一种可信计算支持的 DRM 系统及其安全协议研究

王 剑 张志勇 俞卫华 杨丽君
(河南科技大学电子信息工程学院 洛阳 471003)

摘 要 数字版权管理(Digital Rights Management,DRM)系统旨在端到端地保护数字内容的可控使用,然而客户端平台的安全隐患使得数字内容的合理使用受到威胁。在研究可信计算技术的基础上,提出可信计算技术与 DRM 系统相结合的可信 DRM 系统的一般结构,并重点阐述了可信计算技术在许可证分发和数字内容使用两个重点环节中的应用。进一步地,设计并提出一个可信 DRM 系统的身份认证及密钥协商协议,并给出其安全性分析。该协议实现许可证服务器对 DRM 客户端的身份认证及完整性验证,并产生共享密钥保护数字版权的发放。

关键词 数字版权管理,可信计算,远程证明,SKAE,认证协议
中图法分类号 TP309 **文献标识码** A

Trusted Computing-enabled DRM System and its Security Protocols

WANG Jian ZHANG Zhi-yong YU Wei-hua YANG Li-jun
(Electronic Information Engineering College, Henan University of Science and Technology, Luoyang 471003, China)

Abstract Digital rights management is designed to protect digital content usage from end to end. While, the hidden security problems in client system threaten the reasonable usage of digital contents. Through researching on trusted computing technology, a common architecture of DRM combined with trusted computing was presented. Especially, the application of trusted computing in license distributing and digital content usage was introduced. Then, an identity authentication and key agreement protocol for trusted DRM were designed, and also described with its security analysis. Through the protocol, license server can authenticate the DRM client and validate its integrity. Otherwise, the peer can obtain sharing key to protect the digital license distributing.

Keywords Digital rights management, Trusted computing, Remote attestation, SKAE, Authentication protocol

1 引言

DRM(Digital Right Management,数字版权管理)是一种具有端到端保护功能的数字内容管理机制,通过定义生命周期和用户行为等手段实现对内容使用和消费的管理与控制[1]。然而,对 PC 等通用设备而言,DRM 客户端应用程序的运行环境并不是安全的,不能在可信环境中运行。现有的主流操作系统,有很多公开的安全缺陷,缺乏基于硬件的进程隔离机制。在 DRM 控制器解析出被保护内容之后,攻击者可使用恶意软件将解析后的内容非法传递给其他用户,也可通过访问 DRM 控制器使用的进程来获取。同时,由于现有的计算平台缺乏完整性鉴别和保护机制,攻击者可恶意修改移动操作系统或平台固件来达到攻击目的。也就是说,DRM 控制器可能会失去保护数字内容、强制执行使用控制策略的功能。

因此,必须采取一定的防篡改机制,以保证 DRM 应用程序的安全性和完整性,确保数字内容的合法使用。目前的防篡改技术主要分为基于软件和基于硬件两种。前者采用软件技术手段来增加恶意用户剖析、修改、破坏程序源代码的难度,减少程序被破解的可能性;后者则通过专用的安全硬件设备提供可信空间,以保证相关程序的安全运行,防止外部非法程序的攻击[2]。第二类防篡改机制更加强健,能更好地抵抗各种形式的软件攻击,也是目前备受关注的技术热点,即基于可信计算的 DRM 系统。

目前,国内外已有很多学者在这方面进行了研究。张志勇等[3]综述性地探讨了安全终端平台与数字权利可信执行的发展状况,说明结合可信计算技术及其终端平台(包括 PC、移动终端等)标准规范,研究具有互操作性的数字权利可信分发和转移,是目前存在的挑战;Stamm 等[4]通过为终端颁发行为证书来证明终端的可靠性;Sadeghi 等[5]通过可信软件层对 DRM 控制进行认证,并阐述了可信通道的协议过程;邱罡等[6]给出了可信计算环境下 DRM 的互操作性解决方法;Gallery[7]研究了基于远程证明的移动终端平台验证和 DRM 内容保护问题。但这些研究都没有对可信 DRM 系统中具体

到稿日期:2012-08-16 返修日期:2012-11-30 本文受国家自然科学基金项目(61003234),河南省科技创新人才计划(134100510011),河南省高等学校科技创新人才计划基金项目(2011HASTIT015)资助。
王 剑(1978-),女,博士,讲师,CCF 会员,主要研究方向为可信计算、数字版权管理,E-mail:wangjian_migi@sina.com;张志勇(1975-),男,博士后,副教授,CCF 高级会员,主要研究方向为数字版权管理、可信计算与访问控制;俞卫华(1979-),女,硕士,讲师,主要研究方向为网络安全;杨丽君(1988-),硕士生,CCF 学生会员,主要研究方向为数字版权管理与多媒体社交网络。

的认证协议进行设计。本文将对可信计算技术在 DRM 系统中的应用进行系统的分析和研究，首先给出基于可信计算技术的 DRM 系统的一般结构；然后给出可信计算技术在 DRM 系统的许可证分发和数字内容使用两个重要环节中的应用；最后给出可信 DRM 系统中认证协议的一般模型及其安全性分析。

2 相关研究

2.1 数字版权保护系统

一个典型的 DRM 系统的体系结构中主要包括 3 个核心模块：内容服务器、许可证服务器和客户端[2]。

内容服务器主要实现对数字内容的加密、插入数字水印等处理，并将处理结果和内容标识元数据等信息一起打包成可以分发销售的数字内容。另外一个重要功能就是创建数字内容的使用权利，将数字内容密钥和使用权利信息发送给许可证服务器。

许可证服务器是负责设置 DRM 内容权限的逻辑功能实体，用于产生授权对象，主要用来生成并分发数字许可证，还可以实现用户身份认证、触发支付等金融交易事务。

DRM 客户端主要包括数字内容使用工具和 DRM 控制器。数字内容使用工具主要用来辅助用户通过各种形式使用数字内容。DRM 控制器是设备中负责执行 DRM 客户端功能的可信赖功能实体，负责数字内容的解密使用、使用权利的解析验证，以及强制执行附带在 DRM 内容上的访问权限的控制功能，并实现对 DRM 内容的可控访问。

2.2 可信计算

可信计算是 TCG(Trusted Computing Group，可信计算组)针对目前计算系统不能从根本上解决安全问题而提出的，其通过在计算系统中集成专用硬件模块建立信任源点，利用密码机制建立信任链，构建可信赖的计算环境，使得从根本上解决计算系统的安全问题成为可能。TCG 定义的可信平台模块 TPM(Trusted Platform Module)[8]是可信计算平台的信任根，通常是具有密码运算能力和存储能力的安全芯片，可作为密码运算引擎对外提供加解密的密码运算服务，其内部拥有受保护的安全存储单元，可存储密钥等敏感数据。通过 TPM 的功能支持，可信计算平台能够实现可信度量和报告、远程证明、数据保护等安全服务。

可信计算的核心思想是“信任传递”，信任传递是通过度量和证明来实现的。通过度量和证明，信任被延伸到整个计算机系统，而在计算机需要建立可信网络连接的时候，这种信任传递就要被延伸至网络中，远程证明机制[9]就是使信任能够在网络环境下传递给远程被接入主机的方法。通过远程证明，通信双方不仅可以完成身份的认证，而且由于引入了完整性度量报告，还同时鉴别了通信对象的平台环境配置，使得证明请求者可以检测到被证明的计算机变化，这样可以避免向不安全或安全受损的计算机发送私有信息或重要命令，从而大大提高了通信安全性。

3 可信 DRM 系统结构

3.1 基于可信计算的 DRM 系统结构

在 DRM 系统中，通过加密和授权来实现对数字内容的保护，即 DRM 客户端要使用加密的数字内容，必须拥有许可证服务器颁发的合法许可证。基于可信计算的 DRM 系统与普通 DRM 系统最大的不同在于，DRM 客户端中有一个可信平台模块 TPM，DRM 控制器可以通过 TSS(TCG Software Stack，可信软件栈)提供的 TPM 功能访问接口获取 TPM 产生的完整性度量值、密钥、证书等。基于可信计算的 DRM 系统如图 1 所示。

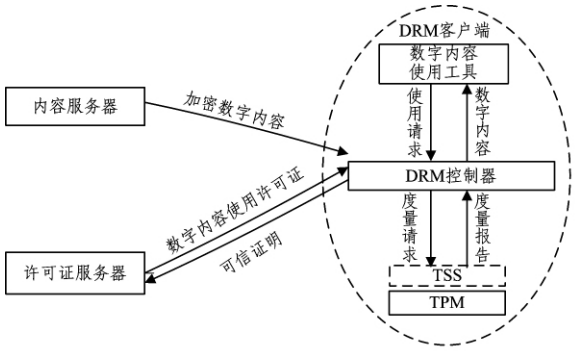

图 1 基于可信计算的 DRM 系统

与普通 DRM 系统不同的是，DRM 客户端包含了 TPM 芯片，并基于 TPM 和 TSS 实现可信的保证。在该系统中，可信度量的实施和报告主要体现在两个过程中：(1)在许可证服务器向 DRM 控制器分发许可证之前，既要验证其是否为被授权的合法身份，还要验证其完整性及运行环境的可信性，这时，作为客户端核心的 DRM 控制器除了实现普通 DRM 系统中数字内容可控使用的功能外，还充当远程证明代理的角色，在验证方服务器和证明方 TPM 之间传递度量结果；(2)在 DRM 控制器将受保护的数字内容交给数字内容使用工具之前，应先验证数字内容使用工具的完整性。此时，DRM 控制器充当完整性值的验证方，对内容使用工具进行完整性检验。

3.2 基于可信认证的许可证分发

许可证的分发是数字版权管理系统的一个关键环节，直接决定了数字内容使用的安全性。在可信 DRM 系统中，数字许可证的申请和分发过程包含着 DRM 客户端向许可证服务器的远程证明过程。许可证申请和分发过程如图 2 所示。

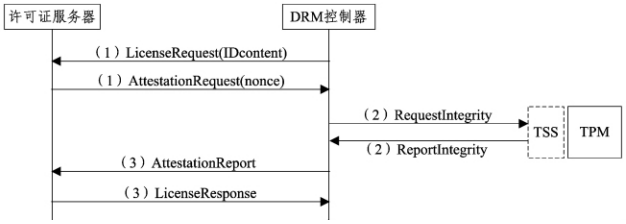

图 2 基于可信认证的许可证分发流程

(1)DRM 客户端中的 DRM 控制器向许可证服务器申请数字内容使用许可证，$ID_{content}$ 是要申请的数字内容的唯一识别码；许可证服务器向 DRM 控制器发出可信证明请求，*nonce* 是伪随机数，用来确保可信证明的新鲜性，以免重放发生。

(2)DRM 控制器通过 TSS 从 TPM 获取完整性度量值；

(3)DRM 控制器将完整性度量结果返回给许可证服务器；许可证服务器对完整性度量结果进行验证，若验证通过，即向 DRM 控制器发放数字许可证。

3.3 基于完整性度量的数字内容使用

对数字内容的可信使用是可信 DRM 系统比普通 DRM

系统更为可靠安全的另一体现。DRM 控制器将被保护的数字内容交付给数字内容使用工具之前，要对播放数字内容的使用工具进行完整性检查，以确认该软件是否是未被篡改的可信软件，流程如图 3 所示。

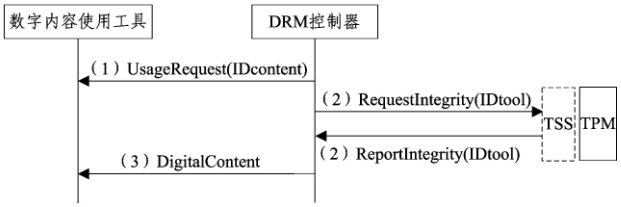

图 3　基于可信度量的数字内容使用流程

(1)数字内容使用工具向 DRM 控制器发出数字内容使用请求，$ID_{content}$ 是要申请的数字内容的唯一识别码；

(2)DRM 控制器通过 TSS 从 TPM 获取数字内容使用工具的完整性度量值，ID_{tool} 是数字内容使用工具的识别码；

(3)DRM 控制器针对度量结果参照完整性期望值进行比对验证，若验证通过，则证明数字内容使用软件是合法软件，将解密后的数字内容交付给数字内容使用工具。

4　可信 DRM 系统的认证协议

第 3.2 节中许可证发放过程首先是 DRM 客户端向许可证服务器远程证明的过程，这个过程要在能够保证通信双方身份互相鉴别真实性的基础上，实现可信度量值的安全传输，以保证可信度量值的真实性、新鲜性及完整性。在普通的基于数字证书的身份认证协议中，终端使用的公钥证书主要用于证明密钥的归属性、完整性和时效性。而在可信 DRM 系统中，DRM 客户端不仅需要通过证书向许可证服务器提供身份证明，还需要向对方申明一些新的属性，比如：密钥产生环境的安全性、平台软硬件配置完整性信息、密钥操作环境的安全性等。TCG 为此专门提出了名为 SKAE(Subject Key Attestation Evidence，主题密钥证言证据)[10] 的 X.509 v.3 证书的扩展项，该扩展项包含了 TPM 产生的完整性度量值以及证明这些度量值真实性和完整性的相关密钥证书信息等数据。因此，SKAE 扩展项可以在身份认证过程中成为完整性度量值的载体，这里给出一个基于 SKAE 证书的可信 DRM 系统认证协议模型，通过该协议，DRM 客户端与许可证服务器之间完成了身份认证、可信验证、密钥协商等过程。下面的介绍建立在读者了解可信平台工作的基本原理以及可信计算所涉及的密钥和证书的基础上，详细内容可以参考 TCG 规范的相关资料[8]，在此不再赘述。

4.1　带 SKAE 扩展项证书的申请

带有 SKAE 扩展项的证书申请过程分为两个阶段——申请 AIK 证书以及申请 X.509 公钥证书；涉及 3 个主要实体：TPM(申请者)、隐私 CA 以及普通 CA。申请流程如图 4 所示。

第一阶段，向隐私 CA 申请 AIK 证书，包括以下步骤：

(1)调用 TSS 中 Tspi_TPM_CollateIdentity Request 函数创建新的 AIK。该函数收集平台的背书证书、平台证书、一致性证书以及新的 AIK 公钥等信息，形成 TCPA_IDENTITY_PROOOF 结构，并由 TSS 产生的一个会话密钥加密，会话密钥的安全由隐私 CA 的公钥来保证。加密后的数据和密钥参数信息保存到结构 TCPA_IDENTITY_REQ 中，该结构作为客户端发送的 AIK 证书请求。

(2)验证平台信息，创建 AIK 证书。隐私 CA 收到 AIK 证书请求消息后，用私钥恢复出用户生成的会话密钥，从而获取明文 TCPA_IDENTITY_PROOOF 结构，并验证其中的平台信息以确定该证书请求时由带有合法 TPM 的平台所产生。验证通过后，隐私 CA 创建 AIK 证书及一个会话密钥加密新证书。然后，隐私 CA 生成 TCPA_ASYM_CA_CONTENTS 结构，将 AIK 公钥摘要及会话密钥保存到该结构中，并用背书密钥(EK)的公钥对该结构加密，确保由指定的接收方接收。

(3)获取 AIK 证书。用户接收到隐私 CA 返回的数据后，调用 Tspi_TPM_ActivateIdentity 函数。该函数用 EK 私钥还原出 TCPA_ASYM _CA_CONTENTS 结构，计算本地 AIK 公钥的摘要并与 TCPA_ASYM_CA_CONTENTS 结构中的进行对比验证。若一致，则 TPM 提取会话密钥，并用该密钥还原出 AIK 证书明文，返回给用户。

第二阶段，向 CA 申请对应的 X.509 公钥证书，包括以下步骤：

(1)调用 TPM_CreateWrapKey 函数创建一对不可迁移密钥。AIK 的私钥只能用于签名 TPM 内部产生的数据，而在认证会话中对 TPM 外部数据进行签名是不可避免的，需要创建一对新的密钥用于对外部数据签名，而 AIK 只能对不可迁移密钥进行证明，因此，只能创建一对不可迁移密钥。

(2)对新创建密钥进行证明。证明需要调用函数 Tspi_TPM_CertifyKey，执行后生成一个由 AIK 签名的数据结构 TCPA_CERTIFY_INFO。该结构中包含描述这对不可迁移密钥的信息，如协议版本号、密钥公钥的摘要及使用算法、PCR 值等。

(3)创建 SKAE 扩展项。用户按 SKAE 扩展项的定义将以上关于密钥的信息组织成相应的数据结构，并将 SKAE 作为证书的一个扩展属性，按照标准格式创建证书请求。最后，用户将请求发送给 CA。通过 SKAE 扩展项可以索引到新创建的 AIK 证书、隐私 CA 的信息、TPM_CERTIFY_INFO 结构等相关数据。

(4)CA 根据 RFC3280[11] 检验证书请求，若符合标准，则会发布带有 SKAE 扩展项的 X509 v.3 公钥证书，并将该证书返回给用户。

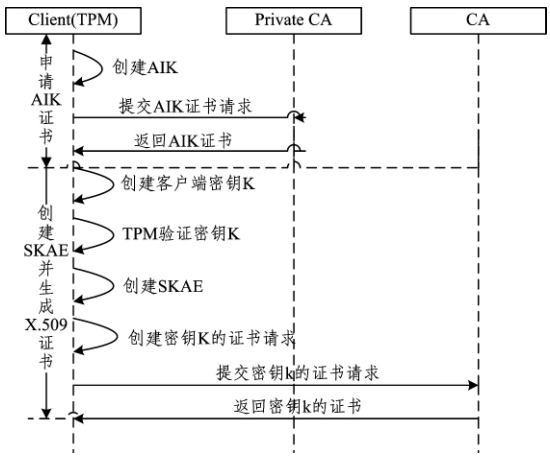

图 4　带 SKAE 扩展项证书的申请流程

4.2 认证协议涉及的密钥及证书

身份证明密钥(Attestation Identity Key,AIK):对应一组公私密钥对,专门对来源于 TPM 的数据进行签名,实现对运行环境测量信息进行签名,从而提供计算平台环境的证言。凡是经过 AIK 签名的实体,都表明已经经过 TPM 的处理。AIK 只用于签名 TPM 内部产生的数据,对于上层数据的签名必须使用其它签名密钥进行。特别地,AIK 只对不可迁移密钥进行证明。

AIK 证书($Cert_{AIK}$):AIK 证书是在 DRM 客户端向隐私 CA(Privacy CA)提交申请之后由隐私 CA 产生,用来证明 AIK 的合法性。AIK 证书不能取代一般的公钥证书作为验证上层应用数据签名的公钥分发证明。

证明加密密钥(Attestation Encryption Key,K_{enc}):非对称密钥对 K_{enc} 是一对不可迁移密钥,可以调用 TPM_CreateWrapKey()函数在需要建立安全连接之前创建,并由 AIK 对其进行证明。由于 AIK 的私钥只能用于签名 TPM 内部产生的数据,不能对由 TPM 外部实体产生的数据进行处理,而在认证会话中对 TPM 外部数据进行加密或签名是难以避免的,因此引入 K_{enc} 作为会话建立时需要的密钥。

K_{enc} 证书($Cert_{enc}$):K_{enc} 证书是带有 SKAE 扩展项的 X.509 v3 证书,用来替代普通身份证书证明客户端身份和可信性。SKAE 证书扩展项中有一个结构 TPMCertifyInfo,该结构实际是由 TPM_CERTIFY_INFO 结构与该结构的签名组成的。TPM_CERTIFY_INFO 结构中包括 PCR 值以及证书中主题公钥的摘要值 pubkeyDigest。TPM_CERTIFY_INFO 的签名是由 AIK 的私钥完成的,因此在验证 TPMCertifyInfo 时,应使用 AIK 的公钥。通过验证 SKAE 扩展项中的 AIK 签名以及主题公钥 PK_{enc} 的摘要可以使验证方相信 K_{enc} 受到 TPM 保护,并且密钥操作都在 TPM 内部完成。带有 SKAE 扩展项的 $Cert_{enc}$ 证书如下所示:

$$Cert_{enc} ::= \{\text{serial\_no}, \text{issuer}, \text{subject}, PK_{enc}, \text{TPM\_CERTIFY\_INFO}, \text{sign}\{\text{TPM\_CERTIFY\_INFO}\} SK_{AIK}, \text{sign}\{Cert_{enc}\} SK_{CA}\}$$

4.3 基于 SKAE 证书的可信 DRM 认证协议

协议的参与方分别为具有 TPM 芯片的 DRM 客户端(DRM Client)以及许可证服务器(License Server)。DRM 客户端中部署的 DRM 控制器(DRM Controller)作为认证协议的执行者,负责与许可证服务器交换消息以及向 TPM 获取度量值等。该协议分为 3 个阶段:证书验证(Certificate Validate)、密钥交换(Key Exchange)以及安全会话(Secure Session)。这里假设,DRM 客户端在每次握手协议开始之前,已创建了不可迁移密钥对 $K_{enc} ::= (PK_{enc}, SK_{enc})$,并申请了对应的 SKAE 证书 $Cert_{enc}$。K_{enc} 是与平台的 TPM 绑定的,因此,只有具有特定的 TPM 才能使用其私钥 SK_{enc}。

协议流程如图 5 所示,其中的符号说明如下:

$Cert_{enc}$:带 SKAE 扩展项的 DRM 客户端证书;

$Cert_s$:许可证服务器的普通身份证书;

$Cert_{AIK}$:AIK 证书;

PK_{AIK}:AIK 公钥;

$K_{enc} ::= (PK_{enc}, SK_{enc})$:DRM 客户端非对称加密密钥对;

$K_s ::= (PK_s, SK_s)$:服务器端非对称加密密钥对;

$Secrets_c$:DRM 客户端计算会话秘钥的秘密值;

$Secrets_s$:许可证服务器端计算会话秘钥的秘密值;

K_s:安全回话密钥。

证书验证:握手双方进行证书交换,当服务器收到客户端提交的带有 SKAE 扩展项的证书后,通过验证 SKAE 扩展项中的 AIK 签名以及主题公钥 PK_{enc} 的摘要可以相信主题密钥受到了 TPM 的保护并且密钥操作都在 TPM 内部完成。验证步骤包括:

(1)根据证书标准字段以及扩展项提供的信息验证 $Cert_{enc}$ 证书的合法性与有效性;

(2)通过 SKAE 扩展项中的 TpmIdentityCredential AccessInfo 索引到 AIK 证书,在验证 AIK 证书的有效性后获得 AIK 公钥;

(3)验证 SKAE 扩展项中 TPM_CERTIFY_INFO 结构的 AIK 签名;

(4)通过计算 TPM_CERTIFY_INFO 结构中表示证书中公钥摘要值的域 pubkeyDigest,验证主题公钥的完整性。

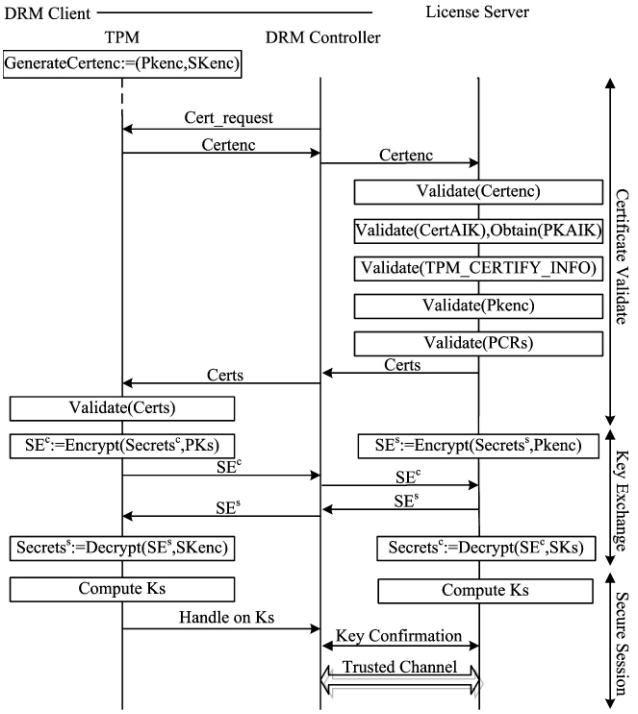

图 5 可信 DRM 认证协议流程

若这些验证全部通过,则证明客户端含有有效的 TPM,并且 K_{enc} 受到了 TPM 的保护。之后,服务器验证 TPM_CERTIFY_INFO 结构中的 PCRs 值,以确认 DRM 客户端平台组件的初始度量值符合服务器的安全要求。如果平台初始状态不可信则不再进行下面的协议流程,服务器拒绝接入。客户端对服务器的认证不再赘述。

密钥交换:协议双方分别用对方的加密公钥对要生成会话密钥的秘密值进行加密交换,以完成密钥协商的过程。

安全会话:双方完成了可信认证和密钥协商后进入安全会话阶段,按照约定计算各自共享的会话密钥 K_s,客户端的会话密钥依然在 TPM 内部生成和保存,DRM 控制器只持有会话密钥 K_s 的句柄,在需要使用会话密钥进行通信时,从 TPM 获取。至此,远程双方之间的安全通信通道已建立,可以用来安全传递许可证服务器向 DRM 客户端颁发的数字许

可证。

4.4 协议安全性分析

端到端的安全：协议遵循远程证明思想，DRM 客户端不仅被许可证服务器验证身份，而且被验证完整性，使得 DRM 客户端平台软硬件环境安全被纳入通信安全保障边界，保证了所建立的许可证分发通道满足端到端的安全保护。

完整的认证链：协议中客户端的身份及完整性认证通过 $Cert_{enc}$ 和 $Cert_{AIK}$ 组成的证书链来保证。$Cert_{enc}$ 由一个 CA 签名，并用其公钥验证有效性。$Cert_{enc}$ 扩展项中的 TPM_CERTIFY_INFO 结构由 AIK 私钥签名，并由 AIK 的公钥进行验证，其完整性和有效性保证了 PCR 值的可信。而同时，该结构中的公钥摘要值域 pubkeyDigest 的验证又保证了主题公钥 PK_{enc} 的完整性。通过这些签名和认证，可以向对方保证平台的完整性值及用于协商的密钥都是被密封和保护在同一个 TPM 内的，是可以被信任的。

隐私的机密性：本着隐私保护的原则，协议设计中所有进行签名、加密的密钥和生成密钥的材料以及 PCR 值都被封存在 TPM 中，平台中的任何其他实体或者通信双方之外的任何第三者都不能获取或访问。而且所有的密钥操作和运算都在 TPM 内部完成，即使 DRM 控制器也只作为建立连接的门户，而不参与任何明文的存取和计算，只能获得最终共享密钥的句柄。

结束语　基于可信计算技术的 DRM 系统能更好地保护数字内容的合法、合理使用。本文首先给出了可信 DRM 系统的一般结构，并具体给出了可信计算技术在许可证分发和数字内容使用两个重要环节的应用。之后，给出了可信 DRM 系统中 DRM 客户端和许可证服务器之间的认证协议，并对其安全性进行了分析，该协议基于可信计算规范定义的带 SKAE 扩展项的证书，实现，许可证服务器对 DRM 客户端的身份认证及完整性验证，能够防止被篡改的、存在恶意软件的客户端平台连接服务器获取数字许可证的危险。在今后的工作中，DRM 客户端平台的可信度量方法以及可信 DRM 认证协议的效率改善将是进一步的研究内容。

参 考 文 献

[1] Rosenblatt W, Trippe W, Mooney S. Digital Rights Management: Business and Technology[M]. New York: M&T Books, 2002

[2] 俞银燕，汤帜. 数字版权保护技术研究综述[J]. 计算机学报，2005，28(12)：1957-1966

[3] 张志勇，牛丹梅. 数字版权管理中数字权利使用控制研究进展[J]. 计算机科学，2011，38(4)：48-54

[4] Stamm S, Sheppsrd N P. Implementing trusted terminals with a TPM and SIDDRM[C]// Proceedings of REM 2007. 2007：73-85

[5] Sadighi A R, Wolf M. Christisn stuble enabling fairer rights management with trusted computing[C]// Proceedings of ISC 2007. 2007：53-70

[6] 邱罡，王玉磊，周利华. 基于可信计算的 DRM 互操作研究[J]. 计算机科学，2009，36(1)：77-80

[7] Gallery E. Authorisation Issues for Mobile Code in Mobile Systems[D]. London: Royal Holloway, University of London, 2007

[8] Grawrock D. TCG Specification Architecture Overview Revision 1.4 [EB/OL]. https://www.trusted computinggroup.org/groups/TCG_1.4_Archiecture_Overview.pdf, 2011-05-01

[9] Sailer R, Jaeger T, Zhang Xiao-lan, et al. Attestation-based Policy Enforcement for Remote Access[C]// Proceedings of the 11th ACM conference on Computer and communications security, CCS'04. 2004：308-317

[10] TCG Infrastructure Workgroup. Subject Key Attestation Evidence Extension Specification Version1.0 [EB/OL]. http://www.trustedcomputinggroup.org/specs/IWG/IWG_SKAE_Extension_1-00.pdf, 2005-06-16

[11] Housley R, Polk W, Ford W, et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280)[Z]. Internet Engineering Task Force, Network Working Group, 2002

(上接第 102 页)

[2] Danezis G, Lesniewski-Laas C, Kaashoek M F, et al. Sybil-Resistant DHT Routing[C]// ESORICS. 2005

[3] Yu H, Kaminsky M, Gibbons P B, et al. SybilGuard: Defending Against Sybil Attacks via Social Networks[C]// Proc. SIGCOMM (Pisa, Italy). New York, NY: ACM Press. 2006：267-278

[4] Urdaneta G. A Survey of DHT Security Techniques[J]. ACM Computing Surveys, 2011, 43(2)：1-35

[5] Rodrigues R, Druschel P. Peer-to-Peer Systems [J]. communications of the ACM, 2010, 53(10)：72-85

[6] Lesniewski-Laas M C, Kaashoek F. Whanau: A Sybil-proof Distributed Hash Table[C]// NSDI'10 Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation. 2010

[7] Viswanath B. An Analysis of Social Network-Based Sybil Defenses[C]// SIGCOMM'10. New Delhi, India, 2010

[8] Castro M, Druschel P, Ganesh A, et al. Secure Routing for Structured Peer-to-Peer Overlay Networks[C]// Proc. 5th Symposium on Operating System Design and Implementation (Boston, MA). New York, NY: ACM Press, 2002：299-314

[9] Dinger J, Hartenstein H. Defending the Sybil Attack in P2P Networks: Taxonomy, Chal-lenges, and a Proposal for Self-Registration[C]// Proc. 1st International Conference on Availability, Reliabilityand Security (Vienna, Austria). Los Alamitos, CA: IEEE Computer Society Press, 2006：756-763

[10] Wang H, Zhu Y, Hu Y. An Efficient and Secure Peer-to-Peer Overlay Network[C]// Proc. 30th Local Computer Networks. Los Alamitos, CA: IEEE Computer Society Press, 2005：764-771

[11] Yu H, Gibbons P B, Kaminsky M, et al. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks[C]// Proc. International Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 2008：3-17

[12] Borisov N. Computational Puzzles as Sybil Defenses[C]// Proc. 6th International Conference on Peer-to-Peer Computing. Los Alamitos, CA: IEEE Computer Society Press, 2006：171-176

[13] 王峰，周佳骏. 基于蚁群算法的对等网络，自适应寻径协议[J]. 计算机工程与应用，2010，17