for composite services, yet assuming that P3P privacy policies of composite services had already existed. Our work proposes a method to obtain P3P privacy policies for composite services, which is the foundation of their work. Dong et al. presented an approach to implement privacy policy aggregation with P3P [10]. But they did not consider the internal relationship between Data elements and Purpose, Recipient, and Retention elements. In our work, we generate the Purpose, Recipient, and Retention values for each Data element, respectively, which avoids potential conflicts between Data elements and other elements.

6. Conclusions and Future Work

Privacy protection in composite services has become an important issue. P3P is an existing technology employed to protect privacy. In order to apply P3P directly to composite services, we propose a method to obtain P3P privacy policies for composite services in the paper. We present the definitions of Purpose, Recipient, and Retention elements as well as Optional and Required attributes for P3P policies of composite services in the method and provide an instantiation to demonstrate the feasibility of the method.

The base data schema of P3P is defined in a hierarchy. It will cause conflicts of data hierarchy constraints if the upper level data has more strict constraints than its lower level data. For example, #user.bdate is the higher level data relative to #user.bdate.ymd.year. If the Optional value of #user.bdate is yes, the Optional value of #user.bdate.ymd.year can be no or yes. But if the Optional value of #user.bdate is no, the Optional value of #user.bdate.ymd.year must be no. In this paper, there is no conflict of data hierarchy constraints in P3P privacy policies. So we do not consider the conflicts of data hierarchy constraints when obtaining P3P privacy policies for composite services. As future work, we plan to consider the conflicts of data hierarchy constraints and enhance our method to resolve it.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant no. 61272083).

References


Submit your manuscripts at http://www.hindawi.com