Using SITDRM for Privacy Rights Management

Farzad Salim
School of IT & CS,
The University of Wollongong,
NSW, 2522, Australia
fsalim@uow.edu.au

Nicholas Paul Sheppard
School of IT & CS,
The University of Wollongong,
NSW, 2522, Australia
nps@uow.edu.au

Reihaneh Safavi-Naini
School of IT & CS,
The University of Wollongong,
NSW, 2522, Australia
rei@uow.edu.au

ABSTRACT

SITDRM [1] is a privacy protection system that protects private data through the enforcement of MPEG REL licenses provided by consumers. Direct issuing of licenses by consumers has several usability problems that will be mentioned in this paper. Further, we will describe how SITDRM incorporates P3P language to provide a consumer-centered privacy protection system.

Categories and Subject Descriptors

H.5 [**Information Interfaces and Presentation**]: User-centered design

General Terms

Design, Languages, Security, Human Factors

Keywords

Privacy Protection, DRM, MPEG-21, P3P

1. INTRODUCTION

In response to consumer's growing concerns about privacy, enterprises publish a *privacy policy* that is a representation of promises made to data owners regarding the uses of their private data. To provide a standard way of communicating privacy policies to consumers, the World Wide Web consortium has proposed a standard policy language, the Platform for Privacy Preferences (P3P) [1]. P3P policies can be read, summarized and matched against users' privacy preferences by P3P-enabled browser software (*P3P agents*). Therefore, data owners can be prompted on exactly what data is collected, for what purposes this data is being used and how long it is retained. However, publishing a P3P policy does not provide any technical guarantee that enterprises act according to their policies once they have obtained users personal data.

To control data handling within enterprises, we have proposed a privacy protection system, [2], *SITDRM* [2]. The core concept of SITDRM is the use of *MPEG REL* licenses that are formulated by consumers and enforced within a SITDRM system. An MPEG REL license is a digital data file that specifies usage rules for the collected data. A rule may specify a range of criteria, such as the person to whom the right is issued, the frequency of access, license expiry date, restriction of transfer to other devices, etc.

Whilst the SITDRM approach to privacy protection binds the enterprise data handling to the privacy promises made to customers, it has three usability weaknesses. First, constructing a license can become a complex task for customers of real world enterprises because licenses are written in a formal language (MPEG REL), therefore consumers are required to have technical knowledge. In addition, consumers may be obliged to construct several licenses as there may exist many users (enterprise employees) who need to access the private data under different conditions. Second, roles/users within an enterprise change more frequently than the purposes for which the data is being collected. Currently, customers must provide a new license each time the roles/users (license holders) change. Third, in SITDRM, templates for creating a license are assumed to be manually constructed by a privacy officer who knows about the enterprise privacy policy and there is no systematic approach for doing so.

To deal with these shortcomings, we employ the P3P language and propose tools to communicate enterprise privacy policies to customers, as well as allowing them to construct data licenses. A P3P policy is more abstract than the access control rules expressed in an MPEG REL license and allows data owners to specify the general purposes for which data are being collected. The combined use of these two languages will bridge the gap between the user friendliness and the abstraction required for consumers to specify their privacy preferences and the precision needed for a license to be enforceable within an enterprise. Hence, issuing a license becomes easier for customers and also bypasses the need for re-issuing licenses when an internal role changes and the purpose remains the same.

2. PROPOSED SITDRM ARCHITECTURE

[1] Smart Internet Technology Digital Rights Management System

[2] Note that due to the shortage of space we do not provide any background information in this paper. Readers are encoureged to refer to the refered papers for more information.

In this section we will describe how SITDRM has incorporated P3P language for presenting privacy policies to customers as well as collecting their preferences. In addition, we will show how P3P preferences are mapped to MPEG REL licenses that are enforceable.

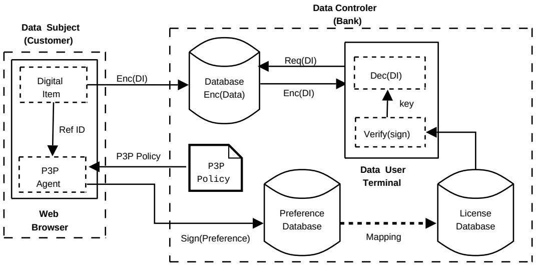


Figure 1: P3P-Enabled SITDRM Architecture

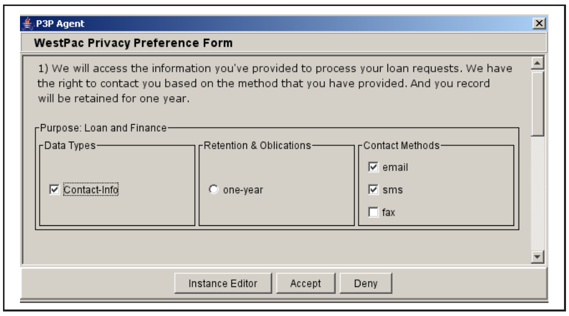
The proposed architecture introduces three new components: a *P3P policy*, a *P3P agent* and *mapping rules*. We assume that there is a Chief Privacy Officer *(CPO)* who writes a which signifies the data handling of the enterprise. The P3P policy agent and mapping rules will be described in the following sections.

2.1 Specifying P3P Preferences

The P3P provides a user friendly language and a protocol to inform data owners of an enterprise privacy practices. In reality, P3P policies after being accepted by consumers, can be considered as their privacy preferences. For instance, consider a policy statement that states that the collected phone numbers will be used for marketing purposes. In this scenario, if a consumers accept the policy statement, we can safely consider the statement as data owner's privacy preference about the use of their phone number.

The design of the P3P Agent is centered around the above idea, to allow a data owner to easily modify an enterprise P3P policy to create their privacy preferences. The P3P agent collects a P3P policy and generates a *preference template*, which is a graphical representation of the statements that constitute the policy. The elements that constitute a statement in the template can either be fixed or modifiable, depending on the attribute that CPO has specified. This allows data owners to modify a policy based on their privacy needs. We refer to the modified P3P policy as *P3P Preferences*. Figure 2 shows a sample P3P preference template where for every statement in the policy, an informal description is followed by a set of modifiable check boxes based on the P3P policy syntax.

Thus far we have described how the P3P agent provides an interface to inform consumers about an enterprise privacy policy in a systematic way. In addition, we have introduced a method by which data owners can specify their preferences through modifying a P3P policy. Whilst P3P language is suitable for the communication of privacy policies/preferences with customers, it is poorly suited for specifying enforceable access control rules. In the following section we will describe how we can automate the process of creating enforcable licences from a privacy preferences.



WestPac Privacy Preference Form

1) We will access the information you've provided to process your loan requests. We have the right to contact you based on the method that you have provided. And you record will be retained for one year.

Purpose: Loan and Finance

Data Types: ☑ Contact-Info

Retention & Oblications: ○ one-year

Contact Methods: ☑ email ☑ sms ☐ fax

Figure 2: P3P Preference Template

2.2 Constructing a License

In this section we will briefly describe the idea behind the *Mapping Console* tool that was developed to assist CPOs to map a P3P preference to an MPEG REL license.

Vocabulary is a fundamental part of a language. Hence, the Mapping Console provides a central point where the necessary vocabulary for creating an enterprise P3P policy and MPEG REL licenses are introduced and stored. In addition, it allows the CPO to specify the rules for transforming an element in P3P policy language to an element in a license.

Figure 3 illustrates the associations between the components of a P3P statement and an MPEG REL grant. Those connections with dotted-lines show the areas where there is no direct relationship between the two components.

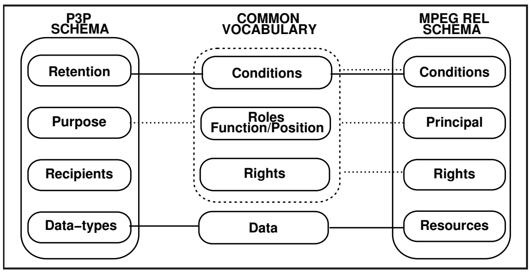


Figure 3: P3P statement & MPEG-REL grant

3. CONCLUSION

In this paper we have discussed our approach to extending SITDRM architecture with a P3P handling component. Our extention will improve the usability of the SITDRM and enable us to address two main goals. First, to facilitate the communication of privacy policies with data owners. This also includes enabling them to easily specify an enforceable privacy preference. Second, to provide a systematic way of creating templates, through which data owners can specify their privacy preferences.

4. REFERENCES

[1] L. Cranor, M. Langheinrich, M. Marchiori, and M. Presler-Marshall. The platform for privacy preferences 1.0 (P3P 1.0) specification. 2002.

[2] N. P. Sheppard and R. Safavi-Naini. Protecting privacy with the MPEG-21 IPMP framework. In *6th Workshop on Privacy Enhancing Technologies*, pages 152–171, 2006.