移动互联网能力开放平台的层次安全服务模型

李 敏[1,2]，秦志光[1]

(1. 电子科技大学计算机科学与工程学院 成都 611731; 2. 四川师范大学计算机学院 成都 610101)

【摘要】从分析面向移动互联网能力开放平台的安全问题及安全需求入手，介绍了面向移动互联网能力开放平台的架构，提出了适用于该架构的层次安全服务模型，对其中的关键技术做了详细说明。该安全服务模型已经在相关项目中得以应用，在应用中体现出了该安全模型具有完善的安全防护并能灵活的提供安全服务等特点。

关 键 词 层次安全服务模型; 开放平台; 安全授权; 安全中间件; 基于SLA的访问控制
中图分类号 TP393 文献标志码 A doi:10.3969/j.issn.1001-0548.2013.02.021

Level Security Service Model for Capability Open Platform Based on Mobile Internet

LI Min[1,2] and QIN Zhi-guang[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731;
2. School of Computer, Sichuan Normal University Chengdu 610101)

Abstract By analyzing the security issues and security demand of mobile internet capability open platform, this paper introduces an architecture of mobile internet capability open platform and proposes a hierarchical security service model and the key technology in detail. The hierarchy security service model has been applied in a related project, the application shows that the security model can provide with perfect safety protection and flexible security services etc.

Key words hierarchical security service model; open platform; safe authorization; security middleware; SLA based access control

能力开放平台[1]是近几年来国内外兴起的一种网络开放模式。2007年由Facebook最先推出开放平台至今，国内外著名的互联网公司及电信运营商(如Google APP、人人网、中国电信等)都陆续进入了开放平台时代。移动互联网能力开放平台[2-3]有以下两大特点：第一是能对底层异构的业务能力进行抽象和封装，以统一Open API[4]的形式开放给第三方应用，从而降低开发门槛；其二是第三方开发的应用以服务的形式统一部署到开放平台中。

由于能力开放平台具有的开放特性，不可避免地会受到很多的安全威胁，如开放平台始祖Facebook就遭受了终端用户隐私泄漏、开放接口越权等安全问题。随着攻击手段的提高，更多针对能力开发平台的安全攻击将不断涌现。综合分析，能力开放平台主要面临如下安全问题：1) 开放接口的越权调用：能力开放平台开放的能力资源大部分是计费的，基于利益驱使，可能会遭受越权访问；2) 第三方应用加入平台带来的安全非独立性问题：第三方应用不仅可以部署到平台中作为服务提供给终端用户，还可以作为能力提供给其他的开发者，因此第三方应用可能会成为整个平台的一个安全后门；3) 访问终端用户数据带来的账户隐私威胁：第三方应用访问终端用户的私有数据(如好友列表、位置、照片等信息)时，需要得到终端用户授权，此时，需要有一种机制去保证在不泄露用户账户信息的情况下进行安全的授权。

因此，搭建一个可信的开放平台[5]成为了能力开放平台发展的重要任务之一。本文从移动互联网下能力开发平台的安全问题入手，提出安全目标，并设计了层次安全服务模型，对其中关键技术进行

收稿日期：2012－08－22; 修回日期：2012－08－26
基金项目：国家科技重大专项(2011ZX03002-002-03)；国家863计划主题项目(2011AA010706)；国家自然科学基金重点项目(61133016)；国家自然科学基金(60903157)；中央高校基本科研业务费专项资金(ZYGX2011J063)
作者简介：李敏(1978－)，女，博士生，主要从事移动互联网安全机制、隐私安全等方面的研究.

了阐述，最后通过具体项目的实现，进一步体现了该层次安全模型的优点。

1 相关工作

能力开放平台作为一种新颖模式，目前还缺乏较完善的安全架构和标准。文献[2]从一般平台安全框架，即应用安全性、网络安全性和系统物理安全性来考虑。文献[3]也提到分层安全性，并提出以认证和访问控制为核心的安全模型。以上文献主要是利用传统的信息安全机制来解决安全问题，该方法能够解决一般平台可能遭受的漏洞和攻击，但是针对开放特性带来的特殊安全问题不具有很强的针对性。本文正是在此基础上，根据能力开放平台的新特性完成安全策略和机制的设计和研究，最终达到安全机制的完美融合,保证能力开放平台真正意义上的功能开放。

对于开放接口的合法调用，需要用到访问控制技术。文献[6-7]均提出基于行为的访问控制(action based access control，ABAC)，该模型适用于复杂的云环境，其中用户到角色的分配同环境、时态等行为状态相关，能有效满足云环境下用户多变性要求，但是仍然不能满足能力开放平台的特殊要求。在进行能力开放前，能力开放平台与开发者之间会签订的一份服务水平协议[8](service level agreement，SLA)。一方面，SLA明确了能力开放平台应提供的服务质量(quality of service，QoS)的水平指标；另一方面，SLA明确了客户的相关权利及责任。能力开放平台需要结合SLA进行访问控制，实现接口的合法开放。如何在资源总量有限的前提下满足尽可能多的SLA，一直都是一个学术研究的热点。文献[9-10]分别提出了线性规划及迭代选择算法，文献[11]提出了启发式算法，文献[12]提出了HPSO算法，文献[13]提出了协同动态调度等有效方法。但是由于开放平台的参与者数量庞大，这类方法直接用到能力开放平台中会造成时间效率过低，因此需要一种更高效简单的基于SLA的分配算法。

能力开放平台的开放性还体现在第三方应用的融入，由于第三方应用自身含有的恶意成分及隐藏的攻击性，因此有必要对要加入平台的第三方应用进行一定的安全监测，防止其成为整个平台的攻击后门。本文可借鉴现有的静态扫描和动态的沙盒监测相结合的技术，有效地保证平台的安全。

在授权给第三方应用访问终端用户的私有数据时，可考虑利用开放的授权协议[14](open authorization，Oauth)保证用户账户的隐私安全。该协议不要求资源拥有者(终端用户)将账户名及密码提交给第三方应用，而是将终端用户引导到认证鉴权服务器进行鉴权，保证第三方应用无法触及到终端用户的账户信息，从而确保了账户的隐私安全，实现了安全的授权。

2 安全服务模型

2.1 面向移动互联网的能力开放平台结构

能力开放平台的模型如图1所示。该模型在PaaS平台的概念模型[15]基础上，结合开放平台特性，提出的适用于移动互联网的能力开放平台结构。

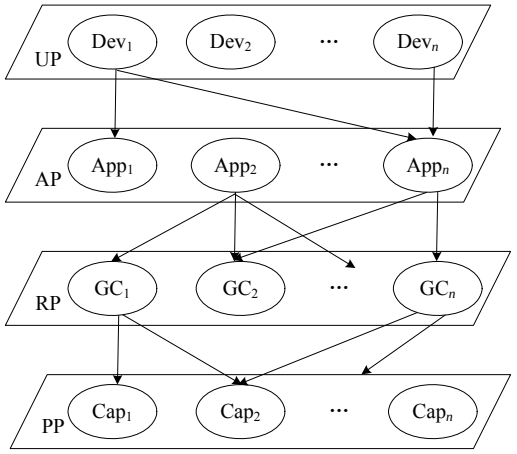

图1 移动互联网下能力开放平台模型

在该模型中，UP层是能力开放平台的目标使用者，即应用开发者(developer，Dev)；AP层是UP层中各种开发者开发的不同类型的第三方应用(application，APP)；RP层有一系列通用容器(general container，GC)组成，主要包含了各种能力API、安全中间件API及第三方应用的部署容器，其中第三方应用也可以作为能力资源提供给其他的应用，该层还包括向下的能力适配模块；PP层由一系列能力(Cap/Capability)组成，包括：短信、彩信等电信能力，地图、云存储等IT能力及终端用户的私有数据能力。

2.2 能力开放平台的层次安全服务模型

针对上述对面向移动互联网的能力开放平台的安全问题及相应的安全机制的分析，结合图1所示平台模型，本文提出移动互联网下能力开放平台的层次安全服务模型，如图2所示。该层次安全模型在UP层和AP层之间增加对每个开发者的身份认证。在AP层和RP层之间加入安全核心安全服务层。在安全

核心层中，在APP部署到平台中时，需要对APP进行接入审核；在APP调用能力API时，需要基于SLA的访问控制来控制APP对能力资源的合法调用，如果调用的是私有数据，需要用到OAuth进行安全的授权；安全服务层主要提供安全中间件，其目的是将安全服务作为能力资源开放给APP。如APP可以调用安全中间件服务器封装好的“数据加密”这个安全服务，开发出具有“数据加密”安全属性的应用，这一安全性的达到无需Dev自己开发。安全中间件提供的安全服务可以进行修改、增加和删除，但对于APP是透明的，而安全功能的改变也不会影响到APP的主体功能。

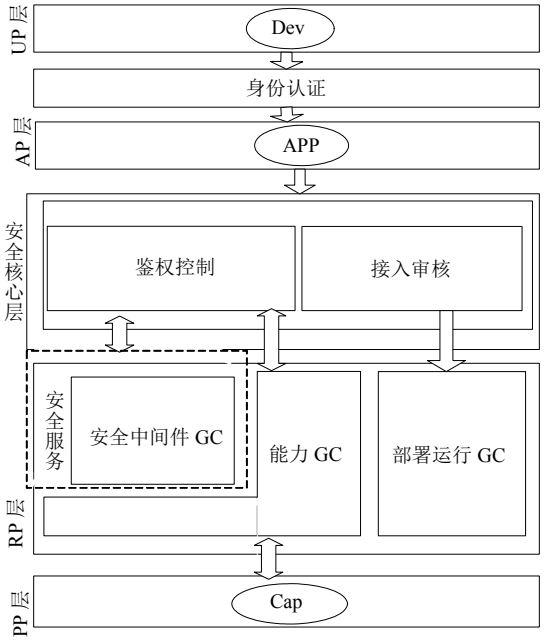

图2　层次安全服务模型

在能力开放平台运行的各个阶段中，该安全服务模型分层次提供了以下安全服务。

1) APP开发阶段：当一个已经注册并同平台鉴定了能力使用合约的开发者进行APP的开发时，首先需要进行身份的认证，确认为合法用户才能登陆平台提供的开发环境。

2) APP部署阶段：当APP开发结束，需要部署到平台中时，要经过测试阶段进行接入审核，当确定为安全的APP时，才可以加入到部署运行GC中。

3) APP运行阶段：当APP运行时，需要用基于SLA的访问控制来限定APP只能调用签约的能力。在这一阶段，安全中间件提供的安全服务同样作为能力资源开放给合法的第三方应用。如果APP访问终端用户的私有资源时，需要利用OAuth协议对APP进行安全授权。

该层次安全模型有如下4个主要贡献：1) 利用基于SLA访问控制，有效地防止了能力资源的合法访问，其中SLA的动态调度算法最大限度的保障了用户的QoS；2) 对第三方应用的接入审核，最大限度地解决了安全的非独立性问题；3) 利用OAuth2.0协议实现私有数据的授权，保护了用户的账户隐私；4)对APP提供的安全中间件服务，满足了APP对于安全性的一般要求，提高APP的开发效率，从而提高了整个平台的实用性及灵活性。

3　关键技术

3.1　基于安全授权的认证鉴权

在APP运行阶段，当APP去调用能力时，首先会经过访问控制模块进行角色权限的判别，会得到一个可访问权限集P(包括访问范围Acc_scope及操作Opr)。如果Acc_scope中存在私有数据，参考OAuth2.0进行授权，得到访问令牌Access Token，APP再经由认证鉴权服务器访问可访问权限范围内的能力资源和安全中间件资源；如果没有私有数据，则无需经过授权即可访问到相关资源。具体执行过程如图3所示，授权流程中，终端用户并没有直接将账户信息交由APP，而是通过重定向到认证鉴权服务器来进行身份识别，从而保护了用户账户隐私，达到了安全授权的目的。

3.2　基于SLA的访问控制

3.2.1　基本模型

在控制APP对能力资源的访问中，本文提出了基于SLA的访问控制模型如图4所示，该模型在传统的访问控制模型基础上提出SLA约定，角色与权限之间有一定的优先层次关系，该模型很好地保障了用户的QoS。图中消费者即能力的访问者，指第三方应用(APP)，其他概念同一般的访问控制模型。角色和权限都分别设置了层次关系。

规则 1　高级别的角色拥有低级别的角色权限，即权限向下继承。在SLA约定中，不同角色的优先级别决定了APP的响应顺序。

规则 2　允许同级别的APP对能力资源有只读权限，高级别APP对低级别能力资源有所有权限(读/写、执行)，低级别APP对高于自己级别的能力资源只具有最小权限(即只可以读取合约规定的部分能

力资源)。

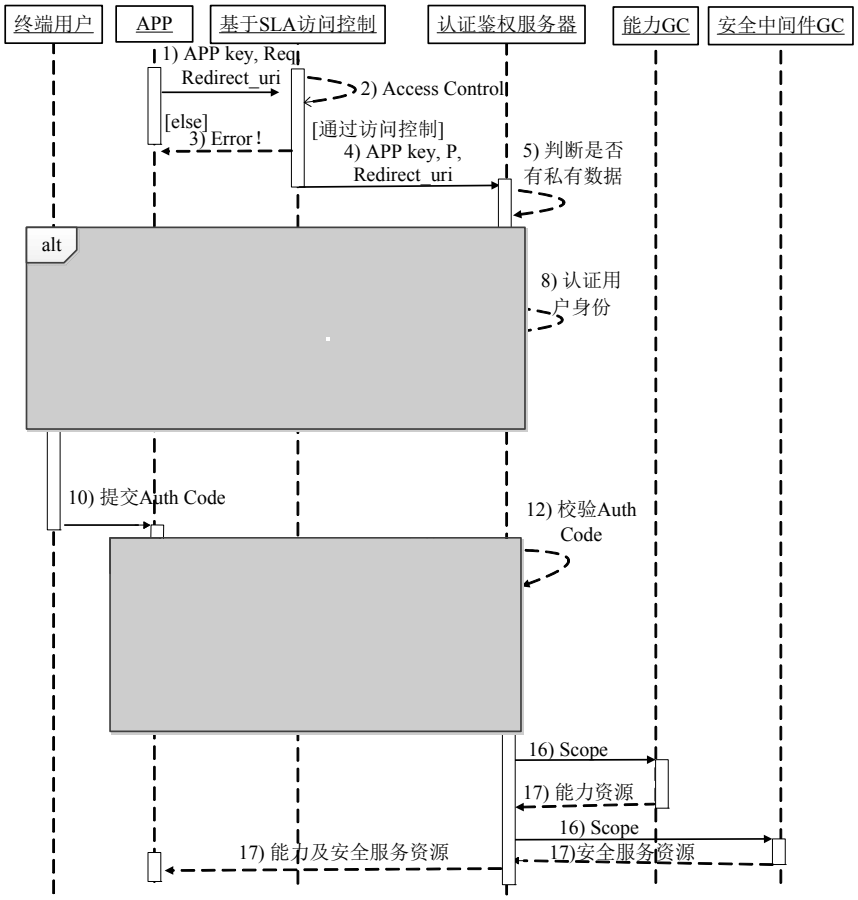

图3 基于安全授权认证鉴权

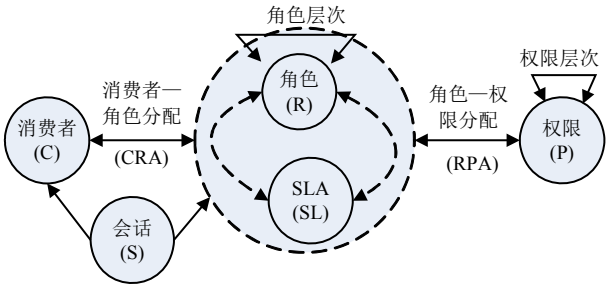

图4 基于SLA的访问控制模型

3.2.2 SLA约定

对于SLA的衡量主要有服务响应时间、吞吐量及可用性等。考虑到实现的方便性及时间效率，SLA的动态调度算法主要考虑服务的响应时间，而响应时间通常同平台当前的请求密度相关。该算法适用于当现有资源难以满足全部活跃用户SLA时，对资源进行动态分配与调度，满足级别高的用户，从而实现能力资源的较优配置。

定义 1 请求密度(request density，RD)。应用在单位时间内发起的能力访问请求的频度，表示了应用为平台带来的负载压力。计算公式为：

$$RD=\Sigma r_i/t \tag{1}$$

式中，Σr_i表示在时间窗t内应用的请求数目；t表示请求处理时间窗。

在资源总量一定情况下，请求密度阈值(rd_1)用于判断平台的稳定性。只要请求数量的增加不会使请求密度超过该阈值，平台对于APP的响应时间基本不会受影响，即不用去考虑APP优先级；而当请求密度超出rd_1时，响应时间会随着请求密度的增加而增大，此时必须选择高优先级的用户来保证其SLA。

在讨论算法前，平台会根据开发者鉴定的不同的开发协议及开发者自身的不同类型(个人、企业等)来决定开发者的等级(同样，该等级会映射到开发者开发的APP)。

算法 1 SLA的动态调度算法：

1) InitQueue(Q_1)//初始化就绪队列
2) InitQueue(Q_2)//初始化等待队列
3) while(r_i)//新请求或轮询Q_2有请求r_i加入
4) {Update(RD)//更新平台的请求密度RD
5) if(RD<rd_1)
//如果平台当前的请求密度低于阈值rd_1时

6) {EnQueue(Q_1,r_i)
//将r_i加入就绪队列
7) Sort(Q_1)
//对就绪队列中各APP请求按优先级排序
8) else
9) {if(r_i优先级>Q_1队尾优先级)
10) DelQueueTail(Q_1,r_j)
//删除Q_1队尾请求r_j
11) EnQueue($Q2$,r_j)//并加入到Q_2
12) go6)//对r_i处理同RD<rd_1的情况
13) else
14) EnQueue(Q_2,r_i)
//将加入等待队列，等待轮询转入步骤3)

该算法中，当有新请求或者轮询等待队列，有请求r_i到达时，首先更新平台的请求密度RD，如果RD低于密度阈值rd_1，则将r_i加入到就绪队列，对就绪队列按角色层次进行排序，按其优先级别响应；如果RD不低于密度阈值rd_1，分成两种情况讨论：1) 如果r_i优先级大于就绪队列队尾优先级，则将就绪队列队尾请求r_j删除并将r_j加入到等待队列，同时将r_i加入到就绪队列，处理情况同RD<rd_1的情况；2) 否则直接将r_i加入到等待队列，进入轮询等待。在算法1中，就绪队列按照该请求在访问控制中的角色级别进行排序，这一角色等级同开发者Dev同平台签约等级相关。

算法1的时间效率主要取决于定时对于Q_2的轮询及对Q_1的排序，如果Q_1的长度为m，Q_2的长度为n，则轮询Q_2的时间复杂度为$O(n)$，而对于sort(Q_1)可以选择时间效率和稳定性较好的堆排序，时间复杂度为$O(m\log m)$。

3.3 接入审核

在第三方应用APP作为服务加入到平台之前，必须经过接入审核系统，确认为安全可信的APP才能加入到部署运行GC中，如图5所示，以保证整个平台的可控性。

接入审核系统分为3个阶段进行审核。

基础审核：主要包括内容安全(有无非法言论，如政治敏感、色情、暴力等)审核及基础规范审核。

服务质量审核：主要针对应用的服务质量、响应速度的审核，还包括应用环境兼容性。

安全审核：主要利用静态扫描分析和动态沙盒仿真审核。沙盒仿真测试是将沙盒和仿真技术结合起来，以沙盒为容器，把被测APP放入沙盒中监控执行，通过记录日志来分析APP的安全性。利用沙盒仿真测试有几个优势：1) 检测过程完善；2) APP中包含的各种攻击对整个平台不造成任何影响。

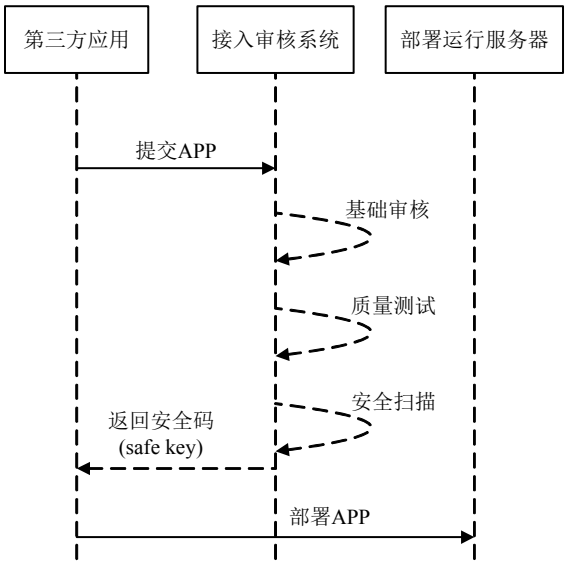

图5　APP接入审核

3.4 身份认证

身份认证在安全服务层次中适用于两个方面：一方面是对Dev进行身份认证；另一方面是图3中第8步对授权者的身份验证。由于讨论的能力开放平台是面向移动互联网的，终端用户主要由桌面终端和移动终端组成，考虑用户在线和离线两种情况：1) 用户在线，主要提供以下两种身份认证方式：① 用户名/密码方式；② 动态消息验证码，需要移动终端(如手机、IPAD等)的参与，其特征在于一次产生一个新的消息验证码并具有一定的时效性，有效地防止了用户名/密码的重放攻击。2) 用户离线，可以利用短消息及动态消息验证码相结合进行身份验证。

4 测试与分析

本文搭建了一个能力开放平台，以一个基于位置的服务(LBS)应用为例进行相关测试。

1) 开发阶段：经过认证的开发者在在线或离线开发生成环境中开发LBS应用，需要调用开发平台提供的地图能力API及安全中间件提供的加密API；

2) 应用部署阶段：在测试环境中经过图4的接入审核，得到一个安全标识后即可部署到部署运行服务器中；

3) 应用运行阶段：当用户调用LBS服务，如查询最近的餐厅位置时，LBS需要得到用户授权获取用户当前位置(如图6中给LBS取名为test)。根据SLA

的访问控制获取地图能力及加密能力(如图7)。

经测试分析，本文提出的层次安全服务模型能解决开放接口的越权调用、阻止第三方应用成为攻击后门及保证授权过程中用户账户安全等问题，同时在资源总量一定的前提下，基于SLA的动态调度算法能较好地进行资源的分配，尽量满足级别高的应用的请求。

图6 授权页面

图7 获取访问令牌

5 结 束 语

为解决能力开放平台中能力开放和第三方融入带来的安全问题，本文提出了一个实用的层次安全服务模型。该层次安全模型提供了身份认证、安全核心层及安全服务层，其中安全核心层提供了基于OAuth安全授权的认证鉴权、基于SLA的访问控制及APP接入审核，安全服务层提供安全中间件服务。通过实际项目的应用，该模型能为能力开放平台提供完善的安全防护并能灵活地将安全作为服务提供给第三方应用，从而提高了整个平台的安全性及方便性。一般开放平台同能力开放平台有相似的安全问题，但是基于SLA的访问控制模型不一定适用于一般开放平台，因此下一步将研究一个更为通用的访问控制模型，以保证资源的合法开放，从而进一步研究适用于一般开放平台的安全服务模型。

参 考 文 献

[1] HAI H E, MEI N S, JUN D S, et al. A new service delivery open platform (SDOP) architecture[C]//IEEE International Symposium on IT in Medicine & Education. Jinan: IEEE, 2009.

[2] 高嘉阳, 孟繁熹. Web开放平台安全体系的研究与设计[J]. 宇航计测技术, 2010, 30(5): 39-42.
GAO Jia-yang, MEN Fan-tao. Research and design of secutity system for web open platform[J]. Journal of Astronautic Metrology and Measurement, 2010, 30(5): 39-42.

[3] 高嘉阳. Web开放平台安全机制的研究与设计[D]. 北京: 北京邮电大学, 2009.
GAO Jia-yang. Research and design of security mechanism for Web open platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2009.

[4] KIM E, KIM K, PETER H, et al. A multi-view API impact analysis for open SPL platform[C]//The 12th International Conference on Advanced Communication Technology (ICACT). Phoenix Park: [s.n.], 2010.

[5] ENGLAND P, LAMPSON B, MANFERDELLI J, et al. A trusted open platform[J]. IEEE Journal of Computer, 2003, 36(7): 55-62.

[6] 林果园, 贺珊, 黄皓, 等. 基于行为的云计算访问控制安全模型[J]. 通信学报, 2012, 33(3): 59-67.
LIN Guo-yuan, HE Shan, HUANG Hao, et al. Access control security model based on behavior in cloud computing environment[J]. Journal of Communications, 2012, 33(3): 59-67.

[7] 李凤华, 王巍, 马建峰, 等. 基于行为的访问控制模型及其行为管理[J]. 电子学报, 2008, 3(10): 1881-1890.
LI Feng-hua, WANG Wei, MA Jian-feng, et al. Action-based access control model and administrator of actions[J]. Acta Electronica Sinica, 2008, 3(10): 1881-1890.

[8] 胡春华, 陈晓红, 吴敏, 等. 云计算中基于SLA的服务可信协商与访问控制策略[J]. 中国科学信息科学, 2012, 42(3): 314-332.
HU Chun-hua, CHEN Xiao-hong, WU Min, et al. A service trust negotiation and access control strategy based on SLA in cloud computing[J]. Scientia Sinica Informationis, 2012, 42(3): 314-332.

[9] CARDOSO J, SHETH A, MILER J, et al. Quality of service for workflows and Web service processes[J]. Web Semantics, 2004, 1(3): 281-308.

[10] SU Sen, LI Fei, YANG Fang-chun. Iterative selection algorithm for service composition in distributed environments[J]. Science in China Series F: Information Sciences, 2008, 51(11): 1841-1856.

[11] OH S C, LEE D, KUMARA S R, et al. Effective Web service composition in diverse and large-scale service networks[J]. IEEE Transaction on Services Computing, 2008, 1(1): 15-32.

[12] HU Chun-hua, WU Min, LIU Guo-ping, et al. QoS scheduling algorithm based on hybrid particle swarm optimization strategy for Web services workow[C]//The 6th International Conference on Grid and Cooperative Computing. Los Alamitos: [s.n.], 2007.

[13] JIANG Wei-jin, ZHANG Lian-mei, WANG Pu. Dynamic scheduling model of computing resource based on MAS cooperation mechanism[J]. Science in China Series F: Information Sciences, 2009, 52(8): 1302-1320.

[14] Network Working Group. The OAuth 2.0 Authorization Protocol draft-ietf-oauth-v2-20[S/OL]. [2012-08-22]. http://tools.ietf.org/html/draft-ietf-oauth-v2-20,2011.

[15] 徐鹏, 陈思, 苏森. 互联网应用PaaS平台体系结构[J]. 北京邮电大学学报, 2011, 35(1): 120-124.
XU Peng, CHEN Si, SU Sen. Architecture of PaaS for

Internet applications[J]. Journal of Beijing University of Posts and Telecommunications, 2011, 35(1): 120-124.

编 辑 税 红