A Novel Method for Supporting Fairness in Digital License Reselling

Tarek Gaber[1] and Ning Zhang[2]

[1] School of Computer Science
University of Manchester
Manchester, UK
gabert@cs.man.ac.uk

[2] School of Computer Science
University of Manchester
Manchester, UK
nzhang@cs.man.ac.uk

Abstract

Current Digital Rights Management (DRM) systems permit a consumer to buy a digital license to access the corresponding content on his device. Under these current systems, however, the consumer is unable to resell the license. To allow the consumer to resell the license, all entities involved in the reselling process must be treated fairly. Fairness means that a reseller should obtain payment if and only if a buyer obtains the expected license and vice-versa. This paper presents a novel method to support fairness in reselling a digital license for DRM protected content. This method enables a reseller to fairly and securely exchange his/her license for payment from a buyer. In addition, it enables the reseller to maximize his profit and the buyer to minimize his cost in the same process. The method is designed such that the buyer can not cheat and the reseller has no incentive to do so. A practical mechanism is proposed to handle any misbehavior by the reseller. In comparison with related works, the method does not make use of any additional trusted hardware device, thus more cost-effective, while satisfying the interests of all the entities involved. The method also prevents reselling a non-resalable license and multiple reselling of the same license.

Keywords: *Concurrent Signature, DRM , Digital License , Fairness , Market power , Non-repudiation , Reselling Deal.*

Published In: *Fifth International Conference on Internet Monitoring and Protection ICIMP'2010, May 9-15 Barcelona, Spain, pp.89-98, 2010.*

Fair and Abuse-Free Contract Signing Protocol Supporting Fair License Reselling

Tarek Gaber[1] and Ning Zhang[2]

[1] School of Computer Science
University of Manchester
Manchester, UK
gabert@cs.man.ac.uk

[2] School of Computer Science
University of Manchester
Manchester, UK
nzhang@cs.man.ac.uk

Abstract

Most of the fair contract signing protocols published to date make use of a Trusted Third Party (TTP) to achieve fairness. In this paper, we have designed a fair contract signing protocol to support fair reselling of a DRM license without using a dedicated TTP. This protocol makes use of the concurrent signature (CS) and the existing license distribution infrastructure. By making use of the CS scheme, and integrating it into the existing license distribution infrastructure, we avoid the use of a dedicated TTP, thus introducing no additional communication overhead in providing fair license reselling. Also, the protocol is designed such that none of the two signers can prove to an outside entity that he is in control of the outcome of the protocol, thus achieving abuse-freeness.

Keywords: *Contract Signing , DRM license , TTP , abuse free contract signing protocol , concurrent signature , fair license reselling , license distribution infrastructure , trusted third party*

.

Published In: The 4th IFIP International Conference on New Technologies, Mobility and Security, February 7 – 10 2011, Paris – France.

A License Revocation Protocol Supporting Digital License Reselling in a Consumer-to-Consumer Model

Tarek Gaber[1] and Ning Zhang[2]

[1] School of Computer Science
University of Manchester
Manchester, UK
gabert@cs.man.ac.uk
and
Faculty of Computers & Informatics,
Suez Canal University,
Ismilia, Egypt

[2] School of Computer Science
University of Manchester
Manchester, UK
nzhang@cs.man.ac.uk

Abstract

Digital Rights Management (DRM) is an important technology supporting e-commerce systems and online marketing, enabling content owners and market intermediaries to securely manage and deliver digital content. In addition, P2P (peer-to-peer) networks play a pro-motive role in e-commerce. However, it facilitates illegal access to copyrighted media which may cause a violation of content owners' rights. P2P could support legal digital content transfer—reselling digital content. One peer (a reseller) could use P2P technology to send a digital content and its license to another peer (a buyer). A reseller could continue to resell it many times, causing content owners to lose revenue. This paper presents a License Revocation Protocol (LRP) to support reselling of a digital license. This LRP protocol enables a license issuer, representing a content owner, to confirm that once a reseller has resold his license, the reseller cannot continue to use the license. With LRP protocol, a reseller does not get the license payment until he revokes his resold license. The LRP protocol does not make use of any additional trusted hardware device, thus making the protocol more cost-effective.

Keywords: *Digital License Reselling, Digital Rights Management (DRM), E-Commerce, License Revocation List (LRL), Peer-to-Peer (P2P), Reselling Deal (RD).*

Published In: *IGI Global publisher, International Journal of Online Marketing (IJOM), Volume 2 (Issue 1),pp 38-49,2012.*

Support consumers' rights in DRM: a secure and fair solution to digital license reselling over the Internet

Tarek Gaber[1]
[1] **School of Computer Science**
University of Manchester
Manchester, UK
gabert@cs.man.ac.uk
and
Faculty of Computers & Informatics,
Suez Canal University,
Ismilia, Egypt

Abstract

Consumers of digital contents are empowered with numerous technologies allowing them to produce perfect copies of these contents and distribute them around the world with little or no cost. To prevent illegal copying and distribution, a technology called Digital Rights Management (DRM) is developed. With this technology, consumers are allowed to access digital contents only if they have purchased the corresponding licenses from license issuers. The problem, however, is that those consumers are not allowed to resell their own licenses- a restriction that goes against the first-sale doctrine. Enabling a consumer to buy a digital license directly from another consumer and allowing the two consumers to fairly exchange the license for a payment are still an open issue in DRM research area. This thesis investigates existing security solutions for achieving digital license reselling and analyses their strengths and weaknesses. The thesis then proposes a novel Reselling Deal Signing (RDS) protocol to achieve fairness in a license reselling. The idea of the protocol is to integrate the features of the concurrent signature scheme with functionalities of a License Issuer (LI). The security properties of this protocol is informally analysed and then formally verified using ATL logic and the model checker MOCHA. To assess its performance, a prototype of the RDS protocol has been developed and a comparison with related protocols has been conducted. The thesis also introduces two novel digital tokens a Reselling Permission (RP) token and a Multiple Reselling Permission (MRP) token. The RP and MRP tokens are used to show whether a given license is single and multiple resalable, respectively. Moreover, the thesis proposes two novel methods supporting fair and secure digital license reselling. The first method is the Reselling Deal (RD) method which allows a license to be resold once. This method makes use of the existing distribution infrastructure, RP, License Revocation List (LRL), and three protocols: RDS protocol RD Activation (RDA) protocol, and RD Completion (RDC) protocol. The second method is a Multiple License Reselling (MLR) method enabling one license to be resold N times by N consumers. The thesis presents two variants of the MLR method: RRP-MR (Repeated RP-based Multi-Reselling) and HC-MR (Hash Chain-based Multi-Reselling). The RRP-MR method is designed such that a buyer can choose to either continue or stop a multi-reselling of a license. Like the RD method, the RRP-MR method makes use of RP, LI, LRL, and the RDS, RDA, and RDC protocols to achieve fair and secure reselling. The HC-MR method allows multiple resellings while keeping the overhead on LI at a minimum level and enable a buyer to check how many times a license can be further resold. To do so, the HC-MR utilizes MRP and the hash chain cryptographic primitive along with LRL, LI and the RDS, RDA and RDC protocols. The analysis and the evaluation of these three methods have been conducted. While supporting the license reselling, the two methods are designed to prevent a reseller from (1) continuing using a resold license, (2) reselling a non-resalable license, and (3) reselling one license a unauthorized number of times. In addition, they enable content owners of resold contents to trace a buyer who has violated any of the usage rights of a license bought from a reseller. Moreover, the methods enable a buyer to verify whether a license he is about to buy is legitimate for re-sale. Furthermore, the two methods support market power where a reseller can maximise his profit and a buyer can minimise his cost in a reselling process. In comparison with related works, our solution does not make use of any trusted hardware device, thus it is more cost-effective, while satisfying the interests of both resellers and buyers, and protecting the content owner's rights

Keywords: *DRM ; Digital Rights Management ; Fairness ; Fair Exchange ; Abuse-freeness ; Non-repudiation ; Digital License Reselling. ; Reselling Deal ; Multiple License Reselling ; Single License Reselling ; License Issuer ; Re-saleability Check. ; Reselling Permission ; RP ; Multiple Reselling Permission ; MRP ; OMA DRM ; ; Windows Media DRM ; WM-DRM ; FairPlay DRM ; Apple DRM ; License Revocation List ; LRL ; Single Resalable License ; Multiple Resalable License ; DRM Client ; DRM Agant ; Non-Resalable License ; In-line TTP ; On-line TTP ; Off-line TTP ; Mocha ; Mocha Model Checker ; ATL logic ; Guarded Command Language ; Contract Signing ; Formal Analysis ; Contract Signing Protocols ; License Selling Process ; Open Mobile Alliance DRM ; Consumer Privacy ; Interoperability ; Trusted Hardware ; Gradual Secret Release Protocols ; Concurrent Signature ; Concurrent Signatures ; Collusion Attack ; License Double Use.*

Published In: e*scholar of the University of Manchester, 2012.*