A Benefits-Centric Multi-Participant Trust Architecture for DRM-Enabling Digital Contents Value Chain Ecosystem

Zhiyong Zhang, Qingqi Pei, Jianfeng Ma
Ministry of Education Key Laboratory of Computer Network & Information Security
Xidian University
Xi'an, P. R. of China
{zhangzy, qqpei, jfma}mail.xidian.edu.cn

Lin Yang
The Research Institute
China Electronic Equipment & Systems Engineering Corporation
Beijing, P. R. of China
yanglin61s@yahoo.com.cn

***Abstract*—A multi-participant trust relationship is essential to implement a successful business transaction in DRM (Digital Rights Management)-enabling digital contents industry. The simple adoption of several increasingly enhanced security policies does not necessarily establish the mutual trust relationship ultimately, and even has a negative effect on the usability and acceptability of DRM system. Therefore, various participants' benefits should be emphasized in the contents value chain. First, a general DRM contents value chain ecosystem was presented without a loss of generality. Then, a benefits-centric Multi-Participant Trust Architecture (abbr. MPTA), which is based on game-theoretic rational adoptions of security policies for participants, was proposed through an anatomy of existing value chain ecosystems. Finally, we formalized the definitions of the security component and service, the security policy and its utility, as well as the Nash Equilibriums of the multi-participant game under pure and mixed security policy profile. Due to the introduction to Game theory, MPTA enables participants to acquire optimal benefits balance when fundamental security requirements are met, and Nash Equilibrium of the game is the chosen security policies combinations from the participants' perspectives.**

Keywords-Digital Rights Management; Security Policy; Multi-Participant Trust Architecture; Game Theory; Nash Equilibrium

I. INTRODUCTION

With the rapid developments of communication network technologies, the Next-Generation Internet, 3G and 4G wireless mobile network have been striding to a large-scale deployment and application. As digital contents like electric books, images, music, movies and application software are easily duplicated without deterioration in quality, an illicit copy, free distribution and unauthorized usage of copyrighted contents have been still a common phenomenon. As a result, digital contents industry could be heavily damaged, and contents value chain could also be interrupted. In order to effectively resolve the issue of copyrights infringement and realize the flexible and legitimate usage of digital rights, Digital Rights Management (abbr. DRM) has emerged at the beginning of the 1990s.

To date, there are fruitful researches on security issues about DRM, but note that a successful digital transaction generally depends on three key factors: security, trust and benefit [1]. Security is to guarantee a secure and persistent process of contents business, and trust is essential requirement for the robustness and survivability of contents value chain. Some studies of trust have received more attentions recent years. Nowadays, the trust is considered based on security policies and mechanisms in general. But, this is no sufficient. How to rationally adopt security policies for participants pursuing maximum benefits is worthwhile considering.

Bechtold [2] stated that, in the future, exploration of a value-centered technology will become a focus point of DRM. It is stated that DRM should balance the interests of the various stakeholders in value chain, to enable the IPR (Intellectual Property Rights)-enabling contents industry to flourish in [3]. Recently, several attempts to explore benefit balance of DRM have emerged. Heileman et.al. [4] made a game-based analysis: consumers have two choices, one is to purchase DRM-enabling contents, the other is to freely download; contents vendors could choose adopt DRM protection technologies or not, in the scenario that is a two-player two-strategy game, each party's choice of two strategies would have effect on benefits of both. Their conclusion is that a Nash Equilibrium exists in the scenario. Further, the interest balance is also achieved based on a rewarding mode in the procedure of contents sharing. A game-theoretic approach to explore digital rights ownership was proposed for optimally balancing benefits between contents industry and individual consumer, not just benefiting the either of both [5]. The Chang's main attempts, from economics and law standpoints, to solve the debate over the DRM ecosystem show that sharing access rights between both parties would be the best outcome for the whole society, and not lean to any of both.

The main contributions of the paper are two folds. One is to propose a general DRM-enabling contents value chains model through a holistic consideration of various participants. The other contribution is the introduction of game theory to present multi-party trust relationship and to analysis the adoptions of security policies with a goal to achieve optimal benefits for the parties. To our best knowledge, it is the first discussion on the relevant issue of DRM.

978-0-7695-3560-9/08 $25.00 © 2008 IEEE
DOI 10.1109/ISBIM.2008.161

II. CONTENTS VALUE CHAINS AND TRUST RELATIONSHIPS

A. Anatomy of Existing Value Chains

In despite of different definitions or depictions in existence, the DRM-enabling digital contents value chain ecosystem has such essential functions: digital contents coding and identification, package and distribution, digital rights assertion and usage, copyrights tracking and monitoring, which are enabled in the entire life cycle of contents from creation, distribution and consumption to monitoring. Apparently, with regard to a general DRM system, an entire value chain principally includes the contents creator, intermediary distributor, rights holder/issuer and end purchaser.

Besides, some functional components/entities are also playing indispensable roles in DRM value chain. For example, Clearing House, which is responsible for license processing, financial and event managements, and DIMS (Distribution Information Management System) that supports a contract mechanisms and maintains program for interoperability, were both introduced in Lee's proposed distribution model [6]. Vassiliadis [7] proposed a multi-party DRM ecosystem was presented for solving interoperability obstacle for DRM wider acceptability and adoption. The ecosystem refers merely to four entities: Creator, Distributor, User and Authority, which are the essential elements of the simple and practical business model of DRM value chain. Here Authority is responsible for issuing contents license based on rules provided by Creator, which aims at supervising legal usage.

In recent years, the need for the mobile industry to manage the usage of digital contents in a controlled manner has been growing, Mobile DRM being a consequence of that. As a leading industry forum and research organization, Open Mobile Alliance (abbr. OMA) and their DRM Specs of Candidate Version 2.1 have already been published in Jul, 2007, which contains openness, industry-wide interoperability and utility [8]. In the OMA DRM Architecture Spec, it is stated that a large number of possible actors in a DRM ecosystem/value chain are in existence, such as content owners, developers and distributors, network service operators and manufacturers of terminal equipment, etc. But, the Spec is mainly involved in three logic functional entities including Content Issuer (CI), Rights Issuer (RI) and DRM Agent, as well as two participants, which are Contents Provider and User. Subsequently, Gallery [9] introduced three new entities on the basis of OMA DRM architecture: Device Manufacturer, DRM Agent Installer and CMLA (Content Management Licensing Administrator) whose functionality is similar to CA.

B. Basic Trust Relationships in Value Chain Ecosystem

Trust in DRM value chain, which belongs to an aspect of trust relations in the digital world, is a crucial part of multi-party and a complicated challenge of realization. In a DRM ecosystem, it is not possible to distinguish the honest users with the dishonest users. Generally speaking, contents consumers are been treated as potential attackers or illegal users, and therefore contents/rights providers adopt some enhanced security policies mentioned above to establish trust relations among entities. Basic trust relationships are listed as follows in a roust DRM ecosystem:

- Contents Providers should trust the purchasers not to access encrypted contents without acquiring key in license; the users also needs trust contents security and integrity.
- Rights Providers needs to ensure that license is trustworthily executed on the user's device, which is to say, the user should have a trusted computing environment.
- The above two participants are collaboratively providing contents and the corresponding license of rights in some DRM business models, there is a negotiation-based trust relationship between them.

These above mentioned essential trust relationships would be established based on participants' security policy and relative mechanisms. But, a simple adoption of several increasingly enhanced security policies does not necessarily implement multi-party mutual trust relationship. Instead, it may increase the overhead of the system and influence the usability and acceptability of DRM.

III. A GENERAL VALUE CHAIN ECOSYSTEM AND MULTI-PARTY TRUST ARCHITECTURE

A. A General DRM Value Chain Ecosystem

Without loss of generality, we proposed a General DRM (abbr. GDRM) value chain ecosystem, as is shown in Fig.1. There include four basic parties participating in the creation, dissemination and usage of digital contents, such as Contents Provider (CP) that includes creator(s) and intermediary distributor(s) mainly responsible for providing contents for sharers; Rights Provider (RP) capable of distributing corresponding digital rights to purchasers could be services provider, copyrights owner, financial center or network operator in Mobile DRM, etc.; Device Provider (DP) provides digital device or sharer electronics for end user of digital contents value chain; Consumer that is a group of terminal entities to access to digital contents, and to pay usage fee towards the former parties of GDRM. Besides, Consumer could be sub-categorized as Delegator and Delegatee, together called Sharer, which respectively denote an entity sharing contents by using superdistribution mechanisms and the other acquiring the shared contents.

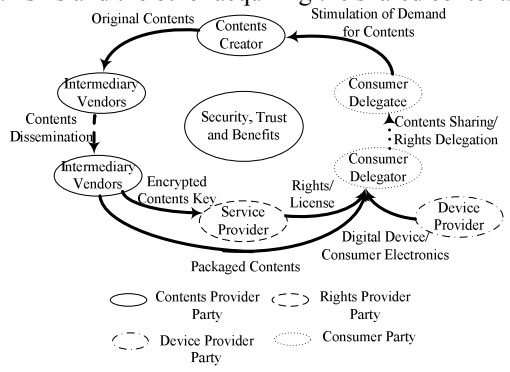

Figure 1. A General DRM Value Chain Ecosystem

B. Multi-Participant Trust Architecture and Hierarchical Analyses

Based on the above proposed a general value chain and the anatomy of fundamental trust relationships, we proposed a Multi-Participant Trust Architecture (MPTA) for DRM-enabling contents value chain, as is shown in Fig 2. It is a multi-layer framework, and also embodies a methodology of hierarchical analysis.

In MPTA, the above two layers consist of DRM value chain and fundamental requirements of security for participants. According to these requirements, there are a group of security components and services that are categorized into basic and optional security component/service denoted by BSC/BSS, OSC/OSS respectively. They can be adopted by participants to implement various practical security policies. So, the forth layer presents a set of security policies for every party. Further, the party in value chain is considered as a Rational Agent (abbr. RA) that can reasonably choose and use a certain security policy, and the consideration is from the assumption of rational agents in the Game Theory. Note that DP is not presented in MPTA, as DP are not involved in the adoptions of security polices, and they only take charge of providing common or enhanced security devices.

From the viewpoint of DRM value chain, the rationality of adopting security policies is based on RAs' game, in which security policies as strategies (or actions) would be rationally chosen, as a result the benefits balance would be achieved. Note that RA should have four basic attributes:

- **Autonomy** denotes an ability of RA to independently make decision on use of strategy.
- **Social Ability** (SA) depicts a capability of considering practical effects of other RAs' actions on self.
- **Reacting** (R) manifests a capability of reaction on adoption of strategy in term of the opposite RAs' choices.
- **Pro-Activeness** (PA) embodies a goal-driven action on rationally acquiring maximum benefits in the game.

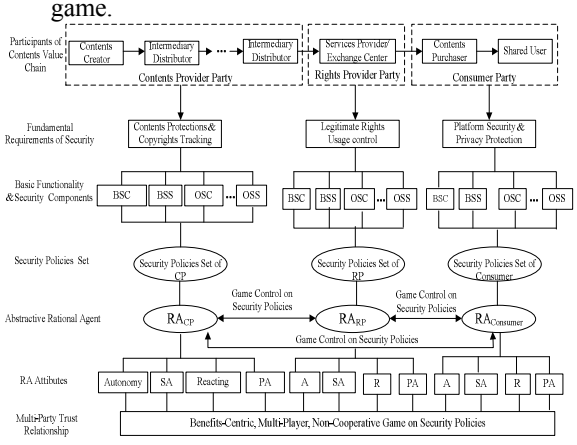

Figure 2. Benefits-Centric Multi-Party Trust Architecture for Contents Value Chain Ecosystem

C. Formalized Security Policies and Multi-Participant Game

Definition 1 (Party) Party $\wp$ denotes a set of some actors α playing the same functional role in DRM value chain.

$$\wp = \{\alpha \mid actor\ is\ responsible\ for\ a\ function\}$$

$$DRM\_ValueChain = \{\wp, Contents, Rights\}$$

$$DRM\_ValueChain_{GDRM} = \{CP, RP, DP, Consumer, Contents, Rights\}$$

Definition 2 (Security Component & Service) in term of fundamental security requirements of each party, an atomic component that may be a program, hardware unit and middleware, as well as a composite service, is realized to accomplish a specific functionality related to security. Security Components/ Services consist of two kinds of basic ones denoted by c^* / s^*, and optional ones written by c / s. Notation *f*, *w*, *u*, and μ denote an actual factor influencing benefit of α when an adoption of *c* or *s*, the weight value of a factor, positive/negative utility of the factor and components/services, respectively.

$$SecurityComponent = \{c_1^*, c_2^*, \ldots c_i^*, c_1, c_2, \ldots c_j\}$$

$$SecurityService = \{s_1^*, s_2^*, \ldots s_m^*, s_1, s_2, \ldots s_n\}$$

$$F(c_p) = \{f_{c1}, f_{c2}, \ldots f_{ci}\},\ F(s_q) = \{f_{s1}, f_{s2}, \ldots f_{sj},\}\ (1 \le p \le j, 1 \le q \le n)$$

$$\mu(c_s) = \sum_{p=1}^{i} u_p (w_p / \sum_{k=1}^{i} w_k),\ \mu(s_t) = \sum_{q=1}^{j} u_q (w_q / \sum_{l=1}^{j} w_l)$$

Definition 3 (Security Policy) *sp* is a set of security components or services including all c^* / s^* and some optional c / s that are adopted by α. Here *sp* has upper abstract.

$$sp = \{c_1^* \ldots c_i^*, s_1^* \ldots s_m^*, c_1, c_2, \ldots c_s, s_1, s_2, \ldots s_t\}\ 0 \le s \le j,\ 0 \le t \le n$$

Definition 4 (Utility of sp) Utility *U* of *sp* is a sum of utilities μ of all components and services involved in *sp*.

$$U(sp) = \sum_{p=0}^{i} \sum_{q=0}^{m} \mu(c_p^*) + \mu(s_q^*) + \sum_{p=0}^{s} \sum_{q=0}^{t} \mu(c_p) + \mu(s_q)$$

Definition 5 (Rational Agent and Payoff) in GDRM, *RA* denotes a rational participant aiming at a maximum of benefits, and makes a decision on adopting a certain security policy. There are four *RA*s with respect to four parties, RA_{CP}, RA_{RP}, RA_{DP}, $RA_{Consumer}$ that includes a specific category of RA_{Sharer}, respectively. The payoff of RA manifests the acquired benefits in participants' policies combination (profile).

Definition 6 (Multi-party Non-Cooperative Game on Security Policies) Multi-Party game of security policies denotes a process of making decision on effective and rational adoption of security policies that have effect on

benefit of the opposing party each other. To achieve utility maximum and balance, a game of MPTA is depicted by a set of three tuple as $< \wp, sp, payoff >$:

$$G = \{< RA_i, SP_i, Payoff(RA_i, RA_{-i}) > | i = \{CP, RP, DP, Consumer\}\}$$

Definition 7 (Nash Equilibrium of Pure Strategy Profile) for any *RA*, when the case that the *RA* adopts a security policy sp^* to acquire benefit greater than the benefit acquired by choosing any other *sp* occurs, the combination of each *RA*'s sp^* is considered as a balance of payoffs by adopting relatively dominant security policies.

$$Payoff(RA_i^{sp^*}, RA_{-i}^{sp^*}) \geq Payoff(RA_i^{sp^j}, RA_{-i}^{sp^*})$$

$$j \in SP_i,\ j \neq *,\ i \in \{CP, RP, DP, Consumer\}$$

$$-i \in \{CP, RP, DP, Consumer\}, -i \neq i)$$

Where $(sp^*_{CP}, sp^*_{RP}, sp^*_{DP}, sp^*_{Consumer})$ is a relatively dominant pure security policy profile.

Definition 8 (Expected Payoff of Mixed Strategy Profile) When any *RA* randomly chooses a pure *sp* from its *SP* set to be an action of a game in term of a specific probability of *sp*, the payoff is uncertain. Expected payoff denotes the uncertain benefit by weighted sum, where let the probability of *sp* be weight.

$$Expected\_Payoff(RA_i, RA_{-i}) =$$

$$\sum_{j \in SP_i} \prod_{k \in \{CP,RP,DP,Consumer\}} p_k(sp_k) * payoff(RA_i^{j,-j})$$

$$\sum_{l=1}^{n} p_k^l = 1\ (\mathrm{k} \in \{CP, RP, DP, Consumer\}$$

$$(1 \leq n \leq \mathbb{C}(SP_k)),\ i \in \{CP, RP, DP, Consumer\})$$

Definition 9 (Nash Equilibrium of Mixed Strategy Profile) for any *RA*, when the case that the *RA* adopts mixed security policies in term of a certain probability combination p^* to acquire benefit greater than the benefit acquired by using other probability combinations occurs, the combination of each *RA*'s p^* is considered as a balance of payoffs by adopting mixed security policies of relatively dominance.

$$Expected\_Payoff(RA_i^{p_i^*}, RA_{-i}^{-p^*_{-i}}) \geq Expected\_Payoff(RA_i^{p_i}, RA_{-i}^{-p^*_{-i}})$$

$$p_i^* = (p_{i1}^*, p_{i2}^*, ..., p_{in}^*)\ (1 \leq n \leq \mathbb{C}(SP_1))$$

$$i \in \{CP, RP, DP, Consumer\}$$

Where $(p^*_{CP}, p^*_{RP}, p^*_{DP}, p^*_{Consumer})$ is a probabilities combination of relatively dominant mixed security policies.

IV. CONCLUSIONS

The paper presented a benefits-centric Multi-Participant Trust Architecture based on a General DRM value chain ecosystem, and formalized security policies and multi-player game. The future works focus on the concrete Game-Theoretic analyses and SWARM simulations of adoptions of some security policies, such as trusted computing-enabling enhanced security policy, under contents acquisition scenario and contents sharing scenario, respectively.

ACKNOWLEDGMENT

The work is supported by National Natural Science Foundation of China Grant No. 60803150 and China National 111 Program of Introducing Talents of Discipline to Universities Grant No.B08038

REFERENCES

[1] O. Petrovic, M. Fallenböck, C. Kittl, T. Wolkinger, "Vertrauen in digitale Transaktionen," WIRTSCHAFTS INFORMATIK, vol. 45, 2003, pp. 53-66.

[2] S. Bechtold, "The Present and Future of Digital Rights Management," Proc. of the Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS 06), IEEE Computer Society Press, Dec. 2006, pp.6.

[3] H. Abie, "Frontiers of DRM Knowledge and Technology," International Journal of Computer Science and Network Security, vol. 7, Jan. 2007, pp. 216-231.

[4] G. L. Heileman, P. A. Jamkhedkar, J. Khoury, and C. J. Hrncir, "The DRM Game," Proc. of 2007 ACM Workshop on Digital Rights Management, ACM Press, Oct. 2007, pp.54-62.

[5] Y. L. Chang, "Who should own access rights? A game-theoretical approach to striking the optimal balance in the debate over Digital Rights Management," Artificial Intelligence and Law, vol. 15, Dec. 2007, pp.323−356.

[6] J. Lee, S. O. Hwang, and S. W. Jeong, et. Al, "A DRM Framework for Distributing Digital Contents through the Internet," ETRI Journal, vol.25, Jun. 2003,:pp. 423-436.

[7] Vassiliadis, Vassileios, and Fotopoulos, et. al, "Decentralising tlie Digital Rights Management Value Chain by means of Distributed License Catalogues," Proc. of 2006 IFIP Artificial Intelligence Applications and Innovations,. vol 204, I. Maglogiannis,., K. Karpouzis, M.Bramer, Eds, Springer Press, 2006, pp. 689-696.

[8] DRM Architecture Candidate Version 2.1. Open Mobile Alliance. Jul., 2007.

[9] E. Gallery, and C. J. Mitchell, "Trusted Mobile Platforms," LNCS 4677, A. Aldini and R. Gorrieri, Eds.: Springer Press, 2007, pp. 282–323.