

文章编号: 1000-5013(2011)06-0638-03

# 互联网用户安全登录平台设计

陈柏生, 吴可沾, 杨育辉

(华侨大学 计算机科学与技术学院, 福建 泉州 362021)

**摘要:** 设计一个开放的互联网用户数据中心 Hagza 开放平台,对互联网的用户和应用资源进行有效整合. 用户可通过该平台快捷地使用各种互联网应用和高效地管理其网络社交关系,而各种网络应用则可借助该平台快速地聚集优质用户. 基于表述性状态转移(REST)架构的风格设计,可降低系统实现的复杂性和保证良好的可扩展性,而通过 P3P,OAuth,OpenID 等复合认证体系,可保证用户隐私和跨平台调用的安全性.

**关键词:** Hagza 开放平台; 互联网; 安全登录; 表述性状态转移; 复合认证

**中图分类号:** TP 393 **文献标志码:** A

日益增长的互联网应用在给人们的生活带来了诸多便利的同时,也给人们带来了许多困扰. 首先,由于互联网应用数量巨大且质量良莠不齐,用户甄别和选择优质网站是一个极困难的工作;其次,各种网络应用彼此分离,各自为政,用户不得不疲于应对千篇一律的注册和登录操作,以及随之而来的大量网络账号的管理和维护. 而与此同时,各种互联网应用服务也为如何更有效地聚集优质用户而烦恼. 基于此,本文设计和开发了一个开放的互联网用户数据中心 Hagza 开放平台(Hagza open platform,简称 HOP),旨在对互联网的用户和应用资源进行有效整合.

## 1 系统总体设计

HOP 的最终目标是要建立一个互联网用户与应用资源整合平台,故系统应具备开放性、可扩展性、分布式和安全性等特性. HOP 系统主要由开放认证、外部(可选)应用、核心应用、开放 API 以及平台管理等 5 大功能模块组成,如图 1 所示. 其中:开放认证、外部应用和核心应用属于用户功能模块;开放 API 模块主要面向站内应用、第 3 方应用开发和第 3 方合作站点群;平台管理只面向 HOP 的管理者.

用户功能模块是 HOP 系统的核心部分,未注册用户可进入系统首页进行注册,也可以通过验证已有第 3 方账号进行快速登陆和注册. 已注册用户选择进入登陆界面,进行通用登陆或第 3 方登陆. 用户登陆 HOP 平台进行各种平台操作,包括直接使用各项已注册的 OAuth 应用,对信任的 P3P 站点进行登陆同步,以及对 OpenID 验证进行认证授权.

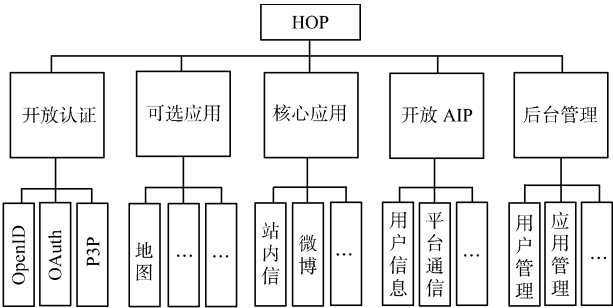


图 1 HOP 系统功能

Fig. 1 HOP system function

## 2 基于 REST 风格的系统架构

HOP 不仅支持站内应用,更支持第 3 方应用及第 3 方合作站点群. 因此,系统设计的首要难点就是跨平台调用问题. 表述性状态转移(representational state transfer,简称 REST)是一种充分利用 Web 特性的分布式超媒体系统架构风格<sup>[1]</sup>. 它将系统中所有信息抽象成资源,利用统一资源标识符 URI 定

位和识别资源,并使用统一的抽象访问接口实现异构平台的互操作. REST 的设计风格极大降低了应用组件的耦合度,使得系统设计更加简洁清晰. HOP 使用基于 OAuth 协议的 REST 架构实现安全的跨平台交互,降低系统设计和实现的复杂度,并保证良好的可扩展性.

REST 架构风格的核心是资源的 URI 表示,要求 URI 具有一定的意义和良好的结构. HOP 系统设计的资源 URI 及其映射主要包括:(1) 核心应用,coreAppName. domain. com;(2) 第 3 方应用,appName. app. domain. com;(3) 系统 API,Api. domain. com/? method = Resource. method&-format = dataType;(4) 系统应用代理服务器,www. domain. com/restfulapp? # appHash;(5) 通用认证登录,www. domain. com/login. php;(6) 可用认证方式,www. domain. com/auth/openid/rp|op(OpenID 认证)和 www. domain. com/auth/p3p/op|rp(P3P 认证);(7) 用户 URI,Username. domain. com.

HOP 系统组件主要包括用户代理、HOP 应用 API,HOP 服务器、第 3 方应用 API,其互操作机制如图 2 所示. 用户通过代理访问 HOP 应用;APP 向 HOP 应用 API 发起认证请求,API 服务器将对用户执行一个标准的 OAuth 认证过程;在验证通过后,API 服务器携带安全的信息签名向 HOP 服务器或者第 3 方的 API 终点服务器发起数据请求;API 服务器验证信息签名,返回数据结果. OAuth 认证是实现 HOP 组件互操作的核心,它提供对应用 API 的认证;同时,HOP 也通过对用户的认证,实现“一账户通行”的应用站点间自由穿行,而这个功能由 OpenID 认证提供.

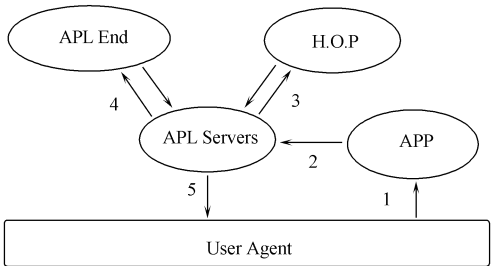
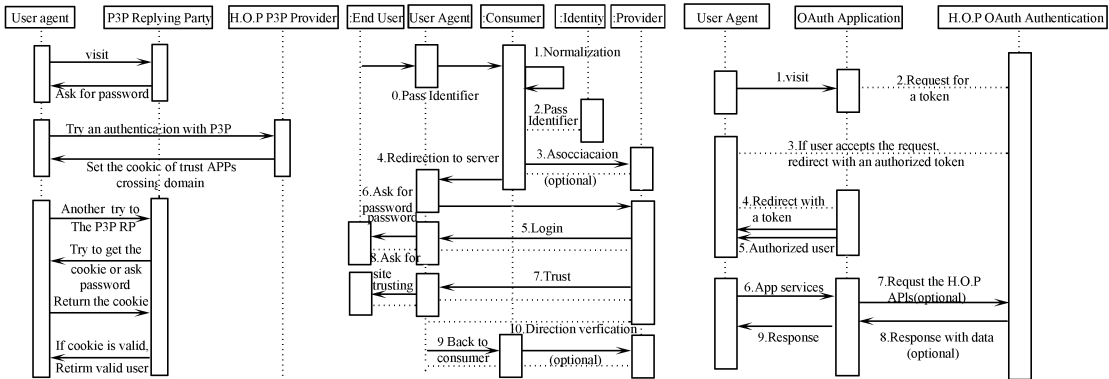


图 2 HOP 组件互操作机制  
Fig. 2 HOP components and their inter-operation

### 3 开放认证模块

开放认证模块作为 HOP 开放性和可扩展性计划的一部分,为用户提供账号资源的统一管理,并为第 3 方应用和第 3 方站点群共享可能的优质用户资源. HOP 的权限控制不仅面向用户、网站管理员,还面向 APP 网络应用,因此,要求 HOP 相比多数现有网络应用具有更细粒度的权限控制功能. HOP 联合使用 P3P,OpenID 和 OAuth 等 3 种主流的网络隐私保护策略协议,来实现用户账号登录、退出的同步及用户资料的多点共享.

P3P 是万维网联盟(W3C)公布的一项隐私保护推荐标准<sup>[2]</sup>. 图 3(a)为 P3P 的认证流程,有如下几个步骤:(1) 用户访问 P3P 依赖方,P3P 依赖方尝试读取 Cookie,如未读取到有效的 Cookie,则引导用户进入待登陆界面;(2) 执行 P3P 登陆同步,将所有信任的 P3P 依赖方站点写入认证 Cookie;(3) 用户返回 P3P 依赖方站点,P3P 依赖方再次尝试读取 Cookie,如读取成功,则提示用户登陆成功.



(a) P3P (b) OpenID (c) OAuth  
图 3 认证流程

Fig. 3 Certification process

OpenID 是 LiveJournal 和 SixApart 开发的一套身份验证系统<sup>[3]</sup>. 与目前流行的网站帐号系统相比,它不局限于某一个网站或者网站群,可在任意 OpenID 应用网站中自由穿行. OpenID 使用 URI 作为其在互联网唯一的身份标识,URI 由 OpenID 的提供方提供. 用户只需将自己的个人信息存储在

OpenID 帐号的提供方,便能在任何需要的时候,安全快捷地授权给任何 OpenID 应用网站使用.

图 3(b)为 OpenID 的认证流程,有如下几个步骤:(1) 用户通过代理访问 OpenID 依赖方(replying party,RP),代理为其提供 OpenID 标识;(2) RP 对 OpenID 标识执行自动发现,获得其提供者(OpenID provider,OP);(3) 作为可选步骤,RP 对 OP 做一个关联请求,以便在此后的验证中,使用关联所获得的句柄,对消息进行签名,RP 以 HTTP 重定向引导用户进入 OP 的授权页面;(3) 如用户未在 OP 通过身份认证,则 OP 向用户浏览器返回登陆认证界面,否则提示用户输入密码,进行登录;(4) OP 在通过用户认证之后,引导用户进入授权提示界面;(5) 在获得用户授权之后,HOP 携带认证用户所授权的用户数据,引导用户进入 RP 的回调页面;(6) 用户完成在 RP 的 OpenID 登录,进入 RP 的服务界面,作为可选步骤,RP 可再次定向至 OP 以确认认证结果.

OAuth 协议致力于使网站和应用程序能够在无须用户透露其认证证书的情况下,通过 API 访问某个 Web 服务的受保护资源<sup>[4]</sup>. OAuth 为 API 认证提供了一个可自由实现且通用的方法.

图 3(c)为 OAuth 认证流程,有如下几个步骤:(1) 用户访问一个未获 OAuth 认证的 OAuth 应用, OAuth 应用以 HTTP 重定向至 HOP OAuth 认证系统;(2) 若用户未授权当前请求应用,则 HOP OAuth 认证系统引导用户浏览器定向至 OAuth 授权界面;(3) 若当前请求应用已获得用户授权,则由 HOP OAuth 认证系统携带认证,通过参数 authorized\_token 引导用户浏览器重定向至 OAuth 应用的回调页面(callback URI);(4) OAuth 应用依据 authorized\_token 和 app\_key 获取所需的用户数据,引导用户进入应用服务界面. 此后,在一个活跃周期里,OAuth 应用可使用 app\_key,authorized\_token, app\_mac(消息签名)与 HOP 进行安全的数据交互.

4 结 束 语

设计了一个开放、安全和可扩展的互联网用户与应用资源整合平台 HOP, 基于 LAMP(Linux+ Apache+MySQL+PHP)平台开发一个原型系统,并在校园网内进行了小范围测试. 今后工作将进一步扩展 HOP 站内应用,并将 HOP 系统在互联网发布,进行更大范围的测试和推广.

参 考 文 献:

[1] FIELDING R T. Architectural styles and the design of network-based software architectures[EB/OL]. [2000-03-16]http://www.ics.uci.edu/~fielding/pubs/dissertation/top. htm.  
[2] CRANOR L F. P3P Web 隐私[M]. 技桥,译. 北京: 清华大学出版社,2004.  
[3] OpenID group. OpenID authentication 2. 0: Final[EB/OL]. [2007-12-6]http://openid. net/specs/openid-authentication-2\_0. html.  
[4] HAMMER-LAHAV E. The OAuth 1. 0 protocol[EB/OL]. [2009-09-10]http://tools. ietf. org/html/rfc5849.

Design of the Secure Login Platform for Internet User

CHEN Bai-sheng, WU Ke-zhan, YANG Yu-hui

(College of Computer Science and Technology, Huaqiao University, Quanzhou 362021, China)

**Abstract:** A Hagza open platform is designed. It presented an open user-centered internet platform to integrate internet resources of users and applications. With the help of the platform, users could easily use various internet applications and effectively manage their network social relationship, meanwhile applications could quickly accumulate potential users. The platform was schemed as RESTful infrastructure in order to reduce its realization complexity and maintain good scalability. It also secured users' privacy and inter-operation of applications by exploiting combined authentication system of P3P, OAuth and OpenID.

**Keywords:** Hagza open platform; internet; secure login; representational state transfer; composite certification