软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(8):1948−1963 [doi: 10.13328/j.cnki.jos.004945]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

面向服务组合的用户隐私需求规约与验证方法*

彭焕峰[1,2], 黄志球[1], 范大娟[2], 章永龙[3]

[1](南京航空航天大学 计算机科学与技术学院,江苏 南京 211106)

[2](南京工程学院 计算机工程学院,江苏 南京 211167)

[3](扬州大学 信息工程学院,江苏 扬州 225127)

通讯作者: 黄志球, E-mail: zqhuang@nuaa.edu.cn

摘 要: 用户向 Web 服务组合提供隐私数据时,不同用户有自身的隐私信息暴露需求,服务组合应支持用户隐私需求的可满足性验证.首先提出一种面向服务组合的用户隐私需求规约方法,用户能够定义隐私数据及不同使用情境的敏感度,采用敏感度-信誉度函数明确可以使用隐私数据的成员服务,简化隐私需求的同时,提高了隐私需求的通用性.为了验证服务组合是否满足用户隐私需求,首先通过隐私数据项依赖图(privacy data item dependency graph,简称 PDIDG)描述组合中隐私数据项的依赖关系,然后采用隐私开放工作流网(privacy open workflow net,简称 POWFN)构建隐私敏感的服务组合模型,通过需求验证算法验证服务组合是否满足用户隐私需求,从而能够有效防止用户隐私信息的非法直接暴露和间接暴露.最后,通过实例分析说明了该方法的有效性,并对算法性能进行了实验分析.

关键词: 信誉度;服务组合;隐私保护;隐私开放工作流网;隐私数据项依赖图

中图法分类号: TP311

中文引用格式: 彭焕峰,黄志球,范大娟,章永龙.面向服务组合的用户隐私需求规约与验证方法.软件学报,2016,27(8):1948−1963. http://www.jos.org.cn/1000-9825/4945.htm

英文引用格式: Peng HF, Huang ZQ, Fan DJ, Zhang YL. Specification and verification of user privacy requirements for service composition. Ruan Jian Xue Bao/Journal of Software, 2016,27(8):1948−1963 (in Chinese). http://www.jos.org.cn/1000-9825/4945.htm

Specification and Verification of User Privacy Requirements for Service Composition

PENG Huan-Feng[1,2], HUANG Zhi-Qiu[1], FAN Da-Juan[2], ZHANG Yong-Long[3]

[1](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

[2](College of Computer Engineering, Nanjing Institute of Technology, Nanjing 21167, China)

[3](College of Information Engineering, Yangzhou University, Yangzhou 225127, China)

Abstract: Users have different privacy information disclosure requirements when they submit private data to service composition, and the composition should support the verification of users' privacy requirements. This paper puts forward a flexible method for users to produce privacy requirement specifications. Users can define the sensitivity of private data and its usage in different situations, and restrict the member services that can use private data with sensitivity-reputation function. The simplification and universality of the privacy requirements can be improved by using this method. The process first establishes privacy data item relations by using the privacy

* 基金项目: 国家自然科学基金(61272083); 国家高技术研究发展计划(863)(2015AA015303); 中国博士后科学基金(20110491411); 江苏省博士后科研计划(1101092C)

Foundation item: National Natural Science Foundation of China (61272083); National High-Tech R&D Program of China (863) (2015AA015303); China Postdoctoral Science Foundation (20110491411); Jiangsu Planned Projects for Postdoctoral Research Funds (1101092C)

收稿时间: 2014-09-21; 修改时间: 2015-04-08; 采用时间: 2015-11-21; jos 在线出版时间: 2015-12-21

CNKI 网络优先出版: 2015-12-22 14:59:18, http://www.cnki.net/kcms/detail/11.2560.TP.20151222.1459.002.html

data item dependency graph (PDIDG), then models the service composition with privacy open workflow net (POWFN), and at last, makes sure whether service composition meets the user's privacy requirements by privacy requirements verification algorithm. An example is provided to illustrate the effectiveness of the method, and experiment analysis on the performance of the verification algorithm is carried out at the end of paper.

Key words: reputation; service composition; privacy protection; privacy open workflow net; privacy data item dependency graph

Web 服务作为一种基于 Internet 的崭新分布式计算模型,适合作为一种独立而开放的实体在互联网环境中发布和使用[1].用户为使用服务提供的功能,需要提供必要的个人隐私信息,但由于 Web 服务开放、动态和自治的特点,隐私信息一旦被收集,用户就难以控制服务如何使用和暴露这些信息[2].随着用户隐私信息侵犯案例的增加,隐私信息保护问题越来越受到用户的关注,特别是在服务组合的情况下,服务提供者通过将服务进行组合以形成粒度更大的服务,从而实现复杂的业务逻辑[3].用户隐私信息是通过服务组合暴露给成员服务,由于用户与成员服务之间缺乏隐私信息使用的相关协议,因此难以保证在组合执行过程中,隐私信息能否按照用户的意愿进行暴露和使用[4].

用户对隐私信息有着自身的保护需求,对具体隐私数据项的敏感程度也不同,且对隐私数据项组合使用时敏感度更高,例如同时使用身份证号码和姓名时,比单独使用更担心隐私信息的泄露.随着用户越来越重视隐私信息的保护,用户更倾向于选择在隐私保护方面信誉度更高的服务.用户为使用服务组合提供的功能,需要向组合提供隐私数据,这类数据称为直接隐私数据.组合将直接隐私数据提供给某成员服务的行为,称为直接隐私暴露.组合执行过程中会产生新的数据,而有些新产生数据可能会依赖于直接隐私数据,这类数据称为间接隐私数据.组合将间接隐私数据提供给某成员服务的行为称为间接隐私暴露.为提高竞争力,服务组合提供者需要构建隐私敏感的服务组合模型,以能够支持用户隐私需求的验证,且用户隐私需求验证算法能够同时检测非法的直接隐私暴露和间接隐私暴露.

本文主要工作和创新点主要如下:

(1) 提出一种基于隐私保护信誉度的用户隐私需求规约方法.采用此方法,用户能够定义隐私数据项及其组合使用时的敏感度;同时,可以指定隐私数据使用情境的敏感度,并通过敏感度-信誉度函数明确可以使用隐私数据的服务.与其他隐私需求规约方法相比,用户不必指定组合中使用隐私数据的成员服务,从而具有更好的灵活性与通用性,且简化了需求的复杂度.

(2) 通过隐私数据项依赖图描述组合中隐私数据项的依赖关系,使用带隐私语义的开放工作流网构建隐私敏感的服务组合模型,最后,通过隐私需求验证算法验证组合是否满足用户的隐私需求.该方法不但能够检测隐私信息的非法直接暴露,而且能够检测隐私信息的非法间接暴露.

1 相关工作分析

服务计算及云计算中,用户隐私保护研究可以分为面向数据和面向使用行为两类:前者通过对隐私数据进行加密、匿名、扰动等方法对隐私信息进行保护;后者主要关注隐私数据使用行为的分析与约束,包括用户隐私需求规约方法、服务对隐私需求的实施、服务隐私策略与用户需求协商及演化等研究内容[5].本文的研究属于后者.

对用户隐私需求规约方法及实施等方面的研究,许多组织提出了相应的规范与技术框架,例如,W3C 组织提出隐私偏好平台(platform for privacy preferences,简称 P3P)[6]来定义服务提供者的隐私策略,并引入隐私偏好描述语言(a P3P preference exchange language,简称 APPEL)[7]以方便用户定义其隐私需求.但 P3P 与 APPEL 主要针对 Web 站点定义隐私策略及用户隐私偏好,并不能直接用于面向服务组合的隐私需求规约.OASIS 组织提出的可扩展访问控制标记语言(extensible access control markup language,简称 XACML)[8]是一种通用的访问控制策略语言和执行授权策略框架,但主要关注对服务提供者的隐私数据应用隐私保护策略.针对用户使用在线服务时如何表达其隐私需求,研究者从各国或组织对个人隐私数据的法律或指导原则出发提出相应的用户隐私需求规约方法.例如,文献[9]根据经济合作与发展组织(organization for economic co-operation and development,