

可信计数器监控系统的设计与实现

娄嘉鹏¹, 慈云飞¹, 王豪杰^{1,2}, 潘耀明¹

(1. 北京电子科技学院信息安全系, 北京 100070;
2. 西安电子科技大学综合业务网理论与关键技术国家重点实验室, 陕西 西安 710071)

摘要: 在数字作品交易系统中, 可信计数机制有效解决了版权纠纷问题。为了确保可信计数器的正常、安全运行以及对计数器的状态、版本进行监控, 提出了一种基于数字作品交易的可信计数器监控系统的方法及系统, 结合 RSA 等密码技术, 实现对可信计数器运行状态的实时监控和版本升级, 保证在线交易数据的完整性、机密性和不可篡改。详细描述了该系统的体系结构、功能模块和安全数据结构。在数字版权保护领域具有广泛的应用前景。

关键词: 数字作品交易; 可信计数器; 监控系统; 实时监控; 版本升级

中图分类号: TP393.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00078

Research and implementation of the monitoring system of trusted counters

LOU Jia-peng¹, CI Yun-fei¹, WANG Hao-jie^{1,2}, PAN Yao-ming¹

(1. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
2. State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China)

Abstract: In the digital works trading system, trusted counting mechanism effectively solves the disputes of copyright. To ensure credible counter proper, safe operation and control the counter status, version, a method and system based on trusted digital work counter transaction monitoring system, which combines with RSA, and other cryptographic techniques are proposed to achieve real-time monitoring and credible counter version upgrade of the operating state, to ensure the integrity of online transactions, confidentiality and cannot be tampered with. The architecture, function modules and data security structures of the system are described in detail. It has been widely used in the field of digital copyright protection.

Key words: trading of digital works, trusted counting, monitoring system, monitor working status in real time, up-graded versions

收稿日期: 2016-04-16; 修回日期: 2016-07-09。通信作者: 娄嘉鹏, 1301597@qq.com

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0800304); 新闻出版重大科技工程基金资助项目 (No.1681300000119); 北京市自然科学基金资助项目 (No.4152048); 江苏省自然科学基金资助项目 (No.BK20150787); 北京电子科技学院 2016 年春蕾计划基金资助项目 (No.2016CL04)

Foundation Items: National Key Research Program of China (No.2016YFB0800304), The Major Science and Technology Project of Press and Publication (No.1681300000119), The Natural Science Foundation of Beijing (No.4152048), The Natural Science Foundation of Jiangsu Province (No.BK20150787), 2016 Spring Buds Project of Beijing Electronic Science & Technology Institute (No.2016CL04)

1 引言

随着互联网技术、移动技术的研究发展和智能终端设备的普及应用, Wi-Fi 等网络技术为人们提供了更加舒适便捷的服务, 产生的网络化、数字化和虚拟化的资源也越来越丰富, 这些资源在网络间的共享也越来越频繁。信息的传播从印刷媒体向数字媒体过渡, 有价值的信息内容可以在网上进行电子商务的等价交换^[1]。

随着人们对网络数字资源需求的日益增加以及人们对数字版权保护意识的增强, 数字化的作品资源在网络中逐步向有偿付费的分享形式转变。正是由于该需求, 产生了数字版权管理(DRM, digital rights management)技术, 其目标是保护数字作品的版权, 实现对数字作品的创建、处理、分发、消费的管理, 保证数字作品提供者、分销商、零售者和消费者多方的权益^[2]。该项技术目前已经成为推动数字内容在互联网发布的关键技术。

由于数字作品的虚拟性, 在数字作品交易过程中对数字作品的计数不能采用传统的纸质作品交易的计数方式, 对数字作品的可信计数技术应运而生, 可信计数技术能够确保交易系统中销售系统、授权系统和购买者等多方数字作品计数有效合法。可信计数机制以密码技术为支撑, 结合数字作品交易的实际, 引入了可信第三方, 从而保障了交易过程中各方参与者的利益。

现有的可信计数技术虽然能够提供可信计数服务, 但是它们必须运行在安全可靠的环境中。而网络环境复杂多变、极其不安全, 各种攻击和欺骗手段层出不穷, 若计数器受到网络攻击和欺骗, 就不能保证对各方提供的可信计数服务的真实性, 保障数字作品安全交易就成为空谈。

2 相关工作

目前, 国内很少直接在线上交易数字作品, 还是以线上提交订单, 线下发送纸质实体的交易形式为主, 但是线上进行数字作品交易被认为是未来主要的交易模式之一。文献[1]阐述了数字版权保护技术基本概念和系统体系结构, 主要围绕权利描述、使用控制、合理使用、权利转移和可

信执行等关键问题。文献[2]提出了一个通用的多媒体数字版权保护架构, 并实现了一个多媒体数字版权保护原型系统, 在一定程度上消除了版权争端, 但该方案需要依赖于相对安全的软、硬件环境。文献[3]讨论了网络上知识产权保护的问题以及主要的威胁模型并选定具体的计算环境 Netscape Navigator, 采用浏览器的插件作为安全内核, 确保内容的控制使用。文献[4-6]给出了一种数字资源交易中实现可信计数的方法, 用以解决现有数字版权管理中交易计数数据缺乏可信性的问题, 但是客户端代理和服务器之间需要通过安全通信模块进行交互, 且各方具体职责模糊。

文献[7,8]在数字版权保护系统中加入了一些数据清算中心, 用来生成并分发数字许可证, 实现用户身份认证、触发支付等金融交易事务。但在数字作品交易过程中, 销售商与提供商并没有设立可信的第三方作为监管方, 因而无法解决由于交易双方的不信任而产生纠纷的问题。文献[9]针对云计算环境中数字内容安全和用户隐私保护的需求, 提出了一种云计算环境中支持隐私保护的数字版权保护方案; 与现有的云计算环境中数字版权保护方案相比, 该方案在保护内容安全和用户隐私的同时, 支持灵活的访问控制, 并且支持在线和超级分发应用模式, 在云计算环境中具有较好的实用性。文献[10]基于代理重加密机制, 提出一种适应于域环境下内容共享的数字版权保护协议, 解决数字内容共享环境下无法防止域管理端和域内用户非法传播数字内容的安全问题; 该方案一方面杜绝域管理端非法传播数字内容, 另一方面控制域内用户对数字内容的合法访问, 为域管理端和交易平台提供收费凭证, 适应于家庭数字电视共享, 实现对数字电视版权的安全管理。

文献[6,11]提出了基于版权保护的带有可信第三方的数字作品交易数据管理模型, 该模型包含销售系统、授权系统和可信第三方管理平台这3个部分。可信第三方管理平台将授权方数据安全地上传给销售系统, 对交易进行监督, 有效地保证了交易的可信性和不可抵赖性, 消除版权争端。图1描述了云环境下用户基于该管理模型的数字作品在线交易的场景。

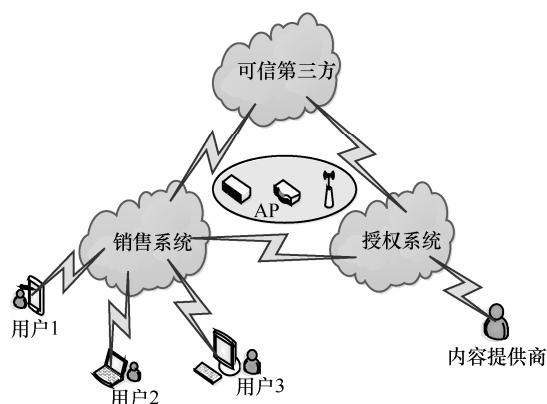


图 1 云环境下基于管理模型的在线数字作品交易场景

该管理模型中的用户数据、销售数据以及授权数据需要有合理可信的计数和保护，才能得到三方的认可、保证交易可行性、维护三方的合法权益。文献[12,13]基于管理模型，在销售系统、授权系统和可信第三方中嵌入可信计数器，其功能如下。

- 1) 规范控制交易数据。即为计数器的计数信息制定合理的数据结构。
- 2) 在销售系统、授权系统和内容提供商之间

建立可靠的计数机制，最终达到可信计数的效果。

3) 在销售系统、授权系统和可信第三方中嵌入可信计数器，保障三方安全通信，保证传输数据的完整性和不可篡改性。

销售系统、授权系统和可信第三方中嵌入可信计数器的体系结构如图 2 所示。

由于网络存在欺骗和攻击等行为，并且可信计数器自身也有可能处于不正常工作状态或者存在漏洞、需要更新版本等情况。文献[14]设计了一种监控系统，通过 Internet 网络随时随地对被监控地点的实时情况进行监控。但它只能监控网络实体的运行状态，并作具体呈现；不能保证监控系统是可信的，且不能对监控的对象进行在线升级。这就要求在数字作品安全交易过程中，实时监控可信计数器的运行状态以及安全升级到新的版本，以确保可信计数器正常工作，正确地数字作品进行计数。

本文提出一种基于数字作品交易的可信计数器的监控系统的方法及系统，它既实现了对可信

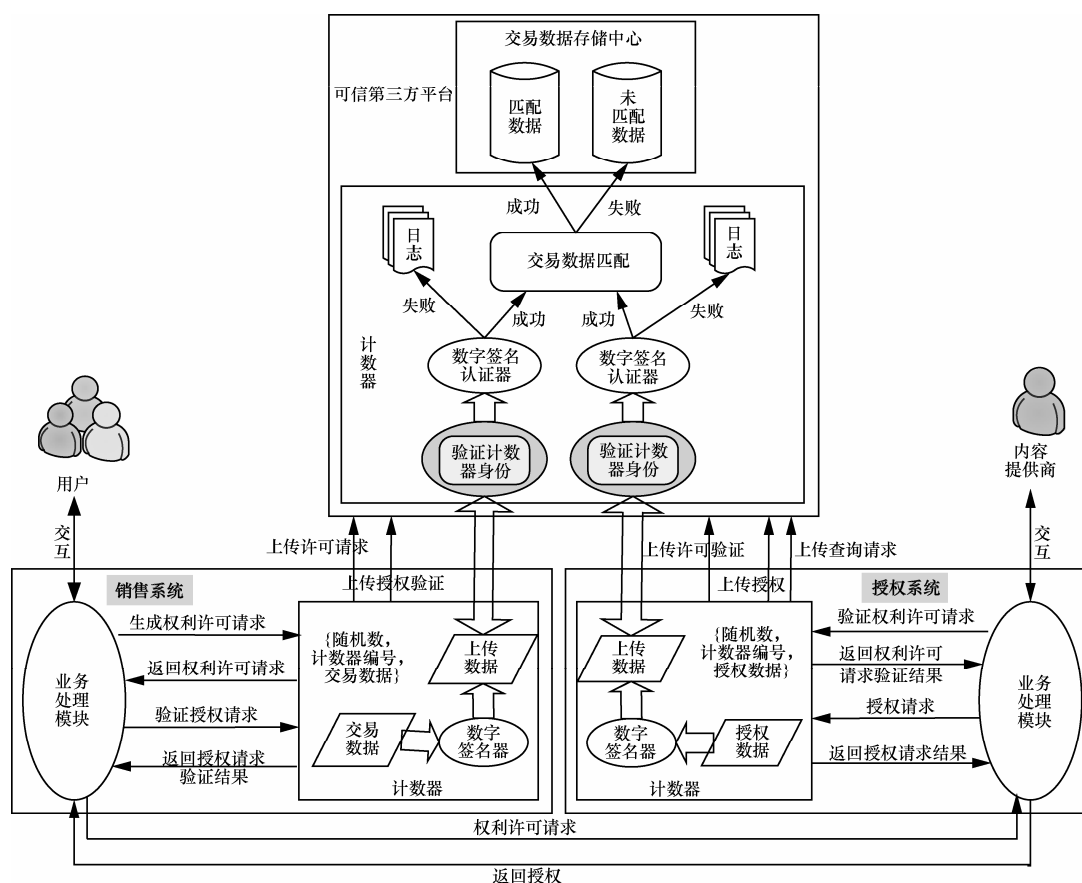


图 2 管理模型中嵌入可信计数器的体系结构

计数器的运行状态的实时监控, 还能确保该监控系统是可信的, 以及对计数器的版本进行安全合法的升级。

3 基于数字作品交易的可信计数器的监控系统

3.1 监控策略

如图3所示, 基于数字作品交易的可信计数器的监控系统是独立于计数器的。在计数器间相互传递数据信息之前, 监控系统首先会验证可信计数器及其配置信息的合法性, 计数器只有通过验证后才能进行相互间的数据传输。在数据传输过程中, 监控系统会对可信计数器进行实时监控及异常报警, 以保证计数器处于安全状态。最后, 还要求监控系统能发现可信计数器新版本并进行安全升级。

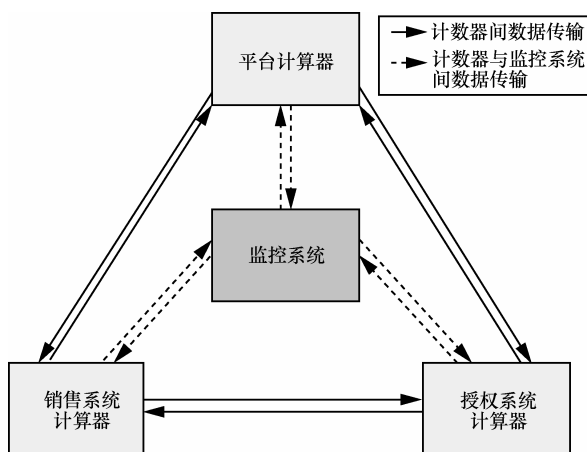


图3 监控系统工作原理

基于数字作品交易的可信计数器的监控系统工作时分为3个阶段: 启动阶段、实时监控阶段和升级阶段。启动阶段主要验证可信计数器及其配置信息的合法性, 实时监控阶段主要对可信计数器进行实时监控及异常报警; 升级阶段主要发现可信计数器新版本并进行安全升级。监控系统正常工作的3个阶段分别对应3个模块: 安全初始化模块、监实时控模块和安全升级模块。还为监控系统从可信计数器获取的初始配置信息、心跳间隔获取的心跳信息以及升级请求标识等信息设计了合理的数据结构。

假设在一个时间周期 T 内, 分配给众多可信计数器向监控系统传递监控信息的时间为

$T' = pT$, 其中 $0 < p < 1$ 。监控系统对可信计数器的初始化和升级花费的时间为 $T - T'$ 。一个可信计数器向监控系统传递监控信息的时间为 t 。则该监控系统在一个周期内最多可以获取 $\frac{pT}{t}$ 个可信计数器的计数信息。

3.2 监控系统工作流程

1) 启动阶段

在管理模型中, 都会为销售系统、授权系统和可信第三方申请并配置一个可信计数器。监控系统首先要启动安全初始化模块, 对可信计数器及其配置信息的合法性进行验证。

安全初始化模块包括3个子模块: 分配子模块、配置子模块和第一判断子模块。

分配子模块用于根据用户请求对用户分配一个合法的可信计数器。可信计数器使用 RSA 私钥加密可信计数器版本信息、所有软件的摘要值、已加载到内存的内存空间摘要值以及配置信息摘要值, 生成密文向监控系统发送。配置子模块用于接收可信计数器发送的经过加密的相关信息, 根据相关信息获取配置信息。第一判断子模块向 CA 服务器请求系统的证书, 向相关注册和授权服务器请求该系统的软件版本、软件及配置的摘要值用于判断可信计数器与所述配置信息是否合法, 如果是, 执行实时监控可信计数器的运行状态 (即进入实时监控模块); 否则, 发送初始化失败信息, 并向注册与授权服务器发送警告信息。安全初始化模块的工作流程如图4所示。

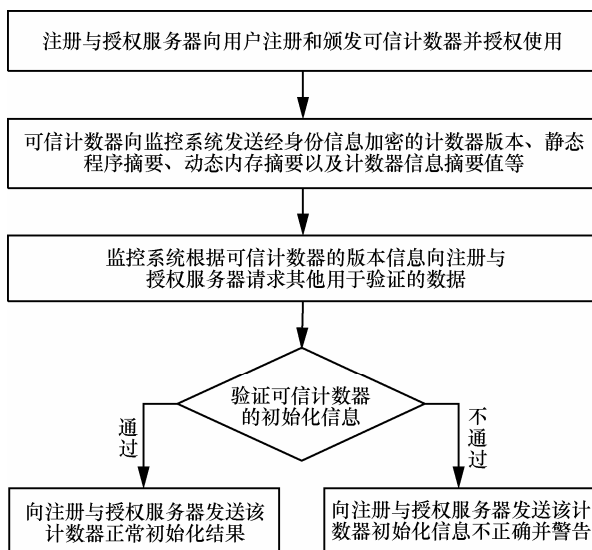


图4 安全初始化模块工作流程

2) 实时监控阶段

可信计数器初始化后进入正常工作模式，监控系统需要对可信计数器的工作运行状态进行实时监控，保障可信计数器正常工作。实时监控模块包括 2 个子模块：信息获取子模块和第二判断子模块。

进入信息获取子模块在可信计数器初始化成功，可信计数器正常启动后监控系统向可信计数器下发心跳策略，设置心跳间隔。心跳策略分为 2 种：一种是在一定的心跳间隔可信计数器自动向监控系统上传心跳信息；另一种是监控系统向可信计数器请求上传心跳信息，可信计数器收到请求后向监控系统上传心跳信息。心跳信息是经过 RSA 私钥加密的可信计数器各部分的运行状态信息。信息获取子模块用于间隔预设时间获取可信计数器的经过加密的运行状态信息，信息获取模块验证其动态内存信息。第二判断子模块向 CA 服务器请求系统的证书，向注册和授权服务器请求该系统的运行正常值，与该系统发送过来的状态信息进行对比，判断可信计数器运行是否正常，如果是，继续运行可信计数器并进入安全升级模块；否则，发送运行异常报警信息并通知注册与授权服务器。实时监控模块的工作流程如图 5 所示。

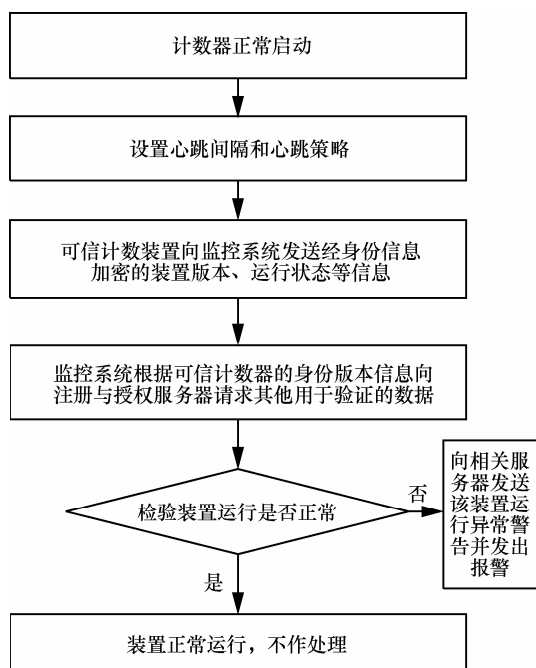


图 5 实时监控模块工作流程

3) 升级阶段

可信计数器会经常发布新的版本，当监控系

统的安全升级模块检测到可信计数器新版本信息时，就会向可信计数器发送升级消息，保证可信计数器安全升级。

安全升级模块包括 2 个子模块：第三判断子模块和升级判决子模块。

第三判断子模块用于判断是否接收到升级请求，如果是，触发升级判断模块；否则，继续运行当前可信计数器。可信计数器向监控系统发送经过 RSA 加密的当前授权信息、当前软件摘要值、配置信息等。监控系统的升级判决子模块向 CA 服务器请求可信计数器的证书，向注册和授权服务器请求该可信计数器经过加密的相关信息，根据相关信息判断当前可信计数器是否可以升级，如果是，进行自动在线升级或者人工离线升级，升级成功后继续运行升级后可信计数器；否则，升级失败，则继续当前运行的可信计数器，通知注册与授权服务器并记录在本地数据库中。安全升级模块工作流程如图 6 所示。

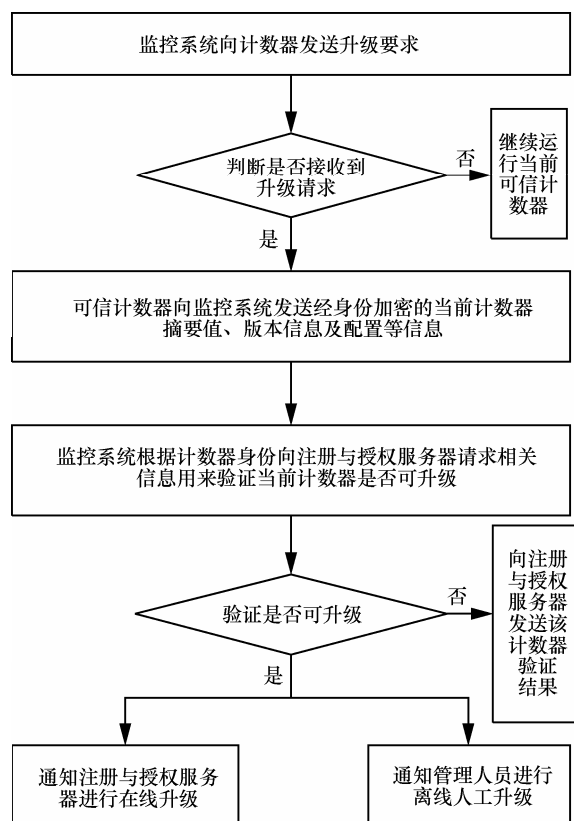


图 6 安全升级模块工作流程

3.3 监控系统数据结构

监控系统为了能够保证可信计算器的启动状态、正常运行状态以及对新版本升级请求进行监

控,就需要获取可信计算器的初始配置信息、心跳间隔获取的心跳信息以及升级请求标识等信息。需要为监控系统从可信计算器获取的初始配置信息、心跳间隔获取的心跳信息以及升级请求标识等信息设计合理的数据结构。

1) 初始化信息的数据结构

初始化信息的基本格式如图7所示,详细说明如下。

计数器类型	配置信息	版本信息	数据签名
-------	------	------	------

图7 初始化信息的基本格式

① 计数器类型,占1 B。

0x01 (0000 0001)表示销售系统可信计数器。

0x02 (0000 0010)表示授权系统可信计数器。

0x03 (0000 0011)表示可信第三方计数器。

其他值保留。

② 配置信息为监控系统从可信计算器获取的初始配置信息,包括Info和Path这2个部分。Info为可信计算器基本信息,包括计算器ID、容器名、平台IP、端口号等;Path为支持可信计算器正常工作的相关路径,包括工作路径、日志路径、证书路径和数据库路径等。配置信息的基本格式如图8所示。

Info					Path				
1	2	3	4	5	6	7	8	9	10

图8 配置信息的基本格式

Info部分的详细信息如下。

a. 机构编号,占2 B。可信计数器类型是0x01或0x02时,分别填充的是销售系统或者授权系统的机构编号;可信计数器类型是0x03时,该项为空,用全0填充。

b. 计数器编号,占1 B。可信计数器类型是0x01、0x02或0x03时,分别填充的是销售系统、授权系统或者可信第三方的可信计算器的编号。

c. 平台计数器编号,占1 B。可信计数器类型是0x01或0x02时,填充的都是可信第三方的可信计算器的编号;可信计数器类型是0x03时,该项为空,用全0填充。

d. 平台IP,占4 B。可信计数器类型是0x01或0x02时,填充的都是可信第三方的IP;可信计数器类型是0x03时,该项为空,用全0填充。

e. 容器名称,占1 B。可信计数器类型是0x01、0x02或0x03时,分别填充的是销售系统、授权系统或者可信第三方的容器名称。

Path部分的详细信息如下。

a. 工作路径,占100 B。可信计数器类型是0x01、0x02或0x03时,分别填充的是销售系统、授权系统或者可信第三方的可信计数器的工作路径。

b. 日志路径,占100 B。可信计数器类型是0x01、0x02或0x03时,分别填充的是销售系统、授权系统或者可信第三方的可信计数器的工作日志路径。

c. 证书路径,占100 B。可信计数器类型是0x01、0x02或0x03时,分别填充的是销售系统、授权系统或者可信第三方的可信计数器中用到的证书存放路径。

d. 缓存路径,占100 B。可信计数器类型是0x01、0x02或0x03时,分别填充的是销售系统、授权系统或者可信第三方的可信计数器传输的数据缓存路径。

e. 数据库路径,占100 B。可信计数器类型是0x01、0x02时,该项为空,用全0填充;可信计数器类型是0x03时,填充的是可信第三方的可信计数器接受到的销售系统或者授权系统上传的数据要存放的数据库的路径。

③ 版本信息为可信计数器当前版本信息,占2 B。

④ 签名部分采用国家密码管理局编制的商用算法,以防数据内容被篡改,占256 B。

2) 心跳信息的数据结构

心跳信息的基本格式如图9所示,详细说明如下。

计数器类型	数据类型	数据内容	数据签名
-------	------	------	------

图9 心跳信息的基本格式

① 计数器类型,与初始化信息的基本格式中的计数器类型相同。

② 数据类型,占1 B。表示可信计数器之间传递的信息类型,目前共有8种类型。

0x01 (0000 0001)表示上传数据类型。若计数器类型是销售系统,则上传数据指权利许可请求数据;若计数器类型是授权系统,则上传数据指授权信息记录数据。

0x02 (0000 0010) 表示测试连通性请求数据。

0x03 (0000 0011) 表示配置计数器请求数据。

0x04 (0000 0100) 表示查询销售系统信用请求数据。

0x81 (1000 0001) 表示上传数据(权利许可请求、授权信息记录)的应答数据。

0x82 (1000 0010) 表示测试连通性数据的应答数据。

0x83 (1000 0011) 表示配置计数器数据的应答数据。

0x84 (1000 0100) 表示查询销售系统信用的应答数据。

其他值保留。

③ 数据内容为监控系统在心跳间隔获取的可信计数器中传输的数据,具体分为之前 8 种类型的数据内容。

④ 签名部分以防数据内容被篡改,占 256 B。其签名算法采用国家密码管理局编制的商用算法,如 SM3 杂凑算法。

3) 升级请求信息的数据结构

bool updateFlag

用于检测到新版本的可信计数器后的升级请求标识符, True 表示允许升级, False 表示不允许升级。

4 监控系统分析

4.1 安全性分析

本方案可以使用应用 RSA、基于身份密码算法等认证算法,这里使用 RSA 算法进行身份认证与加密,并给计数系统颁发相关证书表明各系统身份, Hash 算法可以使用 SHA1 进行相关信息的摘要计算。

系统安全初始化阶段使用 RSA 私钥加密软件版本信息、所有软件的摘要值、已加载到内存的内存空间摘要值以及配置信息摘要值,生成密文向监控系统发送。系统每隔 1s 向监控服务器发送心跳信息,它是经过 RSA 私钥加密的系统各部分的运行状态信息。

当且新版本出现时,监控系统向系统发送升级消息。系统向监控系统发送当前授权信息、当前软件摘要值、配置等,这些都需要经过 RSA 加密。

4.2 功能测试

首先通过对第三方可信平台的计数器进行配

置,然后测试监控系统各模块的运行状态,如图 10 所示。该监控系统操作简单,系统会自动将不正常数据保存在工作日志中。由图 10 可知,该监控系统基本上能准确、及时地对可信计数器的运行状态和版本信息等进行监控。



图 10 可信计数器监控系统测试

4.3 性能分析

假设一个时间周期 $T=30 \text{ min}$, 由于监控系统对可信计数器的初始化和升级花费的时间很少, p 的取值由用户根据实际情况选取, 在此取 $p=0.9$ 。分配给众多可信计数器向监控系统传递监控信息的时间为 $T'=pT=0.9 \times 30=27 \text{ min}$ 。监控系统对可信计数器的初始化和升级花费的时间为 $T-T'=(1-p)T=3 \text{ min}$, 基本上能够满足对可信计数器的初始化和升级, 若在该时间段内不能完成以上工作, 则可以调整 p 的值。一个可信计数器将心跳信息加密并传递给监控系统的时间约为 $t=50 \text{ ms}$ 。则该监控系统在一个周期内最多可以获取 32 400 个可信计数器的计数信息。因此, 该监控系统基本能够对数字作品交易系统中所有可信计数器进行监控。

5 结束语

在数字作品交易系统中, 为了确保可信计数器在复杂多变的网络环境中安全可靠地工作, 并且可信计数器当前以最新的版本运行。本文提出了一种基于数字作品交易的可信计数器监控系统的方法及系统, 它既实现了对可信计数器的运行状态的实时监控, 还能确保该监控系统是可信的, 以及对计数器的版本进行安全合法的升级。

但是目前还只是从理论上对该监控系统的性能进行估算, 还没有在实际的数字作品交易系统中进行验证, 若是以后国内的数字版权观念根深

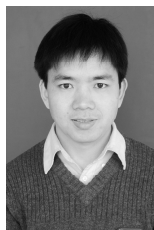
蒂固了,可信计数器的数量庞大,则该监控系统就不能达到对系统中所有可信计数器的监控。为了解决这个问题,可以基于分布式分层管理理论,由若干监控器分别对销售系统和授权系统中的可信计数器进行监控,然后由布置在可信第三方管理平台的监控器对分布在销售系统和授权系统的若干监控器进行监控仲裁。

总体来说,该监控系统能够有效保障在复杂的网络环境下数字作品交易系统中可信计数器的可信计数问题,消除了版权争端,使数字作品版权得到保护,在数字版权保护领域具有广泛的应用前景。

参考文献:

- [1] 俞银燕, 汤帆. 数字版权保护技术研究综述[J]. 计算机学报, 2005, 28(12):1957-1968.
YU Y Y, TANG Z. A survey of the research on digital rights management[J]. Chinese Journal of Computers, 2005, 28(12): 1957-1968.
- [2] 司端锋, 王益冬, 潘爱民, 等. 多媒体数字版权保护系统的研究与实现[J]. 北京大学学报(自然科学版), 2005, 41(5):792-799.
SI D F, WANG Y D, PAN A M, et al. Research and implement on general multimedia digital rights management system[J]. Journal of Peking University (Natural Science Edition), 2005, 41(5): 792-799.
- [3] 庄超. 一种新型的 Internet 内容版权保护的计算机机制[J]. 计算机学报, 2000, 23(10):1088-1091.
ZHUANG C. A new computing mechanism for internet content copyright protection[J]. Chinese Journal of Computers, 2000, 23(10): 1088-1091.
- [4] 綦科, 谢冬青. 数字资源交易可信计数系统的设计[J]. 广州大学学报(自然科学版), 2013, 12(6):69-72.
QI K, XIE D Q. Designing of trusted counting system for digital resource transaction[J]. Journal of Guangzhou University (Natural Science Edition), 2013, 12(6):69-72.
- [5] 綦科, 谢冬青. 数字资源交易中实现可信计数的系统: CN 102495979A [P]. 2012.
QI K, XIE D Q. Realizing credible counting in digital resource transaction system: CN 102495979A [P]. 2012.
- [6] SHI G, SHEN Y, LI F, et al. Research on credible regulation mechanism for the trading of digital works[M]//International Conference on Security and Privacy in Communication Networks. Berlin: Springer International Publishing, 2014.
- [7] ZHU B, Q H, XU K, et al. A portion-based content distribution strategy in streaming media content distribution networks[C]// International Conference on Computer Application & System Modeling, IEEE, 2010. 512-514.
- [8] BJORKQVIST M, CHEN L Y, ZHANG X. Minimizing retrieval cost of multi-layer content distribution systems[C]//IEEE International Conference on Communications(ICC). 2011:1-6.
- [9] 黄勤龙, 马兆丰, 傅镜艺, 等. 云计算环境中支持隐私保护的数字版权保护方案[J]. 通信学报, 2014(2):95-103.
HUANG Q L, MA Z F, FU J Y, et al. Privacy-preserving digital rights management scheme in cloud computing[J]. Journal on Communications, 2014(2):95-103.
- [10] 闫玺玺, 耿涛. 一种面向域环境下内容共享的数字版权保护方案[J]. 密码学报, 2015, 2(3):268-284.
YAN X X, GENG T. Digital rights management scheme for sharing in authorized domain[J]. Journal of Cryptologic Research, 2015, 2(3):268-284.
- [11] 刘东. 面向数字作品交易的数据保全机制设计与实现[D]. 西安: 西安电子科技大学, 2014.
LIU D. The design and implementation of the data preservation mechanism for the digital works transactions[D]. Xi'an: Xidian University, 2014.
- [12] 杨丽莹. 数字作品交易系统中可信计数技术的研究与设计[D]. 西安: 西安电子科技大学, 2012.
YANG L Y. Research and design on credible counting technology for digital products trading system[D]. Xi'an: Xidian University, 2012.
- [13] 胡尧. 数字版权交易用户端可信计数器设计与实现[D]. 西安: 西安电子科技大学, 2014.
HU Y. Design and implementation of customer trusted counter of digital copyright trading [D]. Xi'an: Xidian University, 2014.
- [14] 牛锋刚. 监控系统: CN 101986704 B [P]. 2013.
NIU F G. Monitoring system: CN 101986704 B [P]. 2013.

作者简介:



娄嘉鹏(1977-), 男, 山东菏泽人, 北京电子科技学院讲师, 主要研究方向为嵌入式安全。



慈云飞(1989-), 男, 安徽池州人, 北京电子科技学院硕士生, 主要研究方向为访问控制和信息安全。



王豪杰(1991-), 男, 山东青岛人, 西安电子科技大学硕士生, 主要研究方向为访问控制与网络安全。

潘耀明(1992-), 男, 安徽亳州人, 北京电子科技学院硕士生, 主要研究方向为嵌入式安全。