面向多媒体数字版权保护的委托授权远程证明协议

丰伟宁 张志勇 赵长伟

(河南科技大学信息工程学院 洛阳 471023)

摘 要 现有的委托授权模型主要侧重于受托方是否具有执行委托任务(权利)的能力,没有考虑到受托方平台的可信性;基于此,提出了多媒体环境下基于远程证明(Remote Attestation,RA)的委托授权安全协议,实现了对多媒体数字内容的可信委托授权。协议既保证了委托方对受托方身份与平台完整性的信任、多媒体资源服务器对受托方身份与平台完整性的信任,也实现了多媒体内容的安全访问。阐述了委托验证过程、实体间消息的交互过程以及委托授权可用性验证过程。列举与分析了协议可能遭遇的攻击,同现有的协议相比,应用于数字版权保护(Digital Rights Management,DRM)的委托授权远程证明协议的委托授权过程安全性更高,功能更完善。

关键词 委托授权,可信,远程证明,安全协议

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.4.026

Delegation Authorization Protocol Based on Remote Attestation Applied in Multimedia DRM

FENG Wei-ning ZHANG Zhi-yong ZHAO Chang-wei

(College of Information Engineering, Henan University of Science and Technology, Luoyang 471023, China)

Abstract The main content of existing delegation authorization model is about whether the delegatee can execute the delegated assignment(privilege), and the trust of the delegator's platform is not mentioned. In view of this, the paper presented a delegation authorization security protocol based on remote attestation under multimedia environment. Multimedia contents' trusted delegation authorization can be guaranteed in the protocol. This protocol not only ensures delegator and the multimedia server trust in delegatee's authentication and platform integrity, but also achieves the trusted access to the multimedia. Delegation verification, message interactions between entities were stated. The potential attacks were enumerated and analysed. The delegation authorization protocol based on remote attestation applied in DRM realizes the trusted delegation and the functions are more perfect compared to the existing protocols.

Keywords Delegation authorization, Trusted, Remote attestation, Security protocol

1 引言

数字化媒体的便利传播,使得非法盗版行为日益猖獗。文献[1]提出利用鲁棒水印和脆弱水印对多媒体信息实现水印嵌入来保护内容原创者的合法权益;文献[2]提出了基于MP3动态加密与许可授权的版权保护方案,实现了MP3音频文件的DRM保护。

多媒体委托(转)授权过程对计算平台安全性需求越来越高,远程证明在可信网络连接中起着重要作用;远程证明的目的在于保证终端运行环境的可信性,为远程验证方提供证明方的平台真实运行状态依据[3]。$UCON_{ABC}$(Usage Control: Authorization 授权规则,oBligate 义务,Condition 条件)是使用控制的核心模型[4],文献[5]较早提出基于OM-AM(Objective 目标,Model 模型,Architecture 框架,Mechanism 机制)方法的具有委托授权特点的使用控制模型($UCON_D$),根据委托授权的上下文环境以及授权规则进行授权[6]。文献[7]提出利用加权有向图来表示实体间的信任关系。在委托授权之前进行一致性检验,即必须证明远程实体的证书同本地安全策略相一致。文献[8]的安全委托授权模型中,根据设定的安全规则(如任务状态、受托方工作列表),基于委托组件与授权组件来实现对任务的转授。文献[9]的安全委托授权协议中,委托方直接向受托方发送部分或全部的服务证书信息,受托方接收后发送确认消息给委托方。此模型通过对消息加密、签名实现信息的安全发送,在消息中加入随机值来预防重放攻击。文献[10]分析了基于角色的多种委托授权方式,区分静态与动态委托授权,没有提及可信授权的内容。文献[11]通过在设备证书中注册同一用户的多台设备硬件信息,实现多设备内容共享与数字版权保护。目前的委托授权模型没有考虑不同用户间授权时受托方平台是否可信这一安全问题。一旦将权限授予不可信的受托方,则可能会造成对

到稿日期:2014-05-21 返修日期:2014-08-01 本文受国家自然科学基金(61370220),河南省科技创新人才计划杰出青年基金(134100510006),河南省教育厅科学技术研究重点项目基础研究计划(13A520240,14A520048),河南科技大学研究生创新基金项目(CXJJ-ZR12)资助。

丰伟宁(1989-),女,硕士生,主要研究方向为云计算技术、访问控制等;张志勇(1975-),男,博士后,教授,CCF高级会员,主要研究方向为数字版权管理技术、多媒体社交网络安全、可信计算等,E-mail:xidianzzy@126.com;赵长伟(1971-),男,博士,讲师,主要研究方向为网络信息安全、智能计算等。

多媒体内容的非法操作或权限遭受不可控的扩散。

因此在委托授权关系建立起来之前，必须形成委托方对受托方的信任以及资源服务器对受托方的信任；使多媒体内容必须以一种可预期的、保密的并且可验证的方式[12]进行授权。文中提出的基于远程证明的委托授权模型既实现了多媒体内容的保护，也可以将数字内容访问权限转予其他用户。

2 面向多媒体数字版权保护的委托授权远程证明协议模型

2.1 相关背景

为防止多媒体数字内容（电影、音乐、音视频、流媒体文件）的非法拷贝、未经授权下载等非法行为，国内外众多研究学者对 DRM 系统做了广泛而深入的研究，很大程度改善了数字版权毫无保证的状况。用户可能需要将数字内容访问权限转给其他用户，现有的 DRM 系统限制了不同用户之间进行合理的权利转授。为此本文提出对多媒体内容进行可信的转授权，其既保护了数字版权，也实现了内容的可信分享。

可信计算通过对系统平台组建的完整性度量、存储和报告来确保平台完整性，将远程证明机制引入多媒体转授权模型中。文献[13]通过增加传输层安全性实现可信远程证明，事实上，远程证明中对于身份的证明以及完整性证明是基于安全可信证明信道[14]建立双方间一种单向或者双向的信任关系。此方案包括对等的两客户端进行单向远程证明以及服务器端对客户端进行单向远程证明。委托方通过远程系统（被验证方）发送的平台身份信息以及平台完整性信息来度量平台的可信性，即拥有数字媒体播放或下载权利的用户将权限转予可信任的合法用户。

数字内容受托方（权限接受者）使用平台身份密钥（PIK）对可信密码模块（TCM）中的信息进行数字签名，即可形成平台身份证明以及平台完整性报告。数字内容受托方接收到来自挑战方（委托方或者多媒体服务器）的证明挑战时，将经过签名的平台身份证明以及平台完整性报告发送至挑战方。挑战方首先对签名进行验证，然后根据访问策略以及授权策略决定是否可以将多媒体的浏览、下载甚至继续转授权的权限转予受托方。

2.2 主要组成部分

（1）数字内容委托方（delegator）

委托者（权利转授方）可以通过委托使受托者替代委托者或者协同委托者完成相应的工作。多媒体环境下的委托方即为数字权利的转授权方，可将自身拥有的权利转给其他用户，可以将全部或部分权限转授，如全部或部分播放次数。

委托方在委托授权之前首先与受托方建立单向的信任关系，即委托方对受托方进行认证。委托方为 RA 过程中的验证方，也是 RA 过程的发起者。信任关系建立起来后，委托方将委托授权请求信息以及上下文环境发送至客户端委托授权引用机，由客户端委托授权引用机根据决策规则决定是否允许授权。

（2）数字内容受托方（delegatee）

受托方为 RA 过程的被验证对象（Attestated Object，AO），是 RA 过程的受动者。受托方将身份证明以及平台完整性证明发送至委托方，等待验证结果。若通过验证，受托方向多媒体服务器发送访问请求，多媒体服务器向受托方发送远程证明挑战，受托方继续接受验证，等待验证结果，若验证通过，受托方可以访问相应权限的资源。此协议中的委托方与受托方可以是不同用户的不同设备，也可以是同一用户的不同设备。

（3）客户端委托授权引用机（Client_Delegation Reference Monitor）

客户端委托授权引用机根据委托授权规则以及上下文环境对委托授权请求进行决策，若允许授权，则由委托方和受委托方共同签署委托授权证书。委托方调用客户端委托授权引用机将授权证书发送至受托方，同时将授权证书发送至多媒体服务器。

（4）多媒体服务器

多媒体服务器收到授权证书后向受托方发送证明挑战，表现为 RA 过程的发起者收到证明应答后根据访问决策决定是否允许访问。若多媒体服务器接受受托方的资源访问请求，授权时间范围内，受托方可对资源进行访问，一旦超出授权时间或者超出播放（下载）次数限制，多媒体服务器拒绝其访问。

面向多媒体数字版权保护的委托授权远程证明体系结构如图 1 所示。

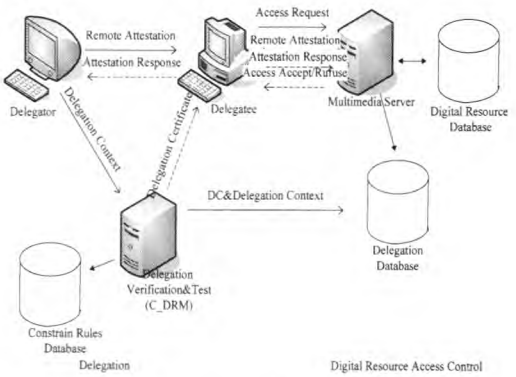

图 1 委托授权远程证明体系结构

3 基于远程证明的委托授权协议

3.1 密钥管理模块

委托方与受托方在进行通信前生成公私钥对；私钥对发送消息进行签名，将公钥公开，以便在对方接收到信息后利用对应公钥进行解密。

会话密钥由委托方和受托方共同协商建立，受托方与委托方分别选择一个大整数，根据 Diffie-Hellman 密钥协商协议协商出共享密钥 k，并不用 k 进行保密通信，而是将 k 作为输入，对其进行哈希计算后的输出结果为 $k^{Delegator\text{-}Delegatee}$，$k^{Delegator\text{-}Delegatee}$，将其作为双方共享的会话密钥。受托方与多媒体资源服务器同样分别选择一个大整数，根据 Diffie-Hellman 密钥协商协议协商出共享密钥 k，将 k 进行哈希函数计算得出共享密钥 $k^{Multimedia\ server\text{-}Delegatee}$。受托方与委托方或多媒体资源服务器通信分别使用密钥 $k^{Delegator\text{-}Delegatee}$ 与 $k^{Multimedia\ server\text{-}Delegatee}$ 对会话加密。

3.2 委托授权的主要原则

委托方与受托方属性可分为委托授权属性与非委托授权

属性[15]；委托授权属性标识了权限拥有方是否具有权限转授的能力，非委托授权属性标识了权限拥有方对多媒体内容浏览以及下载的权限。一旦超出受托方规定的时间(TimeStamp)，权限即被收回，受托方将失去对多媒体内容的操作能力。

委托粒度：委托方对多媒体内容的浏览，下载的权限对应不同的属性(非委托授权属性)；委托方对受托方远程证明后，若接受对方的访问，则将所要委托权限的对应属性继承给受托方，在委托粒度上介于基于角色的粗粒度与基于信任度的细粒度之间。

委托深度：委托深度是指受托方能否将委托方委托(转授)的权限继续转授下去，即对权限的二次转移。可分为单步委托和多步委托，单步委托即只有根节点委托方拥有委托(转)授权权限，多步授权则需要每个转授权的节点都有此权限，可通过对转授权次数(步数)的限制来防止权限的无限转授。

委托广度：委托广度是指多媒体内容委托方最多可将权限转授给受托方的数量，单步委托的权限回收可根据转授次数一次性回收，多步委托的权限回收则需要级联回收。

3.3 协议执行过程

协议过程所涉及到的符号如下。

AO：Attestated Object，被验证对象；RA 过程的受动者，收到验证方的质询后进行可信度量，对验证方作出应答；

AIK：Attestation Identity Key，平台身份证明密钥；

$SK_{Delegatee.\ AIK}$：平台身份证明密钥的私钥；

PCR：平台配置寄存器；

$k^{Delegator\text{-}Delegatee}$：Delegator 与 Delegatee 共享的会话密钥；

$k^{Multimedia\ server\text{-}Delegatee}$：Multimedia server 与 Delegatee 共享的会话密钥；

C_DRM：Client Delegation Reference Monitor，客户端委托授权引用机；

Delegation Verification：委托授权证明；

DC：Delegation Certificate，授权证书；

MMS：Multimedia server，多媒体服务器；

TM：可信度量；

DeleContext：委托授权上下文环境；

TML：完整性度量日志；

MITM：Man-in-the-MiddleAttack，中间人攻击。

此协议过程包括两次远程证明过程以及完成的委托授权过程。基于远程证明的委托授权过程如下：

(1)为确保远程证明的有效性，远程挑战方发送证明请求(Attestation Request)后，需要建立安全信道来共享密钥。

(2)Delegator 向 Delegatee 发送远程证明质询消息，包括 AO_Names、Nonce。

(3)Delegatee 进行完整性度量，即获得反映平台完整性的平台特征度量值，然后将这些度量的摘要置入 PCR，TML 记录了完整性度量记录在 PCR 中的过程。

(4)Delegatee 向验证方 Delegator 发送证明回应。

Delegator 使用 Delegatee 的 AIK 公钥 $PK_{Delegatee.\ AIK}$ 对 Delegatee 的完整性报告进行验证，根据安全策略与访问控制策略判定 Delegatee 是否可以通过远程证明，并将此决策返回给 Delegatee。

(5)Delegator 收到 Delegatee 的相关信息后，将授权判定所需要的信息发送给 C_DRM，包括受托方信息、委托方信息、委托(转授)的权限以及委托授权的上下文环境。

(6)C_DRM 根据约束规则数据库中的委托授权规则以及 Delegator、Delegatee、Permission、Delegation Context 判定受托方是否可以通过授权。

(7)Delegatee 获得 DC 后向多媒体服务器发送资源访问请求，多媒体服务器对 Delegatee 同样做一次单向远程证明。

(8)Delegatee 重新生成一个随机值 Nonce，并将完整性报告发送给多媒体服务器。

(9)多媒体服务器使用 Delegatee 的 AIK 公钥 $PK_{Delegatee.\ AIK}$ 对 Delegatee 的完整性报告进行验证，根据安全策略与访问控制策略判定 Delegator 是否可以授权予 Delegatee，并将此决策返回给 Delegatee。

(10)Delegatee 通过远程证明即可实施被授予的权限。

协议时序如图 2 所示。

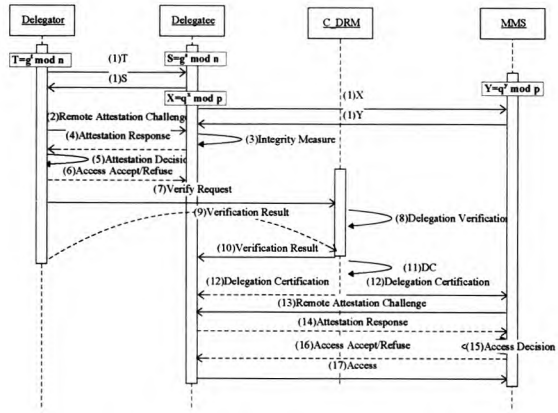

图 2 基于远程证明的委托授权时序

3.4 协议的交互过程

Delegator、Delegatee 与 Multimedia server 公布公钥；Delegator与 Delegatee 约定两个大整数 n，g，然后分别随机选择大整数 s，t，Delegator 计算 $T=g^t \bmod n$，Delegatee 计算 $S=g^s \bmod n$。

Step1 Delegator → Delegatee：T；Delegatee → Delegator：S；

Delegator 计算 $k=S^t \bmod n$；Delegatee 计算 $k=T^s \bmod n$；双方计算的 k 相等，以 k 为输入，进行哈希函数计算即可得到会话密钥；Delegatee 与 Multimedia server 协商密钥与上述步骤相同；

Step2 Delegator → Delegatee：Remote Attestation Challenge；

Step3 Delegatee：Create 160bit nonce & TM；

Step4 Delegatee → Delegator：$\{Signature(PCRs \parallel TML \parallel Nonce, SK_{Delegatee.\ AIK}), PCRs, TML\}_{k^{Delegator\text{-}Delegatee}}$；

Step5 Delegator：Verify($\{Signature(PCRs \parallel TML \parallel Nonce, SK_{Delegatee.\ AIK}), PCRs, TML\}_{k^{Delegator\text{-}Delegatee}}$)；

Step6 Delegator → Delegatee：Access Accept/Refuse；

Step7 Delegator → C_DRM：VerifyReq(Delegatee，DeleContext，TimeStamp，Nonce)；

Step8 C_DRM：Delegation Verification；

Step9 C_DRM → Delegatee:DC;C_DRM → Multimedia server:DC;

Step10 Multimedia server → Delegatee:Remote Attestation;

Step11 Delegatee:Create 160bit nonce &TM;

Step12 Delegatee → Multimedia server:{Signature(PCRs ‖ TML ‖ Nonce,$SK_{Delegatee.AIK}$),PCRs,TML,DC}$_{k_{Multimedia\ server\text{-}Delegatee}}$;

Step13 Multimedia server:Verify({Signature(PCRs ‖ TML ‖ Nonce,$SK_{Delegatee.AIK}$),PCRs,TML,DC}$_{k_{Multimedia\ server\text{-}Delegatee}}$);

Step14 Multimedia server→Delegatee:Access Accept/Refuse;

Step15 Delegatee → Multimedia server:Access Resources。

3.5 抵御攻击类型

1)MITM 攻击

被验证方发送平台可信度量值给验证方时遭受攻击方窃听,成功截获可信度量值,过程如下:

Delegator→Delegatee:Remote Attestation;

Delegatee → Attackers:{Signature(PCRs ‖ TML ‖ Nonce,$SK_{Delegatee.AIK}$),PCRs,TML}$_{k_{Delegator\text{-}Delegatee}}$。

如果攻击方截获了 Delegatee 发送的应答消息,但消息是由 Delegator 与 Delegatee 共同协商密钥的哈希值进行加密的,并且双方密钥协商过程对大整数的选择是随机的,所以攻击方很难解密消息。

2)重放攻击

Delegatee 为可信平台,Attackers 为非可信平台,为了获得授权,Attackers 将 Delegatee 的可信度量值发送给 Delegator。由于 Delegatee 的验证回应消息中加入了 160bit 随机值,Attackers 将同样的平台度量值发送至 Delegator,验证无法通过。

3)合谋攻击

合谋攻击是指两个或多个用户联合起来对系统进行攻击。若有攻击者 A1、A2 分别截获到了受托方向委托方和多媒体资源服务器发送的信息,过程如下:

Delegator→Delegatee:Remote Attestation;

Delegatee→ Attacker A1:{Signature(PCRs ‖ TML ‖ Nonce,$SK_{Delegatee.AIK}$),PCRs,TML}$_{k_{Delegator\text{-}Delegatee}}$;

Attacker A1 → Delegator:{Signature(PCRs ‖ TML ‖ Nonce,$SK_{Delegatee.AIK}$),PCRs,TML}$_{k_{Delegator\text{-}Delegatee}}$;

Multimedia server → Delegatee:Remote Attestation;

Delegatee → Attacker A2:{Signature(PCRs ‖ TML ‖ Nonce,$SK_{Delegatee.AIK}$),PCRs,TML,DC}$_{k_{Multimedia\ server\text{-}Delegatee}}$;

Attacker A2 →Multimedia server:{Signature(PCRs ‖ TML ‖ Nonce, $SK_{Delegatee.AIK}$), PCRs, TML, DC}$_{k_{Multimedia\ server\text{-}Delegatee}}$。

攻击者 A1、A2 截获信息后将信息发送给受托方或多媒体资源服务器,通信并无异常。A1、A2 可多次截获受托方发送给委托方(可以是多个委托方)或多媒体资源服务器(可以是多个多媒体资源服务器)的身份及平台配置信息,对会话密钥进行分析,即便成功破解会话密钥,也只能获得受托方的 PCRs 与 TML 值,由受托方身份证明密钥 AIK 签名的信息仍无法获取,并且攻击者在没有受托方 AIK 的情况下无法伪装成受托者向委托方与多媒体资源服务器发送身份证明与平台证明,所以合谋攻击不会影响到此协议的委托授权以及数字多媒体内容的安全性。

4 委托授权方案分析与对比

面向多媒体数字版权保护的委托授权远程证明协议同现有的委托授权协议以及数字版权共享与保护协议进行了对比,对比结果如表 1 所列,其中,符号"√"、"×"、"+"分别表示对应方案具备、不具备、没有涉及此性能(功能)。

表 1 各方案性能与功能对比

性能 \ 方案	文献[8]协议	文献[9]协议	文献[11]方案	本文协议
验证平台可信性	×	×	√	√
防滥用资源	√	√	√	√
消息保密性	√	√	√	√
消息完整性	√	√	√	√
不可抵赖性	+	√	√	√
抗重放攻击	+	√	+	√
抗合谋攻击	+	√	+	√
证书不可伪造性	+	√	√	√
委托功能	√	√	×	√

方案可信性对比分析:在权利(任务)安全转授方面,文献[8]中委托组件接收到来自委托方的请求后先向授权组件发送检验请求,授权组件根据委托策略以及任务服务管理器的反馈信息来做决策。文献[13]解决了同一用户不同设备间内容访问权利共享问题,即在设备服务器生成设备注册证书时遍历用户所有设备信息,包括设备的硬件配置信息;确保了对平台的信任;但权利共享仅限于同一用户。文中方案通过受托方发来的 TML 和 PCR 值以及相应的委托授权策略来判断平台状态与可信性。

方案功能对比分析:文献[8,9]中的方案都具有委托授权的功能,文献[8]在委托过程的抗否认性方面未作说明,文中方案在委托方与受托方进行委托交互过程的消息经委托方私钥签名,具有抗委托方(受托方)抵赖功能。文献[11]阐述的委托授权限制于同一用户多台设备集之间对数字内容委托授权。

抗攻击能力对比分析:文献[9]使用委托方私钥签名来预防攻击者假冒/伪造消息,消息中加入随机值预防重放攻击。文中方案委托方(多媒体资源服务器)通过对受托方发来的$SK_{Delegatee.AIK}$签名消息进行验证,完成对受托方身份验证。AIK 为提供身份证明的私钥,也可以根据它追踪到委托发起者(委托方)的终端平台。由 $SK_{Delegatee.AIK}$ 对唯一标识身份的 TML 签名避免了不可信平台假冒可信平台骗取验证方(委托方或资源服务器)的信任。

结束语 本文提出了一种面向多媒体数字版权保护的委托授权远程证明协议,其通过转授权用户以及多媒体服务器分别对受托方的平台身份以及平台完整性进行验证,在保证多媒体内容保密性的同时实现了对多媒体数字内容的可信分享。

(下转第 155 页)

UML 类图、时序图结构的基础上，对时序图模型用数学方法进行抽象表示，给出其形式化定义；提取 UML 类图和 Java 源代码中类基本信息，完成对 UML 模型与 Java 源代码间静态信息的一致性检测；提出了方法(消息)调用图这一概念，提取 UML 时序图信息，并将其转化构造成时序调用图 SD-CG，通过词法分析与语法分析提取 Java 源代码中的方法调用图 CG，最终完成 UML 模型与代码间动态交互信息的一致性检测。

但是该方法还存在以下一些不足：1)在进行一致性检测时，如果出现不一致信息就会终止检测，因此，后续工作可以在此基础上进行改进，使得一致性检测工作能够最终得到一个包含完整的不一致信息的报告清单；2)在研究动态交互信息时提出的方法调用图在对 Java 源代码生成调用图分析上并不全面，未考虑 Java 的继承性与多态性，后续工作可以充分研究类间信息交互，增加对 Java 多态与继承等特性的考虑。

参 考 文 献

[1] Balzer R. "Tolerating Inconsistency" revisited[C]// Proc. of the 23rd Int'l Conf. on Software Engineering. Toronto: IEEE Computer Press, 2001: 665

[2] Ghezzi C, Nuseibeh B. Guest editorial: Introduction to the special section[J]. IEEE Trans. on Software Engineering, 1999, 25(6): 782-783

[3] Easterbrook S, Chechik M. Int'l workshop on living with inconsistency[C]// Proc. of the 23rd Int'l Conf. on Software Engineering. Toronto: IEEE Computer Press, 2001: 749-750

[4] Clarke E, Grumberg O, Long D. Verification tools for finite-state concurrent systems[C]// Lecture Notes in Computer Science 803. London: Springer-Verlag, 1994: 124- 175

[5] Holzmann J. The model checker SPIN[J]. IEEE Trans. on Software Engineering, 1997, 23(5): 279-95

[6] Heitmeyer C, Jeffords R, Kiskis D. Automated consistency checking requirements specifications[J]. ACM Trans. on Software Engineering and Methodology, 1996, 5(3): 231-261

[7] Chan W, Anderson R, Beame P, et al. Model checking large software specifications[J]. IEEE Trans. on Software Engineering, 1998, 24(7): 498-519

[8] Atlee J, Gannon J. State-Based model checking of event-driven system requirements[J]. IEEE Trans. on Software Engineering, 1993, 19(1): 24-40

[9] 丁娜. 带 OCL 约束的活动图多态测试方法的研究[D]. 重庆：重庆大学，2012

[10] 逄瑞娟. 基于 UML 顺序图的场景测试用例生成研究[D]. 青岛：青岛大学，2007

[11] 赵平. Java 源代码静态分析系统的设计与实现[D]. 长春：吉林大学，2013

[12] 章程. 基于机器学习和程序分析相结合的程序调用技术研究[D]. 上海：上海交通大学，2012

[13] 张健. 精确的程序静态分析[J]. 计算机学报，2008, 31(9): 1550-1555

[14] 逄龙，王甜甜，苏小红，等. 支持多程序语言的静态信息提取方法[J]. 哈尔滨工业大学学报，2011(3): 62-66

(上接第 135 页)

参 考 文 献

[1] 孟芳慧，曹宝香，杨义先. 钮心忻多媒体数字产品版权保护模型研究与设计[J]. 计算机科学，2013, 40(1): 98-102

[2] 张硕，马兆丰，芦效峰，等. 音乐内容动态加密与许可授权系统设计与实现[J]. 计算机科学，2011, 38(12): 43-48

[3] 锁琰，徐小岩，张毓森，等. 支持组件动态更新的远程证明[J]. 西安电子科技大学学报，2012, 38(4): 11-19

[4] Park J, Sandhu R. The $UCON_{ABC}$ usage control model[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 128-174

[5] Zhang Z, Yang L, Pei Q, et al. Research on usage control model with delegation characteristics based on OM-AM methodology [C]// IFIP International Conference on Network and Parallel Computing Workshops, 2007 (NPC Workshops). IEEE, 2007: 238-243

[6] Hu X L, Osborn S L. A new approach for delegation in usage control[C]// Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013: 269-276

[7] Lei Jian-yun. Weighted Directed Graph-Based Authorization Delegation Model[J]. Journal of Networks, 2013, 8(12): 2812-2815

[8] Gaaloul K, Proper H A, Charoy F. Delegation Protocols in Human-Centric Workflows[C]// Proceedings 13th IEEE International Conference on Commerce and Enterprise Computing 2011 (CEC 2011). New Jersey, NJ: IEEE Computer Society, 2011: 219-224

[9] Sun Dao-qing. UCSSDAP: Ubiquitous Computing Service Security Delegation Authorization Protocol[C]// 2011 IEEE International Conference on Automation and Logistics (ICAL 2011). New Jersey, NJ: IEEE Computer Society, 2011: 371-374

[10] Osborn S L, He Wang. A Survey of Delegation from an RBAC Perspective[J]. Journal of Software, 2013, 8(2): 266-275

[11] 冯雪，俞银燕，汤帜. 具有硬件适应性的多设备内容共享与版权保护方法[J]. 北京大学学报：自然科学版，2011, 47(6): 1009-1016

[12] Zhang Yong, Xiang Xue, Hai Feng, et al. An anonymous remote attestation for trusted cloud computing[C]// Proceedings 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems 2012. (IEEE CCIS 2012) Washington, DC: IEEE Computer Society, 2012: 426-429

[13] Yu Yue, Wang Huai-min, Liu Bo, et al. A Trusted remote attestation model based on trusted computing[C]// 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013. Washington, DC: IEEE Computer Society, 2013: 1504-1509

[14] Guo Jia-ming, Wei Jiang. Analysis and research of remote attestation based on trusted computing[C]// 2013 Fourth International Conference on Digital Manufacturing & Automation, 2013. Washington, DC: IEEE Computer Society, 2013: 192-195

[15] Li Ya-ping, Zhou Wei-liang. Research on the delegation schemes of the $UCON_{ABC}$[J]. Journal of University of Science and Technology of China, 2012, 42(2): 154-160

面向多媒体数字版权保护的委托授权远程证明协议

作者： 丰伟宁， 张志勇， 赵长伟， FENG Wei-ning， ZHANG Zhi-yong， ZHAO Chang-wei
作者单位： 河南科技大学信息工程学院 洛阳471023
刊名： 计算机科学 ISTIC PKU
英文刊名： Computer Science
年，卷(期)： 2015,42(4)