基于PKI的Web QoS分类系统研究

屈 峰，闫达远

(北京理工大学信息科学技术学院 北京 海淀区 100081)

【摘要】通过对目前的Web请求分类技术进行分析，发现其所采用的分类依据较多，QoS策略实现起来比较复杂，并且其安全性也需要改善。该文提出了一种新的基于PKI 的Web QoS分类系统，该系统采用PKI技术来提高服务器的访问安全性，通过Web QoS策略服务器来实现用户证书和QoS策略的绑定,降低了QoS策略实现的复杂程度,可以更好地满足网络用户的服务质量需求。

关 键 词 公钥基础设施; 环球网; 服务质量; 分类系统
中图分类号 TP393 文献标识码 A

Research on Classification System of Web QoS based on PKI

QU Feng，YAN Da-yuan

(School of Information Science and Technology, BeiJing Institute of Technology Haidian BeiJing 100081)

Abstract Through the analysis of classification technique of Web request, It is we found that a lot of information to classify is needed, so the realization of QoS policy is complex. In this paper, we put forward a new classification system of Web QoS based on PKI, it adopted PKI technique to reform the access security characteristic of Web server. We realized the binding between user's certificate and Qos policy with the use of Web Qos policy server. It makes the QoS policy realize easily. Therefore the demand of network user can be met better.

Key words public key infrastructure; Web; quality of service; classification system

Internet的发展使网络用户对Web服务器的访问量迅猛增长。目前，Web服务器所提供的是一种尽力而为的服务，网络用户的服务请求被不加区分地送入服务器，服务器按照先来先服务的原则尽力为网络用户提供相应的服务。但是，Web服务器的服务能力是一种有限的网络共享资源，这种不加区分的服务方式很容易使网络共享资源被快速耗尽，并导致服务器崩溃。此外，在电子政务、电子商务和国防工业中存在一些重要的网络业务，这些重要业务的服务请求可能会被其他业务服务请求所淹没，无法得到及时的响应，从而影响重要业务信息传递的实时性，严重时会给用户带来不可弥补的损失。

本文的研究试图通过在Web服务器中部署Web QoS业务分类机制来解决上述问题。目前采用的分类机制主要围绕OSI模型中与用户和应用有关的信息来进行，由于所依据的信息繁多，实现起来比较复杂，其安全性能也需要改善。在研究过程中，结合对Web技术、PKI技术和QoS技术的分析，本文提出了一种新的Web QoS分类系统。

1 相关技术介绍

1.1 Web技术

目前，Web技术在Internet中的应用十分普遍。网络用户利用网络终端的浏览器程序通过超文本传输协议(Hypertext Transfer Protocol，HTTP)与Web服务器进行通信，服务器应用软件通过监听网络接口(通常为TCP:80)接收浏览器程序的服务请求信息，服务器进行处理后向浏览器程序返回HTTP应答信息，浏览器程序处理应答信息后将相关信息显示给网络用户。

1.2 QoS技术

QoS技术包括业务分类技术、流量整形技术、准入技术、队列管理技术、队列调度技术和拥塞控制管理

收稿日期：2006 – 09 – 06
作者简介：屈 峰(1973 –)，男，硕士，工程师，主要从事计算机网络方面的研究.

技术等，通过这些技术可以对网络中的处理器资源、链路资源、节点缓存资源等共享资源根据网络用户的需求进行合理的分配和管理，从而更好地满足用户对网络提出的服务质量需求。网络中的QoS策略可部署在主机、路由器、交换机和服务器等网络实体中。

1.3　Web QoS请求分类技术

在Web服务器上部署QoS机制首先要对不同的网络用户业务进行分类，为后续的QoS控制机制的实现打好基础。目前的分类技术主要依据源MAC地址、目的MAC地址、源IP地址、目的IP地址、ToS、业务流类别、流标签、源端口号和目的端口号。此外，如文献[1]所述，还可以根据HTTP cookie、浏览器插件和URL等有关信息进行分类。

通过以上分析可以看出：(1)目前使用的通用Web技术不具有提供可区分的、相对公平的服务的能力，安全性也需要改善；(2)目前的Web QoS分类技术所使用的分类信息繁多，实现起来比较复杂。本文的研究过程中，结合使用目前成熟的PKI技术和QoS技术来解决上述两个问题。

1.4　PKI技术

公钥基础设施(Public Key Infrastructure，PKI)通过提供一种可信任的密钥管理和证书管理机制来支持目前正在使用的各种网络安全协议。典型的PKI系统包括证书权威机构(Certification Authority，CA)、证书注册权威机构(Registration Authority，RA)、证书库(Certificate Repository，CR)、证书申请者(Subscriber)和可信任方(Relying Party)5个基本部分。在具体实现过程中，系统的基本组成部分会有所变化，但所实现的功能是基本一致的，包括支持用户身份认证、保证信息传输的机密性、保证信息的完整性和不可抵赖性。多数PKI系统使用X.500标准，通过LDAP协议按照客户机/服务器模型为用户提供目录查询服务；使用X.509标准为X.500的用户名称提供一种通信实体鉴别机制和证书标准。

2　分类系统总体设计

2.1　分类系统工作原理

本文设计的分类系统的工作方式如图1所示，网络终端与Web服务器之间通过Internet相互访问；Web服务器通过局域网访问Web QoS策略服务器获取用户的证书和QoS策略。分类系统工作流程如图2所示。

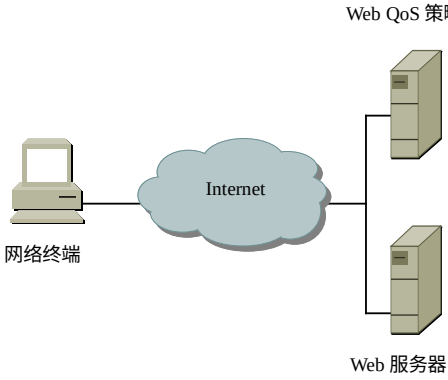

图1　分类系统工作方式图

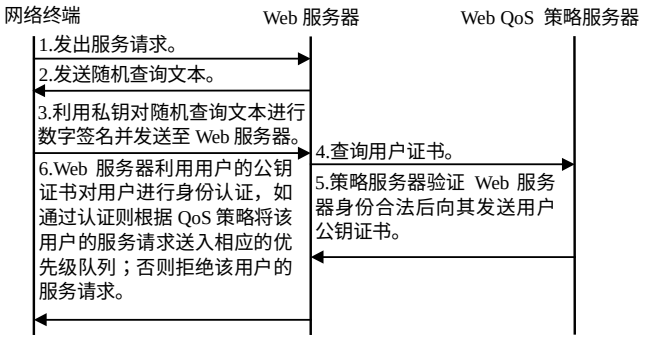

图2　分类系统工作流程

当网络用户向Web服务器发出服务请求时，Web服务器向网络终端发送一个随机查询文本，网络终端通过数字签名程序，利用用户智能卡中的私钥对该查询文本进行数字签名并发送至Web服务器。当Web服务器收到经过数字签名的查询文本后，向Web QoS策略服务器查询该用户证书，Web QoS策略服务器验证Web 服务器身份合法后，将用户的公钥证书发送给Web 服务器，Web服务器利用网络用户的公钥证书对网络用户进行身份认证，认证通过后根据QoS策略将该用户的服务请求送入相应的优先级队列等待服务。如果认证未通过，则拒绝该用户的服务请求。

2.2　分类系统主要功能

网络终端带有智能卡读取设备，用于读取存储于智能卡中的网络用户的私钥。网络终端的主要功能是

通过浏览器程序向Web服务器发送服务请求；响应Web服务器的身份查询请求；通过数字签名程序对Web 服务器发送的随机查询文本进行数字签名，并发送至Web 服务器。

Web服务器的主要功能是：(1) 接收网络终端发送的服务请求；(2) 向网络终端发送随机查询文本；(3) 接收网络终端进行数字签名的文本；(4) 向Web QoS策略服务器查询并获得网络用户的证书-公钥；(5) 使用用户的公钥对数字签名进行解签，以验证网络用户的合法身份；(6) 向Web QoS策略服务器查询获得网络用户的Web QoS服务策略，根据策略内容将用户请求送入相应的优先级队列，等待服务器服务。

Web QoS策略服务器的主要功能是：(1) 利用RA核实用户的合法身份；(2) 利用CA批准证书请求、生成公钥/私钥密钥对、备份密钥、签发证书、发放证书、撤消证书、发布CRL、生成CA根证书、交叉认证；(3) 利用CR存放证书、提供证书、确认证书状态。证书按照X.509v3标准生成，证书库通过X.500标准目录系统和LDAP协议对外提供证书查询服务

Web QoS策略服务器生成的用户证书根据X.509v3标准，利用扩展信息字段进行用户证书与Web QoS服务策略的绑定。ASN.1(Abstract Syntax Notation One)证书扩展信息字段的描述如下[2]：

```
Extensions   ::= SEQUENCE SIZE (1..MAX) OF Extension –证书扩展项定义
Extension    ::= SEQUENCE {
extnID        OBJECT IDENTIFIER,-扩展项类型，用OID表示
critical      BOOLEAN DEFAULT FALSE, -标识该扩展项是否为关键
extnValue     OCTET STRING-扩展项的值
}
```

其中，扩展项类型可以为字符串、数值等；critical标识为关键；扩展项的值对应相应的Web QoS策略服务所需的定义值，就可以完成用户证书与Web QoS服务策略的绑定。

2.3 分类系统结构

本文在对文献[1]所述的HP实验室设计和实现的Web2K服务器体系结构进行分析的基础上，结合PKI技术的需要，对其分类功能进行扩展，以满足提高服务器访问安全性和提供区分服务的需求。

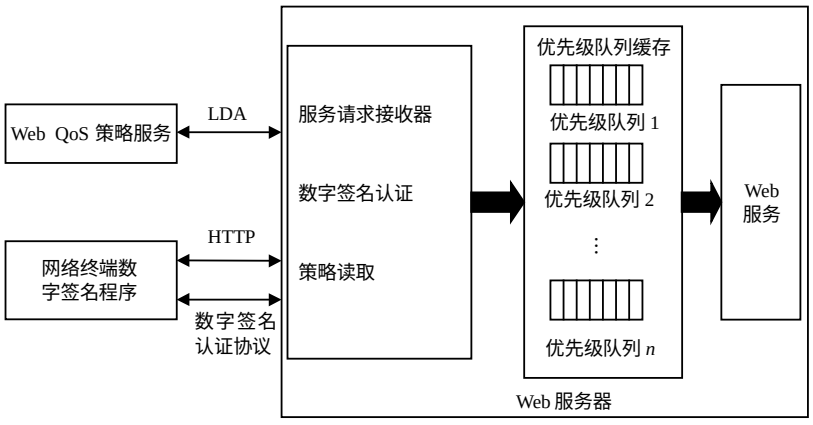

图3 分类系统结构示意图

本文设计的Web QoS分类系统结构如图3所示。Web QoS策略服务器通过LDAP协议为Web服务器提供用户的证书和QoS策略。网络终端通过HTTP协议与Web服务器进行相互访问，通过数字签名认证协议进行数字签名所需信息的传递。该系统通过策略服务器实现用户的证书和QoS策略的绑定；通过数字签名认证提高服务器的访问安全性。

在原有的Web体系结构的基础上，可对接收器和优先级队列的功能进行扩展，在接收器中增加数字签名认证和策略读取模块；将原优先级队列的双优先级结构扩展为*n*优先级结构。接收器的数字签名认证模块负责根据CA证书对网络用户身份的合法性进行认证，允许合法用户对服务器的访问，拒绝非法用户的访问，增强了Web服务器的访问安全性。接收器的策略读取模块负责从策略服务器中获取用户的QoS策略并应用于业务分类。原来的双优先级队列结构在使用中有一定的局限性，不能充分反映网络用户的不同服务质量需求，通过将其扩展为*n*优先级结构，可使其根据网络用户的需求情况进行多类业务的分类处理，以提供一种可区分的、相对公平的服务。

3　结 束 语

本文在对Web技术、QoS技术、Web QoS分类技术和PKI技术进行分析的基础上，提出了一种新的基于PKI的Web QoS分类系统，并对该分类系统的工作原理、功能和结构进行了描述。该系统采用PKI技术，利用用户证书对用户的合法身份进行认证，增强了Web服务器的访问安全性；通过Web QoS策略服务器进行用户证书与Web QoS策略的绑定，增强了QoS策略配置的安全性、简便性和灵活性，可以保证关键业务优先得到服务。由于所采用的技术均是目前正在使用的成熟技术，所以该分类系统在实际应用中容易实现，具有较高的实用价值。在实际使用过程中，可以不断结合新的技术，对该分类系统进行进一步的完善，从而更好地满足用户的服务质量需求。

参　考　文　献

[1] 林　闯, 单志广, 任丰原. 计算机网络的服务质量(第1版)[M]. 北京: 清华大学出版社, 2004.
[2] 汪　弘. 可定制证书的CA系统研究[J]. 计算机安全, 2005, (8): 32-35.

编　辑　熊思亮

(上接第520页)

3　顺控流程仿真

水轮发电机组计算机监控实时仿真系统可实现水轮发电机组的顺控流程仿真，包括机组停机转空载、空载转发电(含同期并列)、发电转空载、空载转停机等，在发电状态下还可实现有功功率及无功功率的调整。图4所示为水轮发电机组停机转空载部分顺控流程图[6]。

4　结 束 语

从该水轮发电机组计算机监控实时仿真系统的整体结构上看，该系统接近工程实际，可对实际工程中即将运行的控制流程加以校验，消除错误和缺陷；该系统还可用于对水电工程人员和软件开发人员的仿真培训工作，具有良好的经济性和可扩展性。如将模拟对象柜中的软件重新组态、修改，然后对LCU的IP地址重新定义，并启动其上的另一套监控流程，即可实现对水电厂闸门、公用设备和开关站的实时仿真监控。

参　考　文　献

[1] 林礼清, 罗　铸, 顾元昌. 水口水电站仿真系统[J]. 系统仿真学报, 2001, 13(1): 50-52.
[2] Devine K L. A digital computer based hydro/substation operator training simulator[C]// Proceedings of the Electric Energy Conference 1985. Newcastle, 1985, 10: 228-232.
[3] 方辉钦. 现代水电厂计算机监控技术与试验[M]. 北京: 中国电力出版社, 2004.
[4] 沈祖诒. 水轮机调节(第3版)[M]. 北京: 中国水利水电出版社, 2001.
[5] 王定一, 伍永刚, 孙扬声, 等. 水电厂计算机监视与控制[M]. 北京: 中国电力出版社, 2001, 8: 56-95.
[6] Luo Zhu. The first hydropower plant operator training simulator in china[C]//Proceedings of the Conference on Medium-small Hydro Equipment, HangZhou, 1993.

编　辑　熊思亮