

数字版权管理的互操作技术研究*)

刘思伟 慕德俊

(西北工业大学自动化学院 西安 710072)

摘要 本文阐述了数字版权管理的概念、模型及现有的数字版权管理系统,着重论述了数字版权管理的互操作问题,特别是互操作的概念、本质、特性以及实现互操作的方法,之后阐述了数字版权管理所出现的问题、原因和实际需求,重点阐述了数字版权管理互操作现有的解决方法。最后指出了安全问题和分层数字版权管理互操作是作为未来工作需要深入展开的。

关键词 数字版权管理, 互操作, 关键技术, 标准

Research on Digital Rights Management Interoperability

LIU Si-wei MU De-jun

(School of Automation, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract Digital Right Management (DRM) concept, model and current DRM system were described. DRM interoperability problem was described in more detail, esp. interoperability concept, essence, character and the method to implement the interoperability. Then the problems, reason and requirement in DRM were addressed, and the current DRM interoperability solutions were presented. Finally the security and layered DRM interoperability were concluded as the future work.

Keywords Digital rights management, Interoperability, Key issues, Standards

1 引言

当今,Internet 拥有越来越多的数字媒体,然而数字媒体的无差别复制和分发使得内容提供商越来越强烈地要求保护其数字内容,因而数字版权管理(DRM)技术得到越来越多的关注。

数字版权管理的主要目的是保护数字财产的使用权利,防止非法使用和复制等操作。它不仅仅是数字版权的保护,同时提供了数字媒体内容的传输、管理和发行等一套完整的解决方案。

本文主要阐述数字版权技术,之后论述了数字版权系统之间互操作的算法,并论述了现有开发数字版权互操作技术的组织及其实现原理。

2 数字版权管理系统

2.1 数字版权管理的概念

首先要明确数字版权管理的概念^[1],其定义如下:

数字版权管理是对数字化智力财产的控制和管理;

数字版权管理是有形和无形资产的各种形式权利使用的表述、识别、交易、保护、监控和跟踪;

数字版权管理一定是权利的数字化管理,而不是数字权利的管理。

数字版权管理是一种限定、解析、增强和管理数字权利的统一表示方法。

这里要注意几个概念:

数字财产(Digital Assets):是指数字领域的任何资源、内

容和服务。

数字权利(Digital Rights):数字财产的创建、分发、使用和管理者优先权。

许可证(Licenses):承载数字权利信息的数字表述或数字对象。

数字版权保护的不仅仅是防止数字财产的非法访问和共享,更重要的是允许以更便捷的方式授权访问和享受更高质量的数字财产,同时为数字财产的创建、分发和消费创造更多的市场和业务。

2.2 数字版权管理模型

数字版权管理涉及到至少四个方面的利益,即内容制作方、内容分发商、权利分发商和用户,其关系如图1。

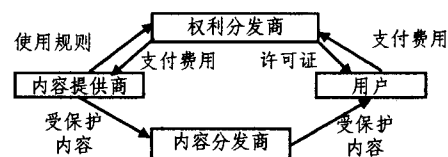


图1 数字版权管理模型

其原理如下:

内容提供商将作者制作的媒体以及对该媒体进行访问的策略通过加密或者水印、数字指纹等技术进行打包,分发给内容分发商,再由实际用户购买。同时,内容提供商将各种媒体各自不同级别的许可证分发给权利分发商(权利代理中心),由权利分发商代理权利销售。

实际用户购买该数字媒体,同时要向权利分发商购买该数字媒体的使用权限(许可证)。

*)航空科学基金项目(基金项目编号:05F53029)、西北工业大学创业种子基金(Z200633)。刘思伟 博士生,主要研究领域为信息安全;慕德俊 博士,教授,主要研究领域为信息安全、并行计算、现代控制理论。

2.3 现有数字版权管理系统问题

针对用户、内容提供商、内容分发商、权利分发商以及作者等各个方面的需求,不同厂商开发了不同的数字版权管理系统。

电子书的数字版权保护系统:Microsoft 公司的 Digital Asset Server, Adobe 公司的用于 PDF 格式的 Adobe Content Server(ACS)电子书的版权保护方案等。

流媒体的数字版权保护主要有 Apple 公司的 FairPlay 系统, Real Network 的 Helix, Yahoo 的 MusicMatch, IBM 的 EMMS 和 Microsoft Windows Media DRM。

电子文档的数字版权保护系统:有微软的 Rights Management Services 系统, SealedMedia 公司的 SealedMedia Enterprise License Server, Authentica 公司的 Active Rights Management, 以及中国的北京书生公司的 SEP 系统, 方正集团的 CEB 系统等。

图像的数字版权保护系统:有美国 Digimarc 公司的数字水印技术和北京华旗数码影像技术研究院的信息隐藏保护与加密系统等。

移动媒体的数字版权保护系统:由于移动设备和移动网络的特点,移动 DRM 的实施较一般 DRM 容易一些。目前,OMA 制定的移动 DRM 标准得到了广泛的支持和认同。

但是,现有的各种数字版权保护系统是互不兼容的独立系统,各自实现标准也不一样,权利表述也不统一,保护技术也具有交互性,造成用户使用过分复杂,且要购买不同的使用许可。为此,数字版权管理的互操作性研究成为当今研究的一个热点。

数字版权管理的互操作意义在于:

实现任何时间、任何地点都能消费带有授权的内容;
降低对单一技术的依赖性;
希望消费电子、移动通讯和 PC 平台能够进一步融合;
未来证实用的商业运作模式;
同时也允许非法的对等内容分发等功能。
下面各节对互操作进行集中阐述。

3 互操作

互操作成了一个热门词汇,如端到端的互操作、内容的互操作、设备的互操作、权利(语言)互操作等等,因此首先要掌握互操作^[2]的一些知识。

3.1 互操作的定义

互操作是:

一个系统使用其他系统的一部分或设备的能力,是一项技术与另外一项技术进行交互以实现一些功能的能力。

计算机硬件或软件系统,在与其他系统(通常是其他提供商设计生长的不同类型的系统)进行交换数据时,有效通讯和工作的能力。

系统或产品一起自动工作的能力。

两个或更多的技术系统能直接交换数据所要满足的条件,才能满足系统的用户。

3.2 互操作的本质

互操作是关于来自不同提供商的不同实体(系统、应用、模块)能互相操作或者共同工作的能力。因此,

对于单个实体,不牵涉到其他实体,是没有意义的。如说一个实体是互操作的(或具有互操作性),必须具备一些其他什么是互操作的上下文。

并不适用于来自单一提供商的一个系统,或其所有组件。

如果两个实体不需要共同工作,就不存在这种互操作问

题。

对于被动对象是没有意义的,如“一门语言是互操作的”。

3.3 互操作的特性

互操作的特性如下:

对称性

如果 $A \Leftrightarrow B$, 则当且仅当 $B \Leftrightarrow A$; 注意这二者的角色是不一样的(客户和服务端)。

不可传递性

如果 $A \Leftrightarrow B$, 且 $B \Leftrightarrow C$, 不能得出 $A \Leftrightarrow C$, 因为 A 与 C 使用不同的通信协议, B 都能与之通信。

组合性

如果 $A \Leftrightarrow B$ 且 $B \Leftrightarrow C$, 那么有可能在 B 的支持下, 使得 $A \Leftrightarrow C$ 成立。B 在这里兼容了两种协议, 起到翻译作用。

3.4 互操作与其他概念的区分

(1) 互操作与“可交换”的区分

“可交换”, 即用一个实体替换另外一个实体。交换部分不需要共同工作, 因此也就没有互操作问题。互操作的问题仅仅存在于可以互操作的各个部分。互操作必须存在于上下文中。

互操作问题发展至今, 难以解决的根本原因在于: 用户拥有太多的消费对象, 如包含各种权利、使用信息、身份、密钥、证书的数据; 各种硬件、各种软件等等。另外, 就是 DRM 系统要解决很多问题, 如权利的表述、保护措施(加密、签名、数字水印)、密钥管理、信任管理、身份验证等等。

互连系统的互操作, 如使用手机、游戏平台、PDAs, PCs, 基于 Web 的内容服务、发现服务、通知服务和更新服务等。

(2) 互操作与兼容性的区分

兼容性的特点:

对称性

如果 $A \rightarrow B$, 并不意味着 $B \rightarrow A$ 。这点与互操作性的对称特点是不同的。

不可传递性

如果 $A \rightarrow B$ 并且 $B \rightarrow C$, 则有 $A \rightarrow C$ 。

组合性

如果通过 X 有 $A \rightarrow B$, 且通过 Y 有 $B \rightarrow C$, 则有通过 X 和 Y 有 $A \rightarrow C$ 。

互操作与兼容性之间的关系:

兼容性意味着互操作, 如果互操作, 也就不需要适应性改变。反之则不成立。

不兼容, 也就意味着不能互操作。

互操作可以通过兼容性来实现。

3.5 实现互操作的方法

基本原则: 当系统或者产品遵循标准的时候, 互操作才有可能。标准可以是业界领先的, 也可以是事实上的标准, 但需要开放的标准, 即通过开放的标准来实现互操作。

如果建立一个新的标准, 则要建立标准的数据格式、标准的接口、标准的协议。如果是基于现有的非互操作的标准, 则要共享标准的可交换的数据格式, 引入标准的接口, 连接标准的中间协议。

不同系统之间, 通过服务或者中间接口实现互操作, 也一定要遵从标准。

(1) 数据匹配, 即将数据由 A 发送给 B, 再将数据发送给 C, 这主要借助权利描述语言进行;

(2) 接口的匹配, 开发各个 DRM 系统之间的互操作接口, 这要涉及不同 DRM 系统接口的调用;

(3) 协议解析, 即数据在不同 DRM 之间, 通过协议保证

数据和权利的转发;

(4) 另外,就是组合上述三种算法来实现。

4 数字版权管理互操作问题

4.1 数字版权管理互操作问题

用户不能在不同的 DRM 系统上使用其购买的内容(如歌曲等),如

(1) 在内容上:一个 DRM 系统创建的内容不能在另外一个系统上使用、分发和保护;

(2) 在权利上:一个 DRM 系统授予的权利,不能在另外一个系统上被接受和强化;

(3) 在保护策略上:一个 DRM 系统所制定的保护策略,不能在另外一个系统上遵守和处理;

(4) 在信任模型上:一个 DRM 系统所建立的信任策略,不能在另外一个系统上得到维护;

(5) 在业务模型上:一个 DRM 系统所建立的业务模型,不能在另外一个系统上得到采纳和执行。

4.2 数字版权管理系统缺乏互操作的原因

每个 DRM 的系统都支持各自不同的文件格式、编码/解码和特定的内容保护方法。最重要的是缺少开放的、通用的标准,如:

内容的打包和防护方法,不同的 DRM 系统有各自不同的打包格式和防护算法;

权利的限定和解析格式;

信任的建立和维护,特别是安全问题,许多开发商也不愿意共享其 DRM 代码,这也就阻止了 DRM 的互操作,如代码被黑客复制;

业务模型的表述和执行等问题。

另外,也要考虑到实现 DRM 系统互操作的代价。

4.3 数字版权管理互操作需求

要实现数字版权管理系统的互操作,必须明确实现互操作时各方面的需求,如表 1 所示。

表 1 数字版权管理互操作需求

	需求
用户	1. 获取数字产品同获取当今非数字化产品一样容易,任何 DRM 产品在任何时间都能被使用(消费);
	2. 能够永久地拥有该数字媒体,能移动、借出、甚至赠予他人;
	3. 能永久的消费该数字媒体;
	4. 尽可能便宜,更多的功能,更加便捷;
	5. 互操作应当是透明、容易;
	6. 选择的多样性,灵活而方便。
提供商	1. 内容和权利一次准备并且能够通过多种获益渠道分发,能够通过任何数字版权管理系统进行消费;
	2. 能一劳永逸的满足所有需求;
	3. 一个系统就能符合所有的市场;
	4. 多种商业模式的选择;
	5. 保证各种服务,未来能证明有效的服务;
	6. 用户渴望获取更多的内容;
	7. 内容安全;
	8. 选择的多样性,灵活,价格有效性。
投资商	1. 系统组件能够替换其他投资商的相似组件;
	2. 市场共享,价格有效性。

5 DRM 互操作现有的解决方法

不同数字版权管理系统达到互操作的一个最根本原则是各个系统遵从统一的标准,包括标准统一的数据格式、界面以及协议等等。

考虑到现有数字版权管理系统的多样性,给用户带来诸多不便,研究人员提出了几种解决方案。

(1) 通过相同的数据格式来实现互操作^[2]

这种解决方案要求建立一个统一的数据格式(数据标准),要求所有的公司或组织统一遵从,像 CD 和 DVD 音频就是遵从统一的数据格式。文献[4,5] 寻求在不同的权利表述语言上,实现互操作,这也是追求相同的数据格式。

该方案的优点:这样就很容易对内容进行生产、分发和使用。

该方案缺点:这种解决方案过去苛刻,统一的数据标准格式开发极其漫长。另外,一旦该系统被破解,那么导致所有的系统都被破解,因此又要重新开发相关标准。

(2) 连通的互操作^[3]

这种互操作解决方案是假定用户连接到网络,进行在线交易。对于内容提供商来说,此方案最简单可行。但是,用户每次传输内容都要进行在线连接。这种方案如文献[6]提出的“媒体协调的网络环境”(NEMO)。

该方案优点:使得不同的系统可以选择各自的解决方案,也保证了安全性,同时为终端用户提供了一定类型的数字版权管理的互操作。

该方案缺点:比通过相同数据格式的互操作方案要复杂,需要解决不同 DRM 系统的语义匹配,以保证边界交叉范围内内容移动的顺畅。另外,有些产品并不能满足在线连接的需求,这就要求在设计数字版权互操作时考虑信任关系的建立策略。

(3) 配置驱动的互操作方法^[3]

这种方案假定用户设备能动态配置自身,以容纳新的数据格式和协议。系统的组件能够被用户下载,并在用户终端上可配置。相当于按照用户的需要,逐渐更新用户终端。理想情况下,用户不会感知该操作。例如 MPEG-4 IPMP-X 就是采用的这种方法。

该方案优点:按照用户的需求来提供终端设备的系统能力。这样安装配置好以后,在线访问就不需要或者比较少访问。

该方案缺点:要求可配置和可下载工具的目标平台能够容纳和支持任意数量的不同配置。这对小型家电难以达到这个能力。多个主机工具要处理多种媒体格式,而组件与主机的信任关系还没有很好解决,如在 MPEG-IPMP 中,就没有得到解决。

(4) 采用分层的架构实现互操作

分层的架构思想起源于 Internet 网的 TCP/IP 分层架构,这种思想应用于数字版权管理互操作,以简化数字版权管理的复杂性,仅仅需要考虑每层内部的功能实现以及层与层之间的接口,来解决数字版权管理的互操作问题。分层的数字版权互操作架构在文献[9,10]进行了详细阐述,如图 2 所示。

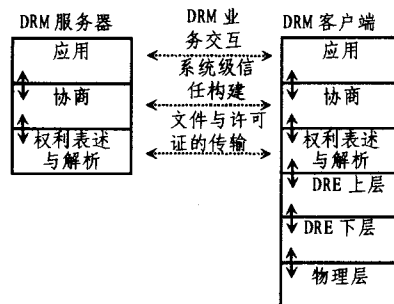


图 2 分层的数字版权管理互操作模型

这里 DRE 是指数字版权管理的增强技术,箭头表述各个

层相互交互通信。

应用层:是关于权利所管理的内容使用方面的应用,为用户提供使用内容时的界面,包括内容选择、个人诚信和资金交易等。

协商层:是建立服务级的信任关系,包括接收许可证的请求、终端设备能力的评估等。协商层的服务级信任关系内容提供商所发送的内容类型或内容的实质。

权利表述与解析层:是最重要的一层,提供所需的数字版权管理服务的最小集,以连接上下层。该层的功能包括许可证的创建、保护的内容、权利受控的内容分发,以及许可证。更具体地讲,权利表述功能负责获取上层的权利信息,以在特定应用中提供版权保护的功能,采用权利表述语言(REL)来实现。权利解析用于解析不同的权利。另外,不同的权利表述语言具有不同的权利集,因此权利解析负责权利的转换、权利的重建、内容和权利的重新打包,像 MPEG-21 权利字典,就是用于不同版权管理的权利表述的转换。

DRE 上层:主要负责权利的管理、内容的访问控制和加密协议,包括高级的权利增强技术,如加密、数字水印和数字证书。

DRE 下层:是关于操作系统级的技术,主要负责低级的权利管理,包括设备驱动认证、防止恶意程序的非法内存访问等。微软的“安全音频路径技术”(SAP)就是一例。

物理层:即用户端设备。

分层的数字版权互操作架构,其突出的优点是在各个层的内部解决该层所要提供的功能,然后考虑各个层的接口功能,以完成较大的数字版权管理功能。

但是,分层的数字版权互操作架构思想目前还需要实际的检验。

(5) 面向服务架构的数字版权互操作系统

文献[10]面向服务架构的数字版权互操作系统的思想,是由五种服务构成服务驱动的架构,包括打包服务、更新服务、订购服务、许可证服务和策略服务。

结束语 数字版权管理系统的互操作问题,要考虑现有的封闭的数字版权管理系统。同时,安全^[11]问题已经成为数

字版权互操作所要特别考虑的问题。不能因为各类数字版权管理系统的互操作,却引发安全问题。因此,这将是数字版权管理互操作的一个新的研究和开发重点。另外,文中提出的几种数字版权管理系统的互操作方案,需要在实际中进一步验证,以不断完善改进。这里分层的数字版权管理互操作系统,具有一定研究前景,开发出实用系统并为用户所认可可是下一步需要推进的。

参考文献

- [1] Ku W, Chi Chi-Hung. Survey on the technological aspects of digital rights management[J]. Lecture Notes in Computer Science, 2004, 3225: 391-403
- [2] Wang Xin. On DRM Interoperability and Compatibility [EB/OL]. <http://www.ieee-cnc.org/2005/conf.html>, 2005
- [3] Koenen R H, Lacy J, MacKay M, et al. The Long March to Interoperable Digital Rights Management [J] // Proceedings of the IEEE, 2004, 92(6): 883-897
- [4] Polo J, Prados J, Delgado J. Interoperability Between ODRL and MPEG-21 REL [EB/OL] // Proceeding of ODRL International Workshop. 2004. <http://odrl.net/workshop2004/program.html> (2007-01-28)
- [5] Prados J, Rodriguez E, Delgado J. Interoperability Between Different Rights Expression Languages and Protection Mechanisms [C] // Proceedings of the First International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS'05) on Automated Production of Cross Media Content for Multi-Channel Distribution. 2005: 145-152
- [6] Bradley B W, Maher D P. The NEMO P2P Service Orchestration Framework [C] // Proceedings of the 37th HICSS - Hawaii International Conference on System Sciences. 2004:4641-4650
- [7] Heileman G L, Jamknedkar P A. DRM interoperability analysis from the perspective of a layered framework [C] // Proceedings of the 5th ACM workshop on Digital rights management table of contents. 2005:17-26
- [9] Jamknedkar A, Heileman L. DRM as a layered system [C] // Proceedings of the 4th ACM workshop on Digital rights management. 2004:11-21
- [10] Filho F M F, de Albuquerque J P, de Geus P L. A Service-oriented Framework to Promote Interoperability Among DRM Systems[J]. Lecture Notes in Computer Science, 2006(4267): 124-127
- [11] Taban G, Cardenas A A, Gligor V D. Towards a Secure and Interoperable DRM Architecture [C] // Proceedings of the ACM workshop on Digital rights management, 2006:69 - 78

(上接第 212 页)

由于存在一些这样的集合 $S_{10} \supset S_{20}$ 和 $S_{20} \supset S_{10}$, 因此可以得出 $S_{10} \cup S_{20} \subseteq S_{11}$ 和 $S_{10} \cup S_{20} \subseteq S_{21}$ 。假设存在 $X \subseteq S_{11} \setminus (S_{10} \cup S_{20})$ 或 $Y \subseteq S_{21} \setminus (S_{10} \cup S_{20})$, 协商将进入下一轮, 则 $n > 1$, 与 $n=1$ 矛盾。可以推导出 $S_{10} \cup S_{20} = S_{11} = S_{21}$ 。

情形 2: 存在这样的集合 $(S_{10} \setminus G_{10}) \supset R_{20}$ 和 $(S_{20} \setminus G_{20}) \supset R_{10}$, 其中 $(S_{10} \setminus G_{10}) \in \text{ANS}(S\text{Reduce}(\Pi_{10}, G_{10}))$, $(S_{20} \setminus G_{20}) \in \text{ANS}(S\text{Reduce}(\Pi_{20}, G_{20}))$ 。

由于存在如上所述的这些集合, 由此可以得出 $(S_{10} \setminus G_{10}) \cup R_{20} \subseteq S_{11}$ 并且 $(S_{20} \setminus G_{20}) \cup R_{10} \subseteq S_{21}$ 。由情形 1 可知, $(S_{10} \setminus G_{10}) \cup R_{20} = S_{11} = S_{21}$ 。类似情形 1, 也不存在任何集合 $X \subseteq (S_{10} \setminus S_{20}) \setminus (R_{10} \cup G_{10})$ 或者 $Y \subseteq (S_{20} \setminus S_{10}) \setminus (R_{20} \cup G_{20})$, 否则协商将进入下一轮使得 $n > 1$ 与 $n=1$ 矛盾。所以可以得出 $R_{10} \cup G_{10} = S_{10} \setminus S_{20}$ 和 $R_{20} \cup G_{20} = S_{20} \setminus S_{10}$ 。

情形 3: 不存在任何关于 (Π_{10}, Π_{20}) 的接受放弃函数 γ 使得有这样的集合 $(S_{10} \setminus G_{10}) \supset R_{20}$ 和 $(S_{20} \setminus G_{20}) \supset R_{10}$ 。根据定义 7, 有 $S_{11} = S_{10}$ 和 $S_{21} = S_{20}$ 。

如果 $n > 1$, 证明过程类似 $n=1$ 的情形。

结束语 本文把一个 ELP 看作是一个协商 AGENT, 提出了一个关于两个 ELP 之间重复协商的形式化框架。作为

下一步的工作, 我们将引入带有优先关系文字的 ELP, 对协商策略进行研究, 从而进一步完善此框架。

参考文献

- [1] Foo N, Meyer T, Zhang Y, et al. Negotiating logic programs // Proceedings of NAC05, Sixth Workshop on Nonmonotonic Reasoning, Action and Change. Edinburgh, 2005
- [2] Foo N, Meyer T, Brewka G. LPOD Answer Sets and Nash Equilibria. Lecture Notes in Computer Science, Springer-Verlag, 2004, 3321:343-351
- [3] Gardenfors P. Knowledge in Flux; Modelling the Dynamics of Epistemic States. MIT Press, 1988
- [4] Gelfond, Lifschitz V. Classical negation in logic programs and disjunctive databases. New Generation Computing, 1991: 365-385
- [5] Lifschitz V. Foundations of logic programming, in Principles of Knowledge Representation. CSLI Publications, 1996: 69-127
- [6] Littman M L, Stone P. Implicit Negotiation in Repeated Games // Proceedings of The Eighth International Workshop on Agent Theories, Architectures, and Languages, August 2001: 393-404
- [7] Lloyd J W. Foundation of logic programming. 2nd ed. New York: Springer-Verlag, 1987
- [8] Sabourian H, Lee J. Complexity and Efficiency in Repeated Games with Negotiation // Econometric Society 2004 North American Summer Meetings. 2004:58
- [9] Zhang D, Foo N, Meyer T, et al. Negotiation as Mutual Belief Revision // Proceedings of AAAI04, Nineteenth National Conference on Artificial Intelligence, AAAI Press, The MIT Press, 2004:317-322
- [10] Zhang Y, Foo N. Solving Logic Program Conflict through Strong and Weak Forgettings. Artificial Intelligence, 2006, 170: 739-778