王珂,曹波,马园,等. 统一身份认证系统在陕西气象网络防护中的应用[J]. 陕西气象,2024(4):77-80.
文章编号:1006-4354(2024)04-0077-04

统一身份认证系统在陕西气象网络防护中的应用

王　珂[1,2],曹　波[1,2],马　园[1,2],党　瑞[1]
(1. 陕西省气象信息中心,西安　710014;
2. 陕西省气象局秦岭和黄土高原生态环境气象重点实验室,西安　710016)

摘　要:随着气象信息化的快速发展,业务系统复杂程度日益提升,数量激增,用户认证复杂化及安全隐患增加。通过构建一套统一身份认证系统,实现用户身份的统一管理、统一认证和统一授权,可以降低系统运行安全风险隐患。采用 OAuth2.0 授权码模式进行认证对接,同时通过 SSL/TLS 和 CA 证书进一步加强安全性,可以实现用户身份的集中管理和单点登录,简化用户的认证流程。以陕西省气象数据共享网为例,对统一身份认证系统应用进行了详细说明。

关键词:统一身份认证;OAuth2.0;单点登录
中图分类号:TP393.08　　**文献标识码**:A

随着气象信息化不断发展,气象行业业务系统的数量持续增长[1],这些业务系统有着各自独立的用户认证体系。从安全角度考虑,不同的业务系统应设置不同的口令,且口令应是强安全口令并定期更换;但对用户而言,多口令记忆负担重,且容易遗忘和混淆,大多数情况下,用户为了方便记忆,通常设置成通用口令、默认口令、弱口令和长期不变口令[2-3],一旦系统被攻击者爆破,会造成严重的安全事件。对于系统管理员而言,需要频繁地在不同业务系统上维护大量账户信息。当人员岗位变更时,每个系统都要进行账户注销或更新,容易因信息不同步带来安全隐患。对于业务系统的开发人员而言,每个系统都要开发一套用户认证模块,易产生资源浪费。基于以上原因,建设一套统一的身份认证系统就显得尤为必要。统一身份认证系统就是各业务系统共用一套身份认证系统,各系统可以根据自身情况按需配置认证手段和认证强度,用户只需一次登录就可以访问其他已授权系统,即单点登录[4-5]。统一身份认证系统的实现可以解决使用不便、管理复杂、资源浪费等问题,很大程度上提升资源利用率,减少安全隐患,提高系统管理员的工作效率。

1　技术介绍

1.1　OAuth2.0 技术介绍

OAuth 是一个验证授权的开放标准[6],用来授权第三方应用获取用户数据。在 OAuth 之前,一般采用用户名、密码的方式进行身份验证,这种方式存在极大的不安全性,OAuth 的出现解决了访问资源的安全性及灵活性,客户端可以安全可控地获取用户的授权,并与服务提供商进行互动[7]。

OAuth 在客户端和服务提供商之间,设置了一个授权层,客户端不能直接登录服务提供商,只能登录授权层,客户端登录授权层所用的令牌与用户的密码不同,用户在登录时,可以指定授权层令牌的权限范围和有效期。客户端登录授权层以后,服务提供商根据令牌的权限范围和有效期,向客户端开放用户储存的资料。客户端必须获得用户的授权,才能使用令牌。

OAuth2.0 定义了四种客户端的授权模式:授权码模式、密码模式、简化模式、客户端模

收稿日期:2023-10-18
作者简介:王珂(1995—),女,汉族,陕西礼泉人,硕士,工程师,从事计算机网络与信息安全研究。
基金项目:陕西省气象局秦岭和黄土高原生态环境气象重点实验室开放基金课题(2022Y-11)

式[8-10]。授权码模式(authorization code)是目前功能最完整、流程最严密的授权模式,通过客户端的后台服务器,与服务提供商的认证服务器进行互动。

1.2 OAuth2.0 授权码模式访问流程

Web 应用需要在统一身份认证系统进行注册,并填写回调地址,获得相应的 client_id 和 client _ secret,用于区分 Web 应用的身份。OAuth2.0 授权码模式访问流程如图 1 所示,具体流程如下。

(1)用户通过浏览器访问 Web 应用,调用授权认证接口 authorize,重定向到统一身份认证服务器进行授权。

(2)用户输入用户名、密码进行授权登录,统一身份认证服务器通过 client_id 确认需要授权的 Web 应用的身份,生成临时凭证 code,浏览器携带临时凭证 code 重定向到指定的回调地址,即 Web 应用的地址。

(3)Web 应用携带临时凭证 code 和自身的 client_id、client_secret 获取令牌 access_token,返回授权信息。access_token 只在短期内有效,且有权限范围,这样既可以让第三方 Web 应用获得权限,同时又随时可控,不会危及系统安全。

(4)应用携带 access_token 获取用户信息接口,统一认证服务器校验 access_token 成功,返回用户信息,完成授权登录。

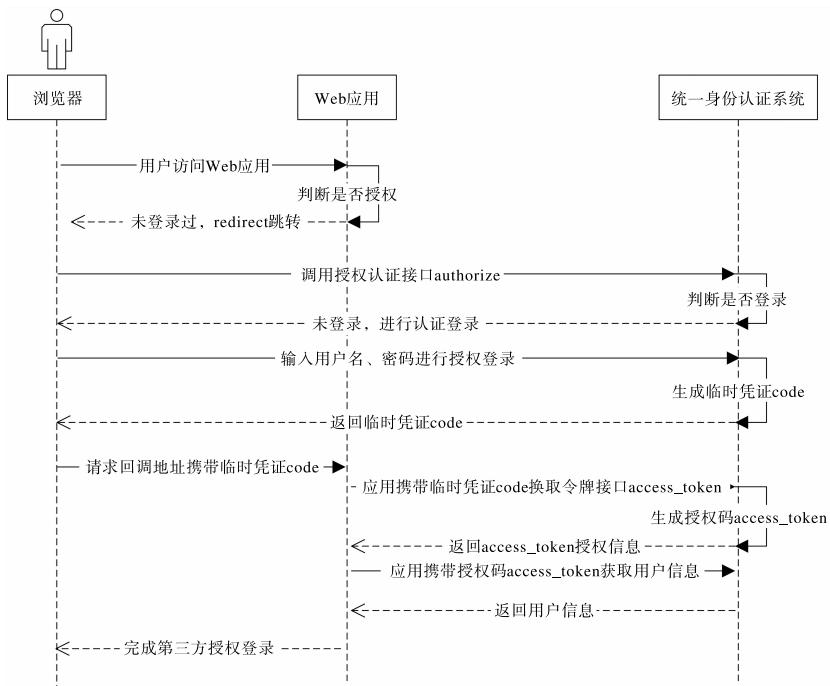

图 1 OAuth2.0 授权码模式访问流程

2 统一身份认证系统的设计与实现

2.1 系统总体架构

该系统遵循中国气象局统一身份认证系统的技术架构,依托中国气象局统一身份认证服务基础支撑平台,实现身份信息及认证手段集约融合共享,提升业务系统认证授权安全能力,系统总体架构如图 2 所示。可对接各种业务系统,提供多种认证手段,系统可实现统一用户,统一授权,统一认证,统一审计四大功能。

统一身份认证系统整体采用一级服务两级部署方式,即在中国气象局建立一套完整的统一身份认证体系,包括统一用户身份服务,统一认证服务,安全审计服务,API 网关服务。在陕西省气象局通过部署用户身份服务和认证服务共同建立陕西省气象局统一身份认证系统。

2.2 安全设计

对于用户认证的接口服务,所有涉及到互联网交互的认证信息,全部采用 SSL 加密传输,不

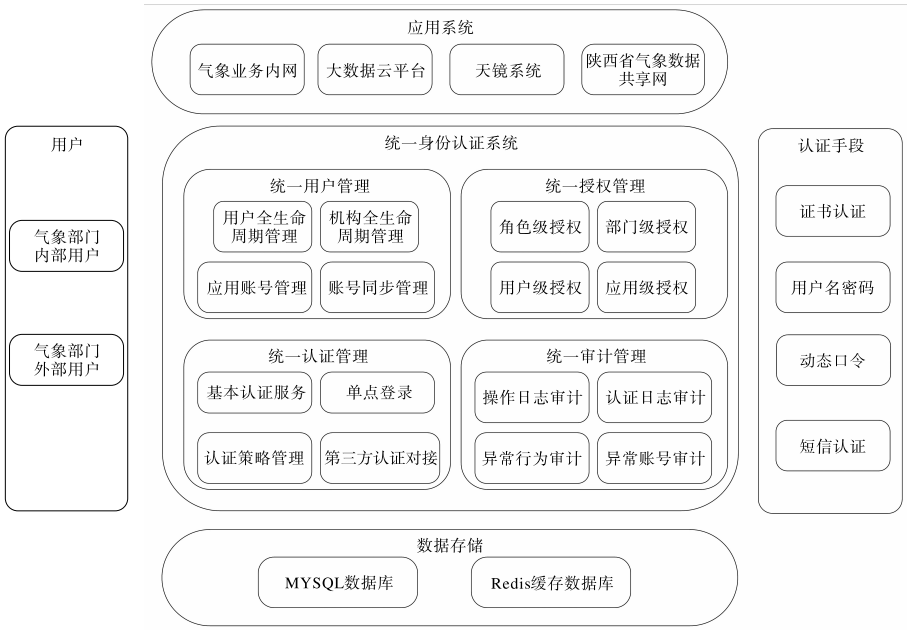

图 2　统一身份认证系统总体架构图

允许通过 HTTP 进行访问。为了避免用户名、密码泄露,所有涉及到用户名、密码的用户信息,全部采用报文整体加密和参数摘要计算,保证了数据传输的保密性以及不可篡改性。

2.3　功能实现

统一身份认证系统由统一用户管理、统一认证管理、统一授权管理、统一审计管理四大功能模块组成。

2.3.1　统一用户管理　统一用户管理提供用户集中存储、全生命周期的闭环管理,同时向业务系统提供用户主数据。解决了用户账号多、密码记不住、操作复杂等问题,仅需要维护一套用户数据,避免了用户信息不同步、权限不可控所造成的安全问题。

2.3.2　统一认证管理　提供统一的认证服务,实现系统间的单点登录。包含多种认证手段,如 CA 证书,动态口令,短信,用户名、密码等多种认证方式,陕西省气象局可根据具体业务环境进行认证方式的扩展,如人脸识别、指纹等生物认证手段。对于安全性要求高的业务系统可基于认证链进行多层级认证。各业务系统无需知道各认证手段的具体实现方式,仅调用认证接口即可实现身份认证。

2.3.3　统一授权管理　统一授权管理可以实现不同业务系统权限的集中管理。提供应用级授权,能够控制用户对业务系统的访问权限。用户只有在管理员进行权限分配后才能进入业务系统,而业务系统内部的权限则由各个业务系统自行分配和管理。

2.3.4　统一审计管理　通过提供集中统一的审计功能,可以对用户访问行为进行分析,及时发现异常登录行为和异常状态的账号,进行风险预警。

2.4　用户数据同步

陕西省气象局统一身份认证节点,上游数据源采用中国气象局 OA 系统(office automation,办公自动化系统)的用户数据,将 OA 系统的陕西气象用户数据同步推送至陕西省气象局统一身份认证节点。

3　具体应用——以陕西省气象数据共享网为例

3.1　陕西省气象数据共享网系统现状

陕西省气象数据共享网(以下简称“共享网”)面向陕西省、市、县三级气象部门用户,是一个丰富、全面、多样化的集气象数据检索、展示、分析等为一体的数据共享平台。该平台允许用户在线查询、检索和获取气象数据,是气象数据获取的重要门户网站。目前,共享网采用用户名、密码的认证方式。由于该平台接入大量气象数据,如果密码泄露,极易引发数据安全问题。

3.2 用户属性需求

在用户属性管理方面,共享网需同步气象部门内部用户信息和外部用户信息。内部用户信息由气象部门的 OA 系统维护,并定期推送至统一身份认证平台,确保数据的一致性和安全性。对于外部用户,则通过统一认证自助服务页面进行信息的维护和管理。

统一身份认证系统的核心是“用户信息”,它所管理的用户属性全部为用户基础属性,包括用户数据、用户类型和组织机构数据等,而业务属性则由业务系统自行维护。

共享网与统一身份认证系统进行用户信息同步对接时,共享网存储的用户属性包括用户名、用户 OAID、用户所属机构编码路径和用户机构名称路径。当用户在统一身份认证系统中完成认证后,返回共享网的用户属性包括用户名、用户 OAID、用户修改时间和用户类型等信息。

3.3 认证对接

为了提升共享网的认证安全性和用户体验,采用 OAuth2.0 授权码模式与统一身份认证系统进行对接,具体步骤如下。

(1)用户通过浏览器访问共享网,系统调用授权认证接口 authorize,引导用户至统一身份认证服务器进行认证。

(2)用户在统一身份认证服务器输入凭据(用户名、密码)进行登录。

(3)成功认证后,统一身份认证服务器生成临时凭证 code,并重定向用户回到共享网。

(4)共享网使用该临时凭证 code 以及预设的 client_id 和 client_secret,向统一身份认证服务器请求 access_token。

(5)获得 access_token 后,共享网通过该令牌获取用户信息,完成单点登录过程,用户只需要认证一次,即可访问所有已授权系统。

此外,共享网采用 CA 证书认证作为增强安全措施,用于验证用户或客户端的身份。客户端和统一身份认证系统之间的通信通过 SSL/TLS 加密,客户端使用 CA 证书来建立安全连接。使用 CA 证书认证进一步增强了 OAuth2.0 授权码模式的安全性,特别是在处理敏感数据或需要高安全级别的操作时。

4 结语

统一身份认证系统在陕西气象网络防护中的应用实现了全省范围内气象用户的统一用户管理、统一认证管理、统一授权管理、统一审计管理,并支持第三方认证方式的扩展,解决了以往用户认证上的不便、系统管理上的复杂、资源上的浪费以及安全上的隐患,在气象信息化系统建设中发挥了重要作用。

参考文献:

[1] 周风. 单点登录技术在气象行业的应用[J]. 信息安全与技术,2013,4(5):105-108.

[2] 周虹霞. 国家博物馆统一身份认证系统的研究与实现[J]. 电子技术与软件工程,2021(3):161-162.

[3] 郭俊. 高校统一身份认证系统设计与实现[J]. 中国新通信,2022,24(2):48-50.

[4] 夏演. 基于 WebVPN 和统一身份认证的融合门户研究与实现[J]. 常熟理工学院学报,2022,36(2):71-76.

[5] 常潘,沈富可. 基于 LDAP 的校园网统一身份认证的实现[J]. 计算机工程,2007(5):281-282+285.

[6] 刘鹏飞,宫志强,韩佳乐. 基于 SSL VPN 的智慧校园统一身份认证平台建设[J]. 网络安全技术与应用,2023(6):91-93.

[7] 朱博昌. 基于 OAuth2.0 协议的授权登录国内应用现状研究[J]. 现代信息科技,2019,3(20):151-154.

[8] 时子庆,刘金兰,谭晓华. 基于 OAuth2.0 的认证授权技术[J]. 计算机系统应用,2012,21(3):260-264.

[9] 高保忠,杜首燕,李信治,等. 基于 OAuth2.0 协议的智慧校园认证系统研究[J]. 中国科学技术大学学报,2019,49(7):564-571.

[10] 吴添君. 为 CAS 统一认证服务集成 OAuth2.0 安全认证协议[J]. 网络安全和信息化,2021,60(4):125-128.