Web 服务可信评估要求①

Requirements for Trust Evaluation of Web Services

王秀利　王宏伟　(中央财经大学 信息学院 北京 100081)

摘　要： 与抽象的信任评估模型不同，从可用性、可靠性和安全性三方面对 Web 服务的可信需求进行分析，进而给出面向用户的、易于操作的、定性和定量相结合的 Web 服务可信评估要求，包括可用性、可靠性和安全性要求。

关键词： Web 服务　可信评估　可用性　可靠性　安全性

1　引言

Web 服务被认为是一种推动分布计算向前迈进的革命性技术[1]，是对象/组件技术在 Internet 中的延伸[2]。然而，Web 服务的相关标准协议都没有对 Web 服务技术平台提供可信任与授权的完整安全构架。Web 服务如何认证用户？用户能否信任 Web 服务？要在 Web 服务提供者和用户之间建立信任联系，必须解决这些关键问题。Web 服务的可靠性、安全性、高可用性等诸多问题需要进一步研究[3]。

为此，研究人员对 Web 服务的可用性[4]、互操作性[5]和安全性[6]进行了研究，文献[7]则从信任的概念出发，对信任内容和程度进行划分，并给出数学模型用于信任评估。

与抽象的信任评估模型不同，本文对 Web 服务的可信需求进行了详细分析，进而给出面向用户的、易于操作的、定性和定量相结合的 Web 服务可信评估要求。

2　可信需求

尽管人们已经对于高可信软件的重要性达成了普遍共识，但长期以来对于如何精确定义高可信却是众说纷纭。

微软认为，高可信计算是一个十分广义的概念，所指的不仅仅是计算机的安全性，而是计算机整个生态环境。在这个环境里，安全性、可靠性、隐私权、易用性是核心的部分。美国、欧洲、日本等发达国家以及 IBM、HP 等知名 IT 企业也从不同侧面对高可信的性质进行了概括。普遍认为，高可信软件具有安全、可靠的基本特征。此外，易用性、高效性、敏捷性、可存活性以及服务质量等，也是高可信软件所应该具备的属性。

基于以上讨论，本文对可信的定义是：可信=可用+可靠+安全。因此，本文从可用、可靠和安全三方面分析 Web 服务的可信需求。

2.1 可用性

根据国际标准化组织的定义，可用性被定义为“产品被特定的用户在特定的使用环境中使用，以有效并满意地实现特定的目的”(ISO 9241-11)。Web 服务的可用性是测量 Web 服务系统如何能够持续对客户进行服务的尺度，是指系统故障中断工作时间与可持续工作时间的比率。任何一个高可用性的系统都无法避免故障，因此故障恢复的时间和故障的频率必须足够小以获得需要的可用性。

平均无故障时间 MTTF 是系统故障之间的平均时间间隔，平均恢复时间 MTTR 是从这些故障中恢复所用的平均时间。系统的可用性为：MTTF/(MTTF+MTTR)×100%。由此可见，系统的可用性为系统保持正常运行时间的百分比。

通过最大化元件的可用性以及最小化故障修复时间可以获得 99%到 99.9%的可用性。要取得更高的可用性，需要采用冗余设计方法，因为对失效元件的备

① 基金项目:国家自然科学基金项目(60743005,70872120,70872119);北京市自然科学基金项目(9092014);中央财经大学“中财 121 人才工程”青年博士发展基金项目(QBG0702)
收稿时间:2008-10-27

份能够确保系统连续地工作。通过计算从检测出失效元件到切换到备份元件的间隔时间可以进一步计算出这种冗余系统的可用性指标。

2.2 可靠性

可靠性是指计算机系统或者设备在规定环境下、规定时间内、规定条件下，无故障地完成规定功能的概率。可靠性是一个综合特性，其研究涵盖硬件、网络、操作系统、数据库、应用系统等各个层次。

计算机系统的可靠性用平均无故障时间 MTTF 来度量，即计算机系统平均能够正常运行多长时间，才发生一次故障。系统的可靠性越高，平均无故障时间越长。

系统的可用性与可靠性相关联，但不等同于系统的可靠性。系统的可靠性衡量系统失败的频率，系统的可用性衡量系统正常工作的时间百分比。

2.3 安全性

安全性是指系统保障数据资料总是以合法方式被使用的能力。资料的拥有者可通过授权的方式决定哪些人可以看到或修改这些资料。系统必须能够防止未经授权的用户非法获得资料，从而保证数据在整个生命周期内是可以信赖的。

因为本文把可用性和可靠性单独考虑，所以本文认为安全性可以分为机密性、完整性、可控性、真实性和不可否认性。因此，Web 服务的安全性需求如下：

(1) 验证：用来确保业务事务中的各方确实是他们所声称的，因此，身份证明是必需的。这个证明可以以不同的方式获得。如通过提交用户 ID 和密码；使用由信任的认证机构签发的 X.509 证书等。

(2) 数字签名：为了确认在事务中交换的业务信息的完整性，确保在 Internet 上传送期间消息的内容没有被改变或破坏，使用安全性密钥对数据进行数字签名。一个常用的方法是使用发送方的 X.509 证书的私钥对 Web 服务请求的 SOAP Body 进行数字签名。类似地，也可以签署请求中的 SOAP 头代码块，以确保在实际业务上下文范围以外的事务中交换信息的完整性(例如消息 ID、安全性令牌)。同样地，还可以对 Web 服务响应进行数字签名，从而确保数据的完整性。

(3) 机密性：利用加密技术使 Web 服务请求和响应中交换的信息不可读。这样做的目的是确保访问传送中的、内存中的、或已经持久化的数据，任何人都将需要适当的算法和安全性密钥解密数据才能访问实际信息。

3 可信评估要求

信息系统评估方法有多种，可以分为两大类：

一类为定量评估方法，是指运用数量指标对风险进行评估，有因子分析法、聚类分析法、时序模型、回归模型、等风险图法、决策树法等。定量评估方法比较客观，可以使研究结果更科学、更严密、更深刻；但量化可能使本来比较复杂的事物简单化、模糊化，甚至可能被误解和曲解[8]。

另一类为定性评估方法，主要依据研究者的知识、经验对系统风险状况做出判断；它主要以调查、访谈为基本资料，通过理论推导演绎的分析，对资料进行整理，在此基础上做出调查结论。典型的定性分析方法有因素分析法、逻辑分析法、历史比较法、德尔斐法等。定性评估方法可以挖掘出一些蕴藏很深的思想，使评估的结论更全面、更深刻；但它的主观性很强，对评估者本身的要求很高[9]。

相应地，评估指标可分为定性指标和定量指标两种。选择合适的指标体系并使其量化是评估的关键。理论上讲，为了能够科学客观地反映 Web 服务的质量特征，应该尽量选择定量指标。但是，并不是所有的质量特征都可以用定量指标进行描述，所以不可避免地要采用一定的定性指标。指标的确定是采用自顶向下的方法，逐层分解，并在动态过程中反复综合平衡。

Web 服务可信评估基本要求相应地也分为可用性、可靠性和安全性要求三部分。参考文献[10-12]，本文给出 Web 服务可信评估的基本要求。

3.1 可用性要求

(1)可接受的每次最长意外宕机时间；

(2)可接受的每年最多意外宕机次数；

(3)每次故障所需要的平均修复时间 MTTR；

(4)两次故障的平均时间长度 MTBF；

(5)服务工作时间段，即在什么时间段服务有效；

(6)服务执行时间，真正开始执行服务到服务执行

结束所耗费的时间;

(7)平均请求提交延迟，反映服务请求者发出的请求能否及时提交给服务提供者;

(8)延迟时间，延迟时间包括队列延迟时间 QD、初始化延迟时间 ID 和同步延迟时间 SD。QD 是新请求在请求队列开始排队到允许执行该服务之间的延迟。ID 是指从允许开始执行该服务到完成初始化工作真正开始执行服务之间的延迟。SD 是指服务进行中等待其他参数或其他进程结果所耗费的时间。

3.2 可靠性要求

(1)失效率，单位时间内出现的失效次数;

(2)修复率，单位时间内修复的故障数;

(3)故障率，在服务工作时间段的基础上，[1－(有效工作累计时间/服务工作时间段累计时间)]×100%，反映了一段时间内故障出现所造成的影响;

(4)初期故障率，初期故障率指软件在初期故障期(一般以软件交付后三个月内为初期故障期)内单位时间的故障数。可预测什么时候软件可靠性基本稳定;

(5)偶然故障率，指软件在偶然故障期(一般以软件交付后四个月以后为偶然故障期)内单位时间的故障数。它反映了软件处于稳定状态下的质量;

(6)软件容错的能力;

(7)故障分析的能力;

(8)自动恢复到故障前工作状态的能力;

(9)对软件缺陷进行检查的能力。

3.3 安全性要求

(1)合理使用和控制系统资源的能力;

(2)按优先级自动分配系统资源的能力;

(3)对传输和存储数据进行完整性检测和纠错的能力;

(4)记录用户操作行为和分析记录结果的能力;

(5)对用户的误操作行为进行检测、报警和恢复的能力;

(6)安全机制失效的自动检测和报警能力;

(7)检测到安全机制失效后恢复安全机制的能力;

(8)对物理入侵事件进行报警的能力;

(9)能够检测、集中分析、响应、阻止对网络和所有主机的各种攻击的能力;

(10)发现所有已知漏洞并及时修补的能力;

(11)对资源的访问进行严格控制的能力;

(12)对资源访问的行为进行记录、分析并响应的能力;

(13)对恶意代码的检测、集中分析、阻止和清除能力;

(14)防止恶意代码在网络中扩散的能力;

(15)保证鉴别数据传输和存储保密性的能力;

(16)对用户进行唯一标识的能力;

(17)对硬件设备进行唯一标识的能力;

(18)对硬件设备进行合法身份确定的能力;

(19)检测非法接入设备的能力;

(20)对传输和存储中的信息进行保密性保护的能力;

(21)防止加密数据被破解的能力;

(22)路由选择和控制的能力;

(23)信息源的鉴别能力;

(24)持续非活动状态一段时间后自动切断连接的能力;

(25)基于密码技术的抗抵赖能力;

(26)防止未授权下载、拷贝软件或者文件的能力;

(27)网络边界完整性检测能力;

(28)切断非法连接的能力;

(29)对重要数据和程序进行完整性检测和纠错能力;

(30)对敏感信息进行标识的能力;

(31)对敏感信息的流向进行控制的能力。

4 结论

本文主要针对 Web 服务可信度评估进行研究，通过分析 Web 服务的可信需求，给出面向用户的、易于操作的、定性和定量相结合的可信评估要求，包括可用性、可靠性和安全性要求。

参考文献

1 Blaze M, Feigenbaum J, Ioannidis J, et al. The role of trust management in distributed systems security. Secure Internet Programming: Security Issues for Mobile and Distributed Objects. Berlin: Springer-

(下转第 60 页)

(上接第 38 页)

-Verlag, 2001:185－210.

2 Khare R, Rifkin A. Trust management on World Wide Web. Computer Networks and ISDN Systems, 1998, 30(1-7):651－653.

3 Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. Proc of the Symposium on Security and Privacy. Oakland, CA: IEEE Press, 1996:164－173.

4 Cotroneo D, Gargiulo M, Russo S, Ventre G. Improving the availability of Web services. Proc of the ICSE. Orlando, 2002:59－63.

5 Koschel A, Klaus L. Interoperability of standards: Web services & NET, EIB and CORBA. Technical Report, IONA Technologies, Brunnenweg Weiterstadt, 2002.

6 Hondo M, Nagaratnam N, Nadalin A. Securing Web Services. IBM Systems Journal, 2002,41(2):1－5.

7 Abdul-Rahman A, Hailes S. A distributed trust model. Proc of the New Security Paradigms Workshop. Cumbria. UK: ACM Press, 1997:48－60.

8 Schechter SE. Computer security strength & risk: a quantitative approach. [Ph.D. Thesis]. Harvard University, 2004.

9 Hash J, Sabato J, Graffo L, Swanson M, Bartol N. Security metrics guide for information technology systems,2003.http://connect.educause.edu/Library/Abstract/SecurityMetricsGuideforIn/44961?time=1225075377.

10 U.S. Department of Defense. Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985.

11 中华人民共和国国家标准.计算机信息系统安全保护等级划分准则,GB17859－1999.

12 中华人民共和国公共安全行业标准.计算机信息系统安全等级保护通用技术要求,GA/T390－2002.