西安电子科技大学
博士学位论文

数字版权管理中的安全策略分析与选取

(英文详细摘要)

姓　　　　名：张志勇

申请学位级别：博　士

专　　　　业：计算机系统结构

指　导　教　师：杨林　研究员

二〇〇九年九月

Security Policies Analysis and Adoption in Digital Rights Management (Extended Abstract)

A Dissertation

Submitted to Xidian University

in Candidacy for the Degree of

Doctor of Philosophy

in

Computer Science

by

Zhi-yong Zhang

Research Fellow Lin Yang, Supervisor

Xi’an P. R. China

September，2009

Security Policies Analysis and Adoption in Digital Rights Management

Section 1 Research Background, Motivation and Significance

With the rapid development of communication network technologies, the Next-Generation Internet, 3G and 4G wireless mobile networks have been striding to the large-scale deployments and applications. 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 ever before. Under this circumstance, the copyright infringement behaviors, such as the illicit copy, malicious distribution, unauthorized usage, free sharing of copyrights-protected digital contents, have already become a common phenomenon, as the contents like electric book, image, music, movie and application software are very easily duplicated without the deterioration in quality. Thus, the digital contents industry could be heavily damaged. To solve the issue on copyrights protections of digital contents, Digital Rights Management (DRM) is involved with information technologies, economics and copyrights law, and becomes a inter-discipline and challenging study. From DRM techniques' perspective, related works have to date investigated on contents protection and usage control, which refer to three aspects as follows, on behalf of Contents Provider (CP) and Rights Provider (RP). (1) realizing contents protection and secure distribution by using cipher algorithms and secure protocols. (2) Implementing trusted and controlled usage control on digital rights based on open, general-purpose terminal platform or special-purpose multimedia consumer electronics. (3) Tracking and prosecuting piracy by watermarking techniques.

Undoubtedly, the above mentioned security policies and mechanisms are essential to CP, RP and DRM systems, and they are progressively mature. However, DRM-enabling digital contents industry and its value chain embrace an important participant - End User, and various stakeholders are not fully trusted one another due to their own benefits, thus leading to a fact that the security techniques become the basis of multi-participant trust. Noted that from user's perspective, increasingly security policies and mechanisms give birth to several unexpected issues, such as the weaker system interoperability and usability, as well as higher security overheads, for instance when the adoption of trusted computing-enabling devices. If rational decisions on the adoption and deployment on DRM security policies are ignored, and simple adoptions of increasingly security would yield to negative utilities for various stakeholders in the value chain. For this, we have an objective to explore on a tradeoff between DRM security and multi-participant utility, and implement an effective security policies adoptions and deployments, thus an optimal security-utility balance would be established on the participants.

The thesis's original contribution is a cross-discipline study on DRM security policies' multi-participant utilities analysis and adoption in a whole digital contents value chain, especially the introduction of End User participant. This is a novel perspective, and enables parties to acquire optimal security utilities or benefits when various stakeholder' security requirements are meet. In the thesis, the systematic and holistic DRM security policies analysis framework, as well as security components/services and their composable policies-oriented formalism, have an important theory significance on the rational decision on adoptions of security polices. Besides, the proposed trusted computing-enabling DRM typical security policies and their game-theoretical adoption analysis are helpful for contents/services providers to effectively deploy polices and implement the corresponding mechanisms, based on a rational analysis on security-utility. So, our contributions are of application value for digital contents industry. The thesis was sponsored by National Nature Science Foundation of China, Grant No. 60803150, titled by "Research on Multiparty Trust based on Security Policies Game-Theoretic Control in Digital Rights Management", Standardization Administration of The People's Republic of China, Grant No. 20080200-T-339, titled by "Research on National Standard Framework and Terminology for Digital Rights Management", and Key Program of National Nature Science Foundation, P. R. of China, Grant No. 60633020, titled by "Research on Trusted Mobile Internet Theory and Application".

Section 2 Main Studies and Contributions

The thesis is based on the holistic analysis and evaluation on abroad and home related works, and the survey of representative security polices and mechanisms from CP, RP and User's perspectives. The survey includes the preventative techniques as cipher contents protection and usage control, as well as watermarking-based reactive ones. Besides, considering an open issue of multi-party trust in DRM ecosystem, we analyzed several trust model and denoted that enhanced security policies could not effectively solve the issue, and the establishment of a security-utility-centric multi-party framework is needed and feasible. Therefore, based on game theory, fuzzy AHP and risk management, the thesis focuses on the following three aspects: (1) formalizing security policies' utility and game-theoretical analysis on adoptions. (2) proposing a group of DRM enhanced security polices and mechanisms,including trusted computing-enabled remote attestation and digital rights transfer. (3)for two DRM application scenarios, contents acquisition and sharing, analyzing security policies' utilities and decision-marking, respectively.

The main studies and contributions are listed as follows,

(1)**Formalized Analysis on DRM Security Policies' Utility and Adoption**

Firstly, a systematic and holistic formalism framework, which includes utility functions of DRM security components/services and their composite policies, was proposed. The external relativity of components/services are defined as an acquired positive utility, when and only when components/services are meanwhile adopted and active. The property would have a direct effect on the decision-marking of policies. Moreover, by using the definition of Nash Equilibrium of multi-participant non-cooperative game, i.e., a security policies profile having an optimal utility, we gave two propositions on two DRM application scenarios, respectively: when participants adopt security policies, a basic simultaneous-move non-cooperative game and a complicated dynamic & mixed game hold. Furthermore, Super Additivity and Convexity of security utility in a multi-participant operative game were defined, respectively. These above mentioned formalisms underlie further studies, and are used for a guideline of policies decision-marking in other information security.

Secondly，in combination with Fuzzy Analytic Hierarchy Process in decision theory, we proposed DRM security policies analytic hierarchy structure that effectively solves the issue of multiple weights' calculations.

Thirdly，in order to analyze real utility of enhanced security polices, inspired by security risk management, we proposed a novel concept called Risk-Controlled Utility

(RCU). The concept is employed to present the positive utility of enhance policies. Here, User Demand (UD) of digital users is introduced into ALE (Annualized Loss Expectancy). We made fuzzy assessments on UD and other risk factors by the marriage of qualitative and quantitative approaches and fuzzy tri-angle number, and analyzed the maximum occurrence rate of risky events based on VaR(Value at Risk) theory and Poisson Probability Distribution, thus acquiring RCU. The analytic method could be suitable for the assessment and calculation of enhanced policies for CP.

(2)**Trusted Computing-based DRM Security Policies and Mechanisms**

Firstly，based on the analysis on basic properties of remote attestation models, we denoted that these model available could not effectively protect the privacy of attested platform status, further proposed Attestation Proxy Party (APP)-supported Remote Attestation (AP^{2}RA) and its secure protocol. Having accepted the attestation delegation of Challenger, the trusted third party make hardware and software integrity and security attestation on Responder's remote platform, and trustworthily report the boolean value of the present platform status, thus improving remote attestation model based on two parties, as well as effectively protecting platform privacy of Responder. Moreover, compared with other approaches including TCG schema, the proposed approach is capable of resisting against message replay attack and collusion attack from Attested Party together with of tracing terminal platform sponsoring attack on APP, with suitable for resource dissemination and information sharing in trusted network.

Secondly, based on Usage Control basic framework UCON$_{ABC}$，we proposed UCON$_D$ model with delegation characteristic, which is introduced into Authorization-oBligation-Condition. The novel model could be used for digital rights delegation and transfer in contents sharing scenario. Integrating UCON$_D$, we further gave a fine-grained digital rights delegation and trusted distribution policy, in which Transferable Rights Object (TRO) was presented by using ODRL (Open Digital Rights Language), as well as AP^{2}RA-based TRO trusted distribution process was represented. The studies on DRM usage control not only meet the contents sharing requirement in Social Network, but improve controllability and security of rights/license usage and transfer.

Thirdly, considering digital rights negotiation between CP and User, and Java-class application security at user side, two refined security polices are presented, respectively. RP, as a negotiation proxy at user side, could implement non-collision rights dispense, thus solve the issue of illegal contents copy and propagation led by rights composition. Besides, by multi-level certification services, for example, Java third party certification and network operator's contents certification, contents security and controlled execution are achieved.

(3)**DRM Security Policies Analysis and Adoption in Contents Acquisition Scenario**

Firstly，in combination with the above mentioned enhanced security polices and a generic contents acquisition scenario, we gave a group of typical security policies set and their external relativity. The weights of utility-influencing factors were calculated based on Fuzzy AHP, consequently yielding utility functions of participants' security polices profile.

Secondly，a non-cooperative game model among CP, RP and User was emphatically proposed to realize the adoption of security policies, and two Nash Equilibrium results and conditions were yielded by Dominated Policies' Iterated Elimination method. Here, two equilibriums denoted enhanced security policies profile and sub-security profile, respectively, and they are optimal policies combinations for participants.

As Swarm is helpful for multi-agent modeling and simulation, we designed a three-party simultaneous-move game experiment in Eclipse environment. The experiment further verified the above analysis, and clearly show that the trend of adoption a certain security policy after multiple games, i.e., the enhanced polices are step by step stable, with the increase of contents transactions and significant decreases of managerial and session-level overheads led by enhanced security.

Thirdly, in term of the existence of Device Provider (DP) in contents value chain, a cooperative game among CP, RP and DP denotes that if participants together provide and deploy security policies (functionalities), Super Additivity and Convexity would be met. Under this circumstance, all parties acquire their own optimal benefits. At the same time, the corresponding Nash Equilibrium becomes a Pareto Optimality.

(4)**DRM Security Policies Adoption and Risk Management in Contents Sharing Scenario**

For a complicated DRM scenario, the contents sharing is a common phenomenon in social network. Firstly, a tree of the contents sharing between contents original purchaser and his/her sharers was presented to embody the rights transfer and consumption. Based on the simplified tree structure, a Dynamic and Mixed Game (DGM) between *Providers* and *Sharer*, as well as its Nash Equilibrium at every game stage were highlighted.

Secondly，three representative strategies, i.e., All-General Security, All-Enhanced one and Dynamic one, were investigated from *Providers*' perspective in DMG. Besides, with regard to *Sharer*'s three different sharing modes, such as Partial, Modest and Extensive modes, a DMG algorithm and Swarm simulation experiments were designed to implement the corresponding adoption decision-marking. The results show that *Providers*' security policies including the remote terminal attestation refer to high-cost trusted computing devices (components). Therefore, in several concrete Nash Equilibrium conditions, dynamic security strategy is optimal. However, *Providers*' adoptions of All-Enhanced strategy would be gradually stable, with the significant decrease of high security cost and the increase of transferable digital rights.

Thirdly，based on formalized RCU definition, we made assessments on trusted computing-enabling enhanced security policy, and analyzed the effect of different sharing modes on utilities, when digital contents pirate occurs. The simulation experiments show that modest sharing is dominant over the other two modes. Also, a business model suitable for contents sharing scenario was discussed. Here, CP and RP could establish the model through rational adoptions of security policies, controlling pirate in content sharing and acquiring maximum benefits in digital contents transactions.

Section 3 Unsolved Issues and Progress

The thesis includes the following some unsolved issues, which would be further discussed in the future works:

(1) regarding the risk utility analysis, we adopted qualitative and quantitative integrated approaches, including specialists subjective qualitative assessments on risk factors and fuzzy tri-angle number-based data analysis, as well as the quantitatively calculation of risk occurrence probability according to Poisson Probability Distribution of a generic event. These qualitative approaches and random event presentation could simply and fast evaluate security polices' utilities, pros and cons, and accomplish adoption decisions for CP. For quantitative risk assessment, we are intended to employ Monte Carlo simulation and Bayesian Network to study on an effective approach to analysis on RCU,

with a result to a in-depth security cost-benefit analysis and decision. In addition, we would consider Fuzzy Set theory to find a much more effective fuzzy analytic method for multi-factor weights calculations.

(2)Digital contents sharing scenario refers to a social network composed of sharers, and adoptions of security policies are much more complicate for CP and RP. In the thesis, we presented the users' contents sharing tree structure, which simplifies sharing processes among users, and proposed a dynamic and mixed game model between *Providers* and *Sharer*. Considering a complicated social network of users, content sharing is much closer to a bi-directed graph structure. Therefore, one of future works is to explore the effects of contents sharing on adoptions of security polices based on Colored Petri Network, and propose some effective security polices to control risks and digital pirates.

(3) With regard to DRM security mechanisms, trusted computing-enabled enhanced security approaches are used for the trusted distribution and execution of digital contents and transferable license, and DRM contents and devices cipher keys' secure storage and I/O are not discussed in the thesis. Further, we would analyze these issues in combination with trusted computing terminal devices, and resist malicious users and pirates against modifying, unauthorized usage and copy digital contents. Besides, the prototype realization of the proposed conceptual model of Xen-based trusted computing platform is one of future works, in combination with trusted computing technologies progress in the industry realm.

(4)The proposed DRM security policies analytic approach and enhanced security mechanisms are oriented by a generic DRM application, where the digital contents protection and usage control of concrete application systems or network environments are not included, such as Mobile DRM, multimedia contents security, Peer-to-Peer DRM. With respect to these typical DRM applications and related contents formats, some schemes should be proposed and analyzed by using the formalized DRM security-utility analytic framework to solve the issue of policies adoption and deployment in a real application, thus becoming wider application significance.

Key Words Digital Rights Management; Security Policy; Utility Analysis; Game Theory; Security Risk Management

Supervisor Signature:
Date：