UCON et DRM : ÉTAT DE L'ART[1]

Léo Letouzey, Laboratoire Gepasud
Université de la Polynésie Française
leo.letouzey@upf.pf

Résumé

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. Ainsi cet article présentera rapidement un état de l'art dans le domaine des mécanismes de contrôle d'usage (*Usage CONtrol, UCON*) et de la gestion de droits numériques *Digital Right Managment* (DRM).

Mots clé : Gestion des droits numériques, contrôle d'usage.
Keywords :Digital Right Management, Usage Control.

Introduction

La gestion des droits numériques (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 cet article 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.

Ainsi la première partie de cet article s'attardera sur la présentation des mécanismes de contrôle d'usage [2] avec notamment la présentation du modèle UCONabc [3]. La seconde partie présentera comment peuvent être mis en place ces mécanismes au travers des DRM.

1. Contrôle d'usage

Les solutions de sécurité apportées par les modèles de contrôle d'accès *Access Control Mechanisms* (ACM) ne sont plus suffisantes pour répondre aux besoins actuels de contrôle et de protection des données. Les modèles de contrôle d'usage sont une généralisation des modèles de contrôle d'accès. Ils ne proposent plus seulement de spécifier quelles sont les conditions d'accès aux objets, ils permettent également de spécifier les contrôles pendant l'usage de ceux-ci (cf. Fig. 1).

1 Cet article entre dans le cadre du projet ANR-SESUR-2007-FLUOR

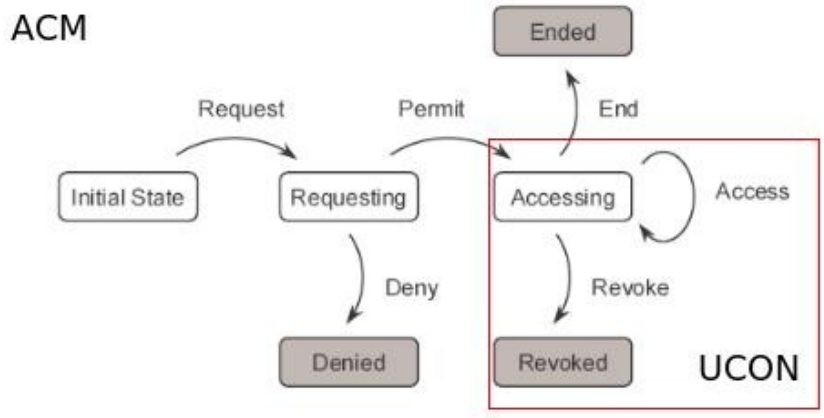

Fig.1 Différence entre ACM et UCON

Là où le contrôle d'accès ne considère qu'une seule étape lors de l'accès à un objet, le contrôle d'usage en considère trois. Ainsi, le modèle UCON effectue des contrôles avant l'accès, pendant l'utilisation et à la fin de l'utilisation (*pre, ongoing, after*). Il apporte ainsi la possibilité de contrôler plus finement l'usage qui est fait de l'objet. Il est maintenant possible par exemple de révoquer l'accès à un objet en cours d'utilisation. Toutes les décisions sont prises en tenant compte des composants suivants : le sujet et ses attributs, l'objet et ses attributs, un ensemble de droits génériques et une politique de sécurité comprenant des autorisations (a), des obligations (b) et des conditions (c). Dans le modèle UCONabc, les éléments de la politique de sécurité sont dits mutables, c'est-à-dire qu'ils peuvent être modifiés. Ces modifications peuvent intervenir à chacune des trois étapes qui caractérisent le contrôle d'usage [4]. 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 un modèle de contrôle d'usage de type UCONabc.

2. Mécanismes DRM

2.1 Présentation

Les mécanismes DRM ont été mis en place pour permettre la distribution de contenus numériques protégés. Ils ont été rendus populaire grâce à leur utilisation dans le domaine de la distribution en ligne de contenus multimédias (musique, Vidéo à la demande...). Cependant ils peuvent être utilisés pour protéger des contenus numériques de toutes sortes (image, texte, logiciel...). Même s'ils sont progressivement abandonnés pour la distibution de musique (abandon par Universal début 2008 et par Apple début 2009), ils sont de plus en plus mis en place par les entreprises pour protéger leurs données sensibles. On parle dans ce cas de E-DRM (*Entreprise-DRM)*. Une architecture DRM (cf Fig. 2) met en relation 3 personnes. Le « Packager » qui fournit le contenu protégé, le serveur de licences qui fournit la licence correspondant au contenu et le client qui accède au contenu conformément à ce qui est défini dans la licence. Cette dernière est au centre des DRM. En effet c'est elle qui contient, en plus de la clé permettant le déchiffrage du contenu, les informations définissant ce qu'il est possible de faire avec le contenu acquis ou, au contraire, ce qui est interdit. Les droits contenus dans une licence sont exprimés à l'aide d'un langage d'expression de droits ou REL (*Right Epression Language*).

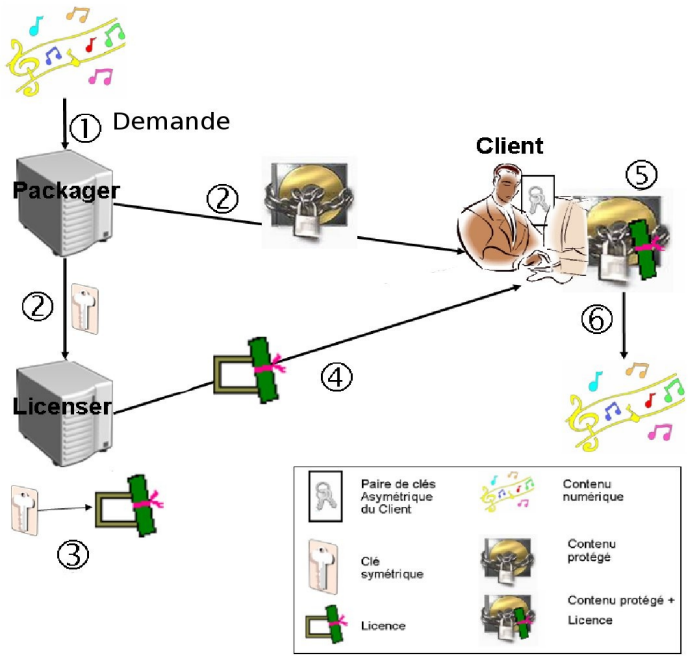

Fig. 2 Modèle DRM

2.2 Langages d'expression de droits

Les deux grands modèles de REL sont ODRL (*Open Digital Right Language*) [5] et XrML (*eXtensible Right Markup Language*) [6]. Ces deux langages « open-source » sont basés sur le modèle XML du W3C [7]. Chacun est supporté par de grands industriels : Microsoft, Abode, HP... pour XrML et l'Open Mobile Alliance pour ODRL. Le langage XrML sert de base à la norme ISO MPEG21-5 (MPEG-REL) [8]. Ces deux modèles ont pour avantage de pouvoir être complétés par des dictionnaires propres à chaque application. Ainsi, si le langage ne suffit plus à définir correctement le modèle de sécurité que l'on souhaite mettre en place, il suffit de construire son propre dictionnaire d'expressions. ODRL dispose par exemple d'un dictionnaire permettant de gérer les licences « Creative Commons » [9]. Ces deux langages ne restent donc pas limités à ce qui existe déjà mais peuvent être étendus.

2.3 Applications des mécanismes de contrôle d'usage aux DRM

Il est possible, à l'aide des REL, d'exprimer les différentes règles du modèle UCONabc. Les DRM peuvent ainsi tirer parti des avantages du contrôle d'usage. La mutabilité de la politique de sécurité peut être mise à profit pour mettre à jour les droits (compteur de lectures, nombre d'utilisateurs, bloquer l'accès à ce qui a déjà été lu, *pay-per-use*...). Le nouveau point de vérification *ongoing* peut spécifier des conditions d'utilisation particulière (bandeau de publicité pendant un temps donné, durée d'accès limitée...). La politique de sécurité gagne alors en précision et peut s'adapter aux besoins de souplesse actuels.

Il reste néanmoins le problème de l'inter-opérabilité entre différents systèmes DRM. La résolution de ce problème permettrait de pouvoir autoriser (et contrôler) l'utilisation par plusieurs applications et utilisateurs d'un même fichier protégé. Il pourrait également être intéressant de rendre possible les échanges (temporaires ou permanents) de contenus protégés. Une approche dans ce sens a été faite dans [10]. Cette solution se base sur le modèle UCONabc mais reste limitée aux applications JAVA. [11] propose la mise en place de signatures déléguées tandis que [12] envisage de poursuivre les recherches sur le problème de délégation de droits. Ces solutions permettraient de pouvoir échanger des contenus protégés sans avoir besoin de contacter le serveur de licences.

Avec la mise en place du contrôle d'usage, les contrôles ne peuvent plus être réalisés coté

serveur, ils s'effectuent maintenant coté client. Il faut donc pouvoir disposer d'une application de confiance chez celui-ci. Cette notion de tiers de confiance est tres importante puisque c'est cette application qui aura en charge de faire respecter les différentes régles définies dans la licence.

3. Conclusion

Le modèle de contrôle d'usage présenté ici permet de définir une politique de sécurité de façon très précise, adaptée aux besoins et à leur éventuelle évolution. La mutabilité de la politique de sécurité permet une grande souplesse dans l'utilisation. Cependant, la mise en place d'un modèle de contrôle d'usage nécessite de se pencher au préalable sur la notion de tiers de confiance, indispensable pour garantir l'application de la politique de sécurité. D'autre part, les mécanismes DRM rendus possibles grâce au contrôle d'usage ne permettent toujours pas le transfert, le prêt ou l'échange de contenus protégés sans intervention du serveur de licences.

Bibliographie :

[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. 2002, Towards Usage Control Models : Beyond Traditional Access Control. SACMAT'02 .

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

[4] : 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.

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

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

[7] : World Wide Web Consortium (W3C) 1998, eXtensible Markup Language 1.0. http://www.w3.org/TR/2008/REC-xml-20081126/

[8] : http://www.chiariglione.org/MPEG/technologies/mp21-rel/index.htm

[9] : http://odrl.net/Profiles/CC/SPEC.html

[10] : Nair S.K. et al. 2008, Enforcing DRM Policies Across Applications. ACM-DRM'08.

[11] : Canard S. Milhau M. et Laguillaumie F. 2008, Trapdoor Sanitizable Signatures and their Application to Content Protection . ACNS 2008.

[12] : Pretschner A. et al. 2008, Mechanisms for Usage Control. ACM Symposium on Information, Computer and Communications Security, ASIACCS ’08.