一种新的基于层次的可信电子服务体系模型研究*

张丽娟，吴振强，温博为
（陕西师范大学 计算机科学学院，西安 710062）

摘　要：针对目前电子服务可信性研究相对独立且缺少系统、明确的体系结构，提出了一种新的基于层次的可信电子服务体系模型（layer-based model of trusted e-service，LMTS），定义了电子服务的可信性和模型中相邻层次间的接口，设计了一种基于 LMTS 的电子服务请求安全协议，在此基础上探讨了基于 LMTS 的可信电子服务信任评估机制。分析表明，该模型具有可信性，提高了服务信息的可信度。

关键词：信任评估；可信计算；服务质量；电子服务
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2013)06-1701-04
doi:10.3969/j.issn.1001-3695.2013.06.025

Novel layer-based model of trusted e-service

ZHANG Li-juan，WU Zhen-qiang，WEN Bo-wei
（*School of Computer Science，Shaanxi Normal University，Xi' an* 710062，*China*）

Abstract：According to the relative independence of e-service trust research and lack of systematic，standard architecture of trusted e-service，this paper proposed a novel layer-based model of trusted e-service called（LMTS）. LMTS has defined the trust of e-service and interface between adjacent layers of the model. It also devised a kind of secure protocol of service request. In addition，LMTS discussed trust evaluation mechanism based LMTS. The analysis proves that LMTS is trusted and enhances the credibility of the service information.

Key words：trust evaluation；trusted computing；QoS；e-service

随着我国向 2050 年全面进入信息社会的目标迈进，大多数行业将会变为高度信息化的行业[1]。尤其是随着信息以及网络技术的发展，网络服务和信息服务的应用出现了空前的盛况。然而在这些服务协同场景下保证信息系统服务和网络服务的可靠性及可信性问题变得尤为突出。例如，丰富的服务资源缺乏专业的、可信的第三方实体对其真实性和可信性进行担保；服务实体通常分布在不同的自治域，服务执行过程对使用者而言不可见且容易被提供者更改，导致服务资源具有极大的不可控性和不确定性、服务质量常常未知等。

为保证信息系统提供的服务是可信的，目前的研究主要集中在以下三方面：a）可靠性研究；b）安全性研究；c）从服务的结果上进行研究。可靠性研究大多数集中在组件级，未考虑人为因素对组件的影响；安全性研究大多是假设人为因素影响的情况下进行安全防护；对服务结果的评价是在事后验证的基础上对系统的服务结果进行反馈，以决定是否继续信赖该系统。三方面的研究相对独立，相互之间缺少数据交换，都不能很好地保证信息系统提供的服务是可信的，在实际应用中也不能发挥出各自的优势。

针对目前电子服务可信性研究相对独立且缺少系统、明确的体系结构，本文从体系结构的视角出发，提出了 LMTS 模型，讨论电子服务提供的可信性，给出可信电子服务一种新的定义，横向研究各层次的信任需求，纵向研究层次间的信任传递，并定义了模型邻层间交互的接口。

1　基于层次的可信电子服务体系模型

1.1　模型描述

可信电子服务的重要性已经达成了比较普遍的共识，但长期以来对可信电子服务的定义仍不尽相同。另外，网络环境的复杂性要求研究者对可信概念进行重新思考。服务可信不止是所提供软件的可用，还应包括整个计算机生态环境的可信。隐私性、安全性、易用性和可靠性是环境的核心部分。计算机硬件、操作系统、软件服务本身等的安全与可靠也将成为影响服务可信的因素。本文对电子服务的可信性进行重新定义，并从服务可信的角度思考，提出了一种三层可信电子服务体系架构 LMTS，并给出基于 LMTS 的描述机制。图 1 为 LMTS 模型描述。

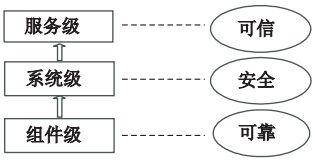

图1　LMTS模型描述

本文对电子服务可信性的定义是：可信 = 可靠 + 安全 + 信任。可靠性是计算机在一定环境中能正常完成所规定任务的能力，评价标准是计算机硬件无故障运行的时间；安全性是系统在保证自身安全的同时保障用户总能根据需要通过合法方

收稿日期：2012-08-20；**修回日期**：2012-10-07　　**基金项目**：国家自然科学基金面上项目（61173190）；国家“863”计划基金资助项目（2007AA01Z438200）

作者简介：张丽娟（1988-），女，硕士研究生，主要研究方向为匿名通信技术、可信计算（lijuanzhang00@126.com）；吴振强（1968-），男，教授，博导，博士，主要研究方向为匿名通信技术、可信计算、普适计算等；温博为（1986-），男，硕士研究生，主要研究方向为匿名通信技术、可信计算.

式安全地使用数据资料;信任是服务应用软件本身保证响应时间、服务质量、保密性、完整性等,是值得信赖的。

LMTS 根据系统对硬件、操作系统及运行时环境的不同,可信需求将服务可信性分为组件级、系统级和服务级三层。传统的对电子服务可信性的理解只停留在服务级,着重研究如何为用户提供快速的服务及如何提高自身信誉度[2]。然而在实际的网络环境中,服务随时面临着计算机硬件故障、操作系统崩溃等安全威胁,单从服务级研究可信已不能适应当今电子服务的发展状况,从组件级、系统级和服务级研究电子服务可信性成为大势所趋。

1.2 可信电子服务体系模型层次化分析

LMTS 综合考虑了用户需求,赋予每一层不同的可信要求。图 2 为可信电子服务体系服务器端的功能模块化,分别列出了三层要达到的可信性目标以及度量是否达到可信性目标的性能指标。

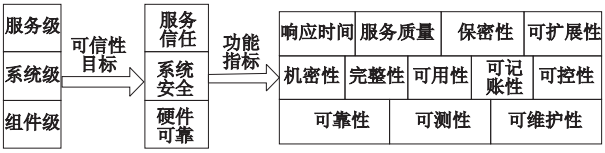

图2 可信电子服务体系的模块化

1)组件级可信性需求 结合可信计算解决终端不安全的问题,以及使终端、网络系统能以主动保护的方式从根本上提高可靠性。可信计算强调行为结果的可控、可预测性。另外,组件级还需保证传送的数据是有效的、真实的和实时的。

2)系统级的可信性需求 可信计算静态保证了组件级的可靠性以及在系统启动时免遭木马等攻击,但不能保证系统动态获取网络服务及运行时刻的安全。这就需要一些系统级的动态监控程序来保证系统级安全,为操作系统的动态运行和服务级的正常工作提供一个安全的运行环境。另外,对于系统级的安全仍需满足以下要求:a)机密性,即避免数据资料泄露;b)完整性,它包括操作系统自身的完整性,敏感信息的完整性,标签、策略的完整性,以及策略执行系统的完整性等;c)可用性,即保障用户随时能访问授权信息,是一个系统处在可工作状态的时间比例;d)可记账性,即系统能提供各种安全问题追踪调查的依据和手段,以便进行系统修复以及追究相关责任;e)可控性,即保障系统组件能代理用户完成预定任务,而且只依据用户授权执行既定操作。

3)服务级的可信性需求 服务级信任需求归纳为服务质量、响应时间、保密性和可扩展性。服务质量是期望的服务与传递的服务的吻合程度[3]。用户对服务质量的感知在具体服务中表现为交互性、可用性、信息质量、易用性。交互性指用户与电子服务系统交互的友好性;可用性注重用户随时能根据需要请求服务并得到满意结果;信息质量指用户得到的服务信息是自身所期望的;易用性指服务系统简便易行、获取的服务简洁易懂。保密性是保证用户在请求服务时的敏感信息不被泄露;可扩展性是强调服务系统扩展以后对用户使用习惯的影响。

LMTS 将可信电子服务体系中服务器端的通信分成有明确定义的三层,其可信状态评估及报告并非并列关系,而是由下到上层层递进,信任关系也存在一条由下到上传递的信任链。上层利用下层提供的功能实现自身功能,同时再为上一层完成某些功能,上层屏蔽下层的操作细节。LMTS 是一个分层结构模型,具有适应性强、独立性强、容易维护和实现以及功能简单的优势。

1.3 LMTS 统一接口设计

本节设计了组件级、系统级与服务级邻层之间通信的接口,对每一层的功能进行了封装,以便上层需要时调用。接口定义以及功能调用过程如下:

a)组件级的 TPM 对部件进行测量获得测量值,并将测量到的信息摘要存入 PCR,系统级调用组件级功能时可由 TPM 读出并形成可靠性报告。

b)系统级通过调用接口 GetComponentState (string PCRDigest)获得组件级的可靠性状态,并且根据此状态验证组件级是否达到可靠性标准。失败则返回错误报告,要求组件级进行部件升级或故障排除;否则返回 OK,并对这些状态信息加工后保存,以便服务级调用时进行信息的封装。PCRDigest 是 TPM 对部件进行测量获得的测量信息摘要值。

c)服务级调用接口 GetSystemState(string system,string CrytoModuleMonitor, string LogFileDigest)获得系统级的安全状态。System 是系统级对组件级可靠状态验证的结果标志,Error 表明组件级不符合可靠性要求,服务级停止系统级状态的读取,并且放弃服务的注册或发布,否则模型继续执行。CrytoModuleMonitor是密码模块协议栈保护操作系统核心代码时监控到的信息,LogFileDigest 是操作系统相关日志文件的摘要。

d)服务级同样验证系统级的安全状态,验证失败则返回错误报告,要求系统级进行安全检查或升级,否则返回 OK。同时,服务级向相关的服务注册中心发出服务注册或者升级请求,并发送自身信任状态报告。其报告内容如下:

```
public class StateReport
{
  string Feedback;
  string PCRIntegrityDigest;
  string InteractionTime;
  string SoftwareMonitor;
  string ID;
}
```

Feedback 是信任管理中心发送给服务提供者的反馈信息;PCRIntegrityDigest 是由 TPM 度量机制对代码的完整性进行度量后形成的度量报告摘要;InteractionTime 是服务提供者记录的与服务使用者的交互时间;SoftwareMonitor 是服务本身对程序进行行为监控时监控到的信息;ID 是服务提供者的标志。服务注册中心验证服务提供者的可信性,只有满足可信性的服务器才能为用户提供服务。

2 可信电子服务场景描述及协议实现

2.1 服务请求过程

LMTS 从体系结构角度根据用户的可信需求研究服务可信性,与面向服务的组件模型 SOA 相统一。SOA 透明、标准化的集成方式使 IT 基础设施具有互操作能力、重用性和柔性[4],注重与其他技术结合用编程语言实现服务。图 3 为服务请求流程。图中将 LMTS 与 SOA 结合,既保证符合 SOA 标准的业务流程[5],又满足用户对服务的可信需求。

基于 LMTS 的服务请求流程如下:

a)服务提供者向服务注册中心发布服务,并且报告自身可信性状态。报告各层次可信性状态时首先评估组件级,评估

可靠之后方可进入系统级安全状态评估,系统级达到预定安全状态才可以进行服务级评估以及服务的正式发布,形成纵向信任链。其中任何一个环节不符合要求,信任关系将不能继续传递,不允许服务发布。

b)服务注册中心向信任管理中心提交服务和可信性状态。

c)发生服务请求时,请求者将请求信息(如服务价钱、信任度)发送给信任管理中心。

d)信任管理中心依据用户的服务请求信息搜索符合要求的服务,并按照一定次序排序后将其发送至服务请求者。

e)请求者执行一定策略选择满意的服务,并与服务提供者进行绑定,两者进行交互。

f)服务使用者完成服务相关过程后对该服务提供者作出相应评价。

g)信任管理中心根据服务使用者的评价信息为服务提供者发送服务反馈信息。

步骤 a)和 b)是服务发布过程,c)~f)是服务请求过程,g)是信任管理中心为服务提供者发送服务反馈信息,以便提供者进行服务改进。实际应用中这是一个复杂的过程,尤其是服务提供者定期进行三层可信状态评估、可信链的传递与报告以及服务发布,信任管理中心综合用户需求对服务进行排序,对服务使用者提供的反馈评价信息进行信任度的量化、综合计算等,都是值得研究和探讨的。

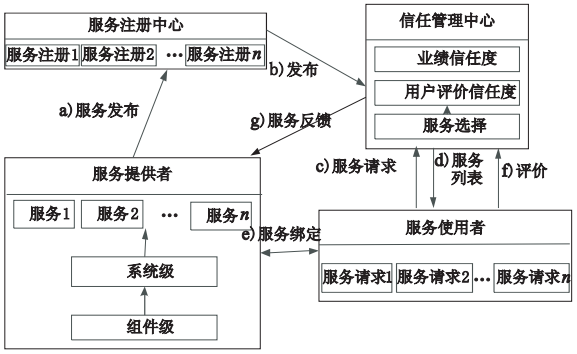

图3　服务请求流程

2.2　服务请求安全协议设计与实现

本节基于图 3 的模型场景设计并实现了一种如图 4 所示的服务请求安全协议。

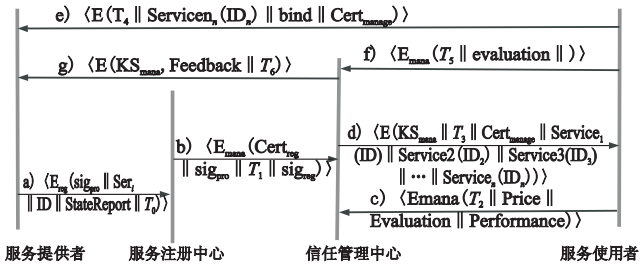

图4　服务请求安全协议

假设 1　服务提供者已经注册了服务注册中心,并且获得了合法的身份标志号 ID。

假设 2　服务注册中心和信任管理中心是可信的,担任可信第三方的角色。通常它们是属于同一实体的两个可信代理。

假设 3　服务注册中心、信任管理中心、服务提供者及服务请求者间有时钟同步机制可确保协议中消息时戳的新鲜性。

a)服务提供者生成时戳 T_0,运行 LMTS 获得可信状态 StateReport,用私钥 $KS_{provider}$ 对 StateReport、待发布的服务 Ser_i 及 ID 进行签名,得 $sig_{pro} = E(KS_{provider}, Ser_i \| ID \| StateReport \| T_0)$,并且将 Ser_i、ID、StateReport、T_0 和签名信息 sig_{pro} 用服务注册中心的公钥加密后得到消息〈$E_{reg}(sig_{pro} \| Ser_i \| ID \| StateReport \| T_0)$〉,然后将其发给服务注册中心。

b)服务注册中心验证服务提供者时戳是否有效、身份是否合法及签名是否真实。验证成功后进行服务注册、生成时戳 T_1,将时戳 T_1、证书 $Cert_{reg}$ 以及接收到的 sig_{pro} 进行签名,然后用信任管理中心的公钥对消息加密,提交给信任管理中心。发送的消息为〈$E_{mana}(Cert_{reg} \| sig_{pro} \| T_1 \| sig_{reg})$〉。其中,$sig_{reg} = E(KS_{reg}, Cert_{reg} \| sig_{pro} \| T_1)$。信任管理中心对此注册服务进行初始化并增加列表。

c)服务使用者生成时戳 T_2,并将其与服务要求如服务价格 Price、评价信任度 Evaluation、业绩信任度 Performance 用信任管理中心的公钥加密得到 $E_{mana}(T_2 \| Price \| Evaluation \| Performance)$,发送给信任管理中心。

d)信任管理中心用私钥解密,验证时戳的有效性,成功后生成时戳 T_3,然后依据用户的请求信息搜索符合要求的服务,并按照一定次序排列后将其与自己的证书 $Cert_{manage}$ 签名后发送至服务请求者,即 $E(KS_{mana}, T_3 \| Cert_{manage} \| Service_1(ID_1) \| Service_2(ID_2) \| Service_3(ID_3) \| \cdots \| Service_n(ID_n))$。

e)服务使用者首先验证时戳的有效性以及信任管理中心身份的真实性和合法性,成功后根据需求执行一定策略选择满意的服务,然后生成时戳 T_4,并发送 T_4 及所选服务提供者 ID_n 的绑定请求。发送的消息为 $E(T_4 \| Service_n(ID_n) \| bind \| Cert_{manage})$。其中 bind 为约定的绑定请求标志。

f)服务使用者完成服务相关过程后生成时戳 T_5,然后向信任管理中心对该服务提供者作出相应评价以及反馈,$E_{mana}(T_5 \| evaluation)$。

g)信任管理中心首先对收到的服务评价信息进行整合和记录,形成为服务提供者发送的服务反馈信息 Feedback 并生成时戳 T_6,然后对 Feedback 和 T_6 签名后发送给服务提供者。发送的信息为〈$E(KS_{mana}, Feedback \| T_6)$〉。

3　服务信任评估机制

各学科关于信任的研究较多,但概念模糊。一种广为接受的概念是:信任是信任主体在交互过程中体现出来的情感喜好和倾向,具有动态性、社会性、历史性和交互性等特征。信任系统已经成为衡量电子商务是否成功的一个重要因素,在服务的可信性方面也同样重要,研究者们提出的信任评估模型以及信任度计算方法同样适用于 LMTS。

目前对服务信任评估问题的研究取得了一些成果。文献[6]根据信任的不确定性和主观性,结合模糊集合论将中间推荐节点的直接交互经验融入到信任的综合评判中,从信任模型的描述机制、评估、实时更新展开了研究。文献[7]以社交认知的思想提出一个基于服务代理的信任评价模型,根据建立的信任本体给出服务代理的信任计算规则,进而进行信任评估和服务选择。文献[8]在研究模糊理论的基础上提出一种基于开放式网络环境的主观信任模型,着重讨论了信任度的传递和更新机制,提高了模型的可用性。除此之外,比较常见的信任模型还有基于贝叶斯网络、D-S 理论、博弈论方法[9]、实体的行为[10,11]、主观逻辑方法[12]等可信评估机制。主观信任评价模型

偏向于模糊集合论和概率论来探讨信任关系。由于通过概率方法得到的信任结果为比较精确的数值,使信任值失去模糊性,因此模糊集合论方法更能描述信任的不确定性和模糊性。

4 LMTS 模型分析

4.1 可信性与合理性分析

LMTS 是从功能角度出发根据用户对服务的可信需求提出的,摆脱了传统对服务可信性的狭义理解,将信息服务系统由下而上分为组件级、系统级和服务级。模型是以用户为主体,充分考虑了系统可能遭受到的传统的安全问题以及新兴的安全威胁,将可信计算技术引入其中,保障系统自下而上的信息流安全,三层可信评估形成信任链,为用户提供可靠、安全、信任以及满意的服务。

4.2 效率分析

LMTS 是三层结构,评估过程自下而上且具有一定的周期性,组件级引用了目前基于硬件芯片 TPM 的可信计算技术,基于硬件芯片的计算效率远高于基于软件的计算,系统级评估过程也可根据系统自带的日志以及备份系统等实现,服务级评估也不花费本地过多资源。整个过程利用较小的代价达到较高的效率,同时保障用户对服务的可信需求。

4.3 可行性分析

LMTS 模型层与层之间是由下而上层层递进的关系,信任关系也存在一条由下而上传递的信任链。评估过程中任何一个环节不符合要求,信任关系将不能继续传递,不允许服务发布和升级。实现过程中,每一层的可信性状态可以通过调用定义好的层间接口进行验证。组件级可靠性状态由 TPM 完成,TPM 对部件进行测量获得测量值,并将测量信息摘要存入 PCR,需要时可由 TPM 读出形成可靠性报告。系统级通过调用接口 GetComponentState(string PCRDigest)获得组件级的可靠性状态,并且根据它们验证组件级是否达到可信标准。系统级的安全性状态可由两种方式获取:通过密码模块协议栈构建安全操作系统时监控到的信息;操作系统相关日志文件的摘要。服务级通过调用接口 GetSystemState(string System, string CrytoModuleMonitor, string LogFileDigest)获得系统级的状态。服务级的信任状态通过四种方式收集:信任管理中心发送给服务提供者的反馈信息;程序代码的完整性度量可由 TPM 的度量机制完成并形成完整性度量报告;程序的行为监控;服务提供者自身记录到的与服务使用者的交互时间,信任状态是这些信息的整合。因此,LMTS 可信服务架构在实现上具有可行性。

5 结束语

随着网络技术及电子服务的迅猛发展,用户在服务交互过程中的安全问题日益突出,为了减少用户在服务交互中利益的损失和保证用户对服务的可信,本文提出了 LMTS 模型,并从服务、系统和组件三个层次研究可信。横向研究可信需求,纵向研究层间信任传递,同时设计并实现了一种基于 LMTS 的可信服务安全协议,并且探讨了可信服务的评估问题和评价模型。本文也给出了每一层次为达到可信性目标所采取的相应措施,以提高服务交互的成功率。分析表明,模型具有可信性,提高了服务信息的可信度。

参考文献:

[1] 中国科学院信息领域战略研究组. 中国至 2050 年信息科技发展路线图[M]. 北京:科学出版社, 2009.

[2] 朱锐,王怀民,冯大为. 基于偏好推荐的可信服务选择[J]. 软件学报,2011,22(5):852-863.

[3] LEWIS R C, BOOMS B H. The marketing aspects of service quality in emerging perspectives on services marketing[J]. American Marketing,1983,3:99-107.

[4] W3C. Service-oriented architecture[EB/OL]. (2004). http://www.w3.org/ TR/ws-gloss.

[5] 张永胜,吴明峰,郑志华,等. 服务计算环境下的信任评估模型[J]. 计算机应用研究,2012,29(7):2693-2695,2707.

[6] 张琳,王汝传,张永平. 一种基于模糊集合的可用于网格环境的信任评估模型[J]. 电子学报, 2008,36(5):862-868.

[7] 朱曼玲,金芝. 一种服务 agent 的可信性评估方法[J]. 软件学报, 2011,22(11):2593-2609.

[8] 陈超,王汝传,张琳. 一种基于开放式网络环境的模糊主观信任模型研究[J]. 电子学报, 2010,38(11):2505-2509.

[9] 罗俊海,范明钰. 基于博弈的 MANETs 信任模型研究[J]. 计算机研究与发展,2008,45(10):1704-1710.

[10] 刘莉平,葛志辉. Grid 环境下基于实体行为的信任评估模型[J]. 计算机应用研究,2008,25(7):2020-2022.

[11] 周茜. 基于行为的动态信任量化机制的研究与应用[D]. 乌鲁木齐:新疆大学,2011.

[12] 林剑柠,吴慧中. 基于主观逻辑理念的网格信任模型分析[J]. 计算机研究与发展,2007,44(8):1365-1370.

(上接第 1684 页)

[2] LI Xian-hua, TAN Shi-li, HUANG Wu-xin. A service robot with lightweight arms and a trinocular vision sensor[J]. Key Engineering Materials,2010,439:396-400.

[3] 孙斌,杨汝清. 开放式机器人控制器综述[J]. 机器人,2001,23(4):374-378.

[4] 康存锋,杨建武,黄仁元. 开放式 PC 型运动控制器的研究[J]. 中国机械工程,2004,5(9):800-802.

[5] GUA J S, De SILVA C W. Development and implementation of a real-time open-architecture control system for industrial robot systems [J]. Engineering Applications and Artificial Intelligence,2004, 17(5):469-483.

[6] 姜勇,王洪光,潘新安. 模块化可重构机器人的构形在线自主辨识[J]. 机械工程学报,2011,47(15):17-24.

[7] 周军,余跃庆. 基于实时位置反馈的模块化机器人轨迹跟踪控制[J]. 北京工业大学学报,2012,38(8):1136-1142.

[8] KIRCHOFF S, MELEK W W. A saturation-type robust controller for modular manipulators arms[J]. Mechatronics, 2007, 17(4-6): 175-190.

[9] CORKE P. Robotics, vision and control[M]. Berlin: Springer-Verlag,2011.

[10] KIM S H, KIM Y H. Realization of a virtual simulator system on Window 98/NT environment[C]//Proc of International Symposium on Industrial Electronics Proceedings. 2001:216-220.

[11] 严勇杰,朱齐丹. 基于 OpenGL 的机械臂控制系统仿真平台研究[J]. 计算机仿真,2006,23(8):252-257.

[12] 孙亮,马江. 六自由度机械臂轨迹规划与仿真研究[J]. 控制工程,2010,17(3):388-392.

[13] 熊有伦,唐立辛,丁汉. 机器人技术基础[M]. 武汉:华中科技大学出版社,2008.