基于 Windows Media SDK 的 DRM 系统开发

Development of DRM System Based on Windows Media SDK

董 纳　杨 静　苑红晓　(山东大学 计算机科学与技术学院 济南 250061)
常立立　(山东大学 信息科学与工程学院 济南 250061)

摘要: 随着网络的发展,数字媒体文件的盗版问题的日益泛滥,Microsoft Windows Media 9 在编码过程中提供了对数字权限管理(DRM)的支持,可实现对数字媒体文件的加密保护。该文简要介绍了 Microsoft 的 DRM 技术原理及工作流程,叙述了如何采用 DRM 技术保护网站上的音频和视频资料。重点描述了如何基于 Windows Media Rights Manager SDK 创建认证服务器,提供认证许可的发放及身份的验证,如何基于 Windows Media Encoder SDK 创建一个数字权限管理(DRM)系统来生成密钥、打包、加密和发行数字媒体内容。

关键词: 数字媒体认证服务Windows Media Encoder SDK Windows Media Rights Manager 数字权限管理(DRM)加密解密

1 引言

现在,网上电子书、音乐、电影、图片等数字内容的传播越来越多,数字媒体文件易于复制和分发,同时还不会降低质量。因此,现在数字媒体文件借助 Internet 这一平台通过授权和未授权的分发渠道得到广泛传播。当缺少安全措施来保护内容时,盗版问题就不可避免地出现。针对数字化信息的特点和数字内容的版权保护,决定了必须有另一种独特的技术,来加强保护这些数字化的音视频节目内容的版权,该技术就是数字权限管理技术——DRM(Digital Right Management)。通过数字权限管理,内容提供商可以保护自己的内容并控制分发,内容提供商可通过为每个数字媒体文件创建许可证来管理有关的权限。许可证注册过程也为这些公司提供了许多重要的客户信息,此类信息有助于内容提供商更了解自己的客户,从而,确保向用户不断提供各种各样最高质量的音频和视频内容。

2 概述

2.1 数字权限管理(DRM)

数字权限管理(DRM)是保护多媒体内容免受未经授权的播放和复制的一种方法。它为内容提供者保护他们的私有音乐或其他数据免受非法复制和使用提供了一种手段。DRM 技术通过对数字内容进行加密和附加使用规则对数字内容进行保护,其中,使用规则可以断定用户是否符合播放数字内容的条件。使用规则一般可以防止内容被复制或者限制内容的播放次数,操作系统和多媒体中间件负责强制实行这些规则。

2.2 DRM 技术的工作原理

首先建立数字节目授权中心,编码压缩后的数字节目内容,利用密钥(Key)可以被加密保护(lock),加密的数字节目头部存放着 KeyID 和节目授权中心的 URL。用户在点播时,根据节目头部的 KeyID 和 URL 信息,就可以通过数字节目授权中心的验证授权后送出相关的密钥解密(unlock),节目方可播放。需要保护的节目被加密,即使被用户下载保存,没有得到数字节目授权中心的验证授权也无法播放,从而严密地保护了节目的版权。

2.3 Windows Media DRM 的基本工作流程如下

图 1 显示了在内容打包程序、版权许可分发程序、媒体许可服务和请求一个特定的未经授权的媒体文件的用户之间的交互。下面所列的项目与图示中的步骤号一一对应:

(1) 内容打包程序用一个许可密钥种子和一个密钥标识生成一个密钥。许可密钥种子是在内容打包程

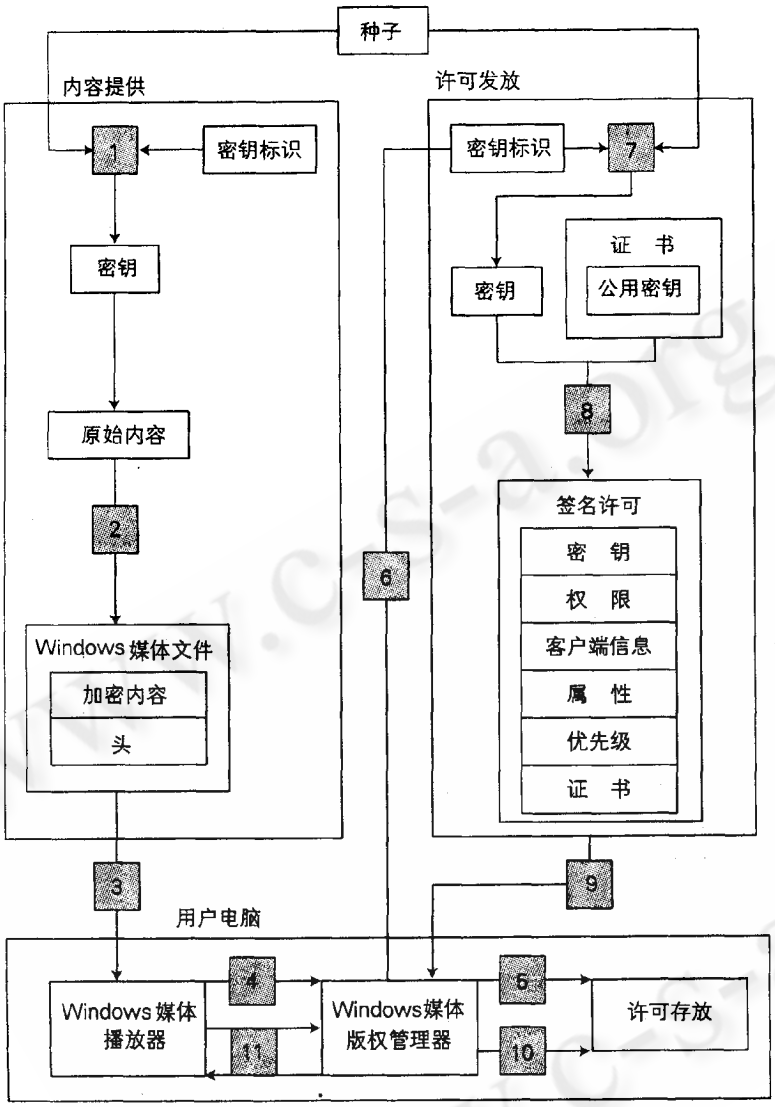

图 1　播放数字媒体文件的流程图

序和许可证书分发程序之间共享的秘密，它是一个不少于 5 字节长的随机值。密钥标识是一个全局唯一标识符。

(2) 内容打包程序使用密钥加密内容，并把密钥标识和用于版权许可分发的互联网地址置入内容头。然后内容打包程序把内容头和加密内容一起打包到一个媒体文件中。

(3) 内容打包程序把媒体文件传递给用户。

(4) 用户的播放器请求媒体版权管理服务器确定其所请求的媒体文件是否可以播放。

(5) 媒体版权管理服务器搜索版权库以获得播放内容的合法版权许可。

(6) 如果媒体版权管理服务器搜索所需的版权许可失败，它会从版权许可分发程序申请一个版权许可。质询(challenge)用于请求内容头中包含的版权许可及与用户电脑相关的信息。

(7) 版权许可分发程序使用共享版权许可密钥和密钥标识生成与第 1 步中由内容打包程序生成的相同的密钥。然后版权许可分发程序加密该密钥。

(8) 版权许可分发程序生成了一个版权许可，并将加密的内容密钥添加到版权许可中，再添加一个从媒体版权许可服务中获得的证书，然后使用证书中的公有密钥对版权许可进行签名。

(9) 版权许可分发程序将签名后的版权许可传送到客户电脑的媒体版权管理器上。

(10) 媒体版权管理器验证该签名，并将该许可放在许可库中。

(11) 媒体版权管理器进行解密，并将所请求的多媒体内容包发送到播放器。

2.3.1 打包

Windows Media 权限管理器将对数字媒体文件进行打包。打包的文件将加密并使用一个"密钥"锁定。该密钥存储在一个加密许可证中，该许可证将单独分发。(这是 Windows Media 权限管理器所独有的功能。)它还会向数字媒体文件中添加其他信息，例如用于获取许可证的 URL。打包的数字媒体文件将保存为 Windows Media Audio 格式(文件扩展名为 .wma)或 Windows Media Video 格式(文件扩展名为 .wmv)。

2.3.2 分发

打包的文件可放在网站上以供下载、放在数字媒

体服务器上以供流式处理、通过 CD 进行分发或使用电子邮件发送给最终用户。Windows Media DRM 还允许最终用户将受版权保护的数字媒体文件发送给朋友。

2.3.3 建立许可证服务器

内容提供者可选择许可证交换中心，该交换中心将存储许可证的特定权限或规则并提供 Windows Media 权限管理器许可证服务。交换中心的作用是对请求许可证的用户进行身份验证。数字媒体文件和许可证是分开存储和分发的，因此更便于管理整个系统。

2.3.4 获取许可证

要播放打包的数字媒体文件，消费者首先必须获取一个许可证密钥为该文件解锁。当用户试图获取打包的数字媒体文件、获取一个预先传递的许可证或首次播放该数字媒体文件时，都将自动启动获取许可证的过程。Windows Media 权限管理器或者引导用户进入注册页(该页要求输入信息或付费)，或者从交换中心检索一个许可证而不提示任何问题。

2.3.5 播放数字媒体文件

要播放数字媒体文件，用户需要能支持 Windows Media DRM 的播放机(Media Player 9.0 以上版本)。然后，用户即可根据许可证中所提供的规则或权限来播放文件。许可证可提供多种不同权限，如开始时间和日期、持续时间以及对操作计数。例如，默认权限可能允许用户在特定计算机上播放数字媒体文件并可将该文件复制到便携设备。但是，许可证是不可转让的。如果用户将打包的数字媒体文件发送给一位朋友，则该朋友必须获取自己的许可证，然后才能播放该文件。这种按 PC 颁发许可证的模式可确保打包的数字媒体文件只能在已获得该文件的许可证密钥的计算机上播放。

3 具体实现

3.1 许可证发放服务(认证服务)的创建

这一部分介绍如何创建一个 DRM 认证服务，在此我们用到微软的 Windows Media Rights Manager 9 Series SDK(MRM)来实现认证服务的创建，用它来产生数字签名证书和四个必需的标识值。

3.1.1 为用户创建一个 DRM Profile

在最终用户能够用 DRM 保护他的产品之前我们需要为他创建一个 DRM profile，它由用来编码并包含下列信息的本地计算机产生，一个 profile 文件通常包括以下要素：

- 一个 DRM profile ID
- 一个名字
- 一个针对产品的描述
- (与名字对应的)属性
- 连接到认证提供服务器的 URL
- 认证获取版本 7 和版本 1(向下兼容 MRM 7.0 和 MRM1.0)内容的 URLs
- 必需的 the individualization version.

用户创建一个 DRM Profile 的步骤：

(1) 用户选择一个认证提供商，建立账户和密码或者用户可自己创建一个认证服务器，在此我们将认证提供商和自己创建的认证服务器统称为认证提供者。

(2) 认证提供者利用 Windows Media Rights Manager 9 Series SDK(MRM) 的 IWMRMKeys2. GenerateSigningKeysEx 和 IWMRMKeys2. GetCertificate 产生 4 个标识值，这些值将作为数字标识被插入被保护文件的头文件。

(3) 认证提供者运行 DRM 客户端代码在用户的计算机上创建 DRM Profile，创建的方法由认证提供者决定。

(4) 创建一个 DRM Profile，将产生一个认证秘钥种子，公有和私有的秘钥标识，认证秘钥种子、公有秘钥标识需要向认证提供者回复，以使他们被认证提供者重载，以实现最终用户文件解密。

(5) 创建完 DRM Profile 后，认证提供者在认证服务器上重载并存储发放认证时需要的值(如：DRM profile ID, license key seed, and public signing key)

(6) 添加 DRM Profile 其他属性的设置(名字，描述，认证获取的 URL, individualization version number 等属性)

(7) 定义完 DRM Profile 后，用户即可以利用它来保护文件，认证提供者也可以按照用户的要求为保护内容提供认证的发放

3.1.2 撤销授权的内容

内容拥有者有权为保护内容撤销认证，也就是说最终用户将无法看到以前授权的内容，这种认证的撤

销需要用 IWMDRMProfile 重载 ContentRevocation 属性,这种撤销基于对特定 DRM profile 的共有和私有标识密钥,也就是只有用这个 DRM profile 保护的内容将被撤销服务。

这种实现相对较为简单,内容拥有者只需重载 ContentRevocation 属性并将它提供给认证提供者,这样,当用户向认证服务器提交申请时认证服务器将拒绝服务,从而无法打开文件。

3.2 利用 DRM 对媒体文件加密的实现

3.2.1 首先,用户须从认证提供者那里建立账号和密码

由于需认证提供者为你保护的内容提供认证的发放,所以你需要先选择一个认证提供者,但你申请账号时,认证提供者会让你选择你认证中需提供的权限,比如你想怎样发放你得认证等。

账号设立完以后,认证提供者将创建一个 DRM profile 并将它存入你的本地计算机,这个 DRM profile 也将只能用于本账号,根据认证提供者的要求,或许允许创建你自己的 DRM profile

3.2.2 创建一个 DRM profile

一个 DRM profile 对保护文件来说是所必需的,他由你得认证提供者创建。如果认证提供者允许或者你通过 Windows Media Rights Manager 9 Series SDK 发放你自己的认证,你都将可以创建自己的产生你自己的 DRM profile,存储在本地计算机中,当然,它只能用于已申请的账号。

当一个 DRM profile 创建好以后,下列值也将被创建并存储在你的本地计算机中:

- 共有和私有标识密钥,认证发放者需要用共有标识密钥来发放认证
- 一个认证密钥种子,它被用来产生每一个加密文件的密钥,认证提供者也要用这个值来再生每个密钥并将它包含进认证中,以便与最终用户解密时使用

如果你要创建你自己的 DRM profile,认证提供者必须首先为你生成 4 个证书和标识值,而一旦你创建完成了你的 DRM profile 文件,你必须在发放加密文件之前,将你生成的 DRM profile ID, 共有标识密钥 和认证密钥种子回复认证提供者,以便于认证提供者重载。

3.2.3 内容保护的实现步骤(以下通过 VC + + 6.0 编译实现)

在你从认证提供者那里设立了账号并拥有了 DRM profile 后,按以下步骤你就可以保护你的文件了(程序代码略):

(1) 通过 WMEncoder 对象重载一个 IWMDRMContentAuthor 对象

(2) 通过 IWMDRMContentAuthor 对象重载一个 IWMDRMProfileCollection 对象

(3) 创建一个 IWMDRMProfile 对象,通过重载 the DRM profile collection,重载你需要的 the DRM profile,同时设置其他必要的属性。

(4) 在 IWMDRMContentAuthor 对象中应用 SetSessionDRMProfile 方法,这个方法将产生一个 key ID (一个用来为加密文件产生 key 的字符串),这个 key ID 出了这样生成外还可以被专门定义,例如你可以共用一个 key ID,但是,所有用同一个 key ID 加密的内容将用同一个认证解密。

(5) 另外,通过 IWMDRMContentAuthor 对象的 GenerateContentI 方法可以产生 content ID,并将它放入当前使用此 ContentID 属性的编码 session,这个 ContentID 被用来唯一的确定你保护的文件或流,例如你可以利用这个 content ID 在数据库里追踪你保护的内容。

(6) 配置你的编码 session,开始编码过程,然后发布。

4 DRM 的不足及展望

(1) 利用 DRM 加密,产生的密钥一般有两把,一把公钥(public key),一把私钥(private key)。公钥用于加密节目内容本身,私钥用于解密节目,私钥还可以防止当节目头部有被改动或破坏的情况,利用密钥就可以判断出来,从而阻止节目被非法使用。上述这种加密的方法,有一个明显的缺陷,就是当解密的密钥在发送给用户时,一旦被黑客获得密钥,即可方便解密节目,从而不能真正确保节目内容提供者的实际版权利益。当然,有一种更加安全的加密方法是使用三把密钥,即把密钥分成两把,一把存放在用户的 PC 机上,另一把放在认证服务器,要解密数字节目,必须同时具备这两把密钥,方能解开数字节目。这样当解密密钥在发送给用户时,即使被窃取,也仍然无法解开加密的内容。

(下转第 56 页)

(上接第 40 页)

对内容提供商而言,必须意识到传送密钥工作的重要性,要严防密钥在传送时被窃取。互联网上的黑客总是喜欢钻这些漏洞。因此我们需要一种安全的严密的方式传送密钥,以保证全面实现安全保护机制。

(2) 由于缺乏统一的标准,DRM 技术的进一步推广受到阻碍,不过 DRM 的商业前景依然巨大。据某分析公司的最新研究,DRM 技术应用将增长十倍,到 2006 年,20% 的内容提供商将采用 DRM 技术。报告声称,随着越来越多的公司逐渐认识到保护知识产权的重要性,DRM 技术因此将得到突飞猛进的发展。就连微软也将在它的"下一代安全计算基础"中把 DRM 作为关键技术。

参考文献

1 John S. Erickson. Information Objects and Rights Management[J]. D-Lib Magazine,2001.04. http://www.dlib.org/dlib/april01/erickson/04erickson.html

2 K. G. Saur München. Functional Requirements for Bibliographic Records[M]. IFLA Study Group on the Functional Requirements for Bibliographic Records, 1998. http://www.ifla.org/VII/s13/frbr/frbr.htm.

3 EDITEUR ONIX International Standard[S],1998.08. http://www.editeur.org/onix.html.

4 T. Berners-Lee, R. Fielding. Uniform Resource Identifiers (URI)[S]. IETF RFC2396,2005.02. http://www.ietf.org/rfc/rfc2396.txt

5 Andrea Pruneda. Developing a License Provider Service for Windows Media Encoder[EB/OL], MSDN Library,2002.11. http://msdn.microsoft.com/library/

6 Jim Skinner. Protecting Audio and Video Content with Digital Rights Management [EB/OL], MSDN Library, 2004.04. http://msdn.microsoft.com/library/