**Web服务中基于信任的安全性**

信息系统研究所分布式系统集团维也纳技术大学由Ao.Univ.Prof Mag Dr. Schahram Dustdar和Univ.Ass Dipl.-Ing Dr.techn Clemens Kerer通过Christian Platzer Samerweg 35 6060 Hall in Tirol

维也纳，2004年5月2日

**1引言**

今天，越来越多的公司采用管理员来维护他们的网络，调整用户的权限和保持一切运行。随着这些公司规模的不断扩大，这些活动的工作量将大大增加，直到一个人不能再忽视这种权限，例外和政策的网络时为止。 除了增加，删除或调整权限所产生的开销，这还可能导致一些严重的安全漏洞。 如果计算机系统能够自行决定是否向请求用户授予访问权限，这不是很好吗？

在软件开发领域中出现的另一个趋势是以Web服务的形式重用功能。 Web服务是在通过网络连接的两个应用程序之间建立通信的平台独立的方式。这里的政策维护甚至更昂贵。分布式应用程序可以使用许多不同的功能，每个单独的功能都需要以正确的方式加以保护。人们正确地调整所有安全级别是一项艰巨的任务，因为需要添加新的功能，而其他的功能已经过时而不再使用。

SimOffice是一个安全感知的网络环境，通过组合通用安全标准和一种全新的方法来判断用户的意图来攻击这些问题。目标是创建一个独立的系统，根据可信赖性做出决策。这样，“思考”是由系统完成的，而一个人的主管在某些特殊情况下仍然可以影响判断。评估本身试图模仿人类行为和人类的信任。当然，该概念不限于Web服务，而是可以应用于计算机网络中的几乎每个安全敏感区域。

SimOffice将模拟办公室内可能的环境，甚至可以通过Web服务访问咖啡机。 什么是更糟糕的惩罚不良行为比拒绝咖啡！

**1.1 动机**

今天，大多数软件公司正在实施基于Web服务的新标准的工具。 考虑到IBM和Microsoft等几家重要软件公司的快速开发和强有力的承诺，很快就可以预见到整个网络中的各种即用型服务。 例如，Google是网络上最受欢迎的搜索引擎之一，已经为Web查询提供了一个Web服务。 基于提供的API的实现是直接的，并且需要基本的编程技能。

但Web上可用的Web服务不会成为这些标准的唯一应用程序。模块性和语言无关性联合应用铺平了道路，甚至在公司封闭的环境中使用基本的Web服务 网络。因此，这是很有可能实现一个公司的应用程序作为Web服务，使他们可以通过公布的描述。这样的优点是显而易见的：服务在整个网络是完全独立的实现或操作系统和可用的到处都是。 鼓励开发人员使用提供的功能，而不需要了解所涉及的代码。 每个Web服务在集中点注册，使服务发现更容易。

计算机系统的发展的另一个趋势是适应人类的思维方式，以解决安全方面，如访问权或其他各方的意图判断。结合两者，网络 服务和直观的访问管理方式是本论文的主要动机。

**1.2 问题的定义**

主要问题是创建一个合理的可访问性和访问限制的组合。

一个Web服务联盟必须满足一些要求，保留有用的性质：首先，如果可用服务的总数增长太大，无法手动维护，则不能固定对单个Web服务的访问权限。需要动态调整访问级别的动态技术。不过，必须有一个设施，以改变访问权限手动。否则管理员 如果有必要，将无法自定义访问限制。

另一方面，整个系统必须访问每一个授权用户。如果没有人能使用它，什么是完美的安全系统？为了满足上述要求，一种机制是利用大多数人每天使用：信任。这种方法打算模仿人类在判断对手的行动是否有利时做出的决定。 目标是创建Web服务的联合，其中通过用于传输和隐私的公共安全技术以及用于访问控制的基于信任的方法来确保安全性。

创建这样的系统不是一件容易的事，因为受信任机制的系统往往是不稳定的长期观点。这将导致一个完整的不信任对方，BLI信任状况。这两种情况都不适用于以提供公共服务为主要任务的计算机系统。本文将对建立信任关系的问题 IPS和评估基于信任的访问控制能力。

**2 Web服务的概念**

在Web服务的定义中给出：“可以通过Internet协议通过有效的XML文档集成到外部系统的任何进程”。 与一般的服务不同，Web服务基于数据传输，方法调用和发布的规范。这常常被误解，当提及Web服务时，它有时指的是在Web上提供的一般服务，例如网页上的天气预报。 天气预报是一种服务，并为各种用户提供其功能，但除非它包括通过SOAP与其他应用程序通信的接口，否则它不是定义的Web服务。Web服务可以被视为软件公司一个接口与其他通信软件组成部分。它们有一个特定的功能，可以通过一种特殊的远程过程调用。事实上，他们甚至演变 传统远程过程调用。二者区别在于界面和运输方法。此外，不能使用普通浏览器查看或使用web服务。他们要求表单表格信息嵌入在XML文档。

**3 HTTP**

在互联网上随处可见，HTTP（超文本传输协议）是用于Web浏览器与服务器之间的数据连接无处不在的协议。该协议是由现行标准HTML文档，虽然它被设计为可扩展到几乎任何格式的文档，如XML为例。HTTP版本1.1在RFC 2068 记录。它运行在TCP连接，通常上到端口80，虽然其他端口可以使用。成功连接后，客户端向服务器发送请求消息，后者将回复消息发送回。最简单的HTTP消息”通过发送命名文档来回复服务器的URL。如果文件不存在，服务器可以发送HTML编码的消息，这说明。这种沟通形式代表性典型的请求/响应机制。客户端向服务器发送对特定文档的请求，并等待响应。如果服务器未响应请求的文档，则由客户端等待超时并再次请求相同的文档。 这种松散耦合类型的通信在客户端 - 服务器架构中是非常常见的。

除了得到请求，客户端还可以发送头和POST请求，其中职位是最重要的。柱用于HTML表单等操作，要求客户发送服务器的数据块。发送页眉和空行后，客户端发送数据。这样，Web服务使用HTTP协议传输数据的有效载荷和服务网络服务的探索。现在是时候解释传输数据的样子了。

**4 XML**

XML是可扩展标记语言的缩写。它旨在通过提供更灵活和适应性更强的信息表示方式来描述数据并改进Web的功能。它被称为可扩展的，因为它的格式不像HTML那样固定。相反，XML是一种元语言，它允许您设计自己的自定义标记语言。标记是一种在文档中指定结构的机制，而向文档添加标记的方式由XML规范定义。但与HTML不同，XML不指定语义或一组标签。没有规定的方法来呈现XML文档，所以语义将由应用程序使用它或样式表来定义。

重要的是指定字符集以避免对提供的数据的误解。下一行描述文档的根元素。元素是在XML文档中存储数据的一种方法。

越来越多的应用程序使用XML存储信息，因为它的好处。其中一些是：

•结构是定义明确的，可以在不同的计算机系统之间传递，否则这些计算机系统将无法通信。

•数据有效载荷封装在标签中，因此可被人类观察者读取。

•由于其文本性质，XML文件与平台无关。这些优点使XML成为Web服务之间通信的完美格式。为了确保为每个Web服务使用平台和语言，开发了SOAP。它是一个具有定义元素和预定义结构的XML应用程序。

**5 发布和查找Web服务**

使用SOAP，Web服务之间的通信是可能的和结构化的，并且每个参与者知道如何发送或接收相应的SOAP消息。 完成Web服务的通信体系结构的最后一步是定义如何在实现后访问服务。 这是Web服务描述语言（WSDL）的步骤。WSDL将服务描述为网络端点或端口的集合。 它再次是一个XML文档与定义的语法，其中端点和消息的抽象定义与其具体的网络部署或数据格式绑定分离。 WSDL文档使用以下元素描述Web服务：

•类型：数据类型定义的容器。 与SOAP相反，WSDL可以使用某种类型的系统（例如XSD)定义类型。

•消息：定义在单个RPC中传递的数据。

•操作：服务支持的操作（方法）的描述。

•端口类型：一个或多个端点支持的一组操作。

•绑定：特定端口类型的具体数据格式规范。

•端口：定义为绑定和可以找到的网络地址的组合的单个端点。

•服务：相关端点的集合。

**参考文献**

[1]T. Dimitrakos。一种面向服务的信任管理框架。在信任，声誉和安全：理论和实践，第53页- 72 法尔科内，Suzanne Barber，Larry Korba和Munindar Singh，2003.

[2] J. Dunn 信托与政治机构，2000.

[3]IBM Web服务联盟语言（WS-Federation），http://www.ibm.com/developerworks/library/ws-fed/，2003.

[4]T. Beth，M. Borcherding，B. Klein开放网络信任的验证，2000.

[5] p.f.pires，m.r.benevides，andm.mattoso buildingreliablewebservices组合物。在Web、Web服务和数据库系统中，第59 - 72页 Akmal B. Chaudrin，Mario Jeckle，Erhard Rahm and Rainer Unland, 2002.

[6] L. Eschenauer，V. D. Gligor，J. Baras。移动ad-hoc网络中的信任建立，2002.

[7]信息保障与安全教育研究中心（CERIAS）。形式化的信任，欺诈，和脆弱性，http://www.cs.purdue.edu/homes/bb/nsftrust.html，2003.

[8]谷歌公司谷歌Web API的开发工具包，http://www.google.com/apis/，2004.

[9] 电子版转载来自社会学系，牛津大学.

[10]IBM Web服务信任语言（WS-Trust）,http://www.ibm.com/developerworks/library/ws-trust/index.html，2002.

[11] ]美国overhagen和P. Thomas阳离子：WS规范使用UDDI指定Web服务的改进。在Web、Web服务和数据库系统中，第100 - 110页。Akmal B. Chaudrin，Mario Jeckle，Erhard Rahm Rainer Unland，2002.

[12] N. Shankar和W. A. Arbaugh。普适计算的信任.

[13] IBM。Web服务安全（WS-Security），http://www106.ibm.com/developerworks/webservices/library/ws-secure/，2003.