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
(中文详细摘要)

姓　　名:
申请学位级别: 博 士
专　　业: 计算机系统结构
指 导 教 师:

二〇〇九年九月

Security Policies Analyses and Adoptions in Digital Rights Management (Extended Abstract in Chinese)

A Dissertation

Submitted to Xidian University

in Candidacy for the Degree of

Doctor of Philosophy

in

Computer Science

by

, Supervisor

Xi'an P. R. China

September，2009

数字版权管理中的安全策略分析与选取

一、研究背景、动机和意义

随着通信网络技术的快速发展，下一代互联网络、3G和4G等无线移动网络正逐步走向大范围的部署和应用。通过不同的网络接入方法，用户能够前所未有地在任意时间、任何地点访问数字资源，体验数字服务。在此情形下，数字内容（电子书、图像、音视频多媒体、移动应用软件等）所具有的无损复制和网络传播等重要特性，引发出一系列版权侵犯行为，例如非法拷贝、恶意分发、非授权访问和随意分享等，这些已成为数字世界的普遍现象，数字内容产业受到严重的影响。为解决数字内容的版权保护问题，数字版权管理(Digital Rights Management, DRM) 涉及信息技术、经济学、版权法律等，成为一个学科间具有挑战性的研究课题。从DRM技术角度，迄今国内外的相关研究工作主要从内容提供商（Contents Provider, CP）和数字权利提供方（Rights Provider, RP）的角度，探讨数字内容的安全保护与使用控制，即集中在以下三个方面：（1）利用密码学算法与安全协议实现内容保护及安全分发；（2）在开放的、一般用途的用户终端设备，或者特殊用途的多媒体设备上可信、可控地使用数字权利；（3）基于数字水印技术的版权追踪和起诉等。

毋庸置疑，上述安全策略与机制对于CP、RP以及DRM系统是必不可少的，也是日趋成熟的。然而，DRM支持的数字内容产业价值链中也涉及到重要的一方——终端用户，并且三方之间由于各自的利益并不存在完全的信任，致使安全技术成为构建多方信任的基础。我们注意到，从用户的角度，不断增强的安全策略与机制也造成了DRM系统互操作性与可用性的显著降低，并带来了较高的安全成本，如可信计算终端设备的选用。如果在选择和部署DRM安全策略时忽视了理性决策，简单地选取不断增强的安全策略必将会给价值链中的各方带来负面的效用影响。为此，我们的研究试图在DRM安全性与多方效用之间寻找折中，实现有效的安全策略选取与部署，从而在各方之间达到一种最优的安全—效用平衡。

本文的创造性贡献主要体现在从完整的数字内容价值链中多方的角度，特别是终端用户的引入，基于多学科的研究方法探讨DRM安全策略的多方效用分析与选取决策。这是DRM研究的一个崭新角度，使得各方在满足自身安全需求的同时，获得最优的安全效用（收益）。本文所建立的较为系统、完整的DRM安全策略分析框架，以及面向安全组件（服务）及其组合策略的形式化效用分析方法，对于实现安全策略理性决策具有重要的理论意义。同时，所提出的可信计算支持的DRM典型安全策略及其博弈论选取分析，有助于数字内容/服务提供商通过安全—效用的理性分析，有效地部署安全策略并实现相应的安全机制。因此，本文研究对于数字内容产业也将具有较好的应用价值。该研究工作得到了国家自然科学基金项目（No. 60803150）“数字权益管理中基于安全策略博弈控制的多方信任研究”、国家标准化技术委员会（No. 20080200-T-339）“数字版权管理（DRM）标准体系与术语研究”、国家自然科学基金重大项目（No.60633020）“可信移动互联网络关键理论与应用研究”等项目的资助。

二、研究方法和主要贡献

本文工作建立在对近年来国内外DRM相关研究的全面地分析与评价基础上，从CP、RP以及终端用户三方的角度，综述了他们各自代表性的安全策略及实现机制，包括以密码学内容保护和使用控制方法为基础的预防式安全技术，以及基于数字水印的侵权追踪等反应式DRM方案。此外，针对DRM系统与价值链中的多方信任这一开放问题，剖析了现有的DRM信任模型，提出了内容价值链中多方之间的基本信任关系，并指出：通过增强的安全策略与机制不能有效地解决多方信任问题，而建立

一种以安全—效用分析为中心的多方信任框架是必要并且可行的。因此，本文基于决策论中的博弈理论、模糊层次分析法，以及安全风险管理等，主要完成了以下三个方面的工作：（1）形式化描述了安全策略的效用并建立了安全策略选取的博弈论分析框架；（2）提出一组DRM安全增强策略及其实现机制，其中包括可信计算支持的用户终端远程证明方案及数字权利转移等；（3）分别针对DRM两个应用场景，即基本的内容获取场景和内容分享场景，实现一组典型安全策略集的效用分析与选取决策研究。

本文主要研究内容及贡献详细列举如下：

（1）**形式化的DRM安全策略效用分析与选取研究。**首先，提出了一个系统、完整的形式化分析框架，其中包括DRM安全组件/服务及其所组合策略的效用函数；定义了安全组件/服务的外部相关性，用于描述当且仅当多个安全组件/服务被多方同时选取并且激活时，将具有安全的正效用。该性质将直接影响到安全策略的选取决策。此外，通过定义安全策略多方非合作博弈的纳什均衡（Nash Equilibrium），即一个相对各方具有最优效用的安全策略组合，进而给出了与DRM应用场景相关的两个命题：多方在选取安全策略时，分别存在基本的同时行动非合作博弈以及复杂的动态混合博弈。同时，形式化描述了多方合作博弈时安全效用的超可加性（Super Additivity）和凸性（Convexity）等。该形式化分析框架将作为本文工作的基础，同时也可用于指导其他安全信息系统的策略选取决策。

其次，结合决策论中的模糊层次化分析法（Fuzzy Analytic Hierarchy Process），提出了DRM安全策略的层次化分析结构，并用于有效解决当大量安全效用影响因子存在时的权重量化问题。

最后，为了分析安全增强策略的实际效用，受安全风险管理的启发，提出了受控风险效用（Risk-Controlled Utility, RCU）的概念，用于描述和分析安全增强策略的正效用影响。这里，并将数字内容的用户需求（User Demand, UD）这一因素引入ALE（Annualized Loss Expectancy）计算，采用定量和定性相结合的方法以及模糊三角数对UD及其它风险影响因子进行模糊评估，并采用风险管理中VaR（Value at Risk）理论和泊松概率分布分析安全风险事件的最大发生概率，从而最终获得安全增强策略的RCU值。该方法可适用于内容提供商评估及量化安全增强策略的实际效用。

（2）**基于可信计算的DRM安全策略与机制研究。**首先，在对现有多个远程证明模型的基本特性分析基础上，指出了现有模型不能有效保护被验证方终端平台隐私这一不足，进而提出了一种支持验证代理方的远程证明（Attestation Proxy Party-supported Remote Attestation, AP^{2}RA）方案及其安全协议。引入的可信第三方通过接受验证方（Challenger）的委托，对被验证方（Responder）远端平台的软硬件完整性及安全性实施校验，并可信地报告平台当前状态的布尔值，从而改进了基于验证双方的远程证明模式，有效地保护了被验证方的平台隐私。与已有的TCG等方案相比，本方案能够抵抗被验证方的消息重放攻击和共谋攻击，并追踪对APP发起攻击的终端平台，可适用于开放网络环境下的数字内容可信分发与共享等应用。

其次，针对使用控制（Usage Control, UCON）基本框架UCON$_{ABC}$，提出了具有权限委托的UCON$_D$模型，在授权-义务-条件（Authorization-oBligation-Condition）基础上引入了委托/转授权（Delegation）能力，该模型可用于内容分享中的数字权利转移与委托。结合UCON$_D$模型，进一步提出了一个细粒度的数字权利委托及可信分发安全策略。这里，采用扩展的ODRL（Open Digital Rights Language）描述了可转移权利对象（Transferable Rights Object, TRO），并给出了基于AP^{2}RA的TRO可信分发协议及用户端可信执行过程。对DRM使用控制的研究不仅满足了数字内容购买者在其社会网络（Social Network）中分享内容的实际需求，同时也保障了数字权利提供方对权利/许可的使用及转移的可控性与安全性。

最后，针对内容提供商与用户之间的数字权利协商，以及用户端的Java类应用安全，分别给出了两个改进的安全策略。通过将RP作为用户端数字权利协商的代理，

可实现无冲突数字权利的分发，有效地解决了由于权限组合所造成的内容非法复制和传播。此外，利用多级认证服务，例如第三方Java认证和网络服务提供商的内容认证等，可实现内容提供商与用户之间的内容安全和可控执行。

（3）**内容获取场景下的DRM安全策略分析与选取研究。**首先，结合上面所提出的安全增强策略，面向一个基本的DRM内容获取场景，给出一组典型安全策略集及其外部相关性。通过模糊层次分析法（Fuzzy AHP）评估该安全策略集中效用影响因子的实际权重，以构成各方安全策略组合的效用函数。

然后，重点提出了CP、RP与用户三方之间安全策略选取的非合作博弈模型，并通过劣势策略迭代消去法得出了两个纳什均衡结果及其存在条件。这里，两个纳什均衡分别表示高安全策略组合和次安全策略组合，它们也是对各方具有最优效用的策略组合。鉴于Swarm软件包适用于多Agent系统的建模和仿真，我们在Java Eclipse环境下设计并实现了三方同时行动博弈的仿真实验。该实验进一步验证了分析结论，并清楚地表明在多个时间步（博弈）后，各方选取某一安全策略的趋势，即安全策略的选取是随着内容交易事务的增加，以及高安全性所带来的管理和会话级成本与开销的显著降低，将逐渐趋于稳定。

最后，考虑到内容价值链中设备供应商（Device Provider, DP）的存在，通过CP、RP和DP三方合作博弈分析得出，提供方之间共同提供和部署安全策略（功能性），将满足安全效用的超可加性和凸性，各方将同时获得最优收益。此时，相应的纳什均衡也将具有帕累托优势（Pareto Optimality）。

（4）**内容分享场景下的DRM安全策略选取及风险管理研究。**对于一个复杂的DRM应用场景，在社会网络中分享数字内容是普遍存在的。首先描述了一个由内容购买用户及其分享者所构成的内容分享树，用于描述数字权利在用户间的转移和消耗。基于这一简化的树型结构，着重提出了一个由提供商（*Provider*s）和分享者（*Sharer*）两方参与的动态混合博弈（Dynamic and Mixed Game, DMG）及其每阶段博弈的纳什均衡。

然后，在该博弈模型中，考察*Providers*面向一组分享者可选择的三种典型安全策略（Strategy），即完全的一般安全策略、完全的安全增强策略和动态安全战略。考虑到*Sharer*三种不同的分享模式，即局部分享、适度分享和广度分享等，设计一个DMG算法和Swarm仿真实验，实现了两方DMG选取决策。实验结果表明，*Providers*所实施的基于终端设备远程证明的安全增强策略涉及到用户端高安全成本的可信计算设备（组件）的选取和激活，因此在一定Nash均衡条件下，对不同分享者采用动态安全策略是最优的。然而，随着高安全成本的显著降低，以及可转移数字权利的增加，*Providers*选取和部署完全的高安全策略将最终趋于稳定。

最后，基于形式化的RCU定义，在DRM系统中对可信计算支持的安全增强策略进行了评估，并进一步分析了在数字内容侵权发生时，不同分享模式对*Providers*所造成的效用影响。并且，通过仿真实验得出，三种分享模式中的适度分享模式相对于其他两种是绝对占优的。进而，也讨论了一个适用于数字内容分享场景的商业模型。内容/服务提供商可以通过合理选取安全策略并建立该商业模型，来控制数字内容分享中的版权侵犯行为，并在数字内容交易中获得最优的收益。

三、存在的不足与展望

本文研究主要集中在DRM安全策略的效用分析及选取决策，同时也给出了一组典型安全策略与机制，其中包括可信计算支持的数字内容可信分发，以及数字权利转移/委托等安全方案。本文研究还存在以下不足，可以作为今后进一步的工作：

（1）在安全策略的效用分析与选取中，对于安全组件/服务的风险效用分析，目前我们所采用的是定性与定量相结合的方法，其中包括专家对风险因素的定性评估与基于模糊三角数的评估数据分析，并采用泊松概率分布描述DRM安全风险事件的发

生。这些定性分析方法与随机事件的表征能够简单、快速地评估安全策略的效用及其优劣，实现内容提供商的选取决策。对于定量的风险评估，目前的研究还有待于深入。为此，我们将采用蒙特卡洛（Monte Carlo）模拟和贝叶斯网络分析方法，研究一种更为有效的量化方法，准确地分析安全策略的RCU。这样将有助于内容提供商进行深层次的安全成本—效用分析，从而完成最终的安全策略选取决策。此外，在计算效用影响因子的权重时，我们将结合粗糙集（Fuzzy Set）理论，进一步寻找有效的模糊层次分析方法，实现多因子权重的分析和计算。

（2）数字内容分享场景涉及分享者构成的一个社会网络，对于内容/服务提供商，安全策略的选取也较为复杂。本文提出了一个内容分享树型结构，简化了社会网络中用户间的分享过程，并给出了一个*Providers*和*Sharer*之间的动态合作博弈。然而，对于一个更为一般的内容分享情形，该网络应描述为一个有向图。进一步的工作，我们将基于着色Petri网（Colored Petri Network）研究用户间的内容分享过程对安全策略选取所造成的影响，并提出有效的安全策略来控制该场景下的安全风险和数字侵权行为。

（3）在DRM安全机制上，本文提出了可信计算支持的DRM安全增强方案，主要用于数字内容以及可转移许可的可信分发与执行，并未涉及DRM系统中内容加密密钥和设备密钥的安全存储与I/O等。进一步，我们将结合可信计算终端设备，探讨这些问题，进一步抵抗恶意用户及盗版者对数字内容的篡改、非授权使用和非法复制等。此外，对于本文所提出的基于Xen虚拟技术的可信计算平台这一概念模型，结合工业界在可信计算领域的进展，研究并实现一个原型系统也将作为今后的工作之一。

（4）本文所提出的DRM安全策略选取分析方法以及安全增强机制都是面向一般意义上的DRM应用，并未针对一个具体的应用系统或网络环境，如移动DRM（Mobile DRM）、多媒体内容安全、Peer-to-Peer DRM等，研究数字内容的保护和使用控制。针对这些典型的DRM应用及具体的数字内容格式，提出相应的解决方案，并依据我们所提出的DRM安全效用形式化分析框架，解决实际应用中的策略选取和部署问题，将具有更广阔的应用价值。

关键词 数字版权管理；安全策略；效用分析；博弈论；安全风险管理