基于可信计算的 DRM 互操作研究

邱 罡[1] 王玉磊[2] 周利华[1]
(西安电子科技大学 CNIS 教育部重点实验室 西安 710071)[1] (南阳理工学院网络中心 南阳 473009)[2]

摘 要 出于对自有数字内容产品的保护,不同的内容提供者采用不同的保护方法,同时也为消费者带来了数字内容使用上的不便。分析当前 DRM 在主流开放式操作系统中实现时存在的问题,指出可信计算(Trusted Computing, TC)环境下 DRM 互操作实现的可靠性,并给出一种基于可信计算的安全的互操作解决办法。

关键词 数字版权管理,互操作,可信计算,DRM 模块

Study on the Interoperability of DRM Based on Trusted Computing

QIU Gang[1] WANG Yu-lei[2] ZHOU Li-hua[1]
(CNIS Key Laboratory of the Education Ministry, Xidian University, Xi'an 710071, China)[1]
(Network Information Center, Nanyang Institute of Technology, Nanyang 473009, China)[2]

Abstract For the protection of their own digital contents, different content provider adopts various DRMs, which makes consumer discomfortable. By analyzing some flaws of the realization of DRM based on mainstream operating system today and indicating the reliability of the interoperability of DRM based on Trusted Computing, a secure architechture for the solution of interoperability based on Trusted Computing was proposed.

Keywords Digital rights management, Interoperability, Trusted computing, DRM module

1 前言

随着计算机网络、宽带技术以及多媒体计算机编码算法的发展,通过互联网进行的数字内容交易变得越来越便利。人们在通过互联网获取媒体信息的同时也可以得到与原始数据完全相同的复制品。由此引发的盗版和侵权问题极度困扰着网络运营商和内容提供者,严重阻碍了网络数字媒体的发展。数字作品的版权保护问题已成为近年来法律界和 IT 业界所面临的一个重要的热点问题和难点问题。

在充分利用数字内容产品在线分发的便利的同时,为了能避免数字内容产品非法再分发,数字内容提供商提出了数字版权管理技术(Digital Rights Management, DRM)。DRM 系统通过将数字内容产品和许可证绑定的方式限制的数字内容产品使用,只有在满足许可证要求的条件下用户才可以使用数字内容产品,其目的就是通过技术的手段,在整个生命周期内,对数字内容产品的知识产权进行保护,确保数字内容产品的合法使用和传播。现有的采用 DRM 技术的产品包括:Apple iTunes' Fairplay [1], Windows Media DRM [2], the Open Mobile Alliance's (OMA) DRM Scheme [3]等。

本文在介绍 DRM 和可信计算(Trusted Computing, TC)的基本原理的基础上,分析 DRM 面临的一些基本问题,提出一种基于可信计算环境下的互操作模型。

2 DRM 基本概念

2.1 DRM 基本原理

数字版权管理的原理是:使用技术手段,对数字内容在分发、传输和使用等各个环节进行控制,使得数字内容只能被授权使用的人按照授权的方式,在授权使用的期限内使用。DRM 的功能模型主要分为 3 个部分:内容服务器、许可证服务器和客户端[4],如图 1 所示。内容服务器通常包括存储数字内容的内容仓库,存储产品信息的产品信息库和对数字内容进行安全处理的 DRM 封装块;许可证服务器包含权利库、内容密钥库、用户身份标识库和许可证生成器,该模块主要对用户发起的申请请求做出反应,根据用户申请的权限和用户的信息发放相应的许可证,还可以实现用户身份认证和触发支付等金融交易事务;客户端主要包含控制器和数字内容使用工具,并负责和许可证服务器进行交互。授权用户得到的许可证中包括了使用权限和解密密钥等信息,它可以存储在硬盘或者其它移动存储设备中。

2.2 DRM 中基本问题

2.2.1 易用性及互操作问题

DRM 技术使得媒体的传统使用方法(如:CD 的二手交易、家庭范围内将数字媒体转移至便携设备或其它设备上的使用,与家人或朋友分享数字内容产品及私人拷贝等)发生了改变,而任何不再支持传统媒体使用方法的 DRM 技术都会遇到是否被接受的问题。如今,由于大多数的 DRM 系统采用的保护方式不尽相同,各 DRM 系统都或多或少地存在与用户使用习惯上的冲突,都会带给用户某种程度上的不适感。许可证条文中对于使用范围、方法、时间等的规定,也使得用户在购买数字内容产品后不可能永远无限制地使用它。

到稿日期:2008-01-22 本文受国家自然科学基金(60672117)资助。
邱 罡 博士生,讲师,主要研究领域为网络信息安全;王玉磊 硕士,讲师,主要研究领域为计算机网络安全;周利华 博士,教授,博士生导师,主要研究领域为计算机网络安全理论与技术、多媒体技术等。

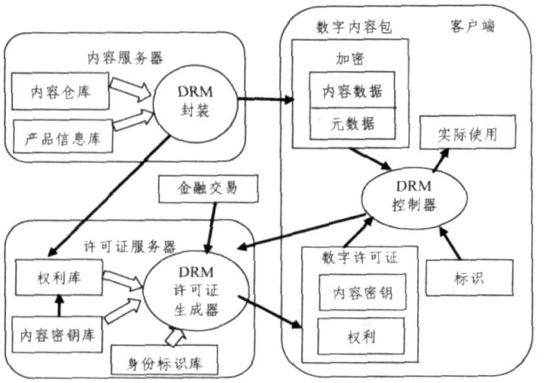

图 1　DRM 基本结构

文献[5]中对 DRM 互操作进行了充分的分析,提出了三种互操作方法来建立互操作的 DRM 系统:完全格式互操作,连接互操作及配置驱动互操作。完全格式互操作是指 DRM 系统中所有参与者都使用统一的标准。虽然该方法会极大地方便消费者,但是为所有参与者和不同商业模式建立一个统一标准是很难的。连接互操作指设备连接到一个在线转换服务器。每次消费者想转换一个数字内容产品到一个不同的设备,则都需要在线连接获取服务。因此,服务提供商就有可能监视消费者对数字内容的使用情况,从而产生隐私权问题。配置驱动互操作方式下,终端用户通过从内容提供商下载相应的工具,在本地转换受 DRM 保护的内容。

通常,数字内容提供商会采用其独有的方式来保护数字内容产品的安全性,同时也很少(几乎没有)考虑到其他 DRM 系统的互操作性。因此,消费者也就不能在其喜欢的设备上播放其购买的数字内容产品。如何提高不同 DRM 系统间的互操作性,是用户及内容和服务提供商共同关心的问题,否则将会降低数字内容产品对消费者的吸引力并阻止数字产业的发展。提高数字内容产品的互操作性,不仅使其在性能和价格上与盗版产品相比处于有利地位,而且会促进合法数字内容产品的广泛采用。

2.2.2　技术问题

DRM 技术上所面临的问题之一是如何确保数字内容的使用是安全的,确保可信的用户决不会得到受保护的产品的非法拷贝。这就要求必须有某种可以保证设备是可信的机制,因此,仅仅依靠密钥保护是不够的。现在通常采用一种"含糊的安全性(Security by Obscurity)"的技术方法来提高数字内容的保护,如 Windows Media DRM 对其技术标准保密,Apple iTunes'Fairplay 则采用一种封闭式系统禁止其它内容提供者和属主的随意使用。此外,用来解密加密内容的密钥也需要分发到用户,该密钥应妥善保存以防止用户利用它对数字内容破解。但是隐藏在用户计算机上的解密密钥还是会面临被识破和攻破系统的危险。当前主流操作系统由于其开放性,特权指令的使用,多任务并发执行及恶意驱动程序的攻击,使得数字内容在解密和播放过程中存在被侦听的可能[6]。

上述问题表明:仅仅依靠加密技术在现有的开放式操作系统环境下,时刻都会受到来自恶意软件、病毒及非法使用者的破坏,因此迫切需要一个有硬件支撑、防篡改环境的保护,可信计算技术的产生和发展为 DRM 的安全使用提供了很好的技术支持。

3　可信计算概述

最近几年,对计算机安全和可靠性的依赖促进了可信计算(Trusted Computing,TC)技术的发展。1999 年,IBM,HP,Intel,微软等美国著名 IT 企业发起成立了可信计算平台联盟 TCPA(Trusted Computing Platform Alliance)。并于 2003 年,TCPA 改组为可信计算组织 TCG(Trusted Computing Group)[7]。TCG 为了向应用软件及平台间提供信任保证,定义了一组提供基于硬件的信任根的标准和一组基本功能。TCG 中的信任根是指主板上的被称为 TPM[8](Trusted Platform Module,可信平台模块)的硬件组件。TPM 通过与 TPM 永不分离的根密钥来保护数据,并提供基本加密功能如随机数生成、RSA 密钥生成和 RSA 非对称密钥算法。更重要的是,TPM 提供了平台完整性的度量,存储和报告,进而提供了严格的保护和证明。

TPM 包含一组平台配置寄存器(Platform Configuration Registers,PCRs)。对受保护的数据和程序代码的度量值反映了被度量对象的特性和特征,如完整性、程序运行状态及配置值。特定的 PCR 的值是通过在当前值上连接新的度量值并使用 SHA - 1 运算得到,即:PCR[i + 1] ←SHA - 1(PCR[i] ‖新度量值)。因此 PCR 值可以记录下运行平台从引导到加载操作系统再到加载运行程序的完整性和状态。

可信计算技术的目标是实现以下 4 个方面的安全功能:

1. 内存屏蔽(Memory Curtaining)　内存屏蔽是指通过一种强健的,硬件增强型的内存隔离特性,避免程序间相互读写内存中内容。

2. 安全 I/O(Secure Input/Output)　某些入侵者通过按键记录器或屏幕扑捉器来收集用户计算机上的信息,如:用户 ID、口令、文档及电子邮件的内容。安全 I/O 提供了一个从键盘到程序再由程序到屏幕的安全路径。

3. 远程证明(Remote Attestation)　平台可以利用完整性度量和存储来产生一个完整性报告,并通过一种称为"证明"的挑战——响应机制传递给其它平台。在证明过程中,平台 A(挑战者)发送证明挑战信息到平台 B(证明者)。平台 B 上的一个或多个 PCR 值使用受 TPM 保护的身份证明密钥(Attestation Identity Key,AIK)签名后提供给挑战者。挑战者通过将签名值和预期的值相比较来验证。证明提供了平台当前完整性、状态和配置的认证。在单个平台内,一个运行程序可以发送证明挑战信息给另一个运行程序以验证其完整性或运行状态。

4. 封装存储(Sealed Storage)　TCG 的目的在于为秘密信息如加密密钥等提供可靠的、基于硬件的保护。由于开放的计算机平台可以运行任何软件,这种目的在于确保被保护的秘密信息只有在平台的软件状态完全符合已定义的度量标准时才可使用。TCG 的封装存储特性可用于将一个受保护的秘密信息和特定的软件配置绑定。如果配置值不符合定义的标准,封装的密钥将不会被释放,从而避免密钥遭到病毒破坏或被入侵者利用。

4　基于 TC 的互操作框架及策略

本节中首先在给定假设前提下,给出了一种在可信计算

提供的安全环境下解决互操作问题的模型,并介绍该模型可实现的基本功能,以及在该模型下实施的安全策略。

4.1 基本假设

·假定在本框架提供的安全环境下,所有数据都是受抵抗攻击保护的,不再特别关注用户层的加密。

·为简化起见,本文中假定将实际系统中由内容提供方、服务提供方、DRM 工具提供方以及消费电子生产商等完成的功能,合并为内容提供方来实现。该假定并不会影响本文提出的模型在一般场景下实现的功能。

·内容提供方使用内容加密密钥 cek 对初始内容加密。与初始内容相关联的是由内容提供方定义的限制消费者行为的一组权利。权利,cek 以及内容标识被用来构成许可证书,并由内容提供方加密并签名。

4.2 基于 TC 的框架模型

模型框架如图 2 所示,其中包含以下实体:

DRM 模块是本框架中的关键组件,其功能是通过解读许可证来向应用层提供几种服务,同时为受保护内容提供中心密钥存储。由于其处于可信框架中,接受系统的认证,同样也是被所有应用程序信任的。该模块包括 3 个基本组成部分:许可证解析器、许可证转换管理器和密钥库。

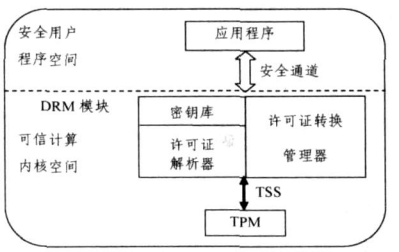

图 2 基于可信计算的框架结构

许可证解析器提供有关许可证验证和解释的服务。消费者必须提供其许可证,由 DRM 模块来决定其是否可以访问数据。如果访问被授权,则 DRM 模块从密钥库中返回内容密钥,然后由播放器播放内容。

许可证转换管理器使用 MPEG-21 REL(Rights Expression Language,权利描述语言)来实现对各种权利描述的实现。MPEG-21 同样为内容识别提供便利,DRM 模块使用唯一的标识将内容与许可证和密钥库中的密钥关联在一起。当外部内容进入系统时,即其使用的是不同于系统内的 REL 时,许可证转换子系统将外部许可证转换为 REL,以便被许可证解析器处理。许可证转换管理器采用一种可扩展的结构,即为不同的许可证格式使用各种插件。转换管理器可用来输出一个其它支持格式的 MPEG 许可证。DRM 模块的导入/导出功能使其实现和其它系统的互操作。

密钥库中保存的是用于系统中受保护内容的密钥。DRM 模块确保仅当请求的操作被许可证允许时才分发内容密钥。密钥库采用表格的组织形式,其中包含内容密钥及唯一的内容标识。密钥库采用加密文件实现,并在安全环境建立起来后由模块进行解密。这是由于 TPM 封存了密钥库的主密钥,使其只有在特别的系统完整状态下才可以被访问。模块也只有在系统安全时才可以恢复使用主密钥。

4.3 安全协议

4.3.1 基本标识

本节给出安全协议中使用的基本标识,如图 3 所示。

DRM 模块(DM)的基本功能:

1. $Seal(H(DM), x)$。该函数的功能是由具有完整性度量值 $H(DM)$ 的 DM 对 x 进行封装。x 只能是在 DM 对应的 PCR 值为 $H(DM)$ 时才可解封。

2. $UnSeal(H(DM), x)$。当前 $H(DM)$ 值是对 x 进行封装时的值时,可使用该函数解封 x。

3. $Attest(H(DM), PK_{DM}) = Sign_{SK_{TPM.AIK}}(H(DM) | PK_{DM})$。该函数返回一个证书,该证书是由 $SK_{TPM.AIK}$ 对 DM 的公钥及其完整性值连接的签名而得到的。

M	受保护内容的明文
CEK	内容加密密钥
R	与内容 M 相关联的权利
PK_i	实体 i 的非对称密钥的公钥部分
SK_i	实体 i 的非对称密钥的私钥部分
P	服务提供方
$cert_i$	由实体 i 公钥签名的证书
$\{M\}_K$	若 K 是公钥(私钥),则{M}K 是使用密钥 K 对消息 M 的加密(签名)
$Enc_k()$	使用公钥 K 的加密算法
$Dec_k()$	使用公钥 K 的解密算法
$Sign_k()$	使用密钥 K 的签名算法
$Verify_k()$	使用密钥 K 的验证算法
$H()$	哈希函数
AIK	AIK 由 TPM 产生,在证明协议中用于对提供给挑战者的 PCR 签名,或为认证而对在平台上运行的应用程序的公钥签名。

图 3 基本标识

4.3.2 协议实现过程描述

4.3.2.1 内容和策略分发

在内容分发前,内容提供方 P 首先验证设备 D 的证书,确保其未被撤销且是可用的。进而通过证明来验证设备的完好性及其软件版本是否已是最新的版本。待以上步骤通过后,内容提供方通过安全通道分发 DRM 打包内容。设备 D 存储接收到的加密内容 $\{M\}_{CEK}$ 和用设备公钥加密的许可证 $\{CEK, R\}_{PK_D}$,以及可由内容提供方 P 公钥验证的许可证签名 $\sigma_{PK_P} = Sign_{SK_P}(CEK, R)$。图 4 中描述了具有可信平台支持的设备 D 的消费者一方向服务提供方 P 请求数字内容的挑战—应答过程。整个过程描述如下:

图 4 数字内容和策略分发

1. 由设备 D 的模块 DM 或可由应用程序 APP 向服务提供方 P 发送访问其内容 M 的请求消息。该消息包括使用设备 D 的 AIK 签名的完整性度量值 $H(APP)$ 合并请求内容的身份 ID_{OBJ}。

2. 服务提供方 P 验证请求应用程序的完整性。

3. 设备 D 调用 $Attest(H(DM), PK_{DM})$ 函数,向服务提供方 P 返回使用 $SK_{TPM.AIK}$ 签名得到的证书。

4. 如果服务提供方 P 信任该设备,即设备 D 具有一个真正的 TPM 且是安全引导的,及 DM 的运行哈希值,则服务提

供方 P 加密内容$\{M\}_{CEK}$,许可证$\{CEK, R\}_{PK_D}$,以及许可证签名σ_{PK_p}传回设备 D 的 DM。

通过证明挑战,服务提供方 P 相信设备 D 上的 DM 会执行服务提供方 P 送过来的策略,其中指明了数字内容可以被设备 D 访问的条件。为保护策略和秘密信息的私密性,设备 D 使用自己的完整性度量值对其进行封装。加密内容和策略等秘密信息被隔离在 DM 的应用程序域,和其它应用程序的通信都是受到保护的。

4.3.2.2 策略执行

在加密内容和策略等秘密信息分发后,设备 D 上的应用程序或过程即可发起访问请求。设备 D 的 DM 在按照策略信息检查应用程序的完整性状态后产生一个授权决策。对 REL 进行解析后,由应用程序 APP 播放内容。图 5 给出了当设备 D 上的应用程序 APP 访问内容$\{M\}_{CEK}$时的策略执行过程。下面给出该过程描述。

1. APP 向 DM 发送"播放$\{M\}_{CEK}$"请求。

2. DM 向 APP 发送证明挑战信息。

3. APP 调用 $Attest(H(APP), PK_{APP})$ 响应挑战。

4. DM 将完整性度量值和按照策略期望的值进行比较。如果 APP 是可信的,DM 生成一个会话密钥 k_s,并使用 APP 的公钥加密后,发送给 APP。同时在 DM 内解封 CEK,使用 CEK 解密$\{M\}_{CEK}$;再使用 k_s 加密 M 后发送给 APP。

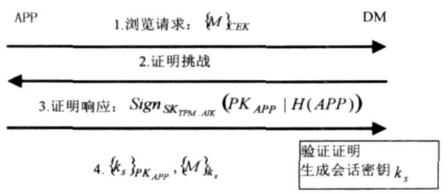

图 5 设备内部的策略执行

4.3.3 安全性分析

通常针对 DRM 系统的攻击有以下 3 种:针对 DRM 协议的攻击;针对客户端设备安全存储的攻击;针对播放应用程序的攻击。其目的都是获取未保护形式的内容产品[9]。针对 DRM 协议的攻击主要攻击的是协议中的客户端和内容提供方之间缺乏相互认证漏洞。针对客户端设备安全存储的攻击通常从安全存储中转储内容密钥或未加保护的内容。针对播放程序的攻击则在使用不安全的程序播放时捕获解密的内容并存储下来。

针对以上问题,基于可信计算的互操作模型提供了以下安全保证:客户端和内容提供方采用远程证明,客户端只有在其度量值得到内容提供方认可的情况下,如:系统已升级并检查没有恶意软件存在等,才可以获取内容产品;客户端得到 cek 和加密内容后存储在受 TPM 保护的 DRM 模块中,杜绝被窃取的危险;内容的解密等操作是在 DRM 模块中完成的,由于 DRM 模块是由 TPM 度量并受 TPM 信任的,因此在此安全环境下的转换同样是可信的。在应用程序度量通过后,通过安全通道传给应用程序播放,而且应用程序之间是相互内存屏蔽隔离的,因而避免其它程序的恶意访问。

结束语 本文针对现有 DRM 系统间实现互操作性的可能性、实施互操作时的技术标准及互操作所使用的协议进行分析,给出了一套在可信计算环境下实施 DRM 互操作的方案,该方案不仅可以实现抵抗现有 DRM 系统中遇到的密钥泄露等攻击,而且为互操作实施过程中内容解密环境提供了安全保证。然而,由于 DRM 系统的复杂性,多种因素尚需要考虑,如权利撤销和迁移等问题,期待在今后的研究中解决。

参 考 文 献

[1] iTunes FairPlay. http://www.apple.com/lu/support/itunes/authorization.html

[2] Microsoft Windows Media Rights Manager. http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx

[3] Open Mobile Alliance. http://www.openmobilealliance.org/

[4] 俞银燕,汤帜. 数字版权保护技术综述[J]. 计算机学报,2005,28(12):1957-1968

[5] Koenen R H, Lacy J, Mackey M, et al. The Long March to Interoperable Digital Rights Management // Proceedings of the IEEE. 2004, 92(6): 883-897

[6] Reid J F, Caelli W J. DRM, Trusted Computing and Operating System Architecture. Australasian Information Security Workshop 2005 (AISW2005). Newcastle, Australia

[7] Trusted Computing Group. TCG Specification Architecture Overview. Specification Revision 1.2. https://www.trustedcomputinggroup.org, April 2004

[8] The Trusted Computing Group. TPM Main Part 1 Design Principles. February 2005

[9] Taban G, Cardenas A A, Gligor V D. Towards a Secure and Interoperable DRM Architecture // Proceedings of the ACM Digital Rights Management workshop DRM '05. Alexandria, Virginia, USA, 2005: 69-78

重视中、英文摘要的编写

国内外公开发行的标准化科技期刊中的文摘已成为科技论文的重要组成部分,读者可根据文摘提供的信息考虑是否阅读、引用原文;如能被利用,才能体现文章的学术价值,提高原文的引用频次。如此看出学术文章中文摘的重要性,它所起的作用不可替代。

1. 中文摘要一般为 200～300 字,英文文摘的长度一般不超过 250words,不少于 150words。

2. 摘要中不涉及图、表、化学结构式以及非公知公用的符号和术语。关键词一般为 3～8 个,每个关键词首字母大写。

3. 文摘是对文献进行主题分析,以此体现主题概念、主题内容等该篇文献最重要的信息,使读者在没有看到全文的情况下,能够很清楚地了解到该篇文献的中心思想。

4. 文摘语言简洁,避免重复的单元与措辞;文摘中的缩写名称在第一次出现时用全称。文字描述中减少对背景信息的介绍;文摘中不涉及该文献谈及的未来计划;首句不得简单重复题名中已有的信息。

5. 文摘包含的信息量要完整,包括目的、过程及方法、结果三方面内容。英文文摘与中文文摘一致,并使用过去时态叙述作者工作,现在时态叙述作者结论。