Chinese Journal of Electronics
Vol.18, No.3, July 2009

Establishing Multi-Party Trust Architecture for DRM by Using Game-Theoretic Analysis of Security Policies*

ZHANG Zhiyong[1,2], PEI Qingqi[1], MA Jianfeng[1] and YANG Lin[3]

(1.*Ministry of Education Key Laboratory of Computer Network and Information Security, Xidian University, Xi'an 710071, China*)

(2.*Electronic and Information Engineering College, Henan University of Science and Technology, Luoyang 471003, China*)

(3.*The Research Institute, China Electronic Equipment and Systems Engineering Corporation, Beijing 100141, China*)

Abstract — A successful transaction of digital contents is primarily dependent on security policies, trust mechanisms and benefits balances, as well as the simple adoption of the combination of enhanced security policies would not effectively establish a trust relationship among various stakeholders in the DRM (Digital rights management) -enabling contents value chain. With respect to a generic DRM ecosystem, the hierarchy analyses of the multi-participant trust architecture were proposed based on the game-theoretic adoptions of security policies. By using formalized definitions of security components and services' utilities, we presented the choice of policies with the external relativity, in the contents acquisition scenario, as a multi-player simultaneous-move game referred to contents provider, digital services/rights provider and consumer. Also, in term of security policies combinations' utilities and benefit effects on participants, we further gained the game's Nash Equilibrium, which is a stable profile of security policies achieving the optimal balance of the security and utilities, thus establishing and strengthening the multi-party trust. The analytic conclusions show that enhanced security policies profile does not necessarily achieve optimal benefits balance in the one-stage game, for a small quantity of digital contents transactions. Whereas, the profile could transform into Nash Equilibrium with the increase of transaction sessions, meanwhile being Pareto Optimality.

Key words — Digital rights management, Trust, Security policy, Trusted computing, Game theory, Nash equilibrium

I. Introduction

With the rapid development 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 a result, by using multiple network admission methods, users could access to digital resources and services in anytime, at anywhere, which is much easier than before. Unfortunately, an illicit copy, free distribution, unauthorized usage of the copyrighted digital contents will also become a common phenomenon, as the contents like electric books, images, music, movies and application software are easily duplicated without deterioration in quality. Under such a circumstance, digital contents industry would be heavily damaged, and its value chain ecosystem could even be corrupted. Therefore, the issue of the copyright protection and legitimate usage is, therefore, crucial.

Digital rights management (DRM) has emerged at the beginning of the 1990s in order to control copyrights infringements. It is an umbrella term involved both in realizations of contents industry realm and in researches on multiple scientific disciplines, for instance, Information technology, economics and law[1]. In the last decade, regardless of a generic DRM or Mobile DRM, the emphasis of related works has been laid on researches on the contents protection, which was based mainly on cryptographic security[2,3] and watermark technologies[4,5], as well as on the controlled usage that was accomplished by Rights expression language[6,7] and Usage control models[8].

Recent years have witnessed the emerging researches on the trust issue in DRM ecosystems[9,10], in combination with trusted computing-enabling applications, which cover to the trustworthily dissemination of licenses presenting the usage policy, the secure storage of contents and encryption keys, together with the trusted execution of DRM controller, also called DRM Agent. Here the remote attestations, seal approaches and integrated trusted platforms were adopted[11]. The trusted terminal platform provided by device vendors is essential to the robust DRM systems, and is also helpful for establishing and strengthening trust relationships among participants. Nowadays, in addition to the trusted PC platform specified by TCG, OpenTC in Europe and Chinese Trusted Computing Union, there exist technical specifications referred to the trusted mobile platform.

As is mentioned above, there are fruitful researches on DRM security issues, but a successful digital transaction should resort to three factors: security, trust and benefit. Security aims at implementing a secure and persistent electronic business to be free from the piracy, and trust is basic requirement for the robustness and survivability of DRM ecosystems. So far, the DRM trust is merely based on security policies and relevant mechanisms, as is no suf-

*Manuscript Received July 2008; Accepted Dec. 2008. This work is supported by the National Natural Science Foundation of China (No.60803150 and No. 60633020), China National 111 Program of Introducing Talents of Discipline to Universities (No.B08038).

ficient. How to rationally adopt security policies for participants pursuing maximum benefits is worthwhile considering. The main contribution of the paper is to propose the multi-party trust architecture for DRM based on game-theoretic analyses of adoptions of security policies, which is the benefits-centric trust, so that various participants could find out a optimal and stable security policies combination in DRM ecosystem.

II. Formalized Multi-Party Game on Security Policies

1. Multi-party trust architecture and hierarchical analyses

A generic DRM ecosystem is composed of various stakeholders as CP (Contents provider), RP (Rights provider), Consumer and Device provider. Based on the anatomy of fundamental trust relationships, Multi-party trust architecture (MPTA) for DRM is a layered framework, where the last party is not referred to, and the above two layers represent the generic value chain and fundamental security requirements for participants, respectively. According to these requirements, the next layer includes a group of security components and/ or services that are categorized into basic security components/services and optional ones. They can be adopted by participants to implement various concrete security policies, and the forth layer presents a set of security policies. The participant is assumed as a Rational agent (RA) that can reasonably choose and deploy security policies based on a complicated game.

2. Basic elements

Definition 1 (Party) A party $\wp$ denotes a set of some actors α playing the same functional role in DRM ecosystem. A party and MPTA value chain are formalized as following sets:

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

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

$$\mathit{DRM\_VauleChain}_{MPTA} = \{\mathit{CP,\ RP,\ Consumer,\ Contents,\ Rights}\}$$

Definition 2 (Security component/service) In term of security requirements for participants, an atomic functionality security component could be a program, hardware/firmware unit and middleware, as well as a functional security service is realized to accomplish a group of related functions. Here basic security components/services are written by c^*/s^*, and optional ones denoted by c/s. Notations f, w, u, μ manifest a factor from the factor set F influencing the whole benefit of $\wp$ for an adoption of c/s, the factor weight value, the factor utility, as well as the positive/negative utilities sum when adopting c/s, respectively. Note that the weight's normalization is based on all factors' weights involved in c/s.

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

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

$$F(c_s) = \{f_{c1}, f_{c2}, \cdots f_{cp}\}, F(s_t) = \{f_{s1}, f_{s2}, \cdots f_{sq}\}, \quad 1 \le s \le j, 1 \le t \le n$$

$$\mu(c_s) = \sum_{i=1}^{p} u_i \left(w_i \Big/ \sum_{k=1}^{h} w_k \right), \quad \mu(s_t) = \sum_{j=1}^{q} u_j \left(w_j \Big/ \sum_{k=1}^{l} w_k \right)$$

Property 1 (External relativity of optional security components/services) If two or more optional components/services that are from different parties need to be adopted simultaneously, otherwise the active c/s has a negative utility on corresponding parties, these components/services are of the external relativity, depicted as follows, where $C(\wp)$ denotes the set cardinality of $\{\wp\}$.

$$\mathit{Relative\_Components} = \{c_1, c_2, \cdots, c_p\}$$

$$\forall i, j\ (1 \le i, j \le p, 2 \le p \le C(\{\wp\}))\exists s, t(s, t \in \{CP, RP, \mathit{Consumer}\}),\ c_i \in C_S, c_j \in C_t, \quad i \ne j \wedge s \ne t \rightarrow \mu(c_i) > 0 \wedge \mu(c_j) > 0$$

$$\mathit{Relative\_Services} = \{s_1, s_2, \cdots, s_q\}$$

$$\forall i, j\ (1 \le i, j \le q, 2 \le q \le C(\{\wp\}))\exists m, n(m, n \in \{CP, RP, \mathit{Consumer}\}),\ s_i \in S_m, s_j \in S_n, \quad i \ne j \wedge m \ne n \rightarrow \mu(s_i) > 0 \wedge \mu(s_j) > 0$$

Definition 3 (Security policy) *sp* is composed of a group of relevant security components/services, which include all c^*/s^* and some c/s that are adopted by $\wp$ with a specific security goal.

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

$$SP_i = \{sp_i^1, sp_i^2, \cdots sp_i^{C(SP_i)}\},$$

$$C(SP_i) = 2^{(j+n)}, \quad i \in \{CP, RP, \mathit{Consumer}\}$$

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

$$U(sp_a^b) = \sum_{p=0}^{i} \sum_{q=0}^{m} \mu(c_p^*) + \mu(s_q^*) + \sum_{p=0}^{j} \sum_{q=0}^{n} \mu(c_p) + \mu(s_q)$$

Property 2 (External relativity of security policies) If two or more different security policies refer to c/s with the external relativity, these security policies are external relative, as written by

$$\mathit{Relative\_Policies}\{sp_1, sp_2, \cdots, sp_n\}$$

$$\forall i, j\ (1 \le i, j \le n, 2 \le n \le C(\{\wp\}))\exists s, t(s, t \in \{CP, RP, \mathit{Consumer}\}),$$

$$\exists p, q(c_p \in sp_i, s_q \in sp_j, sp_i \in SP_S, sp_j \in SP_t)$$

$$(p + q \ge n \wedge i \ne j \wedge s \ne t \rightarrow (c_1, c_2, \cdots, c_p \in \mathit{Relative\_Components}) \vee (s_1, s_2, \cdots, s_q \in \mathit{Relative\_Services})$$

3. Formal game on security policies

Definition 5 (Rational agent) *RA* denotes a rational actor aiming at the benefit maximum, and makes decisions on adopting security policies. In MPTA, there are three *RAs* with respect to three parties, *i.e.*, RA_{CP}, RA_{RP}, $RA_{consumer}$, respectively.

Definition 6 (Payoff of *RA*) In MPTA, the payoff of *RA* denotes the acquired benefit under a security policy combination (profile) that is a vector of security policies adopted by *RA*s' actions. The payoff includes two aspects, one being from *RA* itself and the other being from other *RA*s' moves.

Definition 7 (Multi-party game on security policies) The game depicts a process of making decision on effective and rational adoptions of security policies, where participants' moves have effects on benefits one another. To achieve utility maximum and benefit balance, the game is formalized by a set of the three tuple as $\langle \wp, sp, \mathit{payoff} \rangle$, where SP manifests a set of security policies.

$$G = \{\langle RA_i, SP_i, \mathit{Payoff}(RA_i, RA_{-i}) \rangle | i = \{CP, RP, \mathit{Consumer}\}\}$$

Definition 8 (Nash equilibrium under pure strategy profile) for any *RA*, when the case that the *RA* adopt a sp^* to acquire the benefit greater than one gained by choosing any other *sp* occurs, the combination of each *RA*'s sp^* is considered as the relatively dominant security policies profile met by the benefits balance.

$$\mathit{Payoff}(RA_i^{sp^*}, RA\_{}_i^{sp^*}) \ge \mathit{Payoff}(RA_i^{sp^j}, RA\_{}_i^{sp^*}),$$

$$j \in SP_i,\ j \ne *, i \in \{CP, RP, \mathit{Consumer}\},$$

$$-i \in \{CP, RP, \mathit{Consumer}\},\ -i \ne i$$

where $(sp^*_{CP}, sp^*_{RP}, sp^*_{Consumer})$ is a relatively dominant pure strategy profile.

4. Game of security policies for two scenarios

Proposition 1 (Multi-player simultaneous-move game in contents acquisition scenario) Contents acquisition (purchase) is a general DRM application scenario, where adoptions of security policies are considered as a specific multi-player simultaneous-move game process game among CP, RP and Consumer.

Proof In MPTA, there are RA_{CP}, RA_{RP}, $RA_{consumer}$ in term of Definition 5, and let SP_{CP}, SP_{RP} and $SP_{consumer}$ be a security policies set, respectively. The game is further formalized as $G_{acquisition} = \{\langle RA_i, SP_i, Payoff(RA_i, RA_{\text{-}i})\rangle\}$, where $i = \{CP, RP, Consumer\}$. For the deployment and the initialization of a DRM system, any party needs to choose and active relative security components/services, which is to say, to adopt a specific *sp* from *SP*. In general, the contents acquisition process has temporal order characteristic, taking a DRM Pull model as an example, $RA_{consumer}$ acquires a corresponding license of the purchased content from RA_{RP} after acquiring contents from RA_{CP}. However, each *RA* adopts and initializes *sp* without knowing the moves of other *RA*s' *sp*s, meanwhile the activeness of *sp*s could not change after DRM system initialization for a contents transaction, so the whole process of all *RA*s' moves is a simultaneous-move game on security policies, not a sequential-move game.

Deduction 1 (Repeated-game in contents acquisition scenario) When transactional sessions of contents acquisitions have implemented more times, participant of DRM ecosystem could reactive a game on adoptions of security policies. The new game is seen as a repeated game based on the former game processes and their results, and a new equilibrium could be gained.

Proof In the given scenario, with the increase of contents transactions, the adoptions of security policies would correspondingly change. When RA_{CP}, RA_{RP}, and $RA_{consumer}$ choose security policies over again, a repeated game occurs in combination with the former game and the concrete numbers of transaction sessions, and the newly gained security policies profile becomes a new Nash Equilibrium.

III. Game-Theoretic Analyses of Typical Security Policies

In a general DRM ecosystem, each party has a set of security policies and practical choices as actions in a business transaction. Several typical security policies for CP, RP and Consumer were listed in Section III.1. The next two sub-sections presented every security component/service's utility, as well as effective policies combinations and participants' payoffs, respectively. Finally, a complicated game-theoretic analysis was represented.

1. Typical security policies of participants

We presented several typical security policies, and a practical DRM application may include these policies, but are not limited to. In term of Definition 2 in Section II.2, some security components/services, which are conformable to security requirements of either party, we firstly presented, and then a set of security policies could be easily deduced.

Three participants' security components/services include:

• **Packaging**: by using the functional component, digital contents are encrypted based on a specific cryptographic algorithm, and further encapsulated as a distributable data object format. It is dispensable to a DRM system.

• **WM (Watermarking)**: the basic security service provides a reactive copyrights protection capability and forensic proofs, and is adopted to authenticate the ownership of contents through the detection/decoding of pre-embedded imperceptible watermarking.

• **Identification**: it is employed to accomplish the contents security, for instance, to validate by using a verification service provided by the third party whether a section of malicious codes is embedded into a Java game. And then, Consumer could acquire trustworthy contents when a certain trust level is authenticated. The functionality is optional for CP, whether it is active or not is dependent on CP' intended security policies in content transactions.

• **Transaction-based negotiation with RP (TN)**: for a generic DRM ecosystem, CP and RP are respectively responsible for the dissemination of digital contents and rights/licenses. It is advantageous to the distribution of contents/licenses, and to the creation of business trust relationships between CP and RP. Note that TN is executed when each transaction begins, not when DRM systems establish and initialize.

As the set of CP's c/s is {*Packaging**, *WM**, *Identification*, *TN*}, and obviously, the set of security policies include the following policies: {*Packaging**, *WM**}, {*Packaging**, *WM**, *Identification*}, {*Packaging**, *WM**, *TN*}, {*Packaging**, *WM**, *Identification*, *TN*}, denoted by sp^i_{CP} $(i = 1, 2, 3, 4)$.

• **REI (Rights expression and issue)**: by using it, RP specifies and distributes licenses granting corresponding digital rights in term of purchased contents and user's payments, realizing persistent usage control on contents. The component is considered to be essential to contents legitimate usages from RP's perspective.

• **IA (Identity authentication)**: the authentication provided by the basic component not only ensures the identity of purchaser, but provides a detailed log of the purchase.

• **DA (Device attestation)**: based on trusted computing-enabling devices and the remote attestation, RP could validate the integrity of user devices and DRM Controller. The enhanced functionality is not necessary for DRM or contents transactions, but optional.

• **TN**: it is optional as above mentioned.

Similarly, due to the set of RP's c/s denoted by {*REI**, *IA**, *DA*, *TN*}, the set of security policies is {{*REI**, *IA**}, {*REI**, *IA**, *DA*}, {*REI**, *IA**, *TN*}, {*REI**, *IA**, *DA*, *TN*}}, written by $\{sp^1_{RP}, sp^2_{RP}, sp^3_{RP}, sp^4_{RP}\}$.

• **DRM controller**: this is a key component to effectively control content's legal usages by validating relevant licenses and rights.

• **CRE (Contents restricted execution)**: by the optional service, consumer could discretionarily restrict content's usages and executions in terminal devices according to the different trust level of contents, which is provided by CP.

• **TCD (Trusted computing-enabling device)**: consumers employ this kind of devices in order to safeguard their confidential and sensitive personal data from casually collecting and disseminating.

Consumer-side security policies are composed of {*Controller**}, {*Controller**, *CRE*}, {*Controller**, *TCD*} and {*Controller**, *CRE, TCD*} denoted by $sp^i_{Consumer}$ $(i = 1, 2, 3, 4)$.

2. Utilities of security components/services

Through analyzing typical security policies and their relative c/s above mentioned, we presented the utility impact factors, weights and utilities of c/s in this section. As c*/s* does not change utilities of *sp*, we only need to consider utilities of c/s.

• **Identification service**: the utility-impacting factors mainly refer to the identification overhead, written by f^{CoI}_{CP}, and the benefit from providing trusted contents to consumer, written by f^{PoI}_{CP}. The former is negative utility by u^{CoI}_{CP}, and the latter belongs to positive by u^{PoI}_{CP}.

• **TN component**: its activeness would have significant effect on robust trust relationships between CP and RP. So, this is a positive factor f^{PoTN}_{CP}, and its utility being u^{PoTN}_{CP}. But, the component increases the time delay and computing complexity of each digital transaction, as it is transaction-driven. We define the negative factor and its few utility by f^{CoTN}_{CP} and u^{CoTN}_{CP}, respectively. It should be noted that TN needs to simultaneously active by CP and RP. Thus, if it is adopted only by either of both, u^{CoTN}_{CP} will be neglected. Under this assumption, considering Property 1 in Section II.1, TN adopted by CP and RP is not of the external relativity.

- **DA component**: it implements the function of the attestation on the bootstrap and run-time integrity, as consequently enables RP to ensure that issued licenses will be trustworthily interpreted and executed, further acquiring the utility u_{RP}^{PoDA}. For this, the corresponding impact-factor f_{RP}^{PoDA} benefits RP. The other side of a coin, the adoption and activeness of DA also directly affects the computation and storage overheads of RP-side systems and the establishment cost of the integrity managements according to IMM (Integrity management model) proposed by TCG. These negative factors are together depicted by f_{RP}^{CoDA}, and its utility being u_{RP}^{CoDA}.
- **CRE component**: if CP provides the identified digital contents, consumer could active the component to validate the trust levels of gained contents, and then execute or reject them. The adoption of the component on user terminal device could indirectly protect consumers' sensitive resource, so it has a positive factor by $f_{Consumer}^{PoCRE}$, together with the corresponding utility is denoted by $u_{Consumer}^{PoCRE}$. One the other hand, there are such a negative factor $f_{Consumer}^{CoCRE}$ as the delay of the authentication and control, and its few utility $u_{Consumer}^{CoCRE}$ can be neglected when adopted only by Consumer.
- **Trusted computing-enabling components/services**: these components/services are relative to RP-side DA, meanwhile they also have positive/negative factors and relative utilities, denoted by $f_{Consumer}^{PoTC}$, $u_{Consumer}^{PoTC}$, $f_{Consumer}^{CoTC}$ and $u_{Consumer}^{CoTC}$, respectively. Here, $f_{Consumer}^{CoTC}$ manifests the cost of the trusted computing-enabling terminal device, and $f_{Consumer}^{PoTC}$ being a positive effect on benefits of Consumer, such as improving security of contents and personal confidential data.

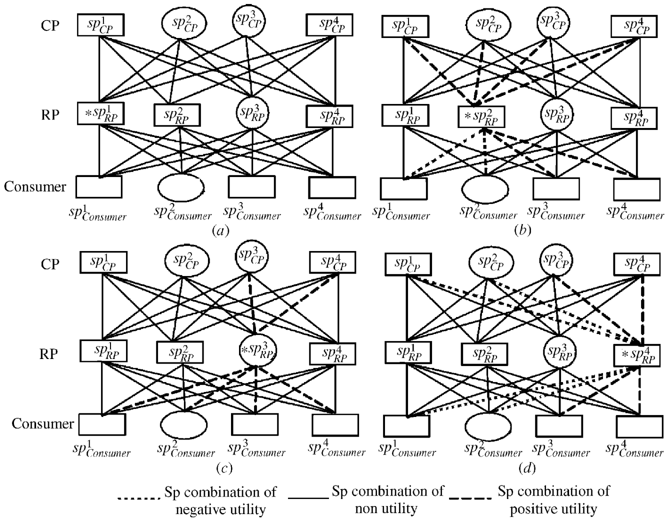


Fig. 1. Security policies combinations from RA_{RP}'s perspective

It is clearly seen that the DA component and trusted computing-enabling device are with the external relativity, moreover the relation between the contents identification and the CRE component is also similar. Therefore, sp_{CP}^2 and $sp_{Consumer}^2$, sp_{RP}^2 and $sp_{Consumer}^3$ are two groups of security profiles with the external relativity.

3. Effective policies combinations and payoffs

As each party has four security policies, there are 64 possible policies profiles in the game. In term of Property 2, Figure 1 illustrated three sorts of profiles from RP's perspective, which manifest the positive utility profile, negative utility one and non-utility one. Here $*sp_i^j$ ($i \in$ {CP, RP, Consumer}, $j = 1, 2, 3, 4$) denotes the discussed object (policy) in a sub-figure.

As c^*/s^* is included in every security policy, the utility of the policy that only consists of c^*/s^* is seen as a baseline utility by $U_i^{baseline}$. According to Definition 4 and Fig.1, the payoffs of participants under various profiles were listed as follows. For RA_{CP},

$$Payoff(RA_{CP}^1, RA_{-CP}^{j,k}) = U_i^{baseline}, \quad 1 \le j \le 4, \quad 1 \le k \le 4 \tag{1}$$

$$Payoff(RA_{CP}^4, RA_{-CP}^{j,k}) = U_i^{baseline} + u_{CP}^{PoI} + u_{CP}^{PoTN} - u_{CP}^{CoI} - u_{CP}^{CoTN}, \; j = 3, 4, \; k = 2, 4 \tag{2}$$

Similarly, for RA_{RP} and $RA_{Consumer}$,

$$Payoff(RA_{RP}^3, RA_{-RP}^{i,k}) = U_i^{baseline} + u_{CP}^{PoTN} - u_{CP}^{CoTN}, \quad i = 3, 4, \quad 1 \le k \le 4 \tag{3}$$

$$Payoff(RA_{RP}^4, RA_{-RP}^{i,k}) = U_i^{baseline} + u_{RP}^{PoDA} + u_{CP}^{PoTN} - u_{RP}^{CoDA} - u_{CP}^{CoTN}, \quad i = 3, 4, \quad k = 3, 4 \tag{4}$$

$$Payoff(RA_{Consumer}^2, RA_{-Consumer}^{i,j}) = U_i^{baseline} + u_{Consumer}^{PoCRE} - u_{Consumer}^{CoCRE}, \quad i = 2, 4, \quad 1 \le j \le 4 \tag{5}$$

$$Payoff(RA_{Consumer}^4, RA_{-Consumer}^{i,j}) = U_i^{baseline} + u_{Consumer}^{PoCRE} + u_{Consumer}^{PoTC} - u_{Consumer}^{CoCRE} - u_{Consumer}^{CoTC}, \quad i = 2, 4, \quad j = 2, 4 \tag{6}$$

4. Multi-party game in contents acquisition scenario

In combination with the above given payoffs and Proposition 1, we proposed a three-dimensional game model, where the game player are CP, RP and Consumer, as well as the game strategies are security policies for there parties. Considering the existing DRM ecosystem, the adoption of enhanced policies, in order to implement the contents security and control the legitimate usage, is a goal for CP and RP, meanwhile consumers have also begun to tend to employ the enhanced security platform. Assume that there is a tendency of adopting sp_{CP}^4 and sp_{RP}^4 for CP and SP, respectively, as well as adopting $sp_{Consumer}^4$ for consumer. Under this assumption, the policies profile $(sp_{CP}^4, sp_{RP}^4, sp_{Consumer}^4)$ is an expected Nash Equilibrium of the game. The next is further game-theoretical analyses of the game model.

Some initial values of c/s utilities and corresponding weights were given in Table 1. Given that $u_i^{baseline} = 5$, where $i \in \{CP, RP, Consumer\}$, payoffs of three parties were calculated according to Eqs.(1)–(6). In addition, there is rational assumption that the adoption of trusted computing-enabling devices needs much more costs u_{Cons}^{CoTC} than a general device. With regard to the multi-player multi-policy game, we gradually decrease on the cardinality of the set of participants' policies by Iterated elimination of (strictly) dominated strategies, further reducing the dimension of the game model, as a consequence, find out a generic equilibrium of Strictly dominant strategies or Nash Equilibrium.

Through analyzing the above listed payoffs of participants under several representative profiles, we could firstly eliminated the three dominated policies of parties, such as sp_{CP}^1, sp_{RP}^1, and $sp_{Consumer}^1$, and the reason is that the payoffs that are acquired by adoptions of these strategies are be certain to be no more than ones resultant with the choices of sp_{CP}^3, sp_{RP}^3 and $sp_{Consumer}^2$, regardless of the strategies chosen by the opposite parties. Thus, the game model, which is initially a $4 * 3$ model, was simplified into a $3 * 3$ model. And then, by the iterated elimination approach, three other strategies, like sp_{CP}^2, sp_{RP}^2 and $sp_{Consumer}^3$, were also expurgated, as they are dominated strategies for sp_{CP}^4, sp_{RP}^4 and $sp_{Consumer}^4$. The $3 * 3$ game model further changed into a $2 * 3$ mode, and the sets of participants' policies were $\{sp_{CP}^3, sp_{CP}^4\}$, $\{sp_{RP}^3, sp_{RP}^4\}$ and $\{sp_{Consumer}^2, sp_{Consumer}^4\}$, respectively. As Consumer's optimal policy should include the security components of $sp_{Consumer}^2$, it was inevitable that CP would be inclined to strictly dominant strategy

Table 1. Initial values of parameters and payoffs of participants

Party	RA$_{\mathrm{CP}}$				RA$_{\mathrm{RP}}$				RA$_{\mathrm{consumer}}$			
factor	f_{CP}^{PoI}	f_{CP}^{CoI}	f_{CP}^{PoTN}	f_{CP}^{CoTN}	f_{RP}^{PoDA}	f_{RP}^{CoDA}	f_{RP}^{PoTN}	f_{CP}^{CoTN}	$f_{Consumer}^{PoCRE}$	$f_{Consumer}^{CoCRE}$	$f_{Consumer}^{PoTC}$	$f_{Consumer}^{CoTC}$
(u, w)	(10, 4)	(5, 2)	(6, 3)	(3, 1)	(10, 5)	(5, 2)	(6, 2)	(3, 1)	(6, 2)	(2, 1)	(4, 4)	(10, 3)
(1,1,1)	5				5				5			
(2,3,2)	8				5				6			
(3,3,2)	6.5				5.9				5			
(4,3,2)	9.5				5.9				6			
(3,4,2)	6.5				4.9				5			
(4,4,2)	9.5				4.9				6			
(4,3,4)	9.5				5.9				3 (one-stage game), 6 (repeated game)			
(4,4,4)	9.5				9.9				4.6 (one-stage game), 7.6 (repeated game)			

$sp_{Consumer}^4$, that is to say that the final profile achieving an equilibrium would include $sp_{Consumer}^4$. So, the $2*3$ model was finally degenerated into a two-player game between RA_{RP} and $RA_{Consumer}$, where both have only two policies. Fig.2 depicted two payoff matrixes between both in the contents acquisition scenario, and one being a one-stage game, the other manifesting a repeated game. Relative dominant strategies profiles would be yielded by analyzing the practical payoffs in Table 1.

Based on these above payoffs of both parties in four profiles, as is shown in Fig.2(a), it was clear that $sp_{Consumer}^4$ is a strictly dominated policy, by which $RA_{Consumer}$ only acquired fewer benefit, 3 or 4.6, than benefit values by $sp_{Consumer}^2$. If it chooses sp_{RP}^4, RA_{RP} would similarly gain fewer interests being 4.9 than 5.9, and we easily found out a Nash Equilibrium $(sp_{RP}^3, sp_{Consumer}^2)$. In combination with sp_{CP}^4 of RA_{CP}, we gained a strategies profile $(sp_{CP}^4, sp_{RP}^3, sp_{Consumer}^2)$ that satisfied the optimal benefits balance for a one-stage game.

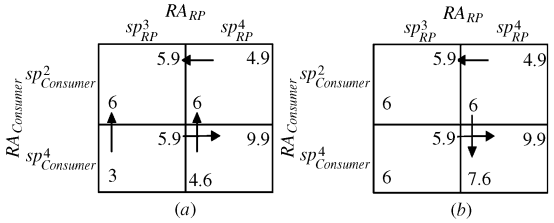


Fig. 2. Analysis of payoff matrix between RP and consumer

5. Results and discussions

The above analyses manifest that the result of the game is a Nash Equilibrium different from the expected one $(sp_{CP}^4, sp_{RP}^4, sp_{Consumer}^4)$, and the result is an inferior optimal security policies profile, not an enhanced policies one in a one-stage game is profile. The reason is that three parties could not achieve the optimal benefits balance under the enhanced security policies profile, consequently they were together inclined to an inferior optimal and stable status, which is a balance of relatively dominant strategies. Under this circumstance, any participant would not acquire more benefits by adopting other policies alone. Obviously, the case that $RA_{Consumer}$ could not choose $sp_{Consumer}^3$ with the external relativity leads to the result, as $sp_{Consumer}^2$ is a strictly dominant strategy for $RA_{Consumer}$. If $sp_{Consumer}^3$ could be chosen, and then consumers would choose $sp_{Consumer}^4$. However, their gained benefit is much fewer than the baseline values 5 by observing Table 1 and Fig.2(a). Therefore, RA_{RP} would merely adopt sp_{RP}^3 with the external relativity.

Besides, some further results and discussions were listed as follows:

(1) In term of Deduction 1, when there is a repeated game on the adoptions of security policies for participants, the game yields a new Nash Equilibrium $(sp_{CP}^4, sp_{RP}^4, sp_{Consumer}^4)$. With the increase of content transactions, for $RA_{Consumer}$, the loss resultant with the adoption of $sp_{Consumer}^3$ would be compensated by much more gained benefits. For this, when a repeated game occurs, its payoffs matrix is illustrated in Fig.2(b). When a consumer's payoff changes from 4.6 to 7.6, and $RA_{Consumer}$ would consider $sp_{Consumer}^4$. Note that $f_{Consumer}^{CoTC}$ has a few of marginal cots in the repeated game. As a rational participant, not doubt that $RA_{Consumer}$ would choose $sp_{Consumer}^4$ by sacrificing short-term benefits and acquiring long-term ones.

(2) When the number of transactions exceeds to a natural number,

$$\lceil |u_{Consumer}^{CoTC} w_{Consumer}^{CoTC} - u_{Consumer}^{PoTC} w_{Consumer}^{PoTC}| / u_{Consumer}^{PoTC} w_{Consumer}^{PoTC} \rceil$$

the gained benefits of $RA_{Consumer}$ would gradually increase, and it would acquire much more than benefits than the baseline.

(3) For the repeated game in the contents acquisition scenario, we found out two Nash equilibriums under pure strategies profile $(sp_{CP}^4, sp_{RP}^4, sp_{Consumer}^4)$ and $(sp_{CP}^4, sp_{RP}^3, sp_{Consumer}^2)$. It should be noted that there does not exist Nash Equilibrium under Mixed strategies profile for the game. Also, $(sp_{CP}^4, sp_{RP}^4, sp_{Consumer}^4)$ is also a Pareto Optimality in comparison with the other Nash Equilibrium, as the former is of absolutely dominant profile for various stakeholders' perspectives.

IV. Conclusive Remarks

The paper presented a game-theoretic analysis of the adoptions of security policies, and acquired optimal security policies profiles in the contents acquisition scenario, so that establish a multi-party trust for a generic DRM value chain ecosystem. We drew significant conclusion that simple adoptions of the combination of enhanced security policies with the external relativity are not certain to achieve optimal benefits balance among participants, that looking for a profile of relatively dominant strategies is crucial to a complicated DRM ecosystem. In addition, the enhanced policies profile could transform into a Nash Equilibrium when a repeated game exists, with the increase of digital content transactions. Our further work aims at the other application scenario of the contents sharing, in which RP' adoptions of security policies and sharing behaviors of Consumer influence each other, thus yields various business model referred to the DRM-enabling contents industry.

References

[1] B. Rosenblatt, "DRM, law and technology: an American perspective", *Online Information Review,* Vol.31, No.1, pp.73–84, 2007.

[2] N.S. Jho *et al.,* "New broadcast encryption scheme using tree-based circle", *Proc. of 2005 ACM Workshop on Digital Rights Management,* Alexandria, Virginia, USA, pp.37–44, 2005.

[3] N. Fazio, "On cryptographic techniques for digital rights management", *Ph. D. Thesis,* New York University, USA, 2006.

[4] P. Wolf, M. Steinebach, K. Diener, "Complementing DRM with digital watermarking: mark, search, retrieve", *Online Information Review,* Vol.31, No.1, pp.10–21, 2007.

[5] M. Steinebach, E. Hauer, P. Wolf, "Efficient watermarking strategies", *Proc. of Third International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution,* Barcelona, Spain, pp.65–71, 2007.

[6] P. A. Jamkhedkar, G. L. Heileman, I. M. Ortiz, "The problem with rights expression languages", *Proc. of 2006 ACM Workshop on Digital Rights Management,* Alexandria, Virginia, USA, pp.59–67, 2006.

[7] C. N. Chong, "Experiments in rights control expression and enforcement", *Ph. D. Thesis,* University of Twente, The Netherlands, 2005.

[8] A. Arnab, A. Hutchison, "Persistent access control: a formal model for DRM", *Proc. of 2007 ACM Workshop on Digital Rights Management,* Alexandria, Virginia, USA, pp.41–53, 2007.

[9] J. Nützel, A. Beyer, "Towards trust in digital rights management systems", *LNCS 4083,* pp.162–171, 2006.

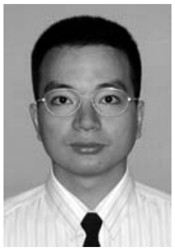
[10] A. Arnab, "Towards a general framework for digital rights management (DRM)", *Ph. D. Thesis,* University of CAPE TOWN, South Africa, 2007.

[11] A. Cooper, A. Martin, "Towards an open, trusted digital rights management platform", *Proc. of 2006 ACM Workshop on Digital Rights Management,* Alexandria, Virginia, USA, 2006.

ZHANG Zhiyong received B.S., M.E. degrees in Computer Science from Henan Normal University and Dalian University of Technology, China, in 1998 and 2003 respectively. He is now a Ph.D. candidate in Ministry of Education Key Laboratory of Computer Network and Information Security at Xidian University. He is also an associate professor at Henan University of Science and Technology. His research interests include Digital Rights Management and trust management, trusted computing and access control. (Email: xidianzzy@126.com)

PEI Qingqi received B.E., M.E. and Ph.D. degrees in Computer Science and Cryptography from Xidian University, in 1998, 2005 and 2008 respectively. He is now an associate professor and a vice-director of CNIS Laboratory, also a Professional Member of ACM and Japan IEICE, Senior Member of Chinese Institute of Electronics and China Computer Federation. His research interests focus on digital contents protection and trusted computing.

MA Jianfeng received B.S. degree in Mathematics from Shannxi Normal University in 1985, and received M.E., Ph.D. degrees in Computer Science and Cryptography from Xidian University in 1988 and 1995 respectively. He was a visiting researcher at Nanyang Technological University, Singapore, from 1999 to 2001, and now is a doctorial supervisor at Xidian University and director of CNIS. He is also a Senior Member of Chinese Institute of Electronics and a Member of IEEE. His research interests include wireless network security and trusted network admission.



YANG Lin received the B.E., M.E. and Ph.D. degrees from National University of Defense Technology of China in 1993, 1996 and 1998 respectively. He is a researcher in The Research Institute, China Electronic Equipment and Systems Engineering Corporation and doctorial supervisor of Xidian University and National University of Defense Technology. Currently his research interests include system security and network security.