

# IPTV 数字版权管理解决方案研究

蒋华龙<sup>1</sup>, 刘智广<sup>2</sup>

(1. 四川理工学院计算机学院, 四川 自贡 643000; 2. 成都三零凯天通信实业有限公司, 成都 610041)

**摘要:**随着三网融合步伐的加快,网络电视(IPTV)的普及已成为必然。如何保证 IPTV 在制作、分发、传播和收看各个环节的安全,建立有效可行的访问控制和版权保护措施是内容创作者和版权所有者普遍关注的焦点。在详细讨论了实现 IPTV 数字版权管理相关技术的基础上,给出了一种 IPTV 数字版权管理的解决方案,基于该方案设计并实现了 IPTV 数字版权管理的演示系统,演示结果表明该方案能对 IPTV 中音视频媒体的版权进行有效保护。

**关键词:** IPTV; DRM; 解决方案; 身份认证

**中图分类号:** TP309

**文献标识码:** A

## 引言

随着计算机技术、多媒体技术和通信技术的发展,特别是宽带网络技术的发展,以数字化和网络化为核心的新一代媒体传播技术—交互式网络电视(IPTV)已成为电视传媒的重要发展方向。IPTV 以宽带网作为基础设施,以家用电视机或计算机作为主要终端设备,集互联网、多媒体、通信等多种技术于一体,通过 IP 协议向家庭用户提供包括数字电视在内的多种交互式数字媒体服务的全新技术。IPTV 可以实现媒体内容提供商和消费者之间互动,能根据用户的选择提供广泛的多媒体服务功能,包括视频广播、视频点播、网页浏览、电子邮件以及娱乐、教育及电子商务等功能<sup>[1]</sup>。但是,在因特网上非法获取和传播数字多媒体内容也十分容易,直接损害了作品版权人的利益,严重影响了创作人的创作积极性,必将阻碍和制约 IPTV 的健康发展<sup>[2]</sup>。因此,如何保证 IPTV 在制作、分发、传播和收看各个环节的安全,建立有效可行的访问控制和版权保护措施是内容创作者和版权所有者普遍关注的焦点。只有解决了版权保护问题, IPTV 才可能真正实施,才能保证 IPTV 应用市场正常有序的发展。

本文在详细讨论 IPTV 数字版权管理相关技术的基础上给出一种 IPTV 数字版权管理的解决方案,基于该

方案设计并实现 IPTV 数字版权管理的演示系统,演示结果表明该系统能对 IPTV 中音视频媒体的版权进行有效保护。

## 1 DRM 技术概述

数字版权管理(Digital Rights Management, 简称 DRM)是一项涉及到技术、法律和商业各个层面的系统工程。它作为一种新型的数字内容保护技术,对数字产品分发、传输和使用等各个环节进行控制,使得数字产品只能被授权使用的人按照授权的方式在授权的期限内使用。DRM 实施的指导思想是对数字内容进行加密和增设附加使用规则来判断用户是否具有使用对应数字内容的授权或者权限<sup>[3]</sup>,为数字媒体的商业运作提供了一套完整的实现手段。DRM 技术的出现,使得版权提供者可采取更灵活的节目销售方式,能较容易地确保数字媒体内容被合法的使用,同时有效地保护知识产权<sup>[4]</sup>。

DRM 不仅仅指版权保护,同时也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,它包含数字版权信息使用、受版权保护的数字媒体内容的管理和分发。

在 IPTV DRM 系统的实现方案中,涉及的技术非常广泛,主要包括密码学技术、身份认证技术、数字签名技

收稿日期:2011-04-06

基金项目:核高基科技重大专项子课题(2009ZX01039-003-001-05)

作者简介:蒋华龙(1968-),男,四川广安人,讲师,主要从事计算机应用技术方面的研究。

术等<sup>[5]</sup>。

### 1.1 内容加密技术

密码技术是信息安全领域的主要技术之一,现有的数字内容保护多采用加密方法实现,即首先将多媒体数据文件加密成密文后发布,使得非法攻击者无法从密文中获取重要信息,从而达到版权保护和信息安全的目的。

目前的密钥体制从原理上可分为两大类,即对称密钥(私钥)体制和非对称密钥(公钥)体制。对称密钥体制与非对称密钥体制是两种不同的加密机制,它们解决不同的问题。对称密码算法速度极快,算法设计简单,并且对选择密文攻击不敏感。目前使用较多的对称加密算法包括:DES、3DES、AES、RC4、Blowfish等。非对称加密算法不要求通信双方事先传递密钥或有任何约定就能完成保密通信,并且密钥管理方便,可实现防止假冒和抵赖,因此,更适合网络通信中的保密通信要求。但非对称加密算法的加密和解密速度慢,因此只适用于对少量数据进行加密。目前使用较多的对称加密算法包括:RSA、ElGamal、ECC、Rabin等<sup>[6]</sup>。

在本方案设计中,使用对称加密算法来加密媒体内容,使用非对称加密算法来保护证书和其他敏感数据,如用来加密内容密钥等。

### 1.2 身份认证技术

身份认证技术是计算机网络中确认操作者身份的一种技术。如何保证以数字身份进行的操作者就是这个数字身份合法拥有者,在IPTV DRM系统中是非常重要的。利用公钥证书可以实现有效的身份认证、设备认证以及权限分配、管理和吊销等功能,对相关设备和存储介质,如机顶盒、硬盘、PC机等分配公钥证书,用于在播放节目前进行身份认证<sup>[7]</sup>。

本方案设计中,通过X.509数字证书和PKI认证体系确立准入控制、验证双方身份、使用交互的不可抵赖性和可审计性,建立IPTV DRM系统中各方的信任体系。

### 1.3 数字签名技术

数字签名是通过密码算法对数据进行加、解密变换来实现的,用DES算法、RSA算法都可实现数字签名。数字签名能够实现对原始信息的鉴别与验证,保证信息的完整性、真实性、机密性和发送者对所发报文的不可抵赖性<sup>[8]</sup>。目前,应用广泛的数字签名方法主要有三种,即RSA签名、DSS签名和Hash签名。这三种算法可单独使用,也可综合在一起使用。

## 2 IPTV DRM 系统方案设计

设计中,所使用的流媒体文件格式为当前比较常用

的MP4文件格式。系统能对基于MP4视频格式的点播流进行加密和打包,并由内容发布服务器进行发布。用户接收到加密流后,不能直接解码收看,必须由认证服务器对用户进行身份认证和授权,然后从密码服务器获得解密密钥后,才能正常播放。

图1为IPTV DRM系统的总体框架,该系统主要包括六个功能模块:内容打包模块,内容分发模块,密钥管理模块,身份认证模块,终端解密模块和终端身份认证模块。根据系统的具体实现,不同的功能模块在系统中扮演不同的角色。各功能模块是逻辑上分离的,但不要各自对应于独立的物理节点(如服务器)。根据具体实现时的系统配置,不同的功能模块可以在相同或不同的物理节点上实现,不同的DRM系统具体实现可以由部分或全部的功能模块组成,这依赖于业务模型对DRM系统的具体要求和配置。

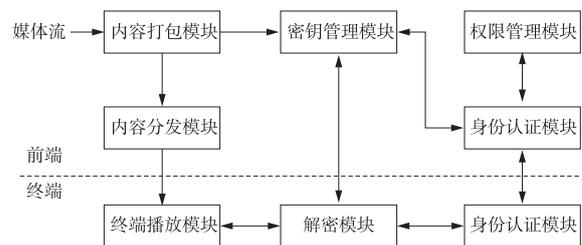


图1 IPTV DRM 系统总体架构

#### · 内容打包模块

主要负责对IPTV播控系统提供的媒体流进行打包和加密处理,并将处理结果发送到内容分发系统。

#### · 内容分发模块

主要负责监听终端用户的播放请求,对请求的音视频内容进行分发。

#### · 密钥管理模块

主要负责维护和管理整个IPTV DRM系统的密钥信息并向版权管理系统提供查询服务。

#### · 证书管理模块

主要负责证书的生成、发放和管理,对终端身份进行认证,提供对证书状态查询等功能,并与权限管理模块交互,通过查询接口获得用户对流媒体的访问权限,实现身份与权限的统一。

#### · 终端解密模块

主要负责利用解密密钥对经过加密处理的视频数据进行解密操作,将解密后的音视频数据送给终端播放模块进行播放。

#### · 身份认证模块

主要负责实现终端与认证系统服务端的双向身份认证,获得认证服务器分发的解密密钥,将获得的解密密钥提供给数据解密模块。

### 3 IPTV DRM 系统实现流程分析

#### 3.1 IPTV DRM 系统流程

IPTV DRM 系统流程如图 2 所示。具体流程描述如下。

第一步、内容提供者将要发布的媒体文件送到打包模块,对媒体文件使用对称加密技术加密和打包,根据一定的规则生成相应的内容 ID,将加密后的媒体文件送内容发布平台,采用非对称加密技术加密内容密钥并将其与内容 ID 一起存入密钥管理数据库。

第二步、用户通过点播平台点播想要收看的节目后,终端接收到来自内容发布服务器推送的节目数据。若节目数据被加密,则调用 DRM 系统的身份认证模块向身份认证服务器发起认证请求,实现认证服务器、终端的双向身份认证。

第三步、认证服务器向播控平台的用户权限管理服务器发起查询请求,确认特定用户对特定视频资源的访问权限。

第四步、认证成功且用户有播放权限,身份认证模块则向密钥管理服务器请求相应节目的解密密钥,终端获得密钥后则调用数据解密模块进行解密,将解密后的数据交给 IPTV 播控平台的视频播放器,从而实现对整个播放过程的有效保护。

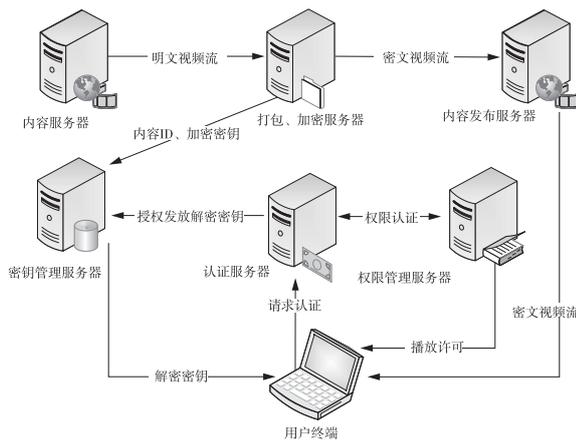


图 2 IPTV DRM 系统流程

#### 3.2 密钥管理流程

密钥管理系统负责产生、存储、分发和管理系统使用的各种密钥,并存储和管理用户证书。密钥管理系统维护节目与内容加密密钥的映射关系,并为节目的加密提供内容加密密钥。密钥管理系统不直接与用户终端系统交互,服务端通过授权管理系统发送权利对象为用户发布密钥。

当内容打包模块将生成的节目信息、内容 ID 信息和内容密钥发送给密钥管理系统后,用户通过业务系统

选定指定节目,请求权限管理系统获取对该节目的权限使用对象;权限管理系统向密钥管理系统查询指定节目的加密密钥;密钥管理系统根据节目的内容 ID 向数据库查询指定节目的加密密钥,并在响应消息中将加密密钥返回给业务系统。权限管理系统向业务系统返回权限使用对象,其中包括指定节目的加密密钥。

#### 3.3 节目发布流程

节目发布系统主要负责打包、加密媒体文件并进行流化发布,其中最重要的两个组成部分是内容发布系统和内容打包、加密系统。内容发布系统是 IPTV 播控系统的关键部分,它承担了将视频信息推送给终端的任务,本系统使用 Darwin Streaming Server 作为内容发布服务器。打包、加密系统主要负责对节目内容进行加密处理,它使用随机生成的密钥对媒体流进行加密,加密后的媒体流发送给内容发布系统,而加密密钥和节目信息将传送给密钥管理系统,由密钥管理系统负责管理该密钥。

#### 3.4 认证授权流程

内容密钥和权限对象的安全传输对 DRM 系统的实现至关重要,认证授权系统包括两个主要组成部分:身份认证系统和权限管理系统。身份认证系统主要负责证书的生成、发放和管理,对终端身份进行认证,提供对证书状态查询等功能,并与 IPTV 播控平台的权限管理系统交互,通过查询接口获得用户对流媒体的访问权限,实现身份与权限的统一。身份认证系统同时负责向密钥管理系统请求获取指定节目的内容密钥,并将该信息返回给已经通过身份认证的终端用户。

IPTV 终端用户在播放节目之前首先应向认证系统进行注册,使用其拥有的用户信息向身份认证系统请求获取 X.509 的数字证书,该证书是身份认证系统的 CA (Certificate Authority) 根据终端用户的用户名、密码、RSA 公钥等信息生成;身份认证系统收到 IPTV 终端的证书申请后,向业务系统进行查询以验证用户的身份,利用其终端身份信息生成对应的 X.509 数字证书,并以 PKCS12 存储结构的形式发送给 IPTV 终端并加以存储;当用户点播节目时,IPTV 终端向内容发布系统请求获取节目,收到请求的媒体流数据后,若数据被加密,终端则利用自己的数字证书向身份认证系统进行身份认证以获取视频数据的解密密钥;身份认证系统向权限管理系统请求获取该用户对节目的权限信息;权限管理系统向数据库查询指定用户拥有的权限信息并返回;身份认证系统查看用户拥有的权限信息,确认其拥有观看指定节目的权限后,向密钥管理系统请求获取指定节目的内容密钥;密钥管理系统响应内容密钥请求并返回,然后身份认证系统将权限信息和内容密钥以许可证的方式返

回给 IPTV 终端, IPTV 终端利用内容密钥对视频数据进行解密播放。

### 3.5 终端点播流程

终端点播是 IPTV DRM 系统整个流程的最终体现。用户点播节目时, 首先由 IPTV 终端向业务系统请求获取节目单; 业务系统收到 IPTV 终端的节目单请求后, 向终端发送指定节目的详细信息和节目所在的内容分发服务器的地址; IPTV 终端根据获得的分发服务器地址向内容发布系统请求获取节目数据; 内容发布系统向终端发送加密的节目视频流; 由于节目是加密的, IPTV 终端的播放器将无法播放, 此时终端将使用获得的数字证书向身份认证系统进行身份认证以获取节目数据的解密密钥; 身份认证系统收到 IPTV 终端的身份认证请求后, 返回包含权限信息和内容密钥的许可证书; IPTV 终端使用许可证书中包含的内容密钥对加密节目进行解密播放。

## 4 结束语

有效保护了 IPTV 节目的版权, 也就保护了节目创作者人和节目版权拥有者的利益, 必将有力促进 IPTV 产业的健康有序发展。本文通过对 DRM 技术的分析, 给出了 IPTV DRM 系统的设计方案, 详细阐述了 IPTV DRM 系统中各主要模块的实现流程。使用对称加密算法加密媒体内容, 使用非对称加密算法保护证书和加密内容密钥等敏感数据, 通过 X. 509 数字证书和 PKI 认证体系确立准入控制、验证双方身份、使用交互的不可抵赖性和可审计性, 建立 IPTV DRM 系统中各方的信任体

系。在此基础上, 设计并实现了 IPTV DRM 演示系统, 演示结果表明该系统能对 IPTV 中的音视频媒体的版权进行有效的保护, 对进一步研究和开发实用的 IPTV DRM 系统具有一定的参考价值。

### 参考文献:

- [1] Sohn D. Understanding DRM[J]. Queue, 2007, 5(7): 32-39.
- [2] 邝代英. DRM 数字权限管理系统的设计与实现[D]. 北京: 北京邮电大学, 2007.
- [3] 俞银燕, 汤帆. 数字版权保护技术研究综述[J]. 计算机学报, 2005, 28(12): 1957-1968.
- [4] 陈江涛. 关于数字版权管理(DRM)技术与应用[EB/OL]. <http://info.broadcast.hc360.com/HTML/001/002/017/67745.htm>, 2004.11.15.
- [5] Ivan I, Toma C, Popa M, et al. Secure platform for digital rights management distribution[J]. WSEAS Transactions on Computers, 2007, 6(3): 478-485.
- [6] Nash A, Duane W, Joseph C, et al. 张玉清等译. 公钥基础设施(PKI)实现和管理电子安全[M]. 北京: 清华大学出版社, 2002.
- [7] 裴庆祺, 高铭鼎, 范科峰. 数字电视领域的数字版权保护技术标准综述[J]. 信息技术与标准化, 2007(4): 33-37.
- [8] Li Jiguo, Huang Xinyi, Mu Yi, et al. Certificate-based signature: Security model and efficient construction[J]. Lecture Notes in Computer Science, 2007, 4582: 110-125.

## Research and Realization of IPTV Digital Copyright Management Solution

JIANG Hua-long<sup>1</sup>, LIU Zhi-guang<sup>2</sup>

(1. School of Computer Science, Sichuan University of Science & Engineering, Zigong 643000, China;

2. Chengdu 30 Kaitian Communication Industry Co. Ltd, Chengdu 610041, China)

**Abstract:** With quick pace of integration of broadcast, TV network, telecommunication network and internet, Internet Protocol television (IPTV) becomes popular. The content originator and copyright owner focus on how to ensure safety of production, distribution, transmission, and watch for IPTV and establish effective and feasible access control and copyright protection measures. Based on detailed discussion of realizing relevant technologies of IPTV digital copyright management, this paper gives a resolution of IPTV digital copyright management. Based on this solution, a presentation system of IPTV digital copyright management is designed and realized. The result of presentation shows that this solution can effectively protect copyright of IPTV's audio and video media.

**Key words:** IPTV; DRM; solution; identity authentication