维普资讯 http://www.cqvip.com

基于 PKI/PMI 的 Web 服务安全框架*)

王晓峻[1] 周晓峰[2] 王志坚[2] 沈祖诒[1]

(河海大学水利水电工程学院 南京 210098)[1] (河海大学计算机及信息工程学院 南京 210098)[2]

摘 要 Web services 的安全性是影响其能否被广泛应用的关键因素之一。目前,Web services 的安全性研究主要集中在对 XML 的扩充和制定 Web services 安全规范方面,但是这些规范仅描述了安全模型的框架,实用性较差。本文利用 PKI/PMI 技术,在不需要改变现有 Web services 协议的基础上,提出了一个基于 PKI/PMI 的 Web 服务安全框架,并给出了服务授权和访问控制的算法。

关键词 Web services,安全框架,PKI,PMI,访问控制

Web Services Secure Frame Based on PKI/PMI

WANG Xiao-Jun[1] ZHOU Xiao-Feng[2] WANG Zhi-Jian[1] SHEN Zu-Yi[2]

(Institute of Hydraulic and Hydro-power Engineering, Hohai University, Nanjing 210098)[1]

(College of Computer and Information Engineering, Hohai University, Nanjing 210098)[2]

Abstract The security is one of the key factors for which Web services can be widely used. At the present, the study of security is mainly centralized on extension of XML and security criterion establishment of Web services, and these criteria only describe the framework of security model, the utility is not good enough. On the bases that do not change the Web services protocol, we utilize PKI/PMI technology to put forward a security framework of Web services, and present the arithmetic of services authorization and access control.

Keywords Web services, Security framework, PKI, PMI, Access control

1 概述

Web services 是对象/组件技术在 Internet 中的延伸,是一种部署在 Web 上的对象/组件。Web services 结合了以组件为基础的开发模式以及 Web 的出色性能。一方面,Web services 和组件一样,具有黑匣子的功能,可以在不关心功能如何实现的情况下重用;同时,与传统的组件技术不同,Web services 可以把不同平台开发的不同类型的功能块集成在一起,提供相互之间的互操作。所以,Web services 被普遍认为是下一代分布式系统开发的模型。

然而 Web services 要得到广泛的应用,其安全性是一个重要因素。在开放的网络上,如果不能保障 Web services 的安全,那么 Web services 的应用将受到很大的限制。人们关注的 Web services 的安全问题主要包括:

(1)一致性。如何保证收到的消息没有被修改。

(2)机密性。如何保证传送消息不被未经许可的人得到。

(3)身份鉴别和验证。如何鉴别通信双方的身份。

(4)授权和访问控制。如何保证用户的操作没有超越他的权限。

目前,Web services 的安全性研究主要集中在两个方面:一是通过扩展 XML 来实现 Web services 的安全,如 XML Signature[1], XML Encryption[2], SAML[3], XACML[4], XrML[5]和 XKMS[6];另一个方面是通过制定 Web services 安全协议来实现 Web services 的安全,如 WS-Security[7], WS-SecureConversation[8], WS-Trust[9], WS-Policy[10]和 WS-SecurityPolicy[11]。XML Signature 和 XML Encryption 是比较成熟的 W3C 推荐规范,定义了数字签名和加密的 XML 编码格式。其他规范都仅定义了消息格式,大多只是定义了一个框架,需要和其他的规范协作,其安全性依赖于其他的安全技术,如 TLS/SSL 和 IPSec 等。

这些规范所定义的 XML 元素常常需要引用其它的网络资源,攻击者可以利用这点来实施拒绝服务攻击。同时,这些规范目前只提供了安全模型的框架,在很多实现的细节上都有待进一步的研究。

我们认为,利用现有的 PKI/PMI 技术,在不改变 Web services 现有协议的前提下,也能达到保证 Web services 安全性的目的。本文提出了一个基于 PKI/PMI 的 Web 服务安全框架,通过分级的 PKI 实现身份论证和加密,保证 Web services 的一致性、机密性、身份鉴别和验证,通过分散的 PMI(位于服务提供端)实现 Web services 的授权和访问控制。

2 PKI/PMI 简介

PKI(Public Key Infrastructure 公钥基础设施)是提供公钥加密和数字签名服务的安全基础设施[12]。PKI 主要包括四个部分:X.509 格式的证书(X.509 V3)和证书废止列表 CRL(X.509 V2);CA 操作协议;CA 管理协议;CA 政策制定。PKI 的基础是公钥证书(PKC , public key certificate),PKC 将用户的身份与其公钥进行绑定,形成用户的数字身份

*)国家自然科学基金(60573098)、江苏省自然科学基金(BK2006168)资助。**王晓峻** 博士生,主要研究方向为水利水电计算机系统;**周晓峰** 副教授,硕士生导师,主要研究方向为网络和分布式操作系统等;**王志坚** 教授,博导,主要研究方向为软件自动化及网络和分布式操作系统等;**沈祖诒** 教授,博导,主要研究方向为水利水电自动化工程等。

维普资讯 http://www.cqvip.com

证。

PMI(Privilege Management Infrastructure,授权管理基础设施)是 X.509 v4 中定义的一种授权机制,它在身份认证的基础上,以属性证书(AC, attribute certificate)的形式来实现授权管理[13]。PMI 体系和模型的核心内容是实现属性证书的有效管理,包括属性证书的产生、使用、吊销、失效等。

授权管理基础设施 PMI 以资源管理为核心,对资源的访问控制权统一交由授权机构统一处理。同公钥基础设施 PKI 相比,两者主要区别在于:PKI 证明用户是谁,而 PMI 证明这个用户有什么权限,能干什么,而且授权管理基础设施 PMI 需要公钥基础设施 PKI 为其提供身份认证。

3 基于 PKI/PMI 的 Web 服务安全框架

基于 PKI/PMI 的 Web 服务安全框架,如图 1 所示,表现为三层结构,主要由安全基础设施层和安全应用支撑层组成,其各部分的主要功能简述如下。

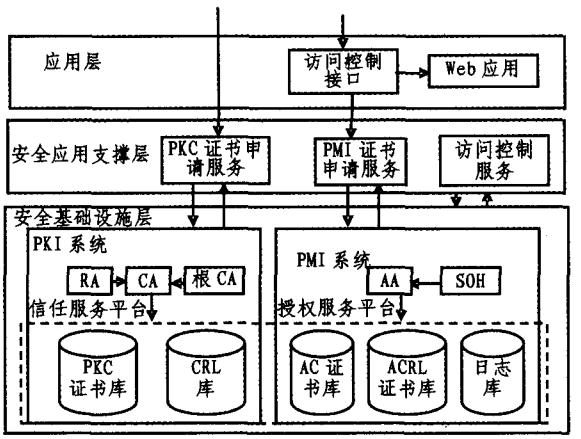

图 1 基于 PKI/PMI 的 Web 服务安全框架

3.1 安全基础设施层

安全基础设施层是整个服务安全框架的基础和核心,它包括信任服务平台和授权服务平台等。

信任服务平台是一个 PKI 的公钥管理系统,为上层应用提供完善的密钥和证书管理机制,具有用户管理、密钥管理、证书管理等功能,可保证各种基于公开密钥密码体制的安全机制在系统中的实现。以证书认证系统为核心,可以实现数字身份的统一互相认证。

授权服务平台采用基于属性证书(AC)的授权模式,向应用系统提供与应用相关的授权服务管理,提供用户身份到应用授权的映射功能。基于 PMI 的授权系统可提供与实际应用处理模式相应的、与具体应用系统开发和管理无关的授权和访问控制机制,可以简化具体应用系统的开发与维护。

3.2 安全应用支撑层

安全应用支撑层作为一个系统的接口,为上层的应用提供可信的基础设施的调用功能,它是一组安全控制组件的集合。

安全应用支撑层的安全组件主要有两类,一类是授权组件,提供 Web 服务的拥有者对 PKI 论证用户进行 Web 服务的访问授权,即确定哪些 PKI 论证用户有使用何种 Web 服务功能的权利;另一类是访问控制组件,实施对用户访问 Web 服务的控制,即判断该用户是否具有访问该 Web 服务的权利。

在该框架下,首先由信任服务平台为每一个用户颁发一个 PKC 证书,并负责对证书进行统一的、集中的管理(可以分级)。在此基础上,Web 服务的提供者利用信任服务平台和安全应用支撑层的安全组件分配 Web 服务的访问权限,Web 服务注册中心对用户提出的服务请求实现统一的访问控制。

4 授权服务算法流程

授权服务可以采用两种方式对 Web 服务的访问用户进行授权:一种是主动式的授权,即由 Web 服务的提供者主动对访问用户进行授权;另一种是被动式的授权,即由访问用户提出申请,然后由 Web 服务的提供者对其进行授权。两种授权服务的算法流程描述如下。

4.1 主动式授权服务算法流程

主动式的授权算法流程如图 2 所示。

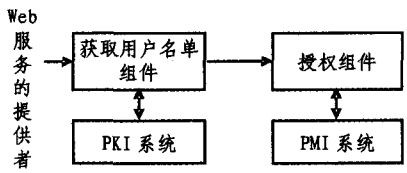

图 2 主动式授权算法流程图

其算法步骤描述如下:

(1)Web 服务的提供者调用安全应用支撑层的“获取用户名单组件”;

(2)“获取用户名单组件”从 PKI 系统中得到所有持有有效 PKC 证书的用户名单;

(3)调用安全应用支撑层的“授权组件”;

(4)“授权组件”调用 PMI 系统对用户进行授权,并生成相应的 AC 证书。

4.2 被动式授权服务算法流程

被动式授权算法流程如图 3 所示。

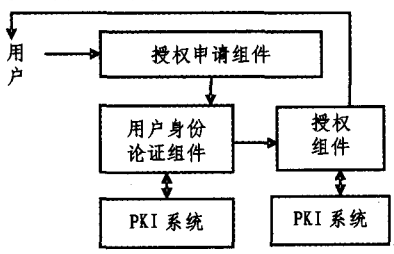

图 3 被动式授权算法流程图

其算法步骤描述如下:

(1)用户调用安全应用支撑层的“授权申请组件”,按 PMI 的要求填写授权申请;

(2)“授权申请组件”提取用户 PKC 证书的属性,然后发送给安全应用支撑层的“用户身份论证组件”;

(3)“用户身份论证组件”调用 PKI 系统,检查该用户是否是合法用户和 PKC 证书的有效性,如是则继续,否则申请失败;

(4)调用安全应用支撑层的“授权组件”;

(5)“授权组件”调用 PMI 系统对用户进行授权,并生成相应的 AC 证书;

(6)返回申请结果。

不管是主动式授权还是被动式授权,生成的 AC 证书均存放在 Web 服务的注册中心,不传输给证书的用户,以减少网络传输量,同时便于证书的分布式管理。

维普资讯 http://www.cqvip.com

5 访问控制服务算法流程

当用户利用 PKC 证书访问某个服务时，Web 服务注册中心调用相应的访问控制组件对服务调用进行相应的控制，以确保服务访问的安全性。访问控制算法流程如图 4 所示。

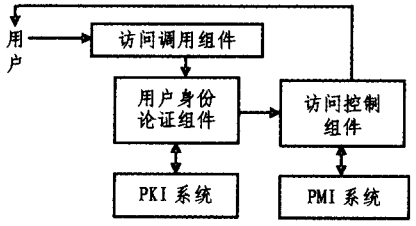

图 4 访问控制算法流程图

其算法步骤描述如下：

(1)用户调用安全应用支撑层的“访问调用组件”，请求调用某个服务；

(2)“访问调用组件”提取用户 PKC 证书的属性，然后发送给安全应用支撑层的“用户身份论证组件”；

(3)“用户身份论证组件”调用 PKI 系统，检查该用户是否是合法用户和 PKC 证书的有效性，如是则继续，否则请求失败；

(4)调用安全应用支撑层的“访问控制组件”；

(5)“访问控制组件”调用 PMI 系统，检查是否有与申请相一致的 AC 证书，以及该证书的有效性；

(6)如通过检查则提供相应的服务，否则拒绝提供服务。

结论 基于 PKI/PMI 的 Web 服务安全框架利用相对成熟的安全技术，来保障 Web 服务的安全，在目前是可以实现的。该安全框架不需对 Web Services 现有的协议作改动，仅需对现有 UDDI 和 SOAP 协议传输的内容进行加密即可。该安全框架提供的授权是分布式的，由服务提供者进行服务授权，经初步实验表明，该框架一方面与 Web services 提供分布式计算相一致，同时可以减少网络的传输量，相应地也降低了传输中的安全隐患。

参 考 文 献

1 Bartel M, Boyer J, Fox B, et al. XML-Signature Syntax and Processing. W3C Recommendation. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

2 Imamura T, Dillaway B, Simon E. XML Encryption Syntax and Processing. W3C Recommendation. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

3 OASIS Security Services TC. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)[S]. OASIS Standard. http://www.oasis-open.org/committees/security/2002-11

4 OASIS Access Control Markup Language TC. eXtensible Access Control Markup Language (XACML) Version 1.0[S]. OASIS Standard. http://www.oasis-open.org/committees/xacml/2003-02

5 OASIS Rights Language TC. eXtensible Rights Markup Language (XrML) Core 2.1 Specification. http://www.oasis-open.org/committees/rights/2002-05

6 XML Key Management Specification (XKMS) Version 2.0. W3C Working Draft. http://www.w3.org/TR/2003/WD-xkms2-20030418/2003-04

7 IBM, Microsoft, VeriSign. Web Services Security (WS-Security) Version 1.0. http://www.ibm.com/developerworks/library/ws-secure/2002-04

8 IBM, Microsoft, RSA Security, VeriSign. Web Services Secure Conversation Language (WS-SecureConversation) Version 1.0. http://www.ibm.com/developerworks/library/ws-secon/2002-12

9 IBM, Microsoft, RSA Security, VeriSign. Web Services Trust Language (WS-Trust) Version 1.0. http://www.ibm.com/developerworks/library/ws-trust/2002-12

10 IBM, Microsoft, BEA, SAP AG. Web Services Policy Framework (WS-Policy) Version 1.0. http://www.ibm.com/developerworks/library/ws-polfram/2002-12

11 IBM, Microsoft, RSA Security, VeriSign. Web Services Security Policy Language (WS-SecurityPolicy) Version 1.0. http://www.ibm.com/developerworks/library/ws-secpol/2002-12

12 ITU-T Recommendation X.509, Information Technology——Open System Interconnection ——The Directory: Authentication Framework, 1993

13 ITU-T Recommendation X.501, Information Technology——Open Systems Interconnection ——The Directory: Models, 2001

(上接第 22 页)

后，算法最终可以收敛到一个稳定的最优解。

之后，随机的选择工作节点死亡。再次运行算法，根据适应度得出最优联盟。算法运行 5 代后无法再次满足约束条件。这时，将分块起始点分别沿水平和垂直方向移动 10m，重新分块，再次运行算法，得到最优解，运行 2 代后，网络最终失效。运行结果如表 2 所示。

结论 在大规模随机散布模式无线传感器网络中在保证全网可靠性的前提下，以较低的能耗、较少的节点数动态地结盟，以延长传感器网络的生命周期，这无疑存在着广阔的研究前景和应用价值。本文针对上述问题，设计了一种基于遗传算法的动态联盟优化模型，该方法具有以下特点：

- 遗传算法本身非常适合在传感器网络内进行分布式计算，即可以在不同的节点上分别进行若干代繁殖，再综合比较得到最优动态联盟。
- 算法具有全局搜索能力，因而可以克服局部最优解问题。
- 算法具有快速性、鲁棒性，并且易于扩展至能解决任何数量级上的传感器网络动态联盟问题。

参 考 文 献

1 Bulusu N, Heidemann J, Estrin D. GPS-less low cost outdoor localization for very small devices: [Technical report]. Computer science department, University of Southern California, 2000

2 Byrne A J. The virtual corporation. Business Week, 1993(2): 98～103

3 Hightower J, Borriella G. Location systems for ubiquitous computing. IEEE Computer, 2001, 34(8): 57～66

4 Zhang H, Hou J C. Maintaining scheme coverage and connectivity in large sensor networks: [Technical report]. UIUC, 2003