Contrôle d'Usage et Mécanismes DRM

Léo Letouzey {leo.letouzey@upf.pf}, Laboratoire GePaSUD
Directeur de thèse : Alban Gabillon Projet FLUOR : http ://fluor.no-ip.fr/
Université de la Polynésie Française, Doctoriales Conjointes UPF-UNC 2009

Introduction

Depuis que l'information est disponible en format numérique, la protection de celle-ci a toujours été quelque chose d'important. Il peut s'agir de protéger une propriété intellectuelle, un *copyright* ou bien de contrôler l'accès à un objet ou encore l'usage qui en est fait. Les modèles de sécurité ont évolué parallèlement aux besoins sans cesse changeants des systèmes d'information.

La **gestion des droits numériques** (*Digital Right Management*) (DRM) a pour but de protéger des contenus numériques variés [1]. Elle permet de contrôler, d'une manière générale, l'accès et l'usage des contenus protégés. Les mécanismes DRM ont permis l'essor dans un premier temps de la distribution en ligne de contenus numériques (notamment la musique) mais ils ne se limitent pas à cela. Les besoins en termes de protection n'ont cessé d'évoluer avec le temps, tant au niveau du distributeur qu'au niveau du client. Ainsi, il a fallu trouver des modèles de sécurité qui puissent s'adapter à ces nouveaux besoins. Le but de ce poster est de présenter ce qu'il est possible de faire aujourd'hui en terme de contrôle d'usage et les applications possibles dans le domaine des DRM.

Contrôle d'Usage

Les modèles de **contrôle d'usage**, UCON [2], sont une généralisation des modèles de **contrôle d'accès**, *Access Control Mechanisms* (ACM). Contrairement aux ACM, le contrôle d'usage propose trois points de contrôle (Fig.1) :

- ***pre*** : avant l'accès;
- ***ongoing*** : pendant l'utilisation;
- ***after*** : à la fin de l'utilisation.

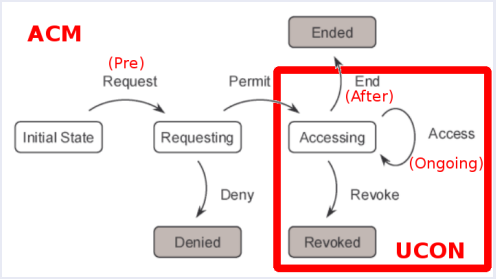

FIG. 1 – Modèles ACM et UCON

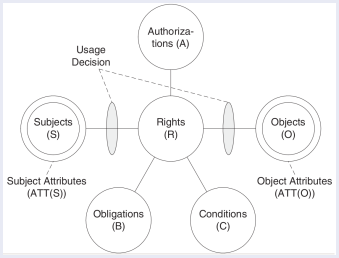

FIG. 2 – Le modèle $UCON_{abc}$

Dans le modèle $UCON_{abc}$, les décisions sont prises en tenant compte des composants suivants (Fig.2) :

- le **sujet** (S) et ses attributs;
- l'**objet** (O) et ses attributs;
- un ensemble de **droits** génériques (R);
- des **autorisations** (a);
- des **obligations** (b);
- des **conditions** (c).

Les éléments de la politique de sécurité sont modifiables au cours de l'utilisation [3]. Ainsi la politique de sécurité est amenée à évoluer tout au long de l'utilisation des objets, apportant la souplesse dont ont besoin aujourd'hui les systèmes de sécurité.
Les mécanismes DRM permettent d'implémenter et de déployer une politique de sécurité basée sur le contrôle d'usage.

Mécanismes DRM

Les mécanismes DRM ont été mis en place pour permettre la distribution de contenus numériques protégés.
Une architecture DRM (Fig. 3) met en relation 3 personnes :

- Le **packager** : fournit le contenu;
- le **serveur de licences** : fournit la licence;
- le **client** : accède au contenu conformément à ce qui est défini dans la licence.

La licence est au centre des DRM. Elle contient entre autre :

- La **clé** qui permet de déchiffrer le contenu;
- Les **droits** qui sont accordés sur le contenu.

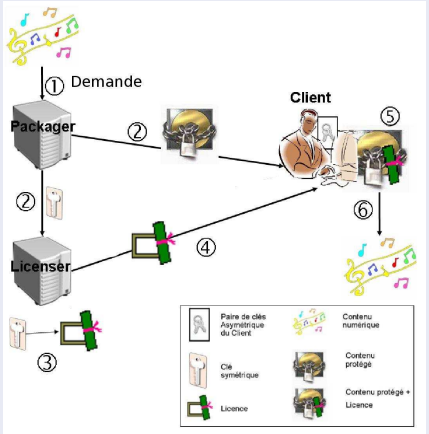

FIG. 3 – Une architecture DRM

Les droits contenus dans une licence sont exprimés à l'aide d'un **langage d'expression de droits** ou REL (*Right Epression Language*)[4] [5].

Applications

Les REL permettent d'exprimer les différentes règles du modèle $UCON_{abc}$.
La mutabilité de la politique de sécurité peut être mise à profit pour :

- mettre en place des compteurs de lecture;
- bloquer l'accès à ce qui a déjà été lu;
- mettre a jour la liste des utilisateurs;
- ...

Les nouveaux points de contrôle ***ongoing*** et ***after*** peuvent spécifier des conditions d'utilisations particulières :

- publicité pendant un temps donné;
- durée d'accès limitée;
- écriture de fichier de *log* en fin d'utilisation;
- facturation en fonction des actions effectuées durant la dernière utilisation;
- ...

Conclusion

Les contrôles d'usage ouvrent de nouvelles perspectives pour les mécanismes DRM. Apportant plus de souplesse et s'adaptant mieux aux besoins du distributeur et du client.

Cependant avec la mise en place d'une politique de contrôle d'usage, les contrôles ne peuvent s'effectuer que du coté client. Il faut donc pouvoir disposer d'une application de confiance chez celui-ci. Cette notion de **tiers de confiance** est très importante puisque c'est cette application qui aura en charge de faire respecter les différentes règles de la politique de sécurité définie dans la licence.

Références

[1] : Sibbert O. et al. 1995, The DigiBox : a self-protecting container for information commerce. Proceedings USENIX Workshop on Electronic Commerce.

[2] : Park J. et Sandhu R. 2004, The UCONabc Usage Control Model. ACM Transactions on Information and System Security Vol. 7, No. 1.

[3] : Park J. Zhang X. et Sandhu R. 2004, Attribut Mutability in Usage Control. 18th Annual IFIP WG 11.3 Working Conference on Data and Applications Security.

[4] : Iannella R. 2002, Open Digital Rights Language (ODRL) Version 1.1. http://www.w3.org/TR/odrl/

[5] : ContentGuard 2001, XrML 2.0 Specifications. www.contentguard.org.

Financement

Ce travail est supporté par le projet ANR-SESUR-2007-FLUOR.