基于PKI的校园网计费认证系统的研究与设计*

陈建奇　吴子文　(福州 福建师范大学数学系与计算机科学系　350007)
张玉清　李学农　(北京 清华大学信息网络工程研究中心　100084)

Development and design of campus network charge and authentication system based on PKI

摘要：PKI (Public Key Infrastructure，公钥基础设施) 是当前信息安全的主流，能为诸多的应用提供很好的安全解决方案.本文即在清华大学校园网计费系统中搭建一个基于PKI的身份认证平台.作者首先概要说明了PKI的大致组成及各组件的功能，并具体分析了设计基于PKI计费认证系统的属性证书技术和Agent技术，最后设计了基于PKI的清华大学校园网计费认证系统。

关键词：PKI　身份认证　计费

1 引言

随着网络的日益普及，人们利用网络进行的社会活动逐渐增多，各行各业的发展也对网络产生了巨大的依赖性.然而，Internet的通信基础是TCP/IP协议，由于历史原因，TCP/IP并没有考虑安全特性，这就阻碍了利用网络开展安全应用的步伐，直接影响了网络的发展.一般地，在网络上传输的信息容易遭到以下几个方面的威胁.

(1) 信息被窃听：信息在传输的过程中，有可能被攻击者窃取。

(2) 信息被篡改：信息在传输过程中，攻击者可能会私自篡改信息的内容。

(3) 信息被重放：攻击者可能把收集到的信息在通信双方会话结束后重放。

(4) 身份假冒：信息的发送方和接收方都有可能假冒别的身份。

随着清华大学"泰山工程"的实施，清华大学各个宿舍楼的局域网已经可以连到校园网上.然而自CERNET (中国教育和科研计算机网) 收取网络分担费后，校园网也面临着向用户合理分摊网络费用的问题，一个能够适应校园网网络现状和发展要求的用户管理和计费系统是保证网络运行的基础.然而校园网络的特殊性给网络计费带来了一些问题，一方面，不能保证校园里每台计算机都有一个固定的IP，另一方面，每台计算机不能保证只有一个人使用，这样按照IP进行计费是不能满足要求的。

针对校园网的实际情况和为了满足校园网建设的"5A" (即任何人在任何地方、任何时间、任意平台都可以享受任意的网络服务) 工程的要求，学校的计费系统采用了身份认证机制，用户通过身份认证来证明自身的合法性，系统依据认证结果给合法用户动态分配IP，将费用直接分摊到用户个人帐号上.这样避开了根据IP进行计费的问题，实现了基于用户帐号的计费方式，但是这对系统提出了新的要求：必须保证用户信息的安全性.虽然说解决计费系统的用户信息安全问题的方法不止一种，人们也已经提出了很多解决方案，但是本文所提出的方案则是利用校园网实施的的公钥基础设施PKI (Public Key Infrastructure) 来实现计费认证系统，它可以很好地解决计费系统的信息安全问题。

2 PKI

公钥认证需要通信双方事先已经拥有对方的公开密钥，因此公钥的分发成为公钥认证的重要环节.在公钥密码体制下公钥是公开的，这提供了一个理想的大范围的密钥交换的可能.但是在开放的网络环境下，通信者如何确保自己所获得的公钥匙真的属于与自己通信的主体还是一个问题.攻击者完全可以自己生成一个公钥/私钥对，然后用该公钥来冒充真正的通信方的公钥，实施中间人攻击。

解决公钥安全的一个有效的方法是建立一个大家广泛信任的第三方权威中心，由它来证明用户公钥的有效性.ITU-T X.509 [2] 标准就是基于这种思路的，该标准定义了公钥基础设施PKI。如图1所示，PKI一般包含认证机构、注册机构和CRL发布等几部分。

(1) 认证机构CA (Certificate Authority)：认证机构是通信双方共同信任的第三方，它使用证书来发布用户的公钥，利用签名来证明证书上与公钥相绑定的用户信息。它还执行证书的发布和撤销任务，从而证书用户可以查询到要使用的有效证书。

(2) 注册机构RA (Registery Authority)：注册机构主要是为用户提供申请证书的接口，审核用户的身份，并把合法用户的证书请求传给认证机构。

(3) 证书撤销列表CRL (Certificate Revocation List) 发布：CRL发布是公布还没有到期而因异常情况不能使用的证书的一种方法。

3 基于PKI的计费认证系统

PKI的建立使用户拥有了标识个人身份信息的电子证书，人们可以利用证书来进行身份认证，通过PKI开展各种安全应用。利用证书开展安全应用的方法有很多种，有些是基于证书的扩展域来确定用户访问特定应用的权利；有些是直接进行一些基本配置，利用应用本身对证书的支

持来开展安全应用，如HTTPS。然而校园网的计费系统是一个具体的客户服务器方式的应用程序，为了用PKI为其提供安全解决方案，必须进行具体的研究与设计。

3.1 计费认证系统的设计原则

(1) 安全。计费认证系统为用户登录计费系统提供身份认证的平台，其操作涉及到与用户高度相关的私人信息，如帐号和密码或者用户上网金额。使用PKI为其提供的安全解决方案必须确实能够保护用户敏感信息的安全性，即能满足计费系统的信息安全需求。这是一条最基本的原则，也是计费认证系统的基本要求。

(2) 高效。校园网计费系统是在实践中经过测试、修改及在使用中不断完善形成的，具有其合理性和实用性。现在计费系统还在正常的服务之中，所以建立计费认证系统不能对现有的系统做较大的改动，因为如果需要改动，不仅需要很大的人力、财力，还可能会影响正常的计费工作。

3.2 设计基于PKI的计费认证系统的技术

计费认证系统既不是简单的安全Web应用，也不属于安全邮件的范畴，这决定了其特殊性的一面，要想利用我们的PKI系统为其提供解决方案，必须利用现有的PKI系统的开发工具来实现，但是如果直接利用开发工具访问PKI的API来实现，则可能需要对原计费系统进行较多的修改，甚至有可能需要重新编写系统程序，从而可能会影响正常的计费工作，这不是我们所希望看到的。于是必须找到一种适当的方法，使得基本上不对原应用程序做任何修改，就可实现计费认证系统。基于这些考虑，我们提出属性证书和Agent技术。

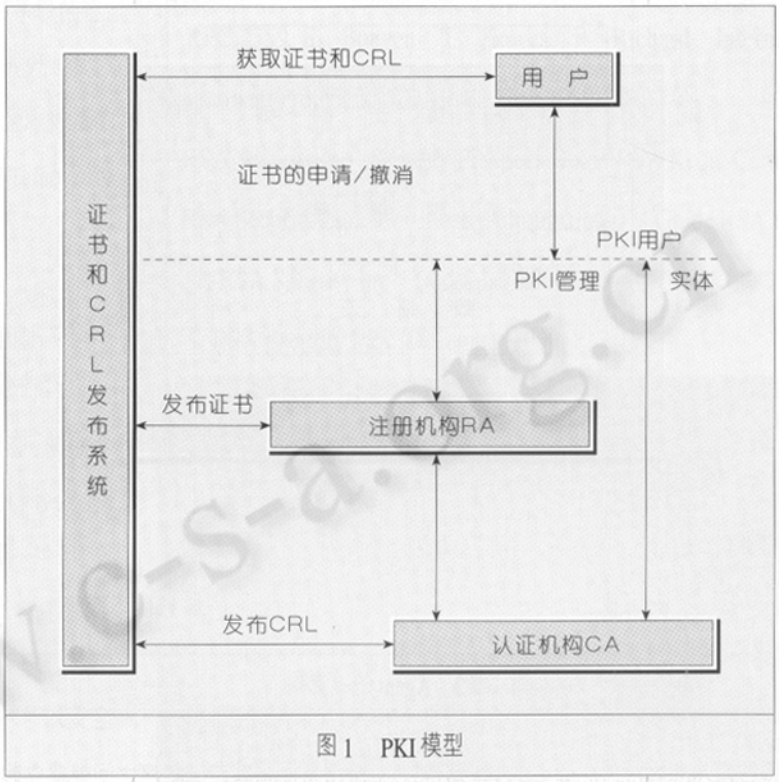

图1 PKI模型

3.2.1 属性证书AC (Attribute Certificate)

近年来，人们在公钥基础设施方面做了很多工作，促进了电子商务的发展。不幸的是，大部分PKI产品只用于认证用户的身份，而不能为合法用户恰当地授权。因此，这些PKI产品只解决了电子商务应用的半个问题。为此，美国国家标准委员会 (ANSI) X9会议提出了属性证书的方法。与公钥证书类似，属性证书通过一个属性机构 (Attribute Authority,AA) 对属性证书的签名把与实体有关的属性绑定到实体上。属性证书与公钥证书的主要区别在于前者包含属性而后者包含公钥。属性证书可以用于各种目的，比如，属性证书可以包含组成员信息、角色信息或者其他与用户相关的授权信息。

依据ANSI X9会议的说明，属性证书可以包含以下几个域：版本(Version)、主体 (Subject)、颁发者 (Issuer)、签名 (Signature)、序列号 (Serial Number)、有效期 (Validy)、属性(Attributes)、颁发者唯一标识符 (Issuer Unique Identifier) 和扩展 (Extensions)。依据校园网的实际需要我们可以在属性域中用国内 (home) 和出国 (abroad) 两个属性来分别标识用户访问免费网站和收费网站的权利。

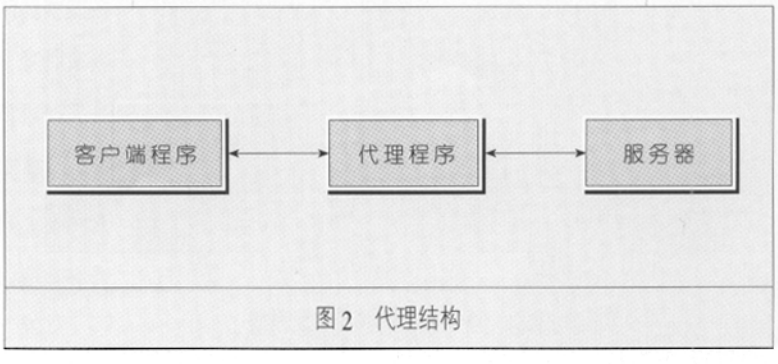

图2 代理结构

3.2.2 Agent技术

为了满足计费认证系统的设计原则，我们不能对原有计费系统做较大的改动，于是就不能运用PKI系统的开发工具直接把开发代码嵌入到系统中。为此，我们考虑了代理方案，即在计费服务器和计费客户端之间使用代理技术，在计费服务器上安装一个代理程序，使原来直接传输给服务器的信息先发送给代理程序，然后再由代理程序转发给计费服务器，如图2。这样客户端到计费服务器的安全问题就转变为客户端到代理程序之间的安全问题。为了方便，我们把这个代理程序称为Agent。因此，要用PKI来建立计费认证系统的具体工作也就转到了如何使Agent和PKI结合起来的问题。

要使客户端到Agent之间的信息得到安全的保障，必须使用加密技术，而校园网PKI的搭建使用户拥有了个人身份证书，于是只要为计费服务器颁发一张服务器证书，那么客户端与Agent之间就可以考虑使用安全套接字层SSL (Secure Socket Layer) 来实现信息传输的安全性。基于这种想法，我们对客户端程序做了一些修改，使其可以访问用户证书，与Agent建立SSL安全信道。由于SSL协议有源代码可以参考，所以对客户端的修改比较容易，重点还是Agent。

Agent一方面要扮演代理的角色，另一方面也要与计费客户端建立SSL信道。当然Agent只是在用户请求享受计费服务时要与客户端协商SSL信道，而其后的信息就可以在已建立的安全信道上传输，所以重点应实现的还是如何在建立SSL后实现代理功能。对此，我们提出过滤技术，即Agent把收到的信息缓存起来进行适当的处理，然后把有用的信息提交给服务器，使用过滤技术的一个主要的原因是由于计费服务器基本上没做什么修改，所以它无法直接识别有关证书方面的一些信息，如果不在Agent上对其进行处理和解释，而把所有信息都直接发送给计费服务器，那么将造成通信混乱。

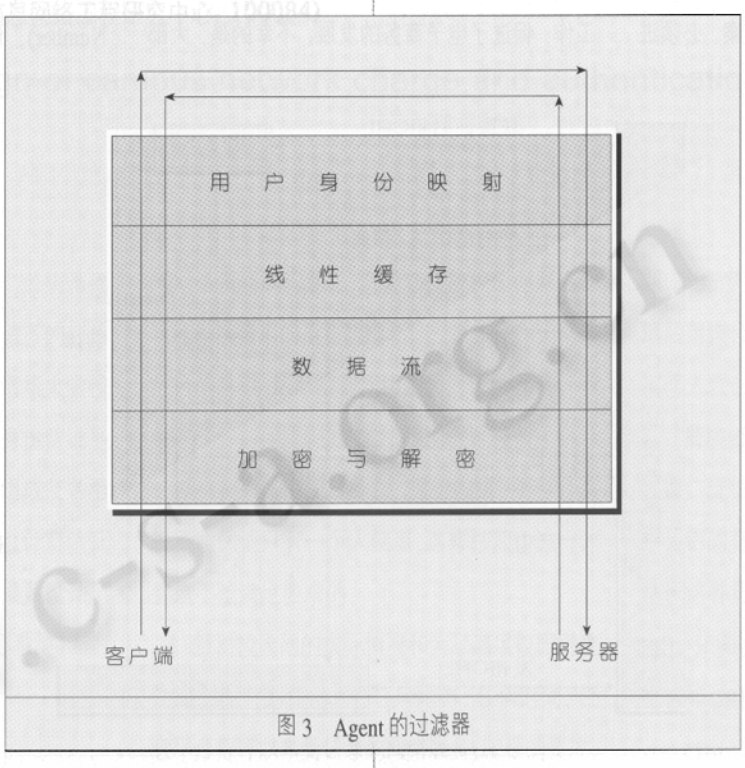

图3 Agent的过滤器

由于使用了加密技术而且还进行代理内容的处理，所以速度可能受到严重的影响，如果每个用户登录系统后没有释放原先建立的SSL信道，每个操作都使用SSL来进行，那么系统开销将是极大的，可能会因此而导致计费服务质量的急剧下降。考虑到清华大学校园网的实际需求，必须解决潜在的影响速度的问题。对此，我们考虑只在用户进行身份认证和授权时要传输敏感的身份信息时使用SSL信道，当认证和授权结束后，系统将自动释放已建立的SSL连接，其他信息的传输将按照原来的方式进行传输。因为身份认证的时间比较短，所以不会对系统造成太大的影响。这样采用Agent的过滤器就主要是对身份信息的解释，如图3所示，其主要包括四个方面的内容：加密与解密、数据流、线性缓存和用户身份映射。Agent收到其中一方的信息后，就把信息缓存起来，然后进行过滤，对证书内容中的身份信息进行解释，接着将解释后的内容送给计费服务器，再由服务器返回结果。

3.3 基于PKI的计费认证系统

属性证书和Agent技术为建立满足校园网实际需要的计费认证系统提供了可能性，为了管理的方便，我们把属性权威和认证服务集中在一个安全服务器上，这样，安全服务器在系统中就起着极为重要的作用。它一方面要检查用户的证书等身份信息，另一方面要为用户签发属性证书。

图4给出了利用属性证书和Agent技术来设计的计费认证系统。如果用户想享受计费服务，那么他就启动计费客户端程序，建立到安全服务器的一条会话，安全服务器把自己的身份证书发送给计费客户端程序，客户端程序检查安全服务器的证书，如果证书可信，那么用户提交用户身份证书给安全服务器，安全服务器也检查用户证书的有效性，倘若用户的证书也有效，那么安全服务器与客户端程序之间就建立起一条SSL信道。接着用户将请求享受计费服务，安全服务器根据用户的请求查看数据库，然后根据数据库中用户的记录信息来决定用户是有权访问国内信息还是可以出国，或者用户无权上网，接着为用户签发包括以上权利属性的属性证书，并把属性证书返回给用户，然后把该事件写入系统日志中。

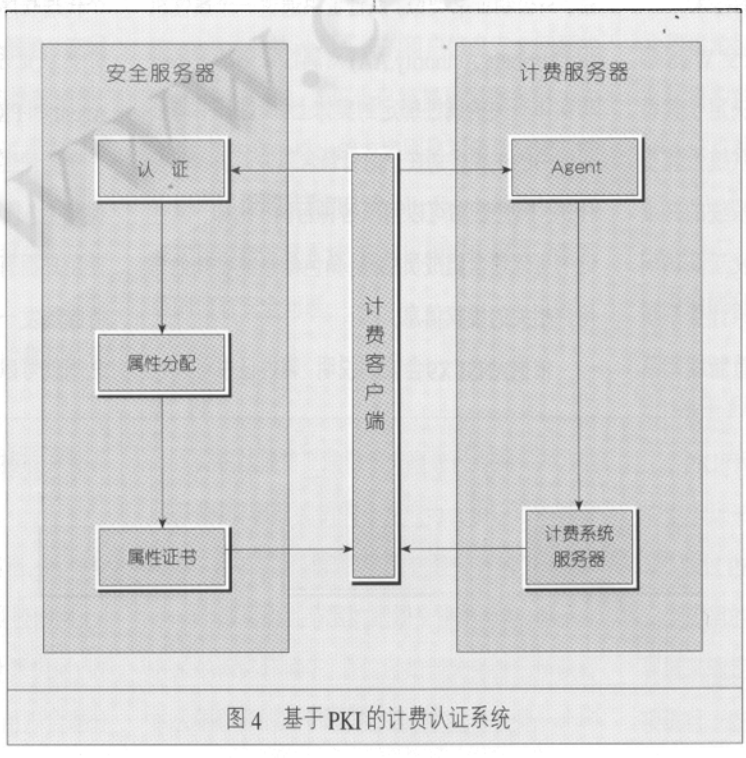

图4 基于PKI的计费认证系统

计费客户端程序收到属性证书后，向计费服务器发出请求，Agent程序把收到的请求信息转发给服务器，并截取服务器返回给用户的信息。接着要求客户端出示彼此的证书来建立起一条SSL信道，然后客户端程序通过SSL信道发送用户的属性证书给Agent，Agent验证属性证书的有效性后使用过滤器来提取权利信息(如出国或者国内属性信息)，把权利信息转发给计费服务器，计费服务器根据特定的权利信息返回给Agent特定的结果。Agent把结果转发给用户，用户就可以享受特定的计费服务了。

这里安全服务器可能会成为系统运行的瓶颈，所以应该考虑如何设置属性证书的有效期，用户可以依据这个信息缓存得到的属性证书，降低访问安全服务器的频率，从而提高系统的性能。另外，也可以把安全服务器设计成分布式服务器群，使用负载均衡技术来提高安全服务器的速度，在我们已经实现的基于PKI的Telnet安全平台就是采用后者来提高性能的。

3.4 计费认证系统的优点

(1) 足够的安全性。系统采用PKI安全平台，用证书的状态来反映用户身份的可靠性，目录服务器拥有最新的用户证书状态，使安全服务器能准确地在对用户的身份进行验证，保证了用户身份的真实性。计费系统客户端与服务器的交互信息全部通过预先建立好的SSL信道上进行传输，这保证了信息在传输过程中不会遭到窃取和修改等威胁，使用户可以安全地进行各种操作。

(2) 透明性。用户只需提交用户帐号和口令，其他工作均由服务器间通过SSL通信来完成。

(3) 方便管理。安全服务器拥有用户身份认证的日志信息，使管理员可以很方便地对用户的使用情况进行管理，能够对具体事件进行跟踪。

4 结束语

结合PKI开展各种安全应用已经成为当前信息安全的主流，也是电子商务的热点。但是利用SSL开展特定安全应用则是一个值得探讨的问题，也有一定的争论。本文提出的使用属性证书和Agent技术来开展应用的方法在国内比较少见，这还是一种尝试，但是从我们以前利用此方法设计和实现的Telnet安全平台来看，这种方法是值得推崇的，因为它具有通用性，可以为符合一定要求的客户服务器程序提供一种完整的安全解决方案，并且不需要对原有的程序做太多的修改。当然由于这仅仅是一些尝试，所以还会碰到一些具体的问题。

参考文献

1 RFC 2459, R. Housley. In W. Ford. W. Polk. Internet X. 509 Public Key Infrastructure Certificate and CRL Profile, January 1999。

2 RFC 2559, S. Boeyen. T. Howes. P. Richard. Internet X. 509 Public Key Infrastructure Operational Protocols - LDAPv2, April 1999。

3 RSA Security Inc. Security Practices Guide RSA Keon Certificate Server v5.

4 RSA Security Inc. Certificate Administrator's Guide RSA Keon Certificate Server v 5. 5. 1, U. S. A RSA Security Inc. December 2000, p23-30。

5. 1, RSA Security Inc. December 2000, P13-19。