基于属性证书的移动代理访问控制解决方案

徐大伟，吕 军

(山东财政学院计算机信息工程学院 济南 250061)

【摘要】分析了移动代理系统的特点，针对移动代理系统的安全需求尤其是访问控制问题，以PKI/PMI做基础服务设施，对应于移动代理和代理平台，引入了代理属性证书和平台属性证书，以扩充移动代理系统处理环境。应用Java虚拟机(JVM)的类动态装载技术和方法调用所提供的简单且有效的方式来支持代理平台的扩展，使该文案具有足够的灵活性，包含的安全策略，适合于大多数基于移动代理的应用。

关 键 词 属性证书； 移动代理； 公钥基础设施； 特权管理基础设施

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.z1.023

Access Control Scheme Based on Attribute Certificates for Mobile Agents System

XU Da-wei and LÜ Jun

(School of Computer Inforimation Engineering, Shandong University of Finance Jinan 250061)

Abstract According to the security requirements of mobile agent system, especially the problem of access control, public key infrastructure/privilege management infrastructure (PKI/PMI) is applied as basic service facility, agent attributes certificates and platform attribute certificates are then introduced to extent the environment of mobile agent systems. This mechanism provides good agility to include a more extendable security policy, and is, therefore, suitable for most of the current mobile agent applications.

Key words attribute certificates; mobile agent; PKI; PMI

针对移动代理系统的安全需求，尤其是访问控制问题，本文分析了移动代理系统的特点和现有方案的缺陷及不足，利用PKI/PMI的优势，提出将属性证书引入移动代理系统，证书与移动代理结合，以扩充移动代理系统处理环境，从而实现更好的授权管理。该方案提供了足够的安全性、灵活性和高效性。

1 移动代理系统分析

1.1 移动代理系统概述

一个典型的移动代理系统如图1所示结构。

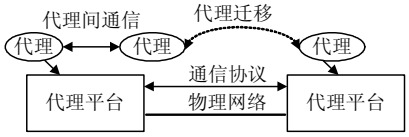

图1 移动代理系统模型

该系统包括两个主要部分：代理平台为代理提供运行环境支持；移动代理通过物理网络迁移到不同平台上，利用其提供的资源执行任务，当平台接收此代理时，它需要对代理进行认证以决定其存取控制权限[1]。

1.2 访问控制方面缺陷

纵观移动代理系统，它们在管理移动代理访问控制方面存在以下的缺点：

(1) 在实际应用中，安全策略经常会变化，而在移动代理系统中，它们一般是固定的、不变的。这种情况导致基于代理的应用程序的开发者编码时只能遵照自己设定的安全策略方案，而方案不一定与应用程序的安全策略相匹配[2]。

(2) 移动代理系统中，策略描述语言、资源等方面的变化，不利于应用程序开发者的修改和扩展。

以上两点结合起来，将把应用程序开发者限制在一个困境中，使编辑的安全策略可能完全不适合应用程序。

(3) 传统方法使用服务器的存取控制表ACL来解决问题[3]，灵活性差、效率低。由服务器来完全实现访问控制，会加重服务器的负担，同时安全性受服务器本身安全性的限制。一旦服务器失效，整

收稿日期： 2009 ↖ 09 ↖ 15

作者简介：徐大伟(1976 ↖)，女，硕士生，讲师，主要从事网络信息安全方面的研究.

个访问控制无法实施。

(4) 采用访问控制列表，不能满足大规模、跨地域范围访问控制的需要，一旦客户增多，服务器无法提供足够空间和时间完成访问控制列表的查询、存储和维护。

在移动代理系统中，安全策略是基于每个代理的，即基于通信通道中的数据，代理的发送方与接收方可以基于不同安全策略。发送方与接收方采用的不同安全策略将为移动代理系统提供更多灵活性。为了提高效率，降低负载，本文将签名的属性证书与代理结合，灵活高效地解决授权管理问题。

2 基于属性证书的移动代理系统模型

2.1 方案模型

模型的基本思想是以PKI/PMI做基础服务设施，对应于移动代理和代理平台，引入两种形式的属性证书，以扩充移动代理系统处理环境。本文使用一个简单的移动代理模式来描述，如图2所示为基于属性证书的移动代理系统。

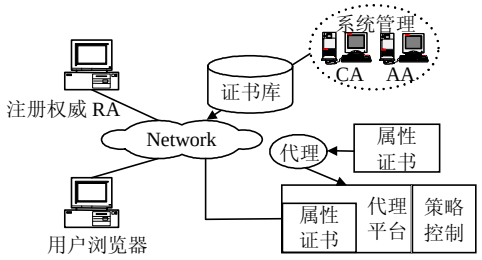

图2 基于属性证书的移动代理系统模型

代理属性证书：移动代理代表用户执行任务必须遵循管理者建立的安全策略。本文模型将安全策略信息置于一个外在实体——属性证书中，而不是放在代理代码中。发行者给属性证书分配一定的权限，并且由发行者签名以保证代理信息的完整性。

平台属性证书：是代理属性证书相对应的说明证书，它将安全策略分配给代理平台。平台属性证书与代理属性证书不同，一般不仅应用于一个单一平台，而要应用到更广的范围。证书应包含尽可能多的安全策略信息，系统管理员只需通过设置配置参数，为平台申请相应的平台属性证书即可。为此，本文设计了一个外部参考策略文件库。

策略控制：由于代理平台为移动代理系统提供运行的计算环境，所以策略处理由代理平台完成。使用一种有关安全的机制——策略计算，它作为代理平台的一个可信的组件来实现，即附加程序组件来支持策略计算的灵活实现，本方案的策略计算组件称为策略控制，负责访问控制处理。

2.2 属性证书

PMI建立在PKI提供的可信身份认证服务的基础上，以属性证书的形式实现授权管理。属性证书是一种轻量级的数字证书，这种数字证书不包含公钥信息，只包含证书所有人ID、发行证书ID、签名算法、有效期、属性等信息。属性证书的规范于2000年推出，世界通信组织ITU给属性证书下的定义是：对用户的属性和其他信息，用发行此证书的证书权威的私钥进行数字签名而形成的证书[4]。

属性证书的优点：

(1) 基于用户的“标识-属性”组合来制定访问控制策略。在移动代理系统中，服务器主机一般基于用户的某些敏感属性值做出访问控制决策。属性证书将用户属性与用户标识符相分离，提高了决策效率与安全。

(2) 属性证书与用户的工作相关联，证书有效期很短。用户参与新工作项目就要向AA申请属性证书，属性证书的有效期是代理完成工作需要的时间，随着代理的撤销属性证书即完成一个生命周期，不会产生大量的CRL，给安全策略规则的增加、删除或更新带来方便。

(3) AA失效带来的影响较小，只对需要该属性参与决策的访问控制有影响。每种属性证书由一个AA来签发，若某个AA失效，只要单独建立新的AA重新签发该类属性证书即可，原AA签发的证书会在证书的有效期过后自动失效。

3 方案实现

模型的一个关键问题是如何将属性证书引入到移动代理中，实现授权管理[5]。Java具有支持代码的迁移性、动态代码下载、数字签名代码、远程方法调用、对象的连续、异构平台等特征，为移动代理系统构成一个理想的基础环境。因此，本文模型使用Java程序语言和运行环境来实现。

Java语言编译器提供Java虚拟机(JVM)，JVM的类动态装载技术和方法调用提供了简单且有效的方式以支持代理平台的扩展。Java还支持一种文件格式称为JAR，相当于一种类似于ZIP文件的压缩格式，可以把类文件和资源合成一个文件进行管理，而且JAR的内容可以用签名来保证鉴定性和完整性。这样，它可以方便地将一个代理的类签名后封装打包，以便于其最初的分配和平台上的迁移。因此，本方案利用JAR格式，来保护代理代码并简化

其管理。另外，一个专门保存私有密钥和相关数字证书的数据库，称为密钥存储，它由Java支持，签署JAR文件时用到它的内容。

本文利用Java提供的以上服务，将属性证书与移动代理系统完美结合，如图3所示。

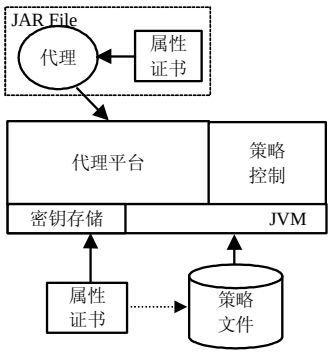

图3 基于Java的模型

另外，Java提供一种标准策略文件，即一个专门指定策略规则的工具。文件的每个条目，说明了代理的授权许可策略。策略规则的描述使用一种“批准”语言模式，即明确地给代理授予许可策略。许可策略中描述的都是已经授权的系统对象的行为，装载者可使用指定的许可策略管理名字空间，为任何加载的代码形成一个保护域。除了这种标准许可策略，开发者也可以专门为某个特殊应用定义许可策略。

3.1 证书策略的实现

3.1.1 代理属性证书

本文方案利用JAR文件运载信息的灵活性来实现属性证书与移动代理的绑定。一个被签名的JAR文件除了包含存档文件外，还包含一对文件：一个签名指令文件和一个数据签名文件。每一个签发者有一个或多个文件存档。这些文件以一种专门的目录META-INF存档，META信息可以包含身份证书，以简化JAR容器中内容的确认处理[6]。

代理的JAR文件有一个容器存放发行给代理的属性证书，一旦移动代理放在JAR文件中，可以与属性证书绑定，证书放在META-INF目录中以备使用。属性证书描述了分配给代理的策略规则，以标准策略文件的形式放在属性证书的“属性”元素中。

可将其他有用信息放在属性证书的“扩展域”部分。“扩展域”包括：一个约束指示域以指明颁发证书的主体是否为终端用户，是否能够为指定数目的撤销者再次分配特权；一个恢复服务域，以决定到期的属性证书是否延时及持续的时间[7]。

3.1.2 平台属性证书

1) 策略规则描述。

策略规则的编辑以代理平台为中心，不考虑与平台无关的证书发行者。在“批准”语言模式下，若要使得代理被认可，最直接的方法就是定义一个批准许可，权限调整可由AA控制管理[8]。

在“批准”语言模式下，策略规则的描述开始于名字“权限调整”，接着是许可用户的密钥存储别名(以“*”代表)，最后以角色的操作结束。一个简单的描述，便可实现代理代码获得属性证书中描述的权限。如要授权给一个由可信的代理开发者(假如名字为ESO)封装的、由可信用户发放的一个代理的代码，Java策略规则描述如下：

```
Grant {
    Permission privilege Adjustment“*” “launchedBy”;
    Permission privilege Adjustment“ESO” “sealedBy”;
}
```

这种方式给系统带来很大的灵活性，一旦需要在系统内加入某个权限及其能处理的事务，只需以这种简单的描述加入策略规则即可。

2) 平台属性证书功能实现。

本方案中平台属性证书有以下功能：

(1) 能够基于证书发行者的级别定义权限等级，并管理证书的数目；

(2) 能够决定谁具有权限改变访问许可；

(3) 能够根据情况调整匿名证书的权限级别。

权限等级的说明放在平台属性证书的“扩展域”中，包括等级和证书数目。一般情况下，用户被默认为他所创建对象的所有者，他可以授予或撤销其他用户对该对象的访问权限，甚至可以是“授权管理”的权限。但是，若授权停止，那么任何未经授权的调整权限等级的企图都被否定，并发一个安全通告。而代理平台策略的说明包括对计算资源的控制信息，因此，它优先级别最高，可以通过平台属性证书中“属性”的稀疏授权矩阵(策略定义者➨权限)有选择地安排权限以适用于其他等级用户。该方案非常灵活，允许每一类证书发行者分别控制各自的等级权限[9]。

Java目前的版本包括定义新的安全属性；为标准策略类指定置换类；定义新的许可策略；在目录中放置可信代码。这些功能可用于授权管理机制。通过定义新的安全属性，处理者可以定位、验证或

将相应的平台属性证书转换为策略控制能够处理的内部形式。通过定义新的许可策略，调整许可的能力可由一个标准策略入口控制。可信扩展，通过将特权管理组件放于虚拟目录的方式，获得对系统资源完全的访问。

3.2 访问控制的处理

3.2.1 策略控制的组织

策略控制分为两个部分：外部策略控制和内部策略控制。外部策略控制的工作是公共的，而内部引擎的操作专门制作以适合特权管理证书的特定内容。策略控制组织如图4所示。

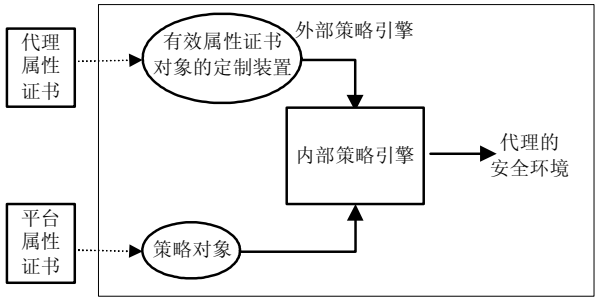

图4 策略控制的组织

外部策略控制负责分析和校验与代理关联的证书，验证证书的内容，包括签名和证书链，排除任何与代理平台不匹配的证书，并根据权限等级定制顺序。外部策略控制要取出平台中与该代理相应的策略，它是在平台初始化时由平台的平台属性证书建立的。证书链的验证是一个复杂的处理过程，包括证书期满或撤销的可能性及信息恢复的必要性。

内部策略控制的工作是利用外部策略控制提供的信息，为平台上运行的代理提供安全环境。它处理与平台策略相对应的有效属性证书的内容，并得出是否允许该代理访问以及什么级别的权限进行访问。

为便于扩展，本文采取内部引擎完成相关的简单的任务，并适应于应用程序的需要；而外部引擎处理复杂的但普遍的、公共的解释和验证工作。

3.2.2 策略处理的实现

策略控制由一对对象类实现，负责执行必要的计算和确定代理的权限。权限由一个已认证的许可策略文件组成，包含属性证书与平台属性证书的策略规则。没有权限即未被授权，处理时不予承认。初始化时，通过标准安全属性文件或系统属性文件的一个入口，策略控制类作为一个可靠组件置于代理平台。由于策略控制的两部分是Java对象类，应用简单，因此，如果需要多个处理或多处应用，可以在一个代理平台上支持多个策略控制。方案在所有证书中的“扩展域”中设置一个关键的定义——“策略标识符”，用于策略控制与证书的匹配。

外部策略控制支持一种单一方法，即校验属性证书，将结果返回许可策略。一旦所有证书被分析并排序后，外部引擎调用内部引擎执行处理。由于所有Java标准策略机制中置换策略类一直保持完整，策略控制在处理中能够得以简化实现过程。

4 结 束 语

综上所述，可以看出本文提供了一个足够灵活的且尽可能地包含了一个很广范围的安全策略机制，适合于大多数基于移动代理的应用。目前，随着经济发展与Internet的结合越来越深入，电子商务商业运作规模不断扩大，Internet移动代理技术可以应用于电子商务，并有广阔的发展前景，而有了PKI/PMI作为后盾，就保证了安全的电子商务管理。

参 考 文 献

[1] ROBERT G S. Agent tcl: A flexible and secure mobile-agent system[C]//Proceeding of the foureh Annual Tcl/Tk Worksshop’96. Monterey, Cal, USA: [s.n.], 1996: 9- 23.

[2] BROOKS R. Mobile code paradigms and security issues[J]. IEEE Internet Computing, 2004, 5/6: 54-59.

[3] GAMAL T E. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans On Information Theory, 1985, IT-31: 469-472.

[4] BOEYEN S. Overview of PKI&PMI frameworks[EB/OL]. [2009-08-22]. http://www.entrust.com/resourcenter/pdf/509-overview. pdf.

[5] HOUSLEY R, FORD W, POLK W, et al. Internet X.509 public key infrastructure certificate and CRL profile [DB/OL]. [2009-08-21]. http://www.ietf.org/rfc/RFC2459.txt.

[6] JANSEN W. Countermeasures for mobile agent security[J]. Computer Communication, 2000, (23): 1667- 167.

[7] MYERS M, LIN X, SCHAAD J et al. Certificate management messages over CMS[EB/OL]. [2009-08-12]. http://www.ietf.org/rfc/RFC 2797.txt.

[8] ITU. ITU-T recommendation X.509[EB/OL]. [2009-08-16]. http://sirius.ac.upc.es/~jbt/learning/x.509.

[9] ADAMS C, FARRELL S. Internet X.509 public key infrastructure certificate management protocols[DB/OL]. [2009-08-05]. http://www.ietf.org/rfc/RFC 2510.txt.

编 辑 张 俊