A Privacy Negotiation Algorithm for Digital Rights Management

Jurairat Phuttharak, and Chanboon Sathitwiriyawong

Faculty of Information Technology, and
Research Center for Communications and Information Technology (ReCCIT)
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
Email: s4067018@kmitl.ac.th, chanboon@it.kmitl.ac.th

Abstract: Internet-based distribution of digital contents provides great opportunities for producers, distributors and consumers, but it may seriously threaten users' privacy. The Digital Rights Management (DRM) systems which one of the major issues, concern the protection of the ownership/copyright of digital content. However, the most recent DRM systems do not support the protection of the user's personal information. This paper examines the lack of privacy in DRM systems. We describe a privacy policy and user's privacy preferences model that protect each user's personal information from privacy violation by DRM systems. We allow DRM privacy agent to automatically negotiate between the DRM system policy and user's privacy preferences to be disclosed on behalf of the user. We propose an effective negotiation algorithm for the DRM system. Privacy rules are created following the negotiation process to control access of the user's personal information in the DRM system. The proposed privacy negotiation algorithm can be adapted appropriately to the existing DRM systems to solve the privacy problem effectively.

Keywords: Digital Rights Management, Privacy Policy, User's privacy preferences, Privacy Negotiation

1. INTRODUCTION

Contents are increasingly in digital forms and are widely distributed via the Internet. The ease of making copies has created a need to develop a means to protect them. Digital rights management (DRM) technology is a solution for controlling the usage of the digital contents. The DRM protects the owner of the digital contents by restricting what actions an authorized recipient may take in regard to those contents [1].

The functional DRM architecture can be divided into three areas: content creation, content management, and content usage. Content creation includes the creation of the digital content and the definition of rights. Content management is about content distribution and trading of the rights. Finally, content usage is used to enforce the rights and to track the usage of contents.

Current DRM has been developed by several companies: InterTrust's Rights|System [11], Microsoft's Windows Media Rights Manager (WMRM) [12], IBM's Electronic Media Management System (EMMS) [13], RealNetworks' Real Systems Media Commerce Suite (RMCS) [14], and so on. DRM systems focus on the rights of the content provider or owner. User information can be easily revealed and tracked the usage. However, DRM systems and framework have not assumed any user privacy. Privacy protection scheme would enable the protection of consumer rights as well as content provider rights [3]. Rights enforcement may be facilitated by user's tracking or by network control of users' computers. However, both techniques are potentially destructive of user privacy [2].

This paper addresses a new protection scheme for users' privacy for digital rights management. Privacy protection can be compromised through the collection of data by owners or distributors. We design the DRM policy and the users' privacy preferences for digital rights management using input parameters as mandatory and optional.

The DRM system policy can declare alternative elements in case that a user does not want to provide some mandatory input parameters. Users can declare how much their personal information can be made available to the DRM system to compromise their privacy preferences with the DRM system. We also propose a negotiation algorithm that provides flexibility and helpful assistant to automatically negotiate the term and conditions when a user is connected to the DRM system. The DRM privacy agent would apply the user's privacy preferences and try to negotiate an agreement to the DRM system. Finally, the privacy rules are created for accessing control on the use of the personal information in the DRM system.

The rest of this paper is organized as follows: In Section 2, we discuss the related works. We describe the basis element of a privacy policy and user's privacy preferences for the DRM system in Section 3. In Section 4, we propose a privacy negotiation algorithm for the DRM system. An example scenario is given to illustrate the concepts in Section 5. Finally, in Section 6, we conclude the paper.

2. RELATED WORKS

InterTrust [11] offers a solution for content packaging, distribution and rights management based on a packager program and rights server technology. This system supports the varieties requirement of electronic commerce such as pay-per-use, rentals, sales, and try-before-buy business model. WMRM [12] is an end-to-end DRM system for the secure distribution of multimedia files over the Internet. The solution is based on Windows Media Player and Server. It provides a flexible platform to content providers for secure distribution of digital media file. The user must acquire a license key to unlock the media file. The supported business model can be subscription, sales, counted operations and secure transfer of protected digital media files to devices or PC. IBM EMMS [13] was developed for the preparation and secure distribution of all forms of digital contents. This system supports pay-per-use, pay-per-time, subscription, controlled printing, and protected transfer to portable devices. RMCS [14] offer a package server, streaming server, license server and a secure file format plug-in for RealPlayer and supports subscription, video on demand and other business model. PrecePt [15] is a protocol that affirms user's anonymity using temporary ID (TID) and token to guarantee anonymity. This protocol protects user privacy when it authenticates a user in issuing a license. The information can be protected from danger which may be flowed out by cryptography.

According to the privacy engineering for digital rights management system, privacy concerns two essential ways [2]. The first way is that the DRM model requires the user to

provide an ID number that links the user's personal information (name, address, transaction history, etc.) with the device or service a person intends to use. The paper said that tracking for the purpose of tying content to a set of devices obviously put at risk some previous private information about the user. The second way is that the DRM model requires the users to reconfirm that they will not copy a product for resale or sharing. The model not only catalogues the user under a user-specific ID, but also catalogues the customer's usage history of a product that has been downloaded from the system that is subscribed to and streamed whenever requested [6].

They suggested an alternative to privacy engineering that avoids the problem of the DRM system. The fair information practice allows the provision of personal information for a specific purpose without the fear that it may later be used for an unrelated purpose without the owner's knowledge or consent. Privacy enhancement should also be built directly into the DRM technology [2].

Among several approaches for privacy management using service policies and privacy preferences, the most mature one is the Platform for Privacy Preferences Project (P3P) [7] developed by the World Wide Web Consortium (W3C). P3P enables web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents like web browsers. The P3P Specification 1.0 [7] includes the definition of the syntax and semantics of a vocabulary to describe data uses, data recipients, data retention policy and other privacy disclosures in P3P privacy policy files. APPEL (A P3P Preference Exchange Language) [8] provides a standard way of defining the user privacy preferences in a set of preference rules, while can be used by the user agent to make automated or semi-automated decisions regarding the acceptance of privacy policies from P3P enabled web sites.

It should be noted that P3P is for web sites and does not intend to exploit DRM. In fact only a few recent works address DRM issues for privacy management.

3. A PRIVACY FRAMEWORK COMPONENTS FOR DIGITAL RIGHTS MANAGEMENT

3.1 Overview of the proposed system

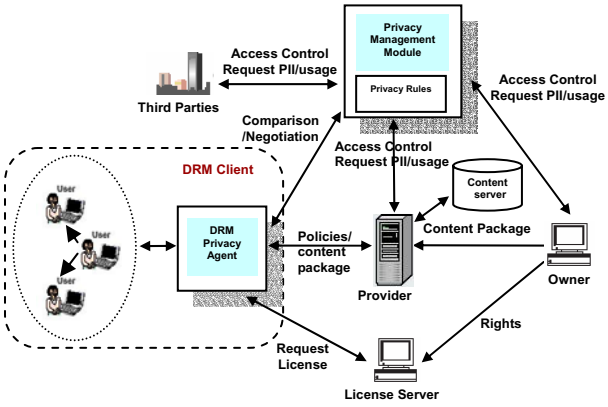

Fig. 1 Privacy framework components for DRM

The DRM system model with the proposed privacy negotiation algorithm is shown in Fig. 1. We propose basic elements for privacy DRM system model. A DRM privacy agent is allowed to compare and automatically negotiate between user's privacy preferences and DRM policy, and then the appropriate privacy rules for each user are generated. The privacy management module is one of the components that collect the privacy rules and access control the user's personal information to the parties. The basic elements comprise the following:

- *Element of Privacy Policy:* A material such as music, movie, documents etc. on DRM systems describes the use of personal user information in policy statements.
- *Requested Data:* The policy statements request the data set from the user as mandatory and optional element of DRM systems.
- *Privacy Preferences:* The user is responsible for declaring his privacy preferences regarding the policy statements of DRM systems. The declaration of privacy preferences are based on three permission levels as NotGiven, Limited, and Free.
- *Rule Evaluation:* This process determines the user's privacy rules regarding the DRM system, to be utilized during the negotiation phase between user's privacy preference and the DRM policy.
- *Negotiation mechanism:* This process is based on the policy declaring the material on DRM system's request and rules describing the privacy preferences of the user. The negotiation mechanism tries to find an agreement between the user and the DRM system. Comparing between the policy statements and user permission levels and the alternative rules, this process generates a privacy rules set that describes the access control of the user personal information that is sufficient for the DRM system and allowed by the user.

The DRM privacy agent stores the privacy preferences of a user. Material on the DRM system describes the requested data and alternative rules. The DRM privacy agent compares the user's privacy preferences with the requested data and alternative rules on the DRM system as shown in Fig. 2.

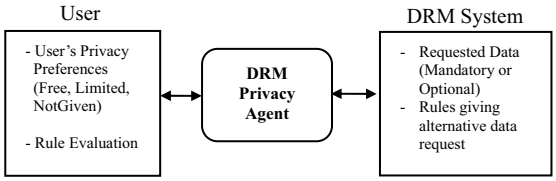

Fig. 2 DRM privacy agent architecture

3.2 Elements of a privacy policy

We introduce the elements of our privacy policy statements that provide a way to describe the data use practices on DRM systems. For each material on the DRM system should also declare their policies regarding such as their purpose to request the data, with whom that they may share the data and when they will retain the data.

3.2.1 Purpose

The purposes declare the basis objective for collecting user's data on the DRM system. We structure the intended use of collected data into categories for the DRM system. Those purposes for collecting data in the DRM system include the following:

- Personalized use for direct marketing
- Quality of service enhancement
- Backup and archives
- Aggregate usage of information for marketing
- Profiling (de)personalized records
- Customer service and retention
- Recommendation service

Those purposes adapted the P3P [7] policy mechanism to DRM systems as shown in Fig. 3.

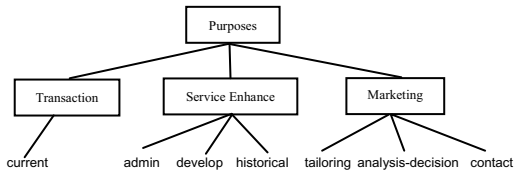

Fig. 3 Hierarchy of purposes for DRM system

3.2.2 Recipient

The recipients describe the parties with whom the data will be shared. The P3P [7] defined six types of recipient policies. We adapt recipient types appropriately for the DRM system as shown in Fig. 4.

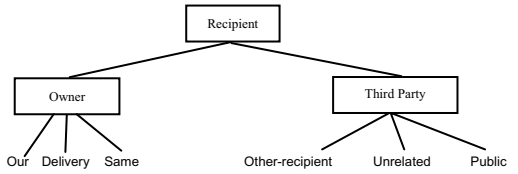

Fig. 4 Hierarchy of recipient for DRM system

3.2.3 Retention

The retentions define the duration for which the collected information will be kept. We adapt retention type for DRM systems as following:

- *License:* Information is retained to meet in period of time by license.
- *Material:* Information is retained to meet in period of time by material.
- *Special-purpose:* Information is retained to meet the special purpose and determined by administration or provider's business practices.
- *Indefinite:* Information is retained for an indeterminate period of time.
- *User define:* Information is retained by user definition.

3.2.4 Data

Information collected in a DRM system may include data about personally identifying information (PII), content retrieval, rights retrieval, content accessing, frequency, times, access location, etc. This information can be obtained by logging server-side or by having client-side DRM software to store relevant usage data. We define data reference by the P3P [7] policy.

3.3 Requested data of the DRM system

The fair information practice is a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. The OECD [10] has written "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" which have been widely accepted to describe their desirable privacy goal. This is particularly well suited for relatively complex systems like the DRM systems, in which there are a number of legitimate purposes for collecting and using information [2].

We define two parts of requested data on the DRM system. The first part comprises a mandatory element and an optional element. The second part provides rules that are used to request alternative elements if the required information is not provided by the user.

Mandatory is essential for DRM to collect and execute the information. Optional is requested for some other purposes. Both mandatory and optional elements consist of a set of purposes, a set of recipients, a set of retention periods, and a set of data, to form a major part of the entire DRM policy. Alternative elements are also defined using "if-then" rules to get some required elements if the required mandatory elements are not given by the user. Fig. 5 and Fig. 6 show the examples for DRM policy.

```
<?xml version="1.0"?>
<policy Material_Name="The Lord Of The Ring" Material_Type="book">

    <mandatory>
        <statement>
          <purpose> <current/> <admin/> </purpose>
          <recipient> <ours/> <delivery/> </recipient>
          <retention defined-by="special-purpose" description="developement"/>
          <data-group>
                <data type="#user.name"/>
                <data type="#user.email.address"/>
          </data-group>
        </statement>
    </mandatory>

    <optional>
        <statement>
          <purpose> <historical> </purpose>
          <recipient> <our/> </recipient>
          <retention defined-by="material" description="marketing"/>
          <data-group>
                <data type="#uclick.stream"/>
          </data-group>
        </statement>
    </optional>

</policy>
```

Fig. 5 Privacy policies in DRM system

```
<rule>

    <IfRule>
          <IfNotGiven>
                <purpose> <current/> </purpose>
          </IfNotGiven>
          <Then>
                <purpose> <admin/> </purpose>
          </Then>
    </IfRule>

    <IfRule>
          <IfNotGiven>
                <data-group> <data type="#user.name"/> </data-group>
          </IfNotGiven>
          <Then>
                <data-group> <data type="#user.email.address"/> </data-group>
          </Then>
    </IfRule>

    <IfRule>
          <IfNotGiven>
                <data-group> <data type="#user.email.address"/> </data-group>
          </IfNotGiven>
          <Then>
                <data-group> <data type="#user.postal"/> </data-group>
          </Then>
    </IfRule>

    <IfRule>
          <IfNotGiven>
                <retention defined-by="special-purpose"/>
          </IfNotGiven>
          <Then>
                <retention defined-by="material"/>
          </Then>
     </IfRule>

    </rule>
```

Fig. 6 An example of conditional statements

3.4 Description of user's privacy preferences

The users define their privacy preferences for the DRM system through a rule-based mechanism. There are three permission level rules that can be imposed on the elements.

- *Free:* the elements are given freely by the user.
- *Limited:* the elements are provided by the user only if it is mandatory for the DRM system.
- *NotGiven:* the elements are not provided by the user.

Sometimes user's privacy preference rules may impose conflicting on the elements. It is considered that NotGiven rule is over other rules. Free rule has the least priority and Limit rule's priority is between these two. Fig. 7 shows an example of user's privacy preferences.

```
<?xml version="1.0"?>
<preference>

    <free>
        <statement>
            <purpose> <current/> </purpose>
            <recipient> <ours/> </recipient>
            <retention defined-by="license"/>
            <data-group>
                  <data type="#user.name"/>
                  <data type="#user.gender"/>
            </data-group>
        </statement>
    </free>

    <limited>
        <statement>
            <purpose> <admin/> <develop/> </purpose>
            <recipient> <delivery/> <other-recipient/> </recipient>
            <retention defined-by="material"/>
            <data-group>
                  <data type="#user.clickstream"/>
                  <data type="#user.telephone"/>
            </data-group>
        </statement>
    </limited>

    <not-given>
        <statement>
            <purpose> <analysis-decision/> </purpose>
            <recipient> <public/> <unrelated/> </recipient>
            <retention defined-by="indefinite"/>
            <data-group>
                  <data type="#user.email.address"/>
                  <data type="#user.home.address"/>
                  <data type="#user.creditcard"/>
            </data-group>
        </statement>
    </not-given>

</preference>
```

Fig. 7 User's privacy preferences rules

4. NEGOTIATION MECHANISM

Negotiation mechanism comprises a set of activities that the user's privacy preferences are compared with DRM policy in order to reach an agreement. If an agreement cannot be reached, the alternative rules are requested through conditional statements provided by the DRM system.

4.1 Rule evaluation

Rule evaluation is the process of comparing user's privacy preferences rules against the DRM policy. We introduce the relevant terms that will be used for rule evaluation. Rules are privacy preferences for each statement, and facts are DRM policy. The following definitions will introduce the term rules and facts.

- U is set of data, where U = $\{d_1, d_2, \ldots, d_n\}$ $d_i, 1 \le i \le n$
- A rule denotes *r* that is defined by a pair (D_r, C_r), $D_r \subseteq U$, $C_r = \{c_1, c_2, \ldots, c_m\}$ c_j, $1 \le j \le m$ and $c_j = (x_j, v_j)$, $1 \le j \le m$, x_j denotes the name and v_j denotes the set of values.
- The facts denotes *f* that are defined by a pair (D_f, G_f) $D_f \subseteq U$, $G_f = \{g_1, g_2, \ldots, g_k\}$ g_j, $1 \le j \le k$ and $g_j = (x_j, v_j)$, $1 \le j \le m$, x_j denotes the name and v_j denotes the set of values.

When a rule was found that is matched by the facts, access to the requested data can be granted. In order to match a rule, the facts need to meet two requirements. Firstly, the facts must satisfy all of the rule's constraints. Secondly, the requested data as specified in the facts must be a subset to the data specified in the rule.

The constraint-matching function (β) is a Boolean function that show whether a name-value pair $p \in G_f$ of the facts matches constraint $c \in C_r$ of a rule.

$$\beta(c,p) = \begin{cases} \text{true, if p satisfies c} \\ \text{false, otherwise} \end{cases} \quad (1)$$

We give facts $f = (D_f, G_f)$ match rule $r = (D_r, C_r)$, if: (2)

(a) $\forall (c \in C_r)$ and $\forall (p \in G_f)$ with $\beta(c, p) = \text{true}$

(b) $D_f \subseteq D_r \leftrightarrow \forall (d_l \in D_f)$ and $\forall (d_l \in D_r)$

4.2 Negotiation algorithm

According to above we use user's privacy preference as rule sets in order to support the automated negotiation. When the data provided by the user does not match with the data requested by the DRM system, the alternative rules are provided by the DRM system. After the rule evaluation component rejects a request for data, we need to find out how the best rule matches the facts. This rule specifies acceptable conditions for the release of a set of data. In order to offer a reasonable alternative to a user's rejected request, it is goal now to find the rule that best matches the facts.

Our approach to find the best rule matching is to compute the weight between the individual rules in the rule sets and the facts. And we also use the alternative conditions as if-then rule to find the best rule matching. The rule with the maximum weight is considered the closest rule and is used to produce privacy rule for user. Based on this weights compute, the rule with the maximum weight, it is needed to determine how well the fact satisfies the constraints of the rule. Firstly, we define a function that computes to what degree the facts satisfy a rule constraint.

The function σ_c is a number of matching between the constraint of the rule $r = (D_r, \{c_1, \ldots, c_n\})$, $c_i = \{x_i, v_i\}$, $v_i = \{a_1, \ldots, a_n\}$ and the facts $f = (Df, \{g_1, \ldots, g_n\})$, $g_j = \{y_j, z_j\}$, $z_j = \{b_1, \ldots, b_n\}$, $v_{then} = \{k_1, \ldots, k_n\}$. It is defined such that:

$$\sigma_c(c_i, f) = \begin{cases} 0, & \text{if } ((z_i \cup v_{then}) \cap v_i) = \phi \\ > 0, & \text{otherwise} \end{cases} \quad (3)$$

Secondly, we define the function σ_d that is a number of matching between a set of data of a rule *r* and facts *f*, D_{then} is a set of data in if-then rules. It is defines such that:

$$\sigma_d(D_r, f) = \begin{cases} 0, & \text{if } ((D_f \cup D_{then}) \cap D_r) = \phi \\ > 0, & \text{otherwise} \end{cases} \quad (4)$$

The function $\partial(r_i, f)$ is a number of matching between a rule and facts on the set of positive integers. $\partial(r_i, f)$ is defined as follows:

$$\partial(r_i, f) = \left[\sum_{i=1}^{n} \sigma_c(ci, f) \cdot w_i \right] + \sigma_d(D_r, f) \cdot w_d \quad (5)$$

The terms w_i and w_d are weights which are related to the n constraints c_i and the data set D_r of a rule. Weights can be used to set the importance of constraint and allow specifying some parts of the rule that are more important than others, while searching for the closest rule.

$$\partial(f) = \sum_{i=1}^{k} L_c \cdot w_i + n \cdot w_d \quad (6)$$

where L_c is a number of value for each constraints.
n is a number of data in the facts.

The function $\partial(f)$ computes the sum between weight of constraints and weight of data in the facts. This result is compared with the function $\partial(r_i, f)$ so that matching rules can be checked.

The function grant(r_i, f) is a Boolean function that shows the matching of the rules.

$$\text{grant}(r_i, f) = \begin{cases} \text{true}, & \partial(ri, f) = \partial(f) \\ \text{false}, & \text{otherwise} \end{cases} \quad (7)$$

The best matching rule is computed from the function as the following.

$$\max(\partial(r_j, f)), \quad (1 \le j \le n) \quad (8)$$

5. PROOF OF AN EXAMPLE SCENARIO

In this section, we provide a scenario to better illustrate the concept presented for the negotiation algorithm in DRM systems. We assume the DRM policies as Facts and user's privacy preferences as Rules, as shown in Fig. 8 and Fig. 9.

```
<mandatory>
   <statement>
      <purpose> <develop/> </purpose>
      <recipient> <ours/> </recipient>
      <retention defined-by="material" description="developement"/>
      <data-group>
            <data type="#user.name"/>
            <data type="#user.age"/>
            <data type="#user.clickstream"/>
      </data-group>
      <rule>
         <IfRule>
            <IfNotGiven>
              <purpose><develop/> </purpose>
            </IfNotGiven>
            <Then>
              <purpose> <admin/> </purpose>
            </Then>
         </IfRule>
         <IfRule>
            <IfNotGiven>
               <data-group> <data type="#user.age"/> </data-group>
            </IfNotGiven>
            <Then>
              <data-group><data type="#user.gender"/> </data-group>
            </Then>
         </IfRule>
       </rule>
    </statement>
 </mandatory>
```

Fig. 8 An example of the DRM system requested data (Facts)

```
<?xml version="1.0"?>
<preference>
   <free>
      <statement>
         <purpose> <current/> </purpose>
         <recipient> <ours/> </recipient>
         <retention defined-by="license"/>
         <data-group>
               <data type="#user.name"/>
               <data type="#user.creditcard"/>
               <data type="#user.age"/>
               <data type="#user.mobilephone"/>
         </data-group>
      </statement>
   </free>
   <limited>
      <statement>
         <purpose> <admin/> </purpose>
         <recipient> <our/> </recipient>
         <retention defined-by="material"/>
         <data-group>
               <data type="#user.name"/>
               <data type="#user.homephone"/>
               <data type="#user.clickstream"/>
         </data-group>
       </statement>
   </limited>
   <not-given>
      <statement>
         <purpose> <historical/> <develop/> </purpose>
         <recipient> <public/> <unrelated/> </recipient>
         <retention defined-by="indefinite"/>
         <data-group>
               <data type="#user.email.address"/>
               <data type="#user.clickstream"/>
               <data type="#user.mobilephone"/>
         </data-group>
      </statement>
   </not-given>
</preference>
```

Fig.9 An example of user' privacy preferences (Rules)

5.1 Rule evaluation

The facts f in Fig. 8 do not match any of the three rules R in Fig. 9 because some constraints are not satisfied and the data set do not match completely from functions (1), (2). In the Free rule statement which has purpose, retention, and some data elements, does not match with the facts f. The Limited rule statement which comprises purpose, retention, and some data elements, does not match with the facts f. Finally, the NotGiven rule statement that comprises recipient, retention, and some data elements, does not match with the facts f. As a result, this process must be passed to the negotiation process.

5.2 Negotiation algorithm

Following the rule evaluation, the facts f do not match any rules R. Negotiation process is provided, the firstly to compute the sum between weight of constraints and weight of data in the facts as following (6). Then the facts are compared with the rules as following the functions (3), (4), (5). Alternative conditions of rules are also provided in the functions (3), (4). Fig. 10 shows the tree of Limited rules and Free rules

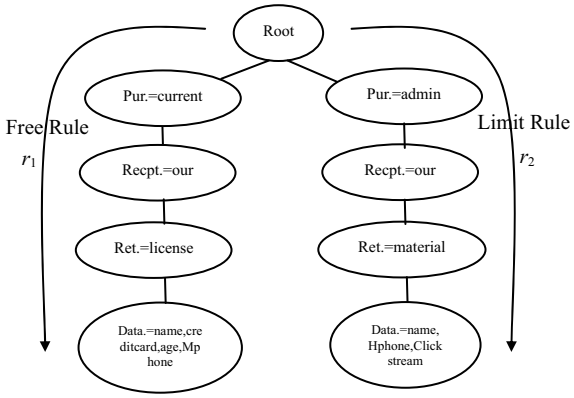

Fig. 10 An example tree of Limited and Free rules set

The user's privacy preferences result in the facts f :

Purpose = *develop*
Recipient = *our*
Retention = *material*
Data = *name*, *age*, *clickstream*
} Mandatory Statement

If *develop* then *admin*
If *age* then *gender*
} Conditional Statements

The facts f do not match any of the two rules in Fig. 10. The user sets the weights w_i and w_d as equal to 1. Using the function (6), the result is as follows.

$$\partial(f) = (1 \cdot 1) + (1 \cdot 1) + (1 \cdot 1) + (3 \cdot 1) = 6$$

However, the rules could be used to find the best matching rules. We get the weights both rules.

$$\partial(r_1, f) = (0 \cdot 1) + (1 \cdot 1) + (0 \cdot 1) + (2 \cdot 1) = 3$$
$$\partial(r_2, f) = (1 \cdot 1) + (1 \cdot 1) + (1 \cdot 1) + (2 \cdot 1) = 5$$

The weights of rules r_1 and r_2 do not equal the weight of the facts such that the best matching rule can be found. The function (8) is provided to find the best matching rule with facts.

$$\max(\partial(r_1, f), \ \partial(r_2, f)) = 5$$

So rule r_2 should be chosen in order to produce the matching. This best matching rule will be offered to the DRM system. The DRM system will use the offered rule for adapting appropriate rule and offer it to the user again.

6. CONCLUSION

The goal of the DRM technology is the distribution of digital contents in a manner that protects the rights of all parties involved, including copyright owners, distributors, and users. The problem of the present DRM system is seriously threatening users' privacy.

In this paper we presented an appropriate privacy policy and user's privacy preferences for the DRM system. The user's privacy preferences define the rules that control the read accessing for personal information. Furthermore the privacy policy model allows DRM systems to declare alternative requested data if a mandatory element is not given by the users. In this way it becomes possible to automate negotiation mechanism with the DRM system to reach an agreement. An effective negotiation algorithm is proposed. The negotiation processes comprise rule evaluation and negotiation mechanism. The rule evaluation determines the user's privacy rules regarding the DRM system, to be utilized during the negotiation between user's privacy preference and the privacy policy of the DRM system. The negotiation mechanism tries to find an agreement between the user and the DRM system, and compare among policy statements, user permission levels, and alternative rules. We believe that this framework can be used to enhance the negotiation capabilities of existing DRM systems, which are currently limited to negotiate the user's personal information.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contribution of the Research Center for Communications and Information Technology (ReCCIT), King Mongkut's Institute of Technology Ladkrabang (KMITL).

REFERENCES

[1] A. Russ, "Digital Rights Management Overview," SysAdmin, Audit, Networking and Security (SANS) Information Security Reading Room, July 26, 2001.

[2] J. Feigenbaum, M. Freedman, T. Sander, and A. Shostack, "Privacy Engineering for Digital Rights Management Systems," the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, pp. 76-105, 2001.

[3] P. Vora, D. Reynolds, I. Dickinson, J. Erickson, and D. Banks, "Privacy and Digital Rights Management," the W3C Workshop on Digital Rights Management for the Web, [Online]. Available: http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi.html, January 2001.

[4] L. Korba, "Privacy in Distributed Electronic Commerce," Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), pp. 4017-4026, January 2002.

[5] L. Korba, and S. Kenny, "Towards Meeting the Privacy Challenge: Adapting DRM," ACM Workshop on Digital Rights Management, pp. 118-136, November 18, 2002.

[6] A. Cavukian, "Privacy and Digital Rights Management (DRM): An Oxymoron," Information and Privacy Commissioner/Ontario, October 2002, [Online]. Available: http://home.inter.net/gt/grabbag/Ontario.drm.pdf.

[7] W3C, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification", [Online]. Available: http://www.w3.org /TR/P3P/, April 2002.

[8] W3C, "A P3P Preference Exchange Language (APPEL)," [Online]. Available: http://www.w3.org/TR/P3Ppreferences.html

[9] B. Rosenblatt, Digital Rights Management Business and Technology, New York, Hungry Minds Inc., 2002.

[10] Organization for Economic Co-operation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," [Online]. Available:http://www.oecd.org/dsti/sti/it/secure/prod/PRIV-EN.HTM, September 1980.

[11] InterTrust, [Online]. Available:http://www.intertrust.com.

[12] Microsoft, "Architecture Microsoft Media Rights Manager,"[Online].Available:http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx.

[13] EMMS, "Electronic Media Management System," [Online]. Available:http://www.ibm.com/software/emms.

[14] RMCS, "Real Systems Media Commerce Suite," [Online]. Available:http://docs.real.com/docs/drm/DRM_WP1.pdf.

[15] P. Bok-Nyong, K. Jae-Won, and L. Wonjun, "PrecePt: A Privacy-Enhancing License Management Protocol for Digital Rights Management," Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA), Volume 1, pp. 574-579, March 2004.