互融DRM：数字版权管理的新进展

张志勇

（河南科技大学信息工程学院　河南　471023）

【关键词】传统数字版权管理（Digital Rights Management, DRM）技术所涉及的安全、可信、可控理论与方法，已无法满足新兴的云媒体社交网络下媒体内容安全与版权保护这一实际应用需要。深入分析了云媒体社交网络及其层次化体系结构，综述了DRM系统跨平台使用、内容共享和消费电子设备互动等关键技术，最后针对新兴的云媒体社交网络场景及应用，提出了数字版权管理的新概念——互融DRM，并指出了亟待解决的开放问题和挑战。

【关键词】云媒体社交网络；互融数字版权管理系统；安全；互操作

中图分类号：TP309　　文献标识码：A　　文章编号：1009-6833（2013）10-096-02

Syncretic DRM: Advance on Digital Rights Management

Zhang Zhiyong

Abstract: Nowadays, the theories and methods for security, trustworthiness, controllability of traditional digital media rights management systems available do not meet the requirements of the novel Internet application. The paper in-depth analyses on cloud media social network and its hierarchy architecture, and also made a survey on cross-platform usage, contents sharing and consumer electronics interaction in DRM system, finally presenting a novel concept of digital rights management, Syncretic DRM, and its burning open issues and challenges.

Keywords: Cloud Media Social Network; Syncretic DRM; Security; Interoperability

0　前言

随着通信网络技术与信息技术的飞速发展，全球下一代高速宽带网络以及3G、4G等无线移动通信网络正逐渐从研究试验阶段向大范围部属和应用阶段迈进，其中各种接入方式也使得用户更加便利地使用网络资源，即可以在任何时间、任何地点得到所需数字信息和服务。近年来，中国互联网及应用也得到了长足发展。2013年1月15日，中国互联网络信息中心（CNNIC）发布第31次《中国互联网络发展状况统计报告》显示，截至2012年12月底，互联网用户规模达到5.64亿，互联网普及率为42.1%。其中，通过移动手机终端上网用户接近4.2亿，其规模占互联网用户的74.5%。移动终端成为互联网应用的主要电子设备和载体。

在如此发展态势下，由于数字内容（包括电子书、数字图像、多媒体音视频等）具有无损复制、易于分发等重要特征，出现了随意批量复制受知识产权法律保护的有价数字内容产品，并将其通过各类通信网络载体进行非授权分发、传播和滥用的侵权行为和现象，给整个经济社会和文化发展，造成严重的不良后果和损失。数字版权管理（Digital Rights Management，以下简称DRM）技术是保障数字内容产业良性、健康发展的关键技术和重要手段，也是多学科交叉研究领域，涉及到信息安全技术、数字版权法律、商业模型，等等。自上世纪90年代中期以来，DRM研究及应用场景主要经历了离线使用、互联网在线、内容分发网络、P2P网络等阶段[1, 2]。

近年来，又涌现出了融合服务器主机计算和客户端计算两种模式的多媒体云计算及应用（Multimedia Cloud Computing）[3, 4]，以及诸如Facebook、Twitter、微博等社会媒体网络（Social Media Networks）服务。据国内权威的信息技术咨询研究机构iResearch发布的数据显示，截至2011年12月，全球有超过12亿的用户每月至少一次使用社交网络网站，2014年预计全球社交网络用户数量将保持两位数增长，社交化元素已成为全球互联网中的基础性应用。社会媒体分享成为社交网络发展的主要驱动力。

然而，传统数字版权管理技术所涉及的安全、可信、可控理论与方法，已无法满足新兴的云媒体社交网络下媒体内容安全与版权保护这一实际应用需要，例如，云媒体安全访问控制、媒体终端可信接入，以及随着媒体社交网络用户数量的急剧增多和大数据的产生，如何发现和控制大量隐式（隐含、潜在可能的）数字媒体权利恶意传播和滥用等。因此，针对新兴互联网应用场景，开展DRM应用基础理论和关键技术研究，显得更为紧迫和亟需。

1　云媒体社交网络及其分层结构

云媒体社交网络（Cloud Media Social Networks，以下简称CMSN）以多媒体云计算为架构组织，是一种主要用于发布、分享和传播数字媒体内容的社交网络平台，如YouTube、SongTaste、土豆网、优酷等。这一新兴互联网应用的基本特性是融合了基于云媒体服务器的集中（在线）式访问和云媒体终端分布（离线）式访问两类模式，为数字媒体用户提供更加便捷、高效、高品质的多媒体服务，用户从中获得了更为丰富的数字内容体验。同时，媒体社交网络具有小世界网络本质特征，易于传播。大量受版权保护的媒体内容及其数字权利，在访问、使用、分享和广泛传播过程中，侵犯版权行为日趋严重，给数字（媒体）内容产业带来了前所未有的负面影响，使得DRM问题更加凸现出来[5, 6]。

在数字内容从创作、生成到发布、使用和分享的全生命周期内，其数字版权保护实现主要基于媒体内容加密和媒体数字权利（使用加密媒体内容的权限和许可）在媒体服务器、通信网络中间件、（移动）客户端等多层次部署和实施，从而构成一个系统完整的数字版权管理生态系统（DRM Ecosystem）。新兴云媒体社交网络场景下，从实体角度，主要涵盖云媒体平台提供方CMSNP（CMSN Provider）、云媒体内容提供方CMCP（Cloud Media Contents Provider）、互联网服务提供商（ISP）、云媒体授权用户CMAC（Cloud Media Authorized Consumer）和云媒体社交网络监管者CMSNM（CMSN Monitor）；从分层角度，主要包括云媒体内容服务层、媒体终端网络接入层和媒体用户社交网络层。如图1所示。

2　DRM系统跨平台使用和共享技术

Keoh SL[7]提出，数字版权管理是用来保护未经授权使用受版权保护的数字内容。如何保持内容共享和权限管理之间的

平衡仍然具有挑战性。此外，DRM系统通常工作在封闭的单一系统中，保护数字内容免受未受权的访问和控制用户消费的方式，经常忽略了互操作性。因此，用户不能在其他DRM兼容设备中消费DRM系统保护的内容。Marlin开发了可互操作的DRM技术开发标准。Marlin的Octopus和NEMO框架是实现无缝的内容共享和权限管理的底层技术，支持多种商业模式。我们演示了依靠Marlin宽带网络服务（MBNS）和Marlin分享域（MSD）这种方式使用Octopus和NEMO。Marlin简单安全流（MS3）被设计以一种简单而有效的方式保护流式内容。文献[8]提出了一个基于配置文件的DRM系统框架，以支持与异构设备的互操作性。提出的框架允许需要尽可能少地改动现有DRM系统时，多个DRM系统无缝地一起工作。

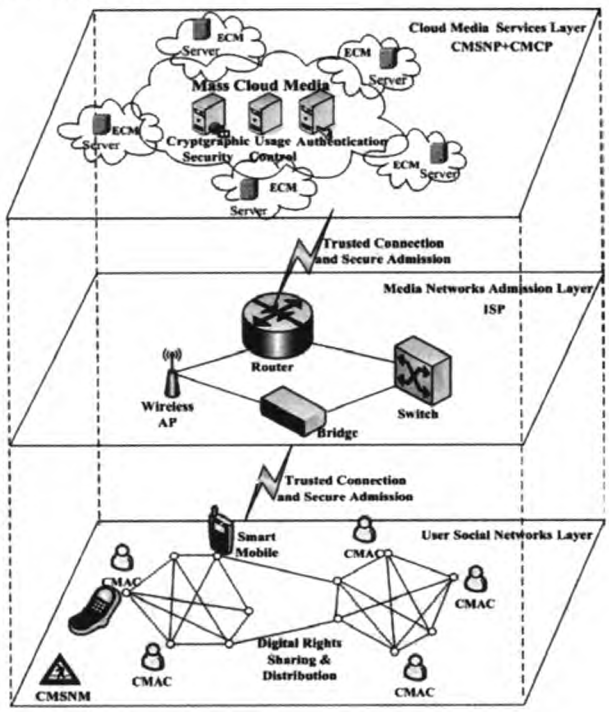

图1 层次化的云媒体社交网络体系构架

数字内容产业正面临着重大的挑战。最重要的挑战之一是知识产权的保护。这一挑战已经得到解决，使用数字版权保护（DRM）系统在第一阶段确保了对数字内容的适当管理。然而，DRM系统若不具备互操作性，将给数字内容终端用户带来了巨大的使用问题。其中之一就是相同的数字内容被不同的、不能相互交换的DRM系统管理。Serrão C[9]给出了VISNET-II卓越网络框架，从而解决DRM系统的互操作问题。此方法作为一种创建一个不同系统之间的互操作环境和方式，包含在服务描述和面向服务的架构的使用中。

Rodriguez DV[10]提出了一个互操作的数字版权管理架构，此架构由MPEG标准组在其新标准MPEG-M或者MPEG可扩展的中间件（MXM）推进。此标准旨在促进MPEG技术的打包和可重用性，并为它制订了一个软件中间件平台和一套完整的API和协议。这些API允许均匀通过一组标准协议进行模块通信，以处理数字内容和开发通用多媒体应用。MXM标准提供了必要的机制来保护数字化知识产权权利，用必要的工具来保护数字媒体，用必要的方式来完成授权权利的执行。

此外，在家庭自动化和数字化时代，随着移动互联网介入的扩散，智能家居及其设备应该可以在任何时间、任何地点访问。现存很多挑战如安全性、隐私性、易于配置、不兼容现有设备、丰富的无线标准和嵌入式系统的有限资源等等。考虑到这些挑战，文献[11]提出了一个可信域家庭自动化平台，通过简单的非专业用户交互及允许通过基于IP的设备如智能手机的远程访问，使得短距离无线设备动态安全地连接异构网络。可信域平台适合现有传统技术，通过管理其互操作性和访问控制，并且它依靠家庭之外的第三方服务器来避免安全问题。

鉴于DRM系统的上述特性，我们提出了“互融DRM”概念。它是一个包含三个重要特性的生态系统，即用户—设备间的互动性（Interactivity）、消费电子设备间的互操作性（Interoperability）和终端用户间的互换性（Interchangeability）。如图2所示。

图2 互融DRM系统

在该系统下，主要解决以下三个问题：

（1）面向云媒体内容的安全访问和互动性，通过研究基于密码方法的云媒体访问控制模型和方法，以及DRM控制器与移动多媒体终端应用相分离的远程执行机制，实现媒体内容（权利）跨域、跨群组、跨平台的授权使用和可控分享，并有效抵抗媒体用户的客户端恶意离线攻击，满足数字媒体内容访问控制安全。

（2）面向固定/移动媒体终端的接入和互操作性，通过研究适合移动终端（用户）的可信接入双向认证安全协议，达到UC可证明安全，实现合法授权的移动终端安全接入和快速切换，以及不同平台下的媒体内容及其数字权利互操作和兼容，进一步提高上层云媒体内容访问和分享过程中的安全性。

（3）面向数字媒体权利的共享和互换性，通过研究基于粗糙集软计算理论的媒体权利潜在传播路径发现及其安全风险评估方法，及时发现媒体权利的恶意传播与侵权行为，从而制定更具针对性的访问控制安全策略。

3 结束语

基于云媒体社交网络及其层次化体系结构的分析，综述了DRM系统跨平台使用、内容共享和消费电子设备互动等关键技术。面向新兴的云媒体社交网络场景及其应用，本文提出了数字版权管理的新方向——互融DRM生态系统，并依据云媒体社交网络的层次化特性，指出了三个亟待解决的开放问题和挑战。

参考文献：

[1]Zhang ZY. “Digital Rights Management Ecosystem and its Usage Controls: A Survey,” International Journal of Digital Content Technology & Its Applications, 2011, 5(3):255-272.

[2]Zhang ZY. Security, Trust and Risk in Digital Rights Management Ecosystem. 北京: 科学出版社, 2012.

[3]Zhu WW, Luo C, Wang JF, Li S P. “Multimedia cloud computing,” IEEE Signal Processing Magazine, 2011, 28(3): 59-69.

[4]Gadea C, Solomon B, Ionescu B, et al. “A collaborative cloud-based multimedia sharing platform for social networking environments,” In: Proc. of International Conference on Computer Communications and Networks, Maui, HI, USA, Aug, 2011.

[5]Diaz-Sanchez D, Almenarez F, Marin A, Proserpio D, Cabarcos P A. “Media cloud: An open cloud computing （下转100页）

对于网络发现机制，是指感染主机如何找到控制服务器或者通过其他的感染主机加入到僵尸网络中。对于防御方来说，如果能够找到并切断感染主机和控制服务器之间的联系，就能从根本上关停整个僵尸网络。集中式僵尸网络多采用简单的固定IP或者域名的方式来发现控制服务器；P2P 僵尸网络多借助于P2P协议的动态发现机制；而近年来的攻击者开始采用多个域名或IP并结合更新机制来提高僵尸网络的抗关停能力。

3 检测和防御技术

3.1 蜜罐检测

大规模网页挂马检测的基本思路是，使用爬虫爬取网站页面，然后将爬取到的URL输入到客户端蜜罐中进行网页木马检测。客户端蜜罐(client honeypot)是由国际蜜网项目组(The Honeynet Project)针对网页木马这种被动式的客户端攻击提出的。在网页挂马的检测中，客户端蜜罐根据URL主动地向网站服务器发送页面访问请求，并通过一定的检测方法分析服务器返回的页面是否带有恶意内容。该技术在后续发展中逐步演化为对僵尸网络进行监测的最为有效的技术。

客户端蜜罐分为高交互式和低交互式两种。高交互式客户端蜜罐采用一个带有漏洞的浏览器与网站服务器交互，并采用基于行为特征判定的方法进行网页木马检测；而低交互式客户端蜜罐则轻量级地模拟出一个浏览器，页面获取模块模拟浏览器向服务器发出页面访问请求，页面检测模块采用基于反病毒引擎扫描、统计或机器学习等方法对获取的页面进行检测。

对于目前的僵尸网络的检测而言，使用蜜罐技术，采用的数据源主要是网络流量以及应用程序的数据（典型的如邮件记录以及DNS的日志记录），而对异常模式的定义主要有传统的基于内容特征的异常和基于特定行为异常。

基于内容特征的检测，是入侵检测系统的常规检测方法，该方法适用于已知的、具有明确特征的僵尸网络，具有准确、快速、易于部署的特点，是目前实际应用最为广泛的检测方法。但其容易被变形、多态等技术所逃避，对未知的僵尸程序或网络不具备检测能力，并且特征串的提取依赖于人工分析，对目前急剧增长的僵尸程序数量可谓束手无策。

基于网络流量行为特征的检测技术需要对骨干网的流量进行采集，得到流量分布图，然后通过随机游走的方法从图中检测出结构化P2P网络的子图，再结合蜜罐来判断是否为僵尸网络。

3.2 主动防范网页木马

网站服务器端的挂马防范是网页木马防范中的首要环节。网页挂马有多种途径，如利用网站服务器的系统漏洞、内容注入等应用层程序漏洞、广告位和流量统计等第三方加载内容挂马。除了关注系统及应用上的安全漏洞外，也有必要对页面中的第三方内容进行充分的安全审计。如基于代理的网页木马防范、基于脚本重写的网页木马防范、基于浏览器不安全功能隔离的网页木马防范等。

还可直接在客户端进行网页木马的防范，如URL黑名单过滤、浏览器安全加固、操作系统安全扩展等。利用URL黑名单过滤，将基于页面静态特征进行机器学习的检测方法与基于行为特征的检测方法相结合，对其索引库中的页面进行检测来生成一个被挂马网页的URL黑名单，从而封堵访问的入口。也可对浏览器进行安全加固，修补所有已知的漏洞；或者对操作系统进行安全扩展。

4 结语

网页木马作为恶意程序传播的一种重要方式，能够在客户端访问页面的过程中高效、隐蔽地将恶意程序植入客户端，基于Web的被动式攻击模式使网页木马能十分隐蔽并有效地感染大量客户端。基于网页挂马为主要传播方式的覆盖网络——僵尸网络危害更大，具有更为专业化的攻击方式以及具备更强的自身安全性的命令与控制机制，已成为互联网多种类型安全威胁的主要源头。本文分析了网页木马和僵尸网络的主要机理和相关检测与防御技术，旨在帮助总结当前互联网安全面临的主要威胁和提供一些积极应对的安防思路。

参考文献：

[1]张慧琳,邹维,韩心慧.网页木马机理与防御技术.软件学报,2013,24(4):843-858.

[2]Provos N, Mavrommatis P, Rajab MA, Monrose F. All your iFRAMEs point to us. In: Proc. of the 17th USENIX Security Symp. Berkele: USENIX Association, 2008. 1-15.

[3]吕磊,基于行为分析的网页木马检测技术研究,哈尔滨工业大学学报,2009.

[4]江健,诸葛建伟,段海新,吴建平,僵尸网络机理与防御技术,软件学报,2012 23(1):82-96.

[5]Rajab MA, Zarfoss J, Monrose F, Terzis A. A multifaceted approach to understanding the botnet phenomenon. In: Proc. of the 6th ACM SIGCOMM Conf. on Internet Measurement. Rio de Janeriro: ACM Press, 2006. 41-52.

[6]孙彦东,僵尸网络综述,计算机应用,2006.

[7]宋富强,蒋外文,刘涛，蜜罐技术在入侵检测系统中的应用研究,现代计算机：下半月版,2008年第3期.

作者简介：

季元叶（1976-），女，江苏苏州，硕士，讲师，主要研究方向：网络信息安全。

（接上97页）middleware for content management," IEEE Transactions on Consumer Electronics, 2011, 57(2): 970-978.

[6] Huang T, Zhang Z Y, Chen Q L, et al. "A Method for Trusted Usage Control over Digital Contents Based on Cloud Computing," International Journal of Digital Content Technology & Its Applications, 2013, 7(4): 795-802.

[7] Keoh SL. Marlin: Toward seamless content sharing and rights management[J]. IEEE Communications Magazine,2011,49(11): 174-180.

[8] Yuan JQ, Zhao F, Zhang WJ, etal. A profile-based interoperable DRM system framework[J]. International Journal of Digital Content Technology and its Applications, 2012,6(4): 268-276.

[9] Serrão C, Rodriguez E, Delgade J. Approaching the rights management interoperability problem using intelligent brokerage mechanisms[J]. Computer Communications, 2011,34(2): 129-139.

[10] Rodriguez DV, Delgado J, Chiariglione F, etal. Interoperable digital rights management based on the MPEG Extensible Middleware[J]. Multimedia Tools and Applications,2011,53(1): 303-318.

[11] Hjorth TS, Torbensen R. Trusted Domain: A security platform for home automation[J]. Computers and Security, 2012,31(8): 940-955.

作者简介：

张志勇(1975-)，男，博士（后），教授，ACM/IEEE高级会员。研究领域：多媒体云计算、数字版权管理、安全风险管理与软计算等。担任国际期刊"International Journal of Digital Content Technology and Its Applications" DRM专题主编，"The Computer Journal"，"Journal of Multimedia" 和"Soft Computing with Applications"（客座）编辑。

基金资助：国家自然科学基金（No.61370220, 61003234），河南省杰出青年基金（No.134100510006），河南省教育厅科学技术研究重点项目基础研究计划（No.13A520240）。

互融DRM:数字版权管理的新进展

作者： 张志勇， Zhang Zhiyong
作者单位： 河南科技大学信息工程学院 河南 471023
刊名： 网络安全技术与应用
英文刊名： Network Security Technology & Application
年，卷(期)： 2013(10)