文章编号:1673-5005(2013)04-0181-05 doi:10.3969/j.issn.1673-5005.2013.04.031

多维度 Web 服务安全性评估

段友祥, 赵德明

(中国石油大学计算机与通信工程学院,山东 青岛 266580)

摘要:安全性已经成为 Web 服务质量的重要指标。通过增加 Web 服务安全评估中心扩展现有基本 Web 服务架构提出一个新的模型,并基于安全属性 SoS(security of service)和用户偏好对 Web 服务进行安全性评估。结果表明,该模型能根据用户偏好修改安全属性的权重,并在提高服务选择的准确度和可用性方面都有较好的效果。

关键词:Web 服务; 安全属性; 多属性决策理论; 信息熵; 用户偏好

中图分类号:TP 393 **文献标志码**:A

Multiple dimension security assessment of Web service

DUAN You-xiang, ZHAO De-ming

(*College of Computer and Communication Engineering in China University of Petroleum*, *Qingdao* 266580, *China*)

Abstract: Security of Web service is an important indicator in quality of service. A new model was developed by adding security evaluation center to expand the existing Web service model, and the security of Web services was evaluated based on security attributes and user's preferences. The results show that this model can set the security attributes according to user preference weights, and improve the accuracy and availability of service selection.

Key words: Web service; security attribution; multiple-attribute decision making theory; information entropy; user preferences

随着 Web 服务发展的日新月异,其面临的安全性威胁日益增大,应用特性造成的未知漏洞也在不断增多,急需对其安全程度给出一个比较明确的定义。Web 服务安全涵盖的内容比较多,主要包括对用户的认证、授权、事务的审计、服务的可用性、所交换的消息的保密性和完整性、请求或消息的不可否认性等方面。当前国外对 Web 服务安全问题的研究大部分集中在制定 Web 服务安全性规范及对应规范的实现[1-3]。国内对 Web 服务安全性的研究大部分集中在对各种安全协议的使用、检测程序应用漏洞[4]、用传统信息安全评估标准对 Web 服务进行安全评估[5-6]。包永堂等[7-8]构建了基于 Soap 注册和安全令牌代理的 Web 服务安全模型,给出了一种量化 SoS(security of service)值和安全等级的方法[8]。由于国内外对 Web 服务安全性的研究主要集中在如何制定和实现 Web 服务安全协议、开发 Web 服务漏洞扫描工具以及分析和跟踪 Web 服务安全性规范方面,而对如何客观、科学地评估安全的研究比较缺乏,对 Web 服务安全性进行测试和评估是非常重要和必要的。笔者通过增加 Web 服务安全评估中心扩展现有基本 Web 服务架构提出一个新的模型,并基于安全属性 SoS 和用户偏好对 Web 服务进行安全性评估。

1 Web 服务安全评估总体架构

1.1 基于基本 Web 服务架构的安全评估模型

Web 服务基本架构中有三个服务角色:服务提供者、服务客户和服务代理。首先在合适的平台或代理(Proxy)上创建一个 Web 服务应用并生成对应的 WSDL 文档,服务提供者基于这个平台发布一个 WS(Web Service,Web 服务)。接着,服务细节被发送到 Proxy 以存储在服务数据库中。调用服务的客

收稿日期:2012-10-20

基金项目:山东省自然科学基金项目(ZR2009GM010);中央高校基本科研业务专项资金资助项目(10CX04040A)

作者简介:段友祥(1964-),男,教授,硕士生导师,主要研究方向为网络与服务计算、数据库及信息系统。E-mail:yxduan@upc.edu.cn。

户向代理注册,然后在 Proxy 的资源库中用 UDDI 检索服务,检索符合用户需求的 Web 服务。最后通过 SOAP 调用该服务。

通过对 Web 服务安全性相关技术的分析,研究已有的 Web 服务安全性测试和评估的方法,结合端到端 Web 服务通信过程,从三个角度对 Web 服务安全进行评估。

(1) 偏好安全:面向 Web 服务请求方,反映用户对安全性的偏好。根据 Web 服务的安全特性,设计一个合理的安全需求问卷,主要包括认证、授权、审计、完整性、可用性、机密性、不可否认性和服务器安全程度,通过网页的形式获得。

(2) 协议安全:主要针对 Web 服务的部分安全性协议。针对国际上普遍采用 XML Signature、XML Encryption 以及 WS-security 技术,通过分析 Web 服务的头文件,确定该 Web 服务使用哪些安全协议,判断是否满足用户的安全需求。

(3) 发送安全:主要针对服务发送端漏洞存在的情况,反映服务发送安全程度,包括传统的与 Web 应用相同的漏洞以及 Web 服务特用的漏洞。前一种漏洞通过扫描工具扫描获得;后一种漏洞则使用前面问卷调查方式获取的特有漏洞结果;最后,针对两种漏洞的存在情况,以风险值的方式给出安全值,为用户选择 Web 服务提供参考。

因此,Web 服务基础架构应该提供一种使用户信任已发布服务安全的机制。于是,在已有 Web 服务架构的基础上,扩展出一个安全评估中心来完成 Web 服务安全评估,形成一个基于基本 Web 服务架构的 WS 安全评估模型,如图 1 所示。按照服务安全评估数据的处理过程,可将安全评估中心分为三个部分:数据收集、数据处理和安全评估。

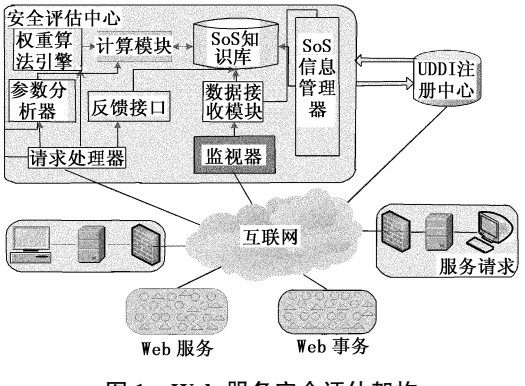

图 1 Web 服务安全评估架构

Fig. 1 Architecture of Web security evaluation

1.2 数据收集

Web 服务的松散耦合性、平台无关性等特点决定了数据收集会面临很多困难,所以能否及时、准确、完整地收集安全评估数据是安全评估过程一个很重要的环节。

监视器负责监测部署在网络上的可选服务以确保其可访问性和可用性,并动态地收集服务实际执行过程中的信息,以获取所有与网络环境有关的 SoS 属性、服务器端的 Web 服务特定漏洞以及应用端的与传统 Web 应用相同的漏洞等数据。

请求处理器是面向用户的模块,该模块主要负责接收用户的反馈,包括用户对各个安全属性的要求,并为用户配置系统参数和偏好提供接口。

1.3 Web 服务安全数据处理

当系统获得及时、准确和完整的 Web 服务安全评估数据之后,需要对这些数据进行初步处理,利用处理后的数据进行初步服务筛选,把不可用或不符合用户需求的服务过滤掉。同时,把服务器端获得的协议及发送安全数据按照一定的原则处理,给出每个 Web 服务的安全属性值,为最后的评估工作提供数据支持。

系统参数分析器获得请求处理器提交的 Web 服务安全评估数据后,利用多属性决策理论分析请求处理模块提交的参数并提交至计算模块,计算模块利用这些结果进行服务的筛选。

权重算法引擎在接收到用户的参数和偏好配置数据后,会利用层次分析法(AHP)处理各个用户偏好,将结果发送至计算模块。

数据接收模块主要是处理监视器获得的服务器端安全数据,包括对 Web 服务采用的安全协议以及服务器的安全程度的计算,并将这些数据提交到 SoS 知识库,为计算模块进行安全评估提供数据支持。

1.4 Web 服务安全评估

经过数据收集和数据处理之后,安全评估中心利用系统参数分析器和权重算法引擎处理后的数据,依据安全评估算法对可选服务进行评估,最终选出更符合用户需求的 Web 服务。

计算模块是安全评估中心的关键部分,包含所有数据计算和 SoS 评估结果。首先,从 SoS 知识库获得 Web 服务的安全数据,同时从权重算法引擎获得用户的偏好权重;然后,利用多属性理论中的信息熵方法对可选 Web 服务进行排序,并将安全评估结果存储到 SoS 知识库。

SoS 知识库是该架构的存储中心。SoS 信息管理器控制和管理 SoS 知识库和 UDDI 注册中心之间

数据转换。当用户使用 Web 服务时,可以通过 UDDI 注册中心查询到该 Web 服务的安全评估值。这样既不需要另外的软件安装和操作,节省大量时间和精力,也能方便快捷地选出适合自己安全需求的 Web 服务。

2　基于用户偏好和 SoS 属性的安全评估

2.1　偏好权重的计算

偏好(preference)是价值比较的一种直觉。即把 A 与 B 就哪一个能给人的某方面提供更大满足的意义进行考察时,可判断 A 优于(Φ)B 或 B 优于(Φ)A,或两者无差(~)的一种直觉。同类简单对象总是可偏好的,即人对于它们所能提供自己的某种需要上的满足,总能通过感官或心理上的直觉比较出来:A(Φ)B,或 B(Φ)A,或 A ~ B。采用层次分析法(AHP)处理用户偏好,以修正安全评估的主观权重,使安全评估结果尽可能精确满足每个用户的需求和偏好。

根据偏好的定义可知,所有偏好关系都可以描述为唯一的二元关系。该定义是构造一对判断矩阵 A 的基础,这样偏好权重算法能更容易利用偏好结构。偏好权重是服务安全评估的主观权重,用来修正信息熵方法计算出的客观比重。基于判断决策者的判断、偏好模型的定义利用 AHP 方法设计了偏好权重算法,流程图见图 2。

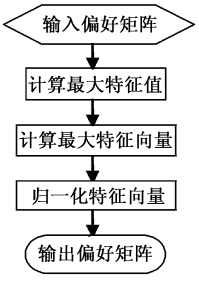

图 2　计算偏好权重流程图

Fig. 2　Flow-chart of calculating preference weight

该算法首先利用用户对 SoS 属性的重要性偏好组成决策矩阵;然后计算该决策矩阵以获得其最大特征值和相应正规化后的特征向量;最后,经过归一化处理得到用户偏好的确定形式,即 n 维向量 $\boldsymbol{P}_W$。

2.2　Web 服务安全性评估

决策矩阵是对多属性决策问题进行建模的一种方法[9]。本文中将 Web 服务安全评估看作一个多属性决策问题,可以定义其决策矩阵 $\boldsymbol{S}$ 如下:

假设有一组 WS 有相同或相似的功能,但其中安全性属性不同,表示为 $\boldsymbol{S}(\boldsymbol{S}=\{s_1,s_2,s_3,\cdots,s_m\})$,用 n 个 SoS 属性 $\boldsymbol{Q}(\boldsymbol{Q}=\{q_1,q_2,q_3,\cdots,q_n\})$ 评估 Web 服务安全,可以得到矩阵 $\boldsymbol{S}$。

$$\boldsymbol{S}=\begin{bmatrix} v_{11} & v_{12} & \cdot & \cdot & v_{1n} \\ v_{21} & v_{22} & \cdot & \cdot & v_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ v_{m1} & v_{m2} & \cdot & \cdot & v_{mn} \end{bmatrix}. \tag{1}$$

其中元素 v_{ij} 表示服务 s_i 中 SoS 属性 q_j 的值。根据上面定义,矩阵 $\boldsymbol{S}$ 就是基于 SoS 属性 Web 服务安全评估的决策矩阵。

于是,SoS 评估就转化为矩阵计算的最优化问题。像其他多属性决策问题一样,需要知道 SoS 各属性之间的相关重要程度,类似地用规范化向量表示 SoS 各属性的权重。例如,如果用户关注 n 个 SoS 属性,则权重向量表示为 $\boldsymbol{W}^{\mathrm{T}}=(w_1,w_2,w_3,\cdots,w_n)$,其中 $\sum_{1}^{n} w_j=1$,偏好权重算法的输出 $\boldsymbol{P}_W$ 最终规范为这种形式。

根据信息熵的方法,将决策矩阵 $\boldsymbol{S}$ 作为计算 SoS 属性信息熵的输入,利用如下方程进行计算[10]:

$$E(E_1,E_2,E_3,\cdots,E_n)=-k\sum_{i=1}^{m} v_{ij}\ln v_{ij}. \tag{2}$$

式中,k 为常量 $\ln m$,m 表示可选服务的数量;E_j 表示 SoS 属性 q_j 的熵。对任意 j,当所有 E_j 都相等时,$E_i=1/n$,$E(E_1,E_2,E_3,\cdots,E_n)$ 最大。

可以根据信息熵直观地计算每个 SoS 属性的权重,也可以利用偏好权重修改这些属性的客观权重[11]。最后,通过矩阵 $\boldsymbol{S}$ 和修改后的权重计算各个可选服务的安全值。为了使用户选取最匹配的服务,修改后的安全评估公式计算如下:

$$L_i=\sum_{j=1}^{n} v'_{ij}w_j. \tag{3}$$

式中,v'_{ij} 为正规化的 v_{ij} 值;L_i 为 Web 服务 s_i 的安全评估值。所有候选服务的评估值可表示为 $L(L_1,L_2,L_3,\cdots,L_m)$。

基于信息熵方法的 Web 服务安全评估算法描述见图 3。

如果用户不提供他们的偏好,则该算法以系统提供的 SoS 属性客观权重计算安全值。最后基于权重,对可选服务进行排序。

信息熵方法基于矩阵 $\boldsymbol{S}$ 各列值的不同而输出客观权重,这些客观权重是与用户偏好和需求独立的。如果矩阵各列的差距很大,相应的 Web 服务安全属

性的客观权重也会较高,反之亦然。当然,利用信息熵方法计算单个服务的客观权重是没有意义的。

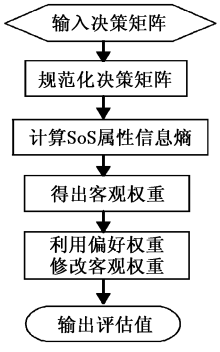

图 3 安全评估流程图

Fig. 3 Flow-chart of security evaluation

3 试验分析

为了证明信息熵理论的客观性,体现客观权重与各个 Web 服务安全属性差异之间的关系,以及偏好对客观权重产生的影响,定义变量 Δd_j 表示各个可选 Web 服务每个安全属性之间的差距。

$$\Delta d_j = \sqrt{\sum_{i-1}^{m} (\boldsymbol{S}_{\max j} - v'_{ij})^2} \ . \tag{4}$$

其中 n 维向量 $\boldsymbol{S}_{\max}$ 的每个元素代表 $S'[m][n]$ 中每列的最大值。

由于 Web 服务的复杂性和多样性,参考其他文献中的方法将安全属性和用户的安全偏好数据采用在不同区间内随机产生,用户的安全参数限制也随机产生[1]。获得数据之后,运行文中模型的关键算法 —— 基于 SoS 属性和用户偏好的安全评估,以验证方法的有效性和准确性。实验时,选择查询服务作为安全评估的实例。如表 1 所示,有 10 个查询 Web 服务,基于 8 个方面对 Web 服务安全进行评估,分别是服务端的风险值(q_1)、认证(q_2)、机密性(q_3)、完整性(q_4)、可用性(q_5)、授权(q_6)、审计(q_7)以及不可否认性(q_8)等。

以表 1 的数据为依据,利用信息熵方法计算各个 SoS 属性的客观权重 $\boldsymbol{W}$;利用公式(3)计算 Δd,结果如图 4 所示。

与客观权重趋势一致,该结果也证实了信息熵评估方法是基于 Web 服务安全属性差异的水平进行的评估。因此,所提方法可以加速可选 Web 服务的分离和区别。

图 4 同时也反映了用户对机密性(q_3)比较敏感的影响,评估值为(0.157 4, 0.091 3, 0.067 5, 0.078 2, 0.090 7, 0.069 3, 0.141 9, 0.070 8, 0.141 6, 0.091 3)。利用对机密性敏感的用户的偏好权重修正后的机密性权重(W^*)有较大提高,其他 SoS 属性的权重变化不大。可选服务根据评估值排序的结果为(s_1, s_7, s_9, s_2, s_{10}, s_5, s_4, s_8, s_6, s_3)。

表 1 查询服务的 SoS 属性

Table 1 SoS attributes values of query Web services

S_i	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8
s_1	110	6	106	0.72	0.99	5	1	0.84
s_2	99	11	120	0.75	0.90	4	2	0.95
s_3	69	15	100	0.82	0.82	3	3	0.81
s_4	108	12	133	0.51	0.94	2	2	0.87
s_5	56	13	133	0.79	0.85	2	4	0.79
s_6	102	14	140	0.73	0.86	5	3	0.83
s_7	88	7	142	0.55	0.89	3	3	0.82
s_8	43	18	122	0.91	0.81	3	1	0.83
s_9	66	6	112	0.76	0.77	2	2	0.86
s_{10}	56	12	102	0.70	0.87	3	2	0.88

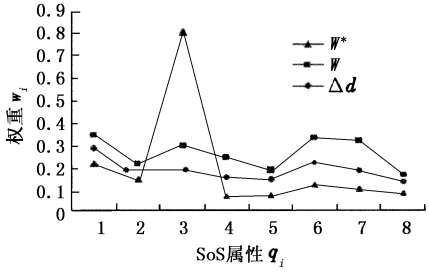

图 4 机密性偏好对客观权重产生的影响

Fig. 4 Objective weight modification effect based on confidentiality

从图 5 可以看出,该评价模型的可用率远远高于传统 Web 服务模型。这是因为以前的模型没有测量候选服务可用性和可访问性的机制。在假设用户随机从候选服务中选择服务的情况下,由于采取了基于用户偏好参数的服务筛选,所以服务选择的可用率和准确率都显著提高。

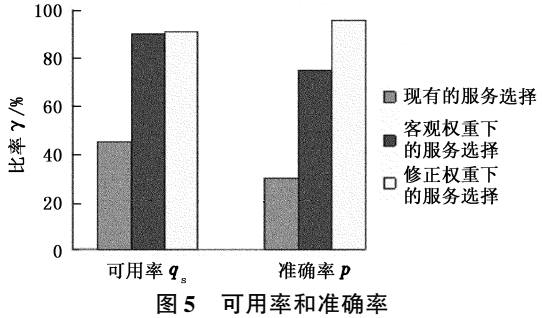

图 5 可用率和准确率

Fig. 5 Availability ratio and precision ratio

4　结束语

结合 Web 服务的特殊性,将多属性决策理论引入 Web 服务安全评估。对现有 Web 服务基本模型进行了扩展,增加了安全评估中心来完成评估。首先,利用多属性决策理论中的信息熵方法计算出安全属性的客观比重;然后,利用层次分析法(AHP)计算用户对各个可选服务的偏好比重,同时利用该比重修改客观比重,使修正后的比重更符合用户安全需求。通过试验验证,改进后的模型在用户选择服务的准确率和可用率上都有一定提高。

参考文献:

[1] CAO Jiu-xin, HUANG Jing-yu, WANG Guo-jin, et al. QoS and preference based Web service evaluation approach: proc of the ICGCC'09[C]. Lanzhou, China: IEEE Computer Society, 2009:420-426.

[2] ROBERT A, van Engelen, ZHANG Wei. An overview and evaluation of Web services security performance optimizations: proc of the ICWS'07, Marriott Salt Lake City Downtown[C]. Salt Lake City, Utah, USA: IEEE Computer Society, 2008:137-144.

[3] CHEN S, ZIC J, TANG K, et al. Performance evaluation and modeling of Web services security: proc of the ICWS'07, Marriott Salt Lake City Downtown[C]. Salt Lake City, Utah, USA: IEEE Computer Society, 2007: 431-438.

[4] 钟鸣. Web 服务安全技术研究与实现[D]. 北京:国防科学技术大学研究生院,2004.
ZHONG Ming. Web services security technology and research[D] Beijing: Graduate School, National Defense University of Science and Technology, 2004.

[5] 杨阔朝. 安全漏洞的统一描述及研究应用[D]. 北京:中国科技大学计算机系,2005.
YANG Kuo-zhao. A unified description and application research of the security vulnerabilities[D]. Beijing: Department of Computer Science, China University of Science and Technology, 2005.

[6] 代丹. 基于 Web 的安全测评技术研究[D]. 重庆:重庆邮电大学计算机科学与技术学院,2006.
DAI Dan. Web-based security assessment technology research [D]. Chongqing: College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, 2006.

[7] 包永堂. Web Services 安全技术研究[D]. 东营:中国石油大学(华东)计算机与通信工程学院,2009.
BAO Yong-tang. Web services security research [D]. Dongying: College of Computer and Communication Engineering, China University of Petroleum (East China), 2009.

[8] 高扬. 基于漏洞测试的 Web 服务安全性测评研究[D]. 东营:中国石油大学(华东)计算机与通信工程学院,2010.
GAO Yang. Web services security evaluation study based on the vulnerability testing[D]. Dongying: College of Computer and Communication Engineering, China University of Petroleum (East China), 2010.

[9] 徐玖平,吴巍. 多属性决策的理论和方法[M]. 北京:清华大学出版社,2006:45-50.

[10] BOUYSSOU D, MARCHANT T, PIRLOT M, et al. Evaluation and decision model: a critical perspective [M]. Dordrecht: Kluwer Academic Publishers, 2000: 77-80.

[11] VINCKE P, COLOMI A, ROY B, et al. A MCDA aide multi criteria ala decision-multiple criteria decision aiding[J]. The European Commission Joim Research Center, 2001,10(3):343-354.

(编辑　修荣荣)