第 28卷第 3期　　南 京 气 象 学 院 学 报　　Vol 28 No 3
2005年 6月　　Journal of Nanjing Institute of Meteorology　　Jun 2005

文章编号: 1000-2022(2005) 03-0416-07

身份认证及访问控制综合过滤平台 WebFilter的研究

戚玉松,　是湘全
(南京理工大学 电光学院, 江苏 南京　210094)

摘　要: 在分析电子政务网络安全建设的现状和不足的基础上, 结合电子政务对应用安全的需求, 设计了电子政务身份认证和访问控制综合过滤平台 WebFilter, 说明了该平台的设计模式、功能及组成, 详述了平台设计的关键技术和实现方法, 在客户端与应用服务器之间构建了安全的数据访问通道, 为其他基于 Internet的应用安全建设提供了有效的解决方案。

关键词: 电子政务; 身份认证; 访问控制; 对称密钥; 公开密钥
中图分类号: TP393. 04　　文献标识码: A

随着国内经济的快速发展, 信息化已经成为各个行业发展的必然趋势, 基于网络拓展传统政务的需求也变得非常迫切, 越来越多的政府部门希望在网上完成日常业务; 同时, 推行电子政务建设对于提高国民经济总体素质、提高现代化管理水平、加强政府监管、提高行政效率及密切政府同社会民众关系等都具有重要作用。电子政务 (e-government)以计算机和网络技术为基础, 以虚拟政府网站为平台将大量频繁的行政管理和日常事务按照设定模式的运行方式, 并逐渐得到广泛应用; 另一方面, 对其运行过程安全性的要求, 也越来越得到广泛的重视。

目前国内在电子政务的网络安全方案主要集中在网络和系统方面, 如防火墙、入侵检测、防病毒等等, 而针对网络应用层的安全平台或产品却较为薄弱, 特别在安全系统与应用系统的结合方面更容易被人们忽视。传统的安全系统与应用系统的结合往往采取在应用系统和操作系统之间插入一个安全插件来实现, 但该方式存在着许多弊端, 其扩展性较差。同时, 安全系统是动态的, 其需求也是在不断变化的, 一旦发生变化则必然导致安全插件的更新, 这就给应用系统的安全维护造成极大的困难和混乱[1]。

1　电子政务身份认证和访问控制综合过滤平台 WebFilter

基于现有电子政务实施过程中对应用安全的讨论, 在现有电子政务平台的基础上, 设计并实现了电子政务身份认证和访问控制综合过滤平台, 在用户与电子政务应用服务器之间构建了一个针对身份认证和访问控制的过滤体系, 从应用层面上补充了现有网络安全平台的不足[2]。

收稿日期: 2005-02-21; 改回日期: 2005-05-01
作者简介: 戚玉松 (1970-), 男, 安徽全椒人, 博士生, 研究方向: 计算机通信. E-mail jsjwshc@ yahoo. com. cn

1.1 WebFilter的设计模式

传统意义上的安全平台往往是建立在应用系统和操作系统之间, 这种模式实现简单, 安全性高, 但由于其通常以 API程序调用来实现的, 必然要求对原有应用系统进行二次开发; 同时, 针对不同的应用都要开发一个独立的安全模块, 开发量大, 也不利于多个安全模块之间的有机结合。WebFilter则不同于这种模式, 所有的安全控制都由独立的 WebFilter过滤服务器来完成, 所有用户与服务器的交互都经由 WebFilter过滤服务器进行安全协调, 不涉及到变更用户或服务器原有的应用系统和操作系统, 唯一要求是在用户主机上安装一个安全代理客户端, 实现与 WebFilter过滤服务器的安全交互 (图 1)。

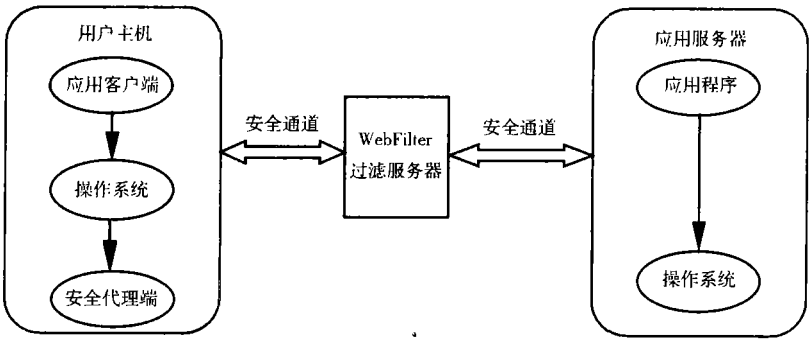

图 1　WebFilter设计模式

Fig 1　Design pattern of WebFilter

1.2 WebFilter的体系结构

WebFilter过滤平台由安全代理客户端和 WebFilter过滤服务器两部分组成, 在实施过程中, 安全代理客户端运行在用户的 Windows操作系统下 (Unix系统在本平台中未予涉及), 提供用户与 WebFilter过滤服务器安全通信的接口, WebFilter过滤服务器则有多个模块组成 (图 2)。

2 WebFilter的功能和特点

WebFilter作为用户与应用服务器之间的过滤平台, 其主要的功能特点有: (1) WebFilter的设计模式不同于传统的介于应用系统与操作系统的中间层平台开发模式, 而是采用在应用客户端和应用服务器之间添加一个中间过滤平台加以实现, 一方面屏蔽了传统模式以 API调用安全功能模块来实现应用系统信息安全的局限性; 另一方面则对所有应用提供统一的接口, 在用户添加新的应用时, 只需在过滤平台上添加相应的资源即可完成对新增应用的信息保护, 因而可扩展性强; (2) WebFilter将身份认证、访问控制、数字签名、抗否认、数据机密性和完整性等多个安全功能无缝结合在一起, 提供了一个整体的安全过滤平台; (3)WebFilter提供多种身份认证机制, 包括基于公钥密码的 PKI/CA数字证书和基于对称密码的 Kerberos。同时, WebFilter不仅仅提供对用户的身份认证机制, 还提供对服务器的身份认证机制, 身份认证介质支持 IC卡和 USB Key; (4) WebFilter提供用户分组和权限分级, 用户可以将平台中的用户与实际组织结构对应起来, 依据不同部门或级别设置不同的管理员权限, 从而使得每个管理员的权限都局限在自己的管辖范围, 从而避免了超级用户的存在[3]。

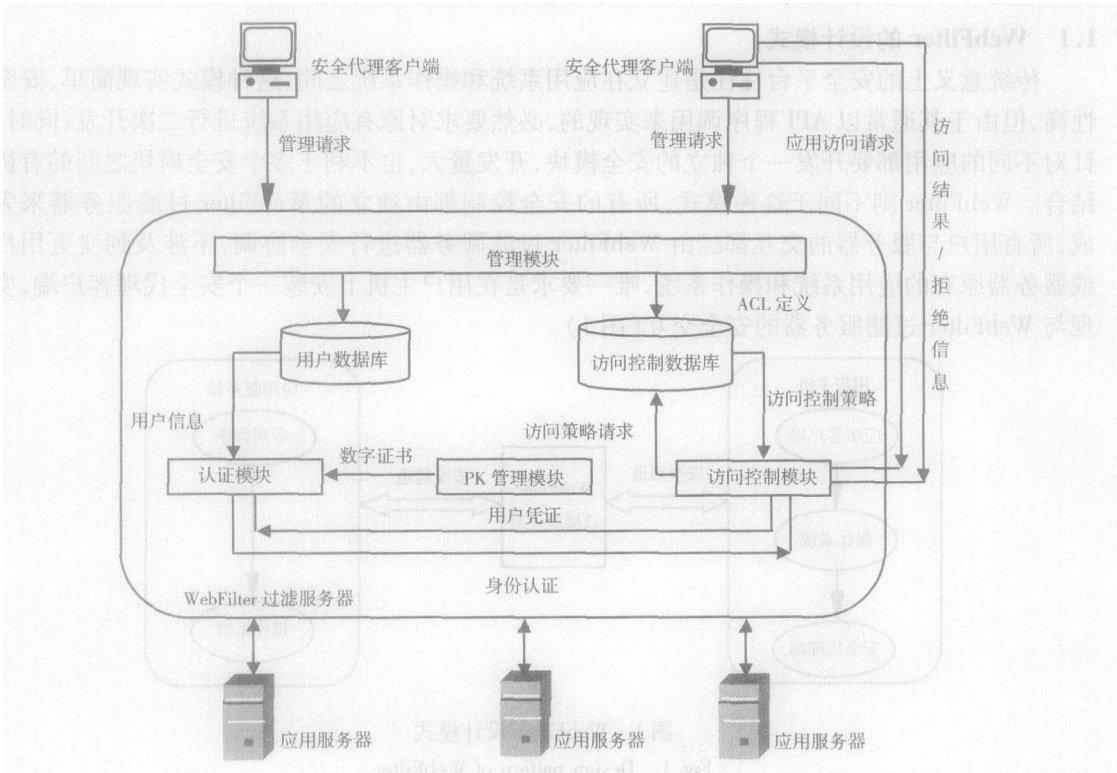

图 2 WebFilter体系结构

Fig 2 System structure of WebFilter

3 WebFilter的组成

WebFilter过滤平台包括过滤服务器和安全代理客户端两个部分, 安全代理客户端以代理模式安装在客户端的轻量级安全代理模块, 与用户原有应用客户端无缝结合, 实现应用客户端与 WebFilter安全机制的安全无缝集成; 过滤服务器平台包括如下几个部分 (图 3):

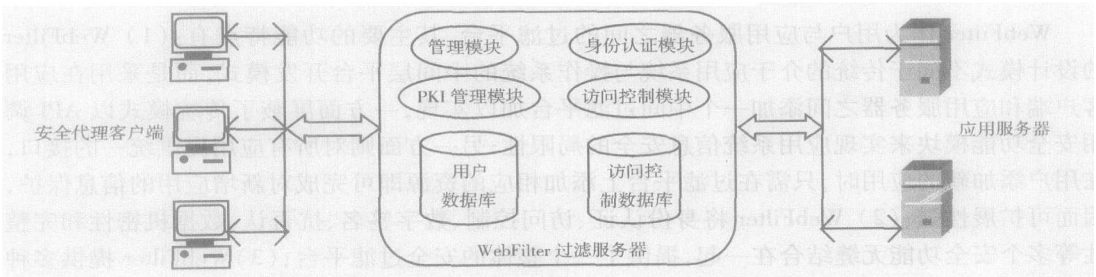

图 3 WebFilter结构组成

Fig 3 Components of WebFilter

(1)身份认证模块。身份认证模块是 WebFilter的核心模块之一, 支持基于公共密钥的 PKI和秘密密钥的 DCE/Kerberos两种身份认证方式。用户的身份认证和应用服务器的身份认证均由该模块实现。用户在进行认证时, 将自己的用户名 /口令或数字证书传送给 WebFilter的身份认证模块, 收到该信息后 WebFilter查询用户数据库并为通过认证的用户发放一个用户凭证。对应用服务器的认证过程与用户认证过程相同, 从而保证了数据交互双方的身份

确认。

(2)访问控制模块。访问控制模块也是 WebFilter的核心模块,其根据访问控制数据库中存储的访问控制策略对用户或服务器的数据请求进行判断识别,并提供对 Http、Ftp、Smtp、Pop3等常见网络服务提供访问控制。WebFilter将应用服务器上的资源定位到单个数据文件。访问控制策略采用 5元组(User, Server, Service, Operation, Data)表示,其可表达为用户 User对 Server上的 Service进行服务请求,可以对数据(文件)Data作相应的 Operation操作。另外,访问控制模块在用户与服务器之间建立了一条 TCP/IP安全访问通道,以类似于 VPN的方式对数据传输进行安全保护,并且访问控制模块与安全代理客户端之间的数据传输采用了 SSL通道,从而进一步加强网络通信端到端的安全保护。

(3) 管理模块。管理模块是 WebFilter提供给用户进行管理的操作平台的辅助模块,主要用于对用户数据库、访问控制数据库的管理和维护,对应用服务器的各个资源进行定义,以及对访问存取列表 ACL的定义和编辑。

(4) PKI管理模块。该模块与身份认证模块紧密相连,用于管理 PKI数字证书与用户的对应关系。

(5) 用户数据库和访问控制数据库。WebFilter实现对访问用户和应用服务器的双向认证,因此 WebFilter用户数据库中的用户信息不仅包括访问用户/用户组的各种属性信息,还包括应用服务器的各种相关信息。访问控制数据库用于存储 ACL,即用户对资源的访问权限,包括对整个电子政务平台中的各种资源定义以及相应的访问授权策略。

4 WebFilter的关键技术

4.1 AAs体系中心

公钥基础设施 PKI(Public Key Infrastructure)是国际上公认的信息安全保障体系的基础设施,目前正在大力推广 PKI/CA的建设,尤其是 CA的建设。由于 CA只是数字证书的签发和管理机构,负责证书的签发和管理,至于如何使用数字证书满足应用系统的安全需求则不是 CA的任务,所以业界正在倡导 CA+AAs的 PKI完整体系的研究,所谓 AAs,即包括身份认证中心(Authentication Authority)、授权中心(Authorization Authority)、管理中心(Administration Authority)等与 CA相对应基于应用的安全中心, WebFilter在整个 PKI体系中担当了 AAs的角色。

4.2 基于公共密钥 PKI/SSL的身份认证技术

WebFilter内置的 PKI管理模块和身份认证模块一起提供基于公共密钥的 PKI/SSL的身份认证。WebFilter所签发的数字证书遵循 X.509标准,把用户名与公钥等信息捆绑在一起,证书包含用户的身份信息、公钥及 CA的数字签名,信任 CA的任何一方(用户或服务器),都可通过验证对方证书上的 CA数字签名来建立起与对方的信任关系,并且获得对方公钥备用。同时,在安全代理客户端与 WebFilter过滤服务器的数据连接中, WebFilter提供 SSL协议保护,从而保证了端到端的数据传输安全性。

4.3 基于对称密钥 DCE/Kerberos的身份认证技术

DCE/Kerberos是一种被证明为非常安全的双向身份认证技术。DCE/Kerberos的身份认证强调了客户机对服务器的认证,而其他技术往往仅解决了服务器对客户机的认证。

在 WebFilter中,基于 DCE/Kerberos的身份认证是在身份认证模块加以实现的,身份认证模块在逻辑上由身份认证服务器和访问授权服务器两个部分组成,其在 WebFilter的元素表达

为: K—密钥; A—身份认证服务器; C—用户; P—访问授权服务器; PAC—访问授权服务器签发的授权凭证; S—应用服务器, 如 WEB服务器、数据库服务器等; $\{\cdots\}K_n$ 表示用 K_n 加密大括号中的内容; 实现步骤如下:

Step1: 用户 C从身份认证服务器 A 获得通信凭据 $\{K_1, C\}K_A$, 该凭证可以理解为由身份认证模块签发的一次性电子身份证或电子护照 (图 4)。

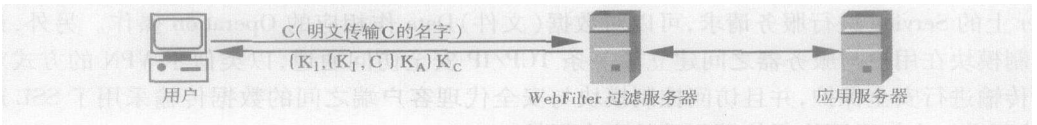

图 4 Step1模型

Fig 4 Step1 model

Step2: 用户 C使用 step1得到的凭据 $\{K_1, C\}K_A$ 申请访问授权服务器 P的通信凭据 $\{K_2, C\}K_P$, 该凭证可以理解为身份认证服务器为用户签发了访问授权服务器的电子介绍信 (图 5)。

图 5 Step2模型

Fig 5 Step2 model

Step3: 用户向授权服务器 P申请授权凭证 PAC。授权服务器根据身份认证服务器签发的电子介绍信, 为该用户签发一次性的出境许可 (图 6)。

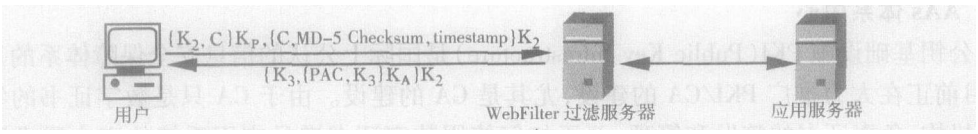

图 6 Step3模型

Fig 6 Step3 model

Step4: 用户申请能够向服务器 S证实自己身份、并得到授权许可的凭证 $\{PAC, K_4\}K_S$, 该凭证可以理解为应用服务器给该用户签发了一次性的入境签证 (图 7)。

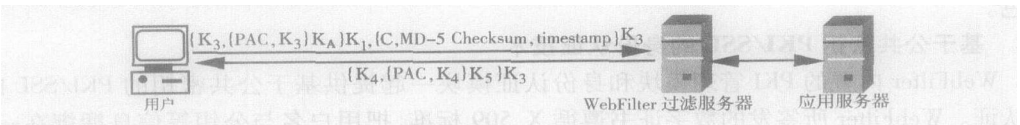

图 7 Step4模型

Fig 7 Step4 model

Step5: 用户 C获得与应用服务器 S通信的密钥 K_S, 该密钥可以理解为应用服务器为用户签发了一次性的境内通行证 (图 8)。

4.4 授权访问控制

WebFilter内置的访问控制数据库中存储了整个平台中的安全访问控制策略, 访问控制策略采用了扩充的自主访问控制矩阵, 每条安全策略定义为访问控制列表 ACL(U, S, P, O, D), U代表用户, S代表服务器, P代表某个指定服务, O代表操作, D代表数据项。比如 ACL(Nor-

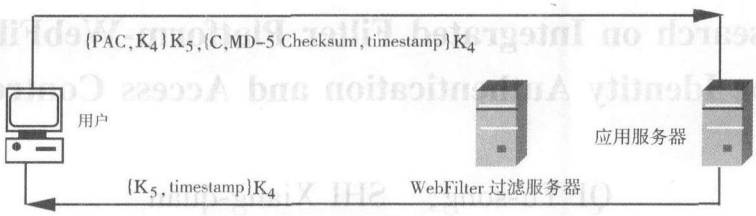

图 8　Step5模型

Fig 8　Step5 model

maUser, FTPServer, FTP, Get, test doc)则表示用户 NormaUser能够对 FtpServer服务器的 21端口进行访问, 且能够获取 test doc文档。WebFilter中应用服务器的资源最小粒度为数据文件, ACL能够控制对该数据文件的读、写、执行、移动等操作, 同时还提供数据文件传输是否加密的参数设置, 进一步加强了数据传输的可操作性。

用户在经过身份认证模块的认证后获得用户凭证, 过滤服务器的访问控制模块查询访问控制数据库, 以确定用户是否拥有对该资源的访问权限。如有则将访问请求传递给后方的应用服务器, 无则返回一个拒绝访问信息。

4.5　身份认证与授权访问控制的隔离

WebFilter过滤平台将身份认证过程和授权访问控制认为是两个相互独立的过程。WebFilter过滤服务器在接受到用户访问请求后, 对用户进行身份认证。在这个过程中包含两个步骤: 第一步即鉴别用户的身份, 第二步则获得描述用户的凭证。认证通过后 WebFilter过滤服务器方去查询访问控制数据库的信息, 然后依据数据库中的 ACL列表判断用户是否具有访问该资源的特定权限。

5　结束语

由于电子政务应用是基于不安全的 Internet的活动, 因此安全是成功进行电子政务的基石。WebFilter在用户与应用服务器之间构筑了一道身份认证和访问控制的屏障, 对用户和服务器进行双向认证和访问控制, 成功实现了访问过滤保护, 在实际应用中已经发挥了重要的作用, 为其他基于网络应用的安全控制提供了一种可借鉴的设计方法和实现途径。

参考文献:

[1]　许长枫, 刘爱江, 何大可. 电子政务安全建设中的访问控制研究[J]. 计算机应用, 2003, 23(7): 21-24.

[2]　谭寒生, 张　舰. PMI与 PKI模型关系研究[J]. 计算机应用, 2002, 22(8): 86-88.

[3]　金　光, 李荣茜. PKI加密技术在电子政务网络安全中的应用[J]. 宁波大学学报, 2003, 16(1): 34-38.

Research on Integrated Filter Platform–WebFilter for Identity Authentication and Access Control

QIYu-song SHIXiang-quan
(SchoolofElectricEngineering and OptoelectronicsTechniques, NJUST, Nanjing 210094, China)

Abstract: Based on the current situation and shortcoming of the e-government network in the process of security building, an integrated filter platform–WebFilter for identity authentication and access control was designed according to the requirement of e-government application security. The pattern of design, function, construction, key technology and implementation method for the platform are explained in this paper. A safe data access channel between user and application server is built, which provides a valid solution for other application security building based on the internet.

Key words: e-government; identity authentication; access control; symmetric key; public key