

家庭网络与数字版权管理技术

Home Networks and Digital Rights Management

摘要: 家庭网络是社会数字化、信息化发展的关注焦点,但如何保障家庭网络中数字内容安全,保证价值链中各环节的合法利益,成为制约其发展的重要“瓶颈”。数字版权管理技术从数字内容及其权限的使用、存储、交换、追踪等方面给出了全面的解决方案。数字版权管理具有系统性、可控性等基本特征,家庭网络中数字版权管理技术需要解决内容与权限在使用、存储、转移中存在的一致性问题,需要研发端到端的安全传输、有条件接收、有条件播出、权限描述等关键技术,以适应家庭网中新媒体、新业务的发展和保护知识产权的需求。

关键词: 家庭网络; 数字版权管理; 数字内容; 权限

Abstract: Home networks are a focus in the development of social digitization and informatization. The bottleneck for developing the home network is how to safeguard the content security and the legitimate interests of every entity in the value-chain. The Digital Rights Management (DRM) is a general solution to utilization, storage, exchange and tracking of digital contents and their rights. The basic characteristics of DRM are systematicness and controllability. In order to meet the requirements of home networks on development of new media and services and intellectual property protection, it is necessary to solve the consistency problems existing in the utilization, storage, transfer of contents and rights and develop key techniques for secure end-to-end transmission, conditional access, conditional play, rights expression in DRM.

Key words: home network; digital rights management; digital content; right

杨成/YANG Cheng¹
王永滨/WANG Yong-bin²

杨义先/YANG Yi-xian³

(1. 中国传媒大学 信息工程学院, 北京 100024;

2. 中国传媒大学 计算机与软件学院, 北京 100024;

3. 北京邮电大学 信息安全中心, 北京 100876)

(1. Information Engineering School, Communication University of China, Beijing 100024, China;

2. Computer and Software School, Communication University of China, Beijing 100024, China;

3. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

中图分类号:

TN915; TN92

文献标识码:

A

文章编号:

1009-6868 (2006) 04-0015-06

家庭网络被定义为^[1]:在特定范围内(例如家庭内部)通过有线或无线方式将多个通信、信息、家电、电器等设备连接起来而形成的内部(私有)网络。目前业界公认的家庭网络的功能主要有:家庭内部通信、家庭娱乐(包括网上音/视频点播、游戏、网上浏览聊天、虚拟实景等,以及对DVD、摄像机、数码相机、PDA、MP3、MP4等的控制)、家庭学习(远程教学、

网上交流、网上图书馆等)、家庭办公、家居生活和家庭监控(包括火警、水警等)。

家庭网络是一个融合的网络,即融合了固定和移动的网络^[2]。随着社会向数字化、网络化、信息化的不断演进,家庭网络正在成为继数字电视、IPTV之后又一个受人们瞩目的焦点。家庭网络的概念也在不断延伸,在技术核心、产业标准、设备研发等方面都正在加紧进行准备,e家佳、闪联、中国通信标准化协会(CCSA)、家庭控制网络标准(ECHONET)等家庭网

络标准也已经进入产品芯片研发阶段,同时家庭网络的融合和互联问题也成为2006年中国下一代互联网(CNGI)的重大项目之一。这些都表明了在中国经济快速持续增长的同时,对未来家庭网络的需求也呈现出强劲增长趋势。而与此同时如何保障家庭网络中数字内容使用、存储、交换时的安全性,如何保证内容提供商、运营商和版权拥有者的合法利益,成为制约家庭网络普及和进一步发展的重要“瓶颈”之一。对数字版权管理的需求应运而生。

基金项目: 中国下一代互联网项目
(CNGI-04-12-2A)

中国版权法规定,数字内容的版权应该得到保护,但是由于数字内容极易被复制、传播的特点,使得在家庭网络中随意分发和非法拷贝内容、任意使用内容、任意修改内容成为可能。为了有效保护家庭网络中数字内容的版权,基于内容安全的数字版权管理技术被广泛研究和使用的。

1 数字版权管理的基本特征

设计和建立数字版权管理应遵循的基本原则是:简单、灵活和开放。数字内容的版权管理涉及到内容提供者、服务运营商、设备制造商、消费者等各个方面的利益,国内外对于版权管理技术的研究也贯穿了数字内容的整个生命周期,这包括数字内容的创建、存储、转移以及使用(接收、播放、显示)等各环节。

数字版权管理可分为3个部分^[3]:第一部分是数字内容,比如MP3、VCD、电子书籍等数字信息;第二个部分是权限,就是用来描述数字内容的使用权限;第三个部分是管理,就是针对数字内容与权限的管理。数字版权管理具有的基本特征包括:技术手段与非技术手段结合(系统性)、对署名权的保护(绑定性)、权限管理与访问控制(可控性)、版权信息与权限信息具有可验证性、盗版可追踪等。

社会道德建设强调提高大众的版权意识,法律对知识产权保护进行规范,技术在不断发展的过程中使知识产权的保护得以实现并逐渐完善,管理定义了知识产权信息的内容,并与技术密切结合形成实际中的版权保护方案。采用密码学、数字水印等在内的信息安全技术为数字化信息的版权执法和权益维护提供支持和手段,并可作为司法鉴别的依据。

数字版权管理将数字内容与其作者或拥有者绑定在一起,如通过安全容器将作者版权信息与数字作品进行加密封装,或将标识作者版权信息的序列号以数字水印的形式嵌入到数字作品中,并通过媒体建立与作

者的联系。任何人获得数字作品的同时也显式或隐式地获得了其作者或拥有者的信息。

版权保护提供对盗版追踪的支持。为了最大限度地打击盗版,数字作品在传播过程中应为其用户添加唯一的用户标识,并将该标识与用户获得的数字作品采用数字水印等方式绑定在一起。

目前,版权保护系统主要采用的是加密技术、数字签名技术、可信模块和水印技术以及他们的结合。加密技术能够阻止对拷贝的直接访问,通过提供解密密钥使得只有授权用户可以对内容进行访问,但是加密仅提供通信信道保护,一旦解密,数字作品将完全暴露,没有任何保护措施;数字签名技术可以提供对信息来源的可靠性和内容的真实性验证,但是数字签名与数字作品相分离,很容易去除,而且只要数字作品稍微修改,签名就无效了,这与图像、视频等数字作品的版权保护应具有一定的抗修改能力不一致;可信模块通常是防篡改硬件,可用来保护解密密钥或发行商制订的其他版权保护策略,但是可信模块要求每个用户都要有相应硬件支持;水印技术通过在数字作品中嵌入一定的信息对其进行保护,可以实现版权确认、版权跟踪以及网络监测等功能。

许多科研机构和公司针对数字媒体的版权保护从各个角度分别展开了研究,比如Intertrust公司的Digi-Box技术,该技术能根据一定的使用规则使受保护的信息在整个生命期内无论传到任何地方都将受到保护;IBM公司的Cryptolope技术,该技术的特征是用安全加密技术封装要保护的数字媒体信息的内容;Digimarc公司在研究基于数字水印的媒体信息版权保护等等。

2 家庭网络中的数字版权管理

家庭网络的核心问题是内容与

控制的问题,其中内容与控制的安全问题将是家庭网络普及和发展的关键因素,而数字版权管理正是解决家庭网络中内容安全的关键。家庭网络的内容安全涉及系统设备制造商、内容提供商,以及网络运营商。完善的家庭网络内容安全解决方案需要各方面的支持和协同工作,需要在他们之间达成某种安全协议^[4]。

具体来说家庭网络中数字版权管理问题包括内容与权限的使用问题、内容与权限的存储问题、内容与权限的转移问题、内容与权限的一致性问题。

(1) 内容与权限的使用问题

家庭网络中所有需要保护版权的数字内容都具有一定的权限,用户需要购买获得权限才能有效地使用内容。作为家庭网络中的设备必须具有条件播出的能力,能够确定内容与权限的关联,并对用户所拥有的实际权限进行解析,进一步根据权限完成对内容的使用,并且能够对节目内容进行认证,包括正版、盗版的验证,合法、非法的鉴别等。

(2) 内容与权限的存储问题

家庭网络中的数字电视、个人录像机、电脑等各种设备都具有通过硬盘或U盘录制、存储内容的能力,而一般情况下,录制、存储的内容其与原始的内容具有相同的使用价值,可以方便地进行复制、修改、传播。存储设备除了要与源设备和目标设备进行安全的端到端传输外,其自身在存储结构和数据访问接口上也要注意安全问题,防止其数据被破坏或者被盗取。

(3) 内容与权限的转移问题

家庭网络中内容与权限的转移分为3个环节,即内容与权限从外部设备或服务器通过公共网络(如HFC网络、电信网络、Internet、蓝牙等)或移动存储设备转移到内部设备;内容与权限在家庭网络内部不同设备之间(如电脑与电视之间、移动设备与固定设备之间)转移;内容与权限从

家庭网络内部通过家庭网关或直接从设备自身通过公共网络或者移动存储设备转移到外部设备或服务上。转移的过程中需要对源设备和目标设备的许可权限进行验证,并对转移的过程进行监控和安全处理。这3个环节都要求家庭网络设备具有完善的权限控制,而且从外部转入内容与权限时,还要求家庭网络具有有条件接收能力,内容与权限在家庭网络内容转移时,还需要家庭网络具有端到端的安全传输能力。

(4) 内容与权限的一致性问题

在内容与权限的使用与转移过程中,需要保持家庭网络中同一数字内容与其权限的一致性。一致性问题包括两个层次,即内容与权限的绑定,内容与权限的更新。内容与权限的绑定是指在内容与权限多对多的基础上,每一个内容只与包含其内容标识的权限关联,每一个权限也只对其包含的内容标识所对应的内容进行限定。内容与权限的更新是指分布在家庭网络中的同一个内容的某个副本被使用时应该对权限的描述进行相应的修改,并使该内容及其权限在家庭网络中的所有副本一致。

3 端到端的安全传输

家庭网络内部设备间端到端的安全传输分为实时和非实时的安全传输,包括内容的安全传输和权限的安全传输。比如机顶盒、TV、VCR之间属于实时的安全传输,因此他们之间传输的内容在进行加密封装等处理时要充分考虑高清、流媒体等实时性的具体要求,而在转录、存储、二次分发等方面的安全传输对实时性要求相对较低。

端到端的安全传输主要解决两个问题:对两个设备间传递的内容加以保护,对内容接收设备的权限进行辨别。内容在家庭网络中流动,可以对设备具有选择性,当某些设备没有获得处理特定内容的权限时,网络可以拒绝这些设备接收特定受保护内

容的请求。此外,对于设备而言,可以具有基本的控制,区分为家庭网络内部和家庭网络外部的设备,内部的设备可以共享权限,而家庭以外的设备无法使用家庭内部被授权的内容。

主要的端到端安全传输系统有数字传输内容保护协议(DTCP)和高速数字内容保护协议(HDCP)。

3.1 数字传输内容保护协议

数字传输内容保护协议(DTCP)由英特尔、东芝、索尼、松下、日立在内的多家公司联合开发。当音频、视频等娱乐内容在符合IEEE 1394-1995接口标准的数字传输设备之间传输时,DTCP能够防止内容被非法拷贝和截取。只有在两个通过认证的设备之间传输的合法内容才受到版权保护系统的保护,这两个设备分别被称为源设备和从设备。DTCP主要包含4个部分,即拷贝控制信息(CCI)、设备认证和密钥交换、内容加密、系统更新。

内容提供者需要一种方法指定内容的拷贝信息,如不允许拷贝、允许拷贝一次等,内容保护系统能够安全地从源设备向从设备传送拷贝控制信息(CCI),CCI的传送方法有两种:(1)加密模式块(EMI)提供了简单安全传送CCI的方法,其中同步包头的高两比特表示CCI;(2)直接在传输的内容流中嵌入CCI。

从设备检查收到的EMI中的CCI。通过设备认证确认从设备的内容、权限接收和存储上的能力,在认证过程中也同时协商得到后续使用的会话密钥,内容数据在会话密钥的控制下使用高级加密标准(AES)完成加密操作并传输给从设备。

此外,DTCP也为设备加入和退出家庭网络提供了支持,在进行完全认证时,可以通过一个不断更新的有效设备列表来判断设备是否属于家庭网络。

3.2 高速数字内容保护协议

高速数字内容保护协议(HDCP)

用来保护一些由高速宽带接口传送的音频或视频内容,这些特定的高速宽度接口称为HDCP保护接口,HDCP保护接口包括数字视频接口(DVI)和高清晰度多媒体接口(HDMI)。在HDCP系统中,两个或多个HDCP设备通过HDCP保护接口连接起来,受HDCP保护的音频或视频内容由上层的HDCP发送者通过一个树形结构发送给HDCP的各个结点和接收者。HDCP主要包括3部分内容:

(1)HDCP发送方对请求发送数据内容的HDCP接收方进行认证。

(2)若HDCP接收方的合法性通过验证,由HDCP发送方向接收方发送加密后的数据内容,其中,加密过程基于双方在验证过程中共享的密钥。

(3)可信设备或机构(如LLC公司)撤销已经不安全的HDCP接收设备,阻止向不安全的HDCP接收设备传送内容。

HDCP接收方可以是一个结点,即可以从上层的发送方接收到内容然后转发给下层的一个或多个接收方。图1是一个简单的HDCP系统的拓扑结构。

HDCP采用了树状的拓扑结构,发送设备对整个拓扑结构中的每个结点和接收设备进行认证,完成认证需要5s的时间,为了使得完成认证的时间不会太长,HDCP规定了一个拓扑结构最多允许有7层结点、128个接收设备。因此采用这种认证机制,限制了整个系统的设备容量,即随着整个系统中连接设备的增多,完成认证的时间也加长。

对于HDCP来说如果一个新的接收设备加入已经通过验证的拓扑结构,若已经通过验证的拓扑结构中的一个接收设备从拓扑结构中分离出来,则发送设备需要重新对整个拓扑结构进行验证,这种机制使得整个系统缺乏灵活性。

此外,HDCP使用了流密码来实现数据加密的高速运转,但是由于流密码存在同步问题,使得系统需要不

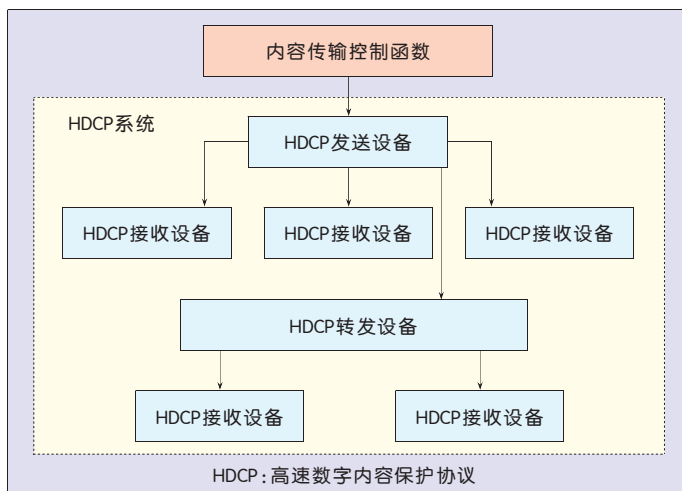


图1
HDCP拓扑结构

断地进行同步验证,增加了整个系统的开销。

4 有条件接收

有条件接收(CA)来源于数字电视广播的授权收费,主要解决内容与权限数据从外部设备或服务器到家庭网络内部时的安全转移问题,包括控制机顶盒等家庭网络内部设备对数据的接收,防止数据在传输过程中被窃取或重放。所谓条件接收就是对视频、音频和数据等信息加扰、加密、传输,采用智能卡等方式对用户进行授权控制管理,并使合法的经授权的用户接收、解密、解扰的过程。未授权用户将无法得到正确的媒体数据流。

CA系统是一个综合性的系统,它集成了多种先进的技术,包括系统控制管理技术、数字视频压缩编码技术、加解扰算法、加解密算法、调制解调技术、机顶盒技术、智能卡技术等,同时也涉及到用户管理、节目管理、收费管理等数据库技术。CA系统一般由节目管理系统、用户管理系统、前端条件接收子系统、加扰复用系统和接收端条件接收子系统5大部分功能实体组成。CA系统的功能实体如图2所示。CA系统基本框架结构如图3所示。

CA系统建立在数字化的MPEG2节目码流传输基础之上,是利用MPEG2标准格式的规定定义其中用

于条件接收的字段含义来实现的。目前,国内外都有一些成功的CA设备提供商,国外的爱迪德、NDS、Nagra等公司,中国近年出现的算通、迪科、永新同方、三洲、中视联等公司都具有相当的实力。由于MPEG2标准在数据编码上的高效率,使得其得到了广泛的认可和应用,各国和组织更是以MPEG2为基础,为数字电视等应用场景制订了一批CA系统标准。目前在国际上占主流地位的CA系统标准主要有欧洲的数字视频广播(DVB)标准、北美的高级视频系统委员会(ATSC)标准及日本的综合业务数字广播(ISDB)标准。

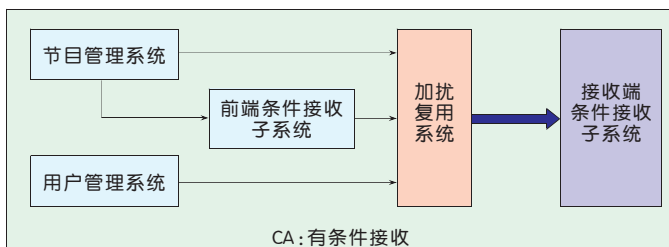
这3种标准对于CA部分都作了简单的规定,并提出了3种不同的加扰方式。其中欧洲DVB组织提出了一种称为通用加扰算法的加扰方式,由DVB组织的4家成员公司授权;ATSC组织使用了通用的三重数据加密标准(3DES)算法;而日本的ISDB使用了松下公司提出的一种加扰算法。

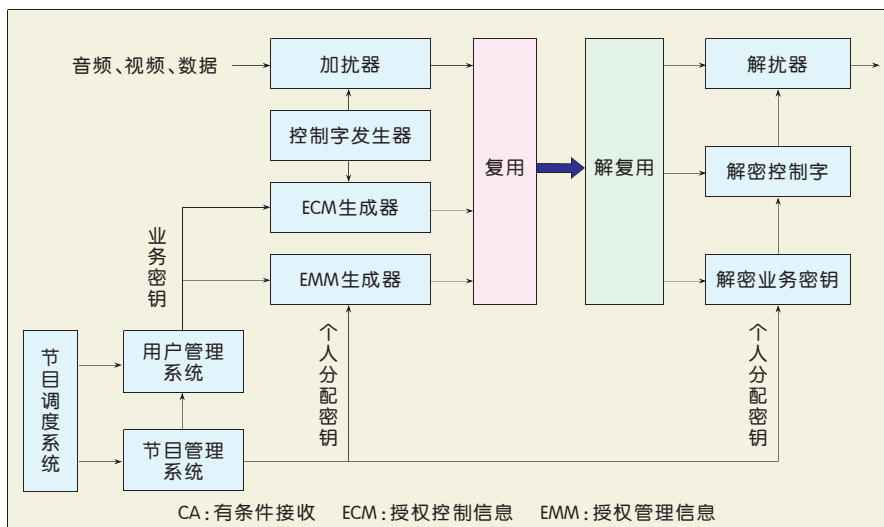
传统的单向DVB-CA系统可划分为加解扰和解密两部分。加解扰是

使用控制字(CW),对MPEG2节目码流采用通用加扰算法(CSA)进行扰乱处理,加解扰部分的设计与实现一般遵循国际标准进行;加解密采用对称和非对称密钥密码体制对加扰用的控制字加密传输,并由授权用户端的解密模块解密获得控制字。由于DVB-CA面向的是单向广电网络而设计的,因此其加解密往往采用多重加密策略,系统复杂,并且属各设备提供商专有。整个CA系统的复杂性在于要在单向网上完成各种密码的分发、更新、共存。一般情况,DVB-CA用到的密钥有与业务相关的业务密钥(SK)、与用户相关的用户个人分配密钥(PDK)。CW被封装到授权控制信息(ECM)中进行传输,SK被封装到授权管理信息(EMM)中进行传输。为了方便用户和业务的管理,CA系统包含了用户管理系统(SMS),完成各种收费服务的记录和执行等功能。

在双向网络中,CA系统中可以使用双向身份认证技术,通过对应的交互协议来确保前端和客户端这两个通信双方的有效性和可靠性。主流的身份认证技术包括两类,即基于公钥基础设施(PKI)的认证和基于标识的加密(IBE)的认证。PKI认证需要认证中心的支持,由认证中心将其生成的身份证书与用户的信息绑定,并且身份认证过程需要认证中心的参与,认证中心作为可信的第三方给出身份确认的证明。IBE认证是采用被认证方公开的标识,如统一资源定位(URL),作为初始值,通过双线性映射函数得到公钥,来认证由被认证方的私钥加密的数据签名。IBE认证过程中不需要第三方认证中心的支持,也不需要身份证书的传递过程,系统得

图2
CA系统的功能实体





▲图3 CA系统基本框架结构

到了简化,安全性也得到了提高。PKI和IBE两种认证技术可以根据不同的应用场景需求进行选择。

传统的CA适用于卫星广播和传统的单向有线网,对于新型的双向智能化网络及IPTV、互动电视等应用,CA系统必须改变自己的结构,发展适合实际需求的的安全的双向CA系统。

5 有条件播出

CA是有条件接收,只对付费频道的电视节目进行加扰加密保护,符合条件的授权用户可以通过自己的个人分配密钥,获得指定的解密密钥,对节目内容解密解扰,属于收费控制。但是家庭网络中在播出数字内容时还需要通过有条件播出(CP)控制用户的权限,并对数字内容进行认证。

5.1 权限控制

权限控制是对版权保护的最基本要求,包括两个方面:

(1)验证内容与权限的关联,具有权限的合法用户能够正常使用数字内容,无权限的用户将部分或完全被禁止对数字内容的访问,比如只可以浏览内容摘要等。

(2)对用户拥有的权限(证书)进行解析,验证权限的有效性,不同的权限具有不同的对数字内容的访问使

用能力,版权保护系统应能区分不同的权限,并根据权限的不同控制用户对数字内容的访问。

拷贝控制、播放控制、处理能力控制、有效期限限制都属于权限控制的范畴。拷贝控制对用户将数字内容在相同或不同设备上复制副本的操作进行限制,比如开放移动联盟的数字版权管理标准(OMADM)一般只允许移动终端之间或移动终端与外部设备之间的数字内容拷贝,但是由于数字内容已被加密保护,其他用户必须再获得使用权限后才能正常使用;播放控制主要对数字内容的播放次数、时间、对象进行限制,像在拷贝保护技术工作组(CPTWG)的DVD版权保护规范中要求采用水印等技术确定影片的播放次数;处理能力控制是指对用户实施到数字内容上的旋转、剪辑、缩放、添加内容等操作的限制,在大多数的版权保护系统中都不允许或只能在微小程度上对数字内容进行更改操作。

用户获得的权限往往是通过统一的格式即权力描述语言(如XrML、ODRL)进行表述的,被描述的权限可能作为权限证书的一部分(如权限管理基础设施(PMI)),也可能直接形成特殊的权限对象与受保护的数字内容一起或分别传递给授权用户(如安

全数字音乐计划(SDMI))。

权限控制的实现方式有很多种,比如有第三方参与的身份认证、PMI权限证书、内容加密、安全容器等。其关键在于权限描述与数字内容的对应关系大多都是通过全局标识来建立联系,但是一旦关系被破坏,权限控制也将失效。此外,数字水印技术也可以用于权限控制,权限描述被作为水印被嵌入到数字内容当中,但是可能造成对内容的水印容量要求激增,可选的方式是外加数据库,嵌入的水印仅是权限描述在数据库中的索引或密钥,但是这样数据库的快速搜索将成为“瓶颈”,而且数据库的增加可能带来新的安全隐患。

5.2 内容认证

由于数字内容的容易复制传播特性,使得家庭网络中可能存在盗版或非法的数字内容。对于盗版的或非法的数字内容除了通过加密封装和权限限制来防控外,也可以通过内容认证手段来完成。

实现内容认证的技术方法主要是数字水印技术,数字水印技术具有透明性、鲁棒性、可验证性、安全性等特点,可以与数字内容融合在一起。在有条件播出中,可以在需要保护版权的数字内容中嵌入标识版权信息的数字水印,并要求所有传送给家庭网络设备的数字内容都必须嵌入经审查机构签名的合法性特征标识水印,表示该节目已经被版权保护和合法性标记。家庭网络的播出使用设备只需要添加数字水印的检测模块,就可以判断接收到的数字内容是否含有版权水印或合法性标识水印,如果是盗版的数字内容,其中不含版权水印,如果是非法的数字内容,其中不含经签名的合法性特征标识水印。

6 权限描述

数字内容提供者通过内容封装机制将其媒体内容封装为DRM媒体格式,同时也向授权中心注册其内

容,并由用户申请获得对DRM媒体内容的使用权限,其中的关键问题在于权限如何描述。而在家庭网络中解决权限管理的一般方法是在每个家庭网络中设置一个家庭网络版权管理代理。家庭网络版权管理代理的作用是管理家庭网络的组成并控制家庭网络设备对内容的接收和使用,在这个过程中一个重要的工作就是对描述的权限进行解析。

权限描述了对数字内容的使用规则,一般包括许可和约束两部分。

许可描述了对数字内容可以进行的操作,比如Play(用于视音频)、Display(用于图片、文本)、Execute(用于程序、游戏)、Print(用于图片、文本)等。许可可以进行组合,比如图片可以同时拥有Display和Print的许可。

约束是指对许可的条件限制。对每个许可,可以使用约束来限定用户对媒体内容的使用。比如计次规定用户可以使用某一媒体内容的次数,使用时间规定从用户第一次使用某媒体内容开始用户可以使用的时间长度,起止时间规定用户只能在在时间范围内使用某媒体内容等等。

对于权限的描述往往采用的是具有通用性的表述语言,所描述的权限可以被用在网站、文本文件、图片、音乐、PDF文档和流媒体中。这些语言中比较有名的是ODRL语言和可扩展权限标记语言(XrML)语言。

6.1 ODRL语言

国际版权保护组织提出的ODRL语言标准为DRM的有效解决提供了一个开放标准,允许采用加密等安全措施来解决数字版权管理问题。对于网络环境,ODRL对数字内容的表达语言和词汇进行了定义。

在ODRL的权限模型中,定义了内容、权限、用户3个层次;定义了权限的4种不同类型的许可,即可用、重用、传输、产品管理;提供了条件和协议的概念(条件是一些能够影响存取数字产品权限的规则。这些条件能够

让你描述权限和权力;协议是一个集合元素,它表达了在一定的系统环境下,特定人员存取特定产品的权限);提供了数字签名和密码算法,以保证产品的完整性和保密性;提供了摘要(包括摘要方法和摘要值),用户保护权限、签名的完整性。

6.2 XrML语言

XrML是一种灵活的、开放的、统一的标准权限描述语言,是可扩展标记语言(XML)的扩展,它为权限管理及包括数字内容和资源的所有资源的安全提供了一种通用管理方法。通过开放的体系结构,保证了数字内容得到最大化的商业应用。

XrML适合于家庭网络的应用。在灵活性上,XrML中权限被定义为各种级别,可以与多个数字内容相关联,支持多种不同的权限保护模式、多种商业模式,如订购、直接购买等。在权限描述上,XrML对各种权限如复制、编辑、使用时间的含义、语法规则,以及权限与数字内容的关联进行了详细规定。兼容性上,XrML与其他的相关工业标准兼容,如公共/私人密钥、基于密码学的数字签名和认证、元数据等,同时XrML描述的权限可以被自动化识别,可以被家庭网络中各种不同的设备共享和分析,最小化了平台的差异性。

作为语言,XrML本身简单易用,语义性强,提供快速有效的描述与分析工具,同时其文档组织好,数据高度结构化,人和机器都可阅读有关标识,标签具有一定的语义。利用XrML可以使浏览器和数字化版权管理系统能够很容易辨识有关的版权管理信息和进行管理控制,很容易按照定义的标签内容进行统计或分类,便于异构系统之间的数据交换及有关权利信息的识别和检索。

7 结束语

家庭网络中信息数字化、网络化的特点,使得数字版权管理成为协调

网络运营商、内容提供商、用户等多方面利益的重要手段。但是数字版权管理依然是一个比较新的领域,家庭网络由于其相对封闭和内部共享的特殊性,给数字版权管理的实施带来了困难,在核心技术、体系结构、实施方案标准等多方面有很多问题仍然没有解决,需要技术、市场、管理等方面的分析融合,需要来自不同领域和不同背景团体之间的协作讨论。

随着三网融合、互动电视、移动流媒体等个性化内容制作与分发的的发展,乃至普适计算概念的提出,势必对家庭网络中数字版权管理提出挑战,需要法律、管理、技术各个方面的人员共同努力来完善发展。

8 参考文献

- [1] 吴军,黄维. 关于家庭网络的思考[J]. 光通信研究, 2006(1): 1-4.
- [2] 魏凯. 家庭网络中的媒体技术[J]. 电信网技术, 2005(6): 26-27.
- [3] 范科峰,赵新华. 数字版权管理技术的研究现状及在数字电视系统中的应用[J]. 信息技术与标准化, 2005(6): 21-25.
- [4] 蒂利?梅雷克斯. 家庭网络环境中的数字版权管理[J]. 世界广播电视, 2005, 19(10): 75-78.

收稿日期:2006-05-15

作者简介



杨成,北京邮电大学毕业,博士。中国传媒大学信息工程学院讲师,从事信息安全、计算机等方面的科研工作,主要研究方向为密码学、数字水印、数字版权管理、网络与通信安全。



王永滨,中国传媒大学计算机与软件学院副院长、教授、博士生导师,计算机学会和电子学会高级会员。主要研究方向为信息安全、数字版权管理、智能信息处理。



杨义先,北京邮电大学信息安全中心主任、教授、博士生导师,长江学者奖励计划特聘教授、中国通信学会会士、中国人工智能学会秘书长。研究方向为密码学、信息安全和通信与信号处理。