NEPP: Negotiation Enhancements for Privacy Policies

Authors: M. Maaser, S. Ortmann, P. Langendörfer; IHP microelectronics GmbH, Im Technologiepark 25, 15236 Frankfurt (Oder), Germany

ABSTRACT

Privacy has been a hot topic in research for several years. A lot of different approaches to protect privacy have been proposed recently. Here we present a privacy negotiation language that combines the capabilities of P3P and APPEL in a more dynamic manner. It enables service providers as well as service users to define their privacy needs and practices by using extended P3P policies. Different extensions, invisible for the negotiation opponent, allow defining privacy protective measures for service users and requirements of service providers. These policies span a certain scope of requirements that comprises any acceptable negotiation result. That provides a basis for both sides to negotiate about the data and their potential recipients, purposes, payment etc.

1. INTRODUCTION

A lot of internet users are concerned about their privacy [3][8]. These concerns have led to the development of P3P [5] and APPEL [4] by the W3C. P3P provides means to service providers to express which data is gathered by the service provider as well as for which purpose etc. APPEL provides means to service users to express their preferences. The P3P approach is a pure opt in or opt out model [11][2]. Thus, if the user preferences and the service provider policy do not fit to each other the only option of the user is not to use this service. This provides nothing more than a simple “take it or leave it” dualism. The drawbacks of such a static approach are on both sides. On one hand at least some service users have to give up more privacy than what they would prefer or are excluded from using interesting services. On the other hand service providers have to balance in their privacy policies, their own requirement to get user data against the user requirement to protect their privacy. At the end this means that the service provider is still loosing some concerned users while it does not get as much data from open minded or naïve users as it could get. A recent study, see [6], shows that a significant percentage of users are willing to provide additional data if the service provider offers incentives like free trial version of software, reduced prices for the service under negotiation etc. Thus, privacy negotiation tools can help to accommodate the needs of both parties, i.e. more data for service providers, better prices or better privacy for certain groups of users.

Privacy negotiation tools should provide service providers and service users with means to express their own policies as well as potential alternatives. Also, **both** parties should be allowed to propose a new policy while negotiating. Note, by the term negotiation we really mean a kind of bargaining about the content of the resulting privacy contract. We intend to enable both negotiation parties to offer counterproposals based on former offers. For example a user offers the service provider to pay a certain amount for the service. Based on that amount the service provider may create a counterproposal meeting own requirements. This is quite different from “negotiation approaches” in which two parties reveal e.g. a list of cipher algorithms they provide and then select those for further communication that are supported on both sides.

2. RELATED WORK

There are several privacy related tools that are based on P3P and APPEL specifications. AT&T’s Privacy Bird [1] is a free plug-in for Microsoft Internet Explorer. It allows users to specify privacy preferences regarding how a website stores and collects data about them. The user’s preferences are set by enabling/disabling different rules out of a set of fixed options. The user is not able to define further rules or specific restrictions. If the user visits a website, the Privacy Bird analyzes the policy provided and indicates whether or not the policy matches the user’s preferences. PAWS [9] also rely on P3P and APPEL means but allows discovery of privacy policies within ubiquitous environments. All these tools are a valuable step into the right direction, but they still lack means to personalize privacy policies.

To the best of our knowledge there are only two approaches that allow step-by-step modification of the originally proposed policy by service user and service provider namely [10][7]. But in both approaches only the service provider is enabled to present new versions of its policy, whereas the user can only accept or reject the proposal. The user side can only provide hints, why the proposed policy was not accepted. These hints may help the service provider to calculate a more suitable proposal.

We do not consider this a real negotiation. Both negotiation opponents should define their secret preferences that specify whose acceptable room to negotiate. Both negotiation parties should be capable to offer counterproposals based on former offers. Finally, successful negotiations should close with a mutually signed privacy contract that contains all negotiated content.

3. ENHANCEMENTS FOR NEGOTIATION

In the P3P and APPEL world there are two types of information: public available privacy policies and secret preferences. The latter is defined by potential service users using APPEL and is never exposed to the service provider side. The service provider has no hidden preferences in the regular P3P/APPEL approach, since it does not need them due to the opt-in opt-out facilities. In our approach both parties need to define their preferences in order to define a certain range for the bargaining procedure. These preferences are never exposed to the opposite side. Successful negotiations finish with a mutually agreed policy, called contract. The exchange of information during the bargaining procedure is done by offering contract proposals. We extended the P3P language to describe those elements. Some of our extensions are applied to the public policies whereas others are only used within the secret preferences. The semantics of extensions used in preferences as well as in contract proposals depends on the document in which they are used. The secret preferences are meant to be used for all contract negotiations. To support this flexibility the secret preferences shall span a certain space to find a compromise as result of the envisioned negotiations.

3.1 General P3P Extensions

According to P3P standard, a policy consists of a set of statements, which are the basis for negotiation. A statement includes the following xml-tags: purpose, recipient, retention and data group. In data-groups, a set of single data elements can be referenced.

We consider a policy to build up a multi-dimensional space. Thereby every statement defines exactly one dimension. Within a statement, purpose, recipient, retention and data group build their own dimensions. Hence any statement also characterizes an n-dimensional space, too. Since P3P only allows statements to contain enumerations as parameters, the content of a policy is exactly defined. Surely this enables to decide about the acceptance of a policy but does not provide flexibility for negotiation. Purpose, recipient and retention will remain unaffected by our approach. We extended the data group and the data elements to receive variable valuations. The range of their values may be Boolean or an enumeration like in P3P. Furthermore they can be expanded to single- or double-bounded intervals. However, any interval of real numbers is supposable. This way, data group and data may be extended by another dimension. Thus, elements have to be developed and integrated which are capable to specify such dimensions. Details on these new language features are discussed below.

3.1.1 Quantity

To enhance negotiation possibilities we extended the P3P standard with language features for measurable data and elements that allow remuneration. Unlike in P3P standard, in our extension a data-group element may also contain measurable data. Therefore the <DATA> element is extended with an option to specify a certain amount. We call this a quantity. Quantities specify a range of values of a <DATA> while those without specified quantity apply only to the mere existence of such data item. I.e. a persons credit card number can only be submitted or not, but her position could be limited to certain granularity. The elements amount, dimension and negotiationbase are integrated into the <DATA> tag. It occurs in the following way now:

<DATA ref=”#name”> amount dimension [negotiationbase] </DATA>

Amount limits the valid range of numbers of the corresponding data. Here dimension is a physical unit like meter for a distance, hour or minute for a time or Ws for energy. It is an element of an enumeration type and different kind of dimensions can be converted and compared to each other. Thus it defines the valid range of values of the data element. An example for using quantities is given in Listing 1. Here a part of the preferences of a guiding service is displayed. The service provider requires the longitude and latitude of the user’s position with a maximum deviation of ten meters. According to the negotiationbase, the initial proposal has to ask for an accuracy of 3 meters. Furthermore, if the deviation specified in a counterproposal is larger than ten meter, the counterproposal is not acceptable for the service provider.

Listing 1: Example preferences of a service provider using Quantities within the P3P <DATA> tag

```
<DATA-GROUP>
  <DATA ref="#user.location.longitude"/>
  <DATA ref="#user.location.latitude"/>
  <DATA ref="#user.location.accuracy">
    <atmost>10</atmost><meter/>
    <negotiationbase>3</negotiationbase>
  </DATA>
</DATA-GROUP>
```

3.1.2 Charge

For remuneration of service usage we consider a special kind of data, which represents the amount of money to be paid for that service. Because money is more substantial than data we augment the <DATA-GROUP> with a new element called <CHARGE>. It is structured in the following way.

<CHARGE>amount currency dimension [negotiationbase]</CHARGE>

The amount defines the valid scope of negotiation. Currency denotes the currencies of the fee. It is of type enumeration and simple pattern matching can be used to detect whether or not a certain type is known. Also comparing different kinds of currencies is possible, if their exchange rates are known. Dimension defines here the accounting period for a <CHARGE>, i.e. per minute or per use. Like currency, it is of type enumeration and different kind of dimensions can be converted and compared to each other. Consequently the combination of amount, currency and dimension sizes the quantity of a charge. Negotiationbase is an additional tag as already shown in the quantity section that may be used to support improved negotiation strategies. It defines the start value for negotiation of amount. Furthermore, it is specified that a <DATA-GROUP> may only contain one <CHARGE> tag. This condition is needed to associate a charge clearly with the corresponding data. An example using <CHARGE> is presented in Listing 2. Here the <CHARGE> defines an interval for negotiation of 0.00 to 0.05 Euro per minute. The negotiationbase tag indicates that the first offer should be 0.01 Euro per minute.

Listing 2: Example of preferences of a service user applying the new tag <CHARGE>

```
<DATA-GROUP>
  <DATA> ... </DATA>
  <CHARGE>
    <atmost>0,05</atmost><eur/><perMinute/>
    <negotiationbase>0,01</negotiationbase>
  </CHARGE>
</DATA-GROUP>
```

3.1.3 Rewards

In addition we introduced a new tag, called <REWARDS>, it can be used to specify incentives that are given to a service user in case she/he reveals additional information. It is an independent xml tag and is included in-plane with <PURPOSE>, <RECIPIENT>, <DATA-GROUP> and <RETENTION>. This enhances the options of the corresponding statement. An offered reward could initiate a user to reveal more information. Also users may claim specified rewards in their preferences for certain data. Rewards can be used in the secret preferences as well as in public contract proposals. A reward defined in a preference is bounded to the related statement. The reward may be released if the corresponding statement is fulfilled. In contrast to that, a reward stated in a contract proposal is applied globally, i.e. it does not belong only to the statement in which it is defined. In fact it is offered to accept the complete contract proposal. Logically there are a lot of rewards imaginable. Thus, rewards are defined as enumerations analogous to currency. A typical reward is a <VOUCHER> or a <TRIAL>. Every type of reward is defined in its own xml tag. Hence, any thinkable kind of reward can be added. But it has to be known to both sides in order to have a positive effect. Otherwise it is ignored. A typical example of a <DATA-GROUP> with <REWARDS> is displayed in Listing 3. Here the specification of rewards granted for accepting the related <STATEMENT>, is displayed. The offered rewards are a <TRIAL> of at most five days and a <VOUCHER> of at most five US dollar. The engagement and the final volume of this reward are open to negotiation. Note that <REWARDS> is an optional tag. This ensures backward compatibility with P3P.

Listing 3: Example preference of a service provider stating <REWARDS>

```
</DATA-GROUP>
<REWARDS>
  <TRIAL><atmost>5</atmost><days/></TRIAL>
  <VOUCHER><atmost>5</atmost><usd/></VOUCHER>
</REWARDS>
...
```

3.1.4 Digital Signature

Successful negotiations close with a mutually signed contract. Digital signatures were integrated into such contracts to link the negotiated content to the negotiating parties. The P3P standard does not provide an opportunity to integrate digital signatures. Thus, to ensure backward compatibility, we use xml comments to integrate the digital signatures.

3.2 P3P Extensions for Secret Preferences

APPEL allows potential service users to define their privacy guidelines by constituting a set of rules. Detected policies are checked to verify whether or not they meet the user preferences. The result determines acceptance or denial of the policy. However the user side only can use APPEL. To the best of our knowledge, there is no known way to allow secret preferences on the service provider side. To enable a real bargaining both negotiation parties should be able to define secret preferences. In our concept both parties have their own secret preferences, written as an enhanced P3P policy. The secret negotiation preference specifies an n-dimensional space. That space comprises of all potentially acceptable and only these policies – without explicit enumeration.

Surely unique requirements of users and service provider have to be considered. In order to enable individualization three new tags were integrated into the policies. These tags are <PROHIBITED/>, <ALLOWED/> and <OPTIONAL/>.

3.2.1 Prohibitions and Permissions

Users are able to define statements in their requirements, which are explicitly prohibited or allowed. To mark statements as prohibited ones, the <PROHIBITED/> tag is used. In this way users are capable to prohibit single data or groups of data for certain purposes, recipients or retentions. It is also possible to prohibit data or groups of data for all purposes or all recipients etc. Even prohibiting certain purposes or recipients without referencing specified data is feasible. That is, prohibitions specify domains that are explicitly prohibited. Preferences that are solely composed of prohibitions, implicitly allow all non-stated data. Users are also enabled to define rewards they want to receive to release normally prohibited data. Listing 4 shows preferences - containing prohibitions - of a user willing to use a guiding service. The first statement (beginning at line 02) prohibits accepting any accuracy within 0 to 8 meter. The next statement (line 12) forbids giving the users last name anyhow. Declaring no recipient and purpose prohibits stated data for anything and anybody. The third statement (line 19) prohibits paying more than 0.10 Euro per minute for guiding. The last statement (line 28) forbids gaining the users email unless the service provider releases a voucher about at least 3 US Dollar.

Listing 4: Example preference of a potential user willing to use a guiding service

```
01 <POLICY>
02   <STATEMENT>
03   <PROHIBITED/>
04     <PURPOSE> <guiding/> </PURPOSE>
05     <RECIPIENT> <ours/> </RECIPIENT>
06     <DATA-GROUP>
07       <DATA ref="#user.location.accuracy">
08                 <atmost>8</atmost><meter/>
09       </DATA>
10     </DATA-GROUP>
11   </STATEMENT>
12   <STATEMENT>
13   <PROHIBITED/>
14     <DATA-GROUP>
15       <DATA ref="#user.lastname"/>
16     </DATA-GROUP>
17   </STATEMENT>
18   <STATEMENT>
19   <PROHIBITED/>
```

```
20      <PURPOSE> <guiding/> </PURPOSE>
21      <RECIPIENT> <ours/> </RECIPIENT>
22      <DATA-GROUP>
23        <CHARGE> <atleast>0,10</atleast><eur/>
24          <perMinute/>
25        </CHARGE>
26      </DATA-GROUP>
27    </STATEMENT>
28    <STATEMENT>
29    <PROHIBITED/>
30      <DATA-GROUP>
31        <DATA ref="#user.email"/>
32      </DATA-GROUP>
33      <REWARDS>
34        <VOUCHER>
35          <atleast>3</atleast><usd/>
36        </VOUCHER>
37      </REWARDS>
38    </STATEMENT>
39  </POLICY>
```

Similarly, the <ALLOWED/> tag declares permissions. Like prohibitions, they explicitly permit data for certain purposes or recipients. If user preferences contain permissions, all non-stated data are implicitly prohibited. Needless to say, there is no point in using rewards in permissions.

Regarding privacy demands, the security of user data is ranked first. Consequently, prohibiting statements are more restrictive than permitting ones. If preferences solely state prohibitions or permissions, the matter is simple to understand. Consider the case of using prohibitions and permission together in preferences. This may simplify the complexity of defining preferences. Since permissions implicitly prohibit all non-stated data, it doesn't make any sense to define additional prohibitions outside the permitted domain. Their combination can be used to prohibit certain intervals inside a permitted domain. I.e. a user possesses three different data items A, B and C. The user wants to protect C completely and allows either A or B. For that purpose the user defines three statements in her preferences. The first two statements solely allow A and B respectively. The third statement prohibits the combination of A and B. As the result, A and B are explicitly allowed by their permissions. Additionally C is implicitly prohibited by these permissions. Finally the stated prohibition directly forbids to request A and B together.

3.2.2 Optional

For service providers, the secret preference contains the data they want to collect und the purposes, retentions and recipients they want to use the data for. Above all, the concept allows dividing different classes of data items to accentuate the need for them. Thus the data items have to be classified into requirements and optional data, by using the <OPTIONAL/> tag. This tag is placed directly into the <STATEMENT> in the same level as <PURPOSE>. Statements in the secret preference of service provider that contain no optional tag are classified as requirements automatically. Consequently the usage of different data classes depends on the negotiation strategy of the service. Logically contract proposals are never acceptable until all requirements are fulfilled.

3.3 Contracts and Contract Proposals

Contract proposals contain a set of paragraphs that conform the preferences of the proposing negotiation party. Logically these documents contain public exchanged information. Since these proposals could be used to determine a contract, they shall not include scopes of negotiation. Amounts of charges and quantities have to be fixed as Boolean or enumerations. Furthermore, listing secret information, regarding the <OPTIONAL/>, <ALLOWED/> and the <PROHIBITED/> tag, is prohibited. It is required that all statements in contract proposals are numbered to identify them in counterproposals. Since contract proposals may become a mutually signed privacy contract, they are signed by the offering party. Contracts are composed in the same manner as contract proposals. Thereby they contain the complete negotiation result and the respective digital signatures of both negotiation parties.

To summarize, it is also possible to negotiate without our extensions. In that case items such as recipients, purposes and the corresponding data items can be discussed. Thus, backward compatibility to regular P3P is guaranteed.

4. SUMMARY & OUTLOOK

This article determines our position and the situation in stating and contracting privacy in the Internet. Lacking negotiation capability has been identified as a shortcoming. Introduced P3P enhancements allow service users and service providers to negotiate about data and its potential recipients, purpose, payment etc. Therefore every negotiation-enabled device has to define own secret preferences as an enhanced P3P policy. To define a certain room to negotiate that is not only selected by enumeration, the P3P known elements statement, data-group and data were extended and new elements like charge are added. To regard unique requirements of service users and service providers new tags that inform about the intended use of statements, where integrated into the preferences. Every negotiating party may accept, change or reject single statements as well as whole policies. Successful negotiations end up with a mutually signed contract. Digital signatures were integrated into such contracts to link the negotiated content to the negotiating parties.

To demonstrate the abilities of our P3P enhancements and the negotiation concept we implemented a negotiation-enabled client and a negotiation-enabled server. Both are capable to negotiate automatically based on their secret preferences. The client as well as the server are backward compatible to P3P and are capable to operate on static P3P policies and known tools like Privacy Bird.

In the future the two negotiation parties and thus their respective preferences with permitted, prohibited, required and optional statements must be merged, in order to have a tool which can perform both sides of negotiation. This will enable negotiations between enterprises and in the peer-to-peer domain. Due to the complexity of enhanced P3P appropriate editor tools should be designed to support the every day user in creation of preferences.

5. REFERENCES

[1] AT&T Privacy Bird, AT&T Corporation, http://privacybird.com; last visited December 2005

[2] Bennicke M., Langendörfer P., *Towards Automatic Negotiation of Privacy Contracts for Internet Services.* Proceedings of 11th IEEE Conference on Computer Networks, IEEE Society Press, 2003

[3] Cranor L.F., Beyond Concern: Under-standing Net Users' Attitudes About Online Privacy. In Ingo Vogelsang and Benjamin M. Compaine, eds. *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy.* Cambridge, Massachusetts: The MIT Press, p. 47-70, 2000

[4] Cranor L.F., Langheinrich M., *A P3P Preference Exchange Language 1.0.* http://www.w3.org/TR/P3P-preferences/, 2002-04-15

[5] Cranor L.F., Langheinrich M., Marchiori M., *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification.* http://www.w3.org/TR/P3P/, 2002-04-16

[6] Drücke R., *Einstellungen und Haltungen bezüglich Privatsphäre beim Mobiltelefonieren. Eine empirische Untersuchung unter Studierenden,* Technical Report, MIB Europa Universität Viadrina Frankfurt Oder, Große Scharrnstrasse 59, D-15230 Frankfurt Oder

[7] El-Khatib K., *A Privacy Negotiation Protocol for Web Services,* Workshop on Collaboration Agents; Autonomous Agents for Collaborative Environments Halifax, Nova Scotia, Canada. October 13, 2003

[8] Jupiter Research: *Consumers worried about online privacy*, 2002 available at: http://www.nua.com/surveys/index.cgi?f=VS&art_id=905358019&rel=true; last visited Dec. 03

[9] Langheinrich M.: *A Privacy Awareness System for Ubiquitous Computing Environments*. In: Gaetano Borriello, Lars Erik Holmquist (Eds.): 4th International Conference on Ubiquitous Computing (Ubicomp 2002), LNCS No. 2498, Springer-Verlag, pp. 237-245, September 2002.

[10] Preibusch S., *Implementing Privacy Negotiation Techniques in E-Commerce*, 7th IEEE International Conference on E-Commerce Technology, IEEE CEC 2005, July 19-22, 2005, Technische Universität München, Germany

[11] Thibadeau R., *A Critique of P3P: Privacy on the Web*. The eCommerce Institute, School of Computer Science, Carnegie Mellon University