基于 Java SIM 卡的流媒体数字版权管理研究①

A Study of Streaming Media Digital Rights Management Based on Java SIM Card

王明华　钮心忻　杨义先　(北京邮电大学网络与交换技术国家重点实验室 100876)

摘要:为了解决移动网络中流媒体业务的数字版权保护问题,便于对数字内容进行使用控制和计费管理,提出一套用于移动网络的流媒体数字版权管理系统,基于移动终端中的 Java SIM 卡开发了数字版权管理代理,在版权提供商和终端用户之间建立安全的密钥分发机制,使用 AES 算法对于 MPEG 结构中的 I 帧的宏块前 16 个字节进行加密,能够在移动终端上以很低的计算代价完成数字版权管理。

关键词:数字版权管理 Java 卡 流媒体 安全

1 引言

随着移动通信网络和终端技术的迅速发展,移动用户不仅可以获取文字、图片、铃声、动画等传统服务,还可以获取到数字音乐、视频节目等丰富多彩的流媒体服务。如何管理这些流媒体数据的版权,防止盗版以及不合理的使用,如何对于数字内容的使用进行控制和计费,来保护内容提供商、网络运营商、终端用户的利益就成为一个亟待解决的问题。

Java SIM(Subscriber Identity Module)卡是用在移动终端上的抗篡改安全设备,能够容易的在上面构建安全的计算环境,被用于移动用户入网时的身份鉴权和认证。我们以移动终端上的 Java SIM 卡为中心,建立了一套移动网络中的流媒体数字版权管理系统(Streaming Media Digital Rights Management, SMDRM),采用数字内容和权限分离的方式,将数字内容保存在移动终端上,将数字版权和对于版权的管理部署在 Java SIM 卡上。卡上的 SMDRM 代理通过安全信道和版权提供商进行信息的交换,并获取版权对象。服务提供商将流媒体的关键部分进行有选择的加密后通过网络发布,用户在移动终端上由浏览器提供的资源定位信息选择播放;流媒体播放器开始数据下载的同时,依据下载到的流媒体标识符向 SIM 卡上的 SMDRM 代理请求版权,在得到版权许可后使用流媒体解密密钥对于数据进行解密播放。

2 流媒体数字版权管理研究

DRM 系统是商业、法律和技术因素的融合,使得数字产品能够被安全的交易[3]。应用于数字对象中的数字版权可以看作是在提供者和请求者之间进行交易的结果。请求者在购买数字内容的同时和提供者达成协定,得到对于数字内容的使用权利许可并接受一定的使用限制,DRM 将这一协定转换为数字版权,强迫用户在存取数字内容的时候遵守。

DRM 系统首先通过对于数字对象使用的限制,来保证数字对象在付费以后才能够被使用,从而保护数字对象的拥有人;其次通过阻止没有获得授权的用户对数字对象的访问来保护诸如未成年人等数字对象的使用者;再次通过对于访问次数、访问权限和访问时间的限制来保护数字对象本身;最后通过 DRM 还可以用来追踪数字对象的存取[4]。

从功能实现的角度来分析,移动网络中流媒体数字版权保护系统主要包括内容提供商,版权提供商、SMDRM 代理和移动终端四个部分。

移动终端和 Java SIM 卡构成用户终端,用户通过

① 本课题得到国家重点基础研究发展规划项目(TG1999035804)、国家自然科学基金项目(60473016)教育部优秀青年教师资助计划项目资助

终端来存取受保护的数字内容。SMDRM 代理作为一个嵌入的可信任实体运行在卡中，用来对于数字内容进行许可和限制，并通过和版权提供商进行相互的认证，获取版权对象。移动终端上的流媒体播放器能够和卡上的 SMDRM 代理交互，通过安全信道获得用于解密当前流媒体内容的密钥信息。

内容提供商是发布 DRM 内容的实体，它对于所提供的数字流媒体内容进行加密，并通过网络发布。在用户终端的请求下，能够将数字内容从各种信道传送到移动终端上。

版权提供商对于 DRM 内容的许可和限制进行管理，并产生版权对象。版权对象是一个基于 XML 的文档，用来表述和一系列相关联的数字内容的权限信息。版权对象被传递到 SMDRM 代理，用来限定版权数字内容如何被使用。如果版权数字内容没有相关联的版权对象，那么数字内容不能够被解密，从而不能被使用。SMDRM 代理保证了版权数字内容只能在版权对象许可的范围内使用。

用户可以通过网络或者通过 SMDRM 代理向版权提供商购买版权，并在移动终端上通过网络下载 DRM 流媒体内容。移动终端的流媒体播放器在开始接受到流媒体内容的时候，根据流媒体的标识符，向 SMDRM 代理请求流媒体版权。SMDRM 代理在本地的版权库中寻找匹配的版权对象，如果找到许可的版权，那么将版权对象中的解密密钥交给移动终端的流媒体播放器。如果没有找到，那么提示用户 SMDRM 代理需要通过网络向版权提供商申请版权对象，在得到用户许可后，SMDRM 代理和版权提供商进行互相认证，并由版权提供商向 SMDRM 代理下发相应的版权对象；SMDRM 代理根据版权对象中对于时间、使用次数的规定对于版权对象进行本地管理，在需要的时候向流媒体播放器提供相对应的解密密钥。

3　流媒体加密技术研究

随着移动终端和无线网络技术的不断发展，特别是基于无线网络的 MPEG－4 视频流技术的进步，使得诸如视频点播（Video－On－Demand，VOD），多媒体信息服务（Multimedia Massaging Service）等无线流媒体应用开始迅速繁荣。基于移动网络的流媒体数据业务的安全分发就成了研究的焦点。

MPEG（Moving Pictures Expert Group）自身并没有为数据的安全传送提供相应的加密机制。在 MPEG 编码完成以后，有两种加密机制来为数据提供安全保障。一种是加密 MPEG 数据流中特定的一部分；另一种是加密全部 MPEG 数据流。移动终端的计算能力有限，因此在我们的数字版权保护系统中不能采用对于流媒体内容全部加密的方式。

MPEG－1 和 MPEG－2 视频编码是采用帧间 DPCM 和帧内 DCT 相结合的方法。MPEG－4 采用的是基于对象的视频编码，编码单元是对象，它主要是针对纹理、形状和运动三种信息的编码技术。依据 MPEG 帧的时间结构，选择性加密算法[5]只对帧内编码 I 帧进行加密。I 帧使用的是 JPEG（Joint Pictrues Expert Group）编码，是前向预测编码和双向预测编编码的基础。B 帧和 P 帧是基于 I 帧进行的预测编码，在 I 帧被加密后，B 帧和 P 帧不能被准确的被播放。

Gunhee Kim 等[6]提出，由于 I 帧是在 Huffman 编码和运动长度编码以后产生，因此对于 I 帧的宏块开始 8 个字节进行加密就足以破坏媒体信息的可视质量。采用了最小代价加密机制，充分利用 MPEG 结构的特点，使用 DES 对于 I 帧的开始 8 个字节进行加密，或者对于 I 帧、P 帧和 B 帧的开始 8 个字节都进行加密，能够达到和对于媒体全部信息进行加密相仿的效果，并且加密以后的数据长度和未加密以前的数据长度一致。

在我们的流媒体数字版权管理系统中，为了保证数字内容安全，并尽可能的减少移动终端在播放流媒体时候进行解密引入的计算代价，我们采用对于流媒体的 I 帧宏块开始的 16 个字节使用 AES 算法进行加密。

4　基于 Java SIM 卡的数字版权代理

从第二代移动通信系统开始，移动终端开始采用智能卡作为国际移动用户身份识别模块，用于网络对于用户身份的鉴权。在智能卡中保存着用户的密钥，并根据网络送来的挑战随机数，按照规定的鉴权算法进行运算后返回应答，从而完成网络对用户的身份鉴权。我们在本文将用于 GSM、CDMA 和 WCDMA 中的鉴权智能卡通称为 SIM 卡。

Java Card 除了具有传统智能卡的数据安全性之

外,它最大的特点就是 Java 技术所特有的平台无关性。Java SIM 卡是采用了 Java Card 技术的 SIM 卡。Java Card Applet 是遵从 Java Card 规范要求,使用 Java 语言编写能够运行在 Java Card 上面的应用程序,从而能够在移动终端上动态的提供增值业务。Java SIM 卡的管理可以通过符合 GSM3.48 协议规定的加密短消息空中下载(Over To Air, OTA)的方式进行,实现应用的远程下载、删除、维护、更新和管理。在 Java SIM 卡发售以后,运营商或者独立的服务供应商在获得授权后,可以把新增服务动态下载到卡上。随着卡上 Applet 的增加,Java SIM 同时也可用作数字版权管理、电子钱包、医疗保险等功能,从而在移动用户终端上构成多应用可信计算平台。

我们基于 32 位的 RISC 智能卡芯片,实现了 Java Card 2.2.1 规范,完成了 GSM 框架要求的功能和接口,构建了基本的 Java SIM 卡多应用可信计算平台。在此平台的上开展移动 DRM 系统的研究,开发了用于 SMDRM 代理的 Applet。

SMDRM 代理在卡内对于版权对象进行管理,因此版权对象不能被外界窃取、伪造和修改。如果版权对象限定了能够被访问的次数或者能够被访问的时间,那么 SMDRM 代理通过在卡内维护版权对象的状态信息,可以保证版权信息不会被滥用。

5 实验结果

基于 Java SIM 卡实现的流媒体数字版权管理系统引入的时间开销主要包括三个部分。第一部分是移动终端在播放流媒体时候执行解密操作引入的时延;第二部分是移动终端向 Java SIM 卡上的数字版权代理请求解密密钥引入的时延;第三部分是数字版权代理通过网络向版权提供商请求版权对象引入的时延。

基于 ARM9 处理器的移动终端执行一次 128bit 的 AES 解密操作用时 0.15ms,由于 I 帧在整个帧序列中占的比例很小,因此在主观评测时候感觉不到时延的存在。

在播放流媒体时候,移动终端播放器需要通过安全信道向版权管理代理申请解密密钥。在基于 ARM7 处理器的 Java SIM 卡上进行测试,版权管理代理使用 DES 算法构建的安全通道,完成一次密钥传递用时 319ms;使用 AES 算法用时 308ms,使用 512bitRSA 算法用时 559ms,使用 1024bitRSA 算法用时 1154ms。

数字版权代理通过网络向版权提供商申请版权对象平均用时 3.8s。该操作用时最长,但只是发生在第一次使用本地没有的数字内容时才会发生。

6 总结

移动网络中流媒体数字版权管理系统采用数字内容和权限分离的方式,允许用户随意对于流媒体进行下载。由于 SMDRM 代理存在于抗篡改的 Java SIM 卡中,因此在没有从 SMDRM 代理取得相应的权限之前,流媒体播放器无法对于数字内容进行正确的播放。从而在移动终端以很少的计算时间为代价,完成了流媒体数据的安全分发和版权管理。通过对数字内容加密技术的改进,可以将该系统从针对移动流媒体的 DRM 推广到其它数字业务中去,这是我们今后研究工作的重点。

参考文献

1 DRM Architecture [J/OL], http://www.openmobilealliance. 2004.7.15.

2 DRM Specification V2.0 [J/OL], http://www.openmobilealliance. 2004.12.10.

3 Willem Jonker and Jean – Paul Linnartz. Digital Rights Management In Consumer Electronics Products [J], IEEE SIGNAL PROCESSING MAGAZINE. 2004. 82 – 91.

4 James Simon, Jean – Noel Colin. A Digital Licensing Model for the Exchange of Learning Objects in a Federated Environment [C]. Proceedings of the First international Workshop on Electronic Contracting. 2004. IEEE.

5 G. Spanos and T. Maples. Performance Study of a Selective Encryption Scheme for the Security of Networked, Real – time Video[C]. Proceedings of 4th International Conference on Computer Communications and Networks . 1995.

6 Genhee Kim. Dongkyoo Shin and Dongil Shin. An Efficient Methodology for Multimedia Digital Rights Management on Mobile Handser[J]. IEEE Transaction on Consumer Electronics. 2004. Vol. 50 No 4. 1130 – 1134.