智慧校园下“企业微信+CAS”的统一身份认证方案设计

张刚刚

（首都师范大学 数字校园建设中心，北京 100048）

摘　要：在智慧校园建设不断推进的背景下，云计算、物联网、大数据等新兴技术已深入到学校管理、教学的方方面面。统一身份认证系统在智慧校园总体框架中位于平台支撑层，在智慧校园体系中提供身份认证、应用授权、角色管理及单点登录等功能。统一身份认证系统的登录方式需要很好地平衡易用性与安全性，因此提出“企业微信+CAS”的统一身份认证系统改进方案，将企业微信的OAuth身份认证功能与CAS认证协议进行有效结合，统一了智慧校园中各系统身份认证入口，在简化登录操作的同时，提高了用户身份认证时的安全性。实践结果表明，应用改进方案后可逐渐取代账号密码的认证方式（占比80%以上），对于其他高校的智慧校园建设可提供一定参考借鉴。

关键词：智慧校园；企业微信；统一身份；OAuth2；CAS；单点登录；无感知登录

DOI：10.11907/rjdk.212054　　开放科学（资源服务）标识码（OSID）：

中图分类号：G434　　**文献标识码**：A　　**文章编号**：1672-7800（2022）001-0034-06

Unified Identity Authentication Scheme Design of “WeCom + CAS” in Smart Campus

ZHANG Gang-gang

（*Digital Campus*, *Capital Normal University*, *Beijing* 100048, *China*）

Abstract: In the context of deepening the construction of smart campus, cloud computing, Internet of things, big data and other emerging technologies are constantly applied to school management and teaching. The unified identity authentication system is located in the platform support layer in the overall framework of smart campus, which provides identity authentication, application authorization, role management and other functions for the smart campus system. The login mode of unified identity authentication system needs to balance ease of use and security. This paper proposes an improved scheme of “WeCom +” unified identity authentication system, which effectively combines the OAuth identity authentication ability in WeCom platform with CAS protocol, unifies the identity authentication entrance of each system in smart campus, simplifies the login operation, and improves the security of user authorized login. After the application of the improved scheme in the author's company, it gradually replaced the authentication method of account password (accounting for more than 80%). Practice shows that the unified identity authentication scheme of “WeCom +” has a high promotion value for similar universities that use WeCom as the smart campus mobile portal.

Key Words: smart campus; WeCom; unified identity; OAuth2; CAS; single sign on; senseless login

0　引言

在“互联网+”概念的背景下，为进一步提升高校治理体系的现代化水平，各高校都在积极推进智慧校园建设。通过建设满足各种应用场景的业务系统，以提升管理、教学的效率与便捷性。在诸多业务系统建成后，以往的线下业务转为在线办理后产生了大量业务数据。业务系统建设早期大多以独立的账号密码作为系统登录方式，用户在使用不同系统时可能设置不同的登录密码，因此需要记住大量的用户名和登录密码，而且独立的系统认证入口很容易成为整个网络环境的安全短板。因此，在智慧校园总体

收稿日期：2021-08-18

基金项目：农产品质量安全追溯技术及应用国家工程实验室开放课题（AQT-2020-YB8）

作者简介：张刚刚（1989-），男，首都师范大学数字校园建设中心工程师，研究方向为教育信息化、智能信息系统。

框架中,身份认证成为支撑平台层的重要组成部分,为上层应用层提供统一的认证入口。在各业务系统独立认证用户身份的情况下,会因人员在职状态更新不及时、部门信息更新不准确及人员角色授权不统一等数据一致性问题严重影响业务系统对工作效率的提升效果。为改善这一问题,王群等[1]提出基于LDAP的实验室统一身份认证方案,以解决实验室中多个系统的身份认证问题;谷宁静[2]提出基于系统原有账号的跨域SSO单点登录系统设计方案,从而实现各业务系统进行统一身份认证、分层灵活授权管理的工作机制。这些研究者从多个业务系统共享身份认证的角度提出统一认证解决方案,一定程度上解决了身份共享、多系统单点登录问题,但未对统一身份认证的方便性与安全性作进一步研究。

本文在智慧校园总体框架下,将企业微信的身份认证功能与统一身份认证相关技术相结合,提出管理统一、方便易用、安全可靠的统一身份认证中心,从而为高校内各业务系统的身份认证提供技术支撑。用户可在企业微信客户端“无感知”地完成身份认证,改善了传统统一身份认证登录的体验,提高了智慧校园中业务系统的身份认证效率及安全防护水平。

1　相关技术

1.1　统一身份认证

在高校信息化建设早期,各应用系统身份认证普遍采用独立维护账号密码的方式。随着学校业务系统的不断增多,极端情况下用户在访问每个业务系统时都需要输入不同账号和密码。为降低记忆账号、密码的难度,用户通常会设置非常容易破解的简单密码,从而导致信息泄露的安全隐患。在智慧校园框架的平台支撑层,统一身份作为最重要的支撑设施,为整个智慧校园的应用层提供了统一的身份认证保障。在典型的身份认证过程中,业务系统应当完成包括消息完整性、发送方与接收方的不可否认性等业务逻辑。为保证所有业务系统在身份认证过程中业务逻辑的一致性与完整性,通过统一的身份认证入口进行系统登录成为智慧校园框架下的必然选择。

如图1所示,统一身份认证中的角色可分为身份提供者(Identity Provider,IdP)和服务提供者(Service Provider,SP)两种。IdP存储用户的身份信息与凭证信息,为SP提供身份验证、会话保持等技术支持,SP依赖IdP提供的身份信息并结合SP中的身份关联配置为有效用户提供授权服务。用户在IdP完成身份认证后,访问SP提供的授权资源服务。

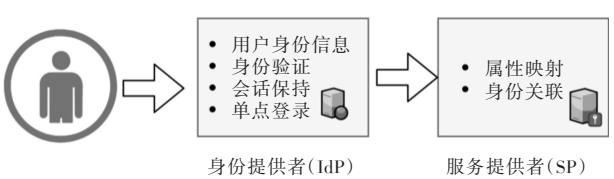

Fig. 1　Unified identity authentication role

图1　统一身份认证角色

如图2所示,在实现方式上,身份认证主要分为3种模型,分别是独立认证模型(Isolated Model,IM)、中心认证模型(Centralized Model,CM)与联合认证模型(Federated Model,FM)[3]。本文简要阐述这3种认证模型,并提出适用于高校内部进行身份认证的模型。

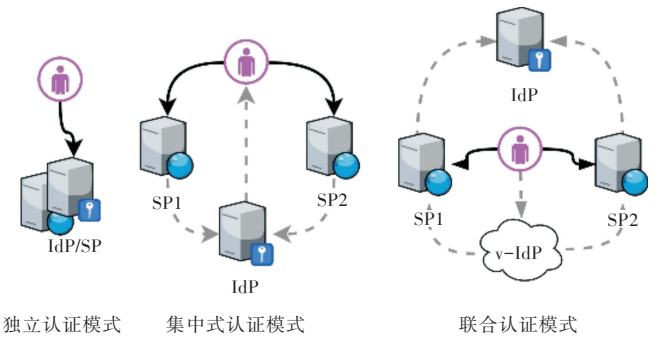

Fig. 2　Unified identity authentication model

图2　统一身份认证模型

(1)独立认证模型(IM)。该模型是高校信息化发展初期应用的模型,即身份认证模块完全耦合于业务系统中,用户使用不同系统时输入不同登录凭证完成身份认证。这种模型虽然简单,但在便利性与安全性方面存在诸多问题[4]。

(2)集中式认证模型(CM)。该模型包含中心化的认证服务,为其他业务系统提供统一的身份认证服务,同时为同一身份域内的各个业务系统提供单点登录(SSO)服务。该模型解决了独立认证模型中身份一致性差及不同业务系统重复登录的问题。

(3)联合认证模型(FM)。该模型在集中式认证模型基础上给出了跨系统、跨身份域的认证方案。用户在访问身份域A中的SP1服务时,SP1可根据用户所在组织身份域B中IdP提供的身份信息完成资源的访问授权。国内的中国教育科研网统一认证与资源共享基础设施(CARSI)就是联合认证模型的一个典型应用[5]。

智慧校园中的业务系统主要在校园网这一身份域中,若相同身份域内的业务系统使用相同账号、密码进行身份认证,可提高用户使用系统的效率及便利性。同时,为提高账号的安全性,不同业务系统在进行身份认证时,均应满足相同的安全约束。因此,在智慧校园框架下,采用集中式认证模型(CM)为各业务系统提供统一的身份管理、身份鉴权及安全策略,既解决了用户在使用多系统时记忆不同账号、密码的问题,又从业务系统的登录入口统一了身份认证安全级别。

1.2　单点登录

单点登录(Single Sign On,SSO)是指用户通过统一身份认证后,在访问同一身份域的不同业务系统时无需进行重复的身份认证过程。用户将已获得的票据提交给统一身份认证即可完成身份验证,该过程通常由统一身份认证系统自动完成。目前应用较广泛的单点登录技术方案有Cookie、Shibboleth、CAS、RADIUS及OAuth等,本文简要阐

述适用于高校的单点登录方案CAS。

CAS(Central Authentication Service)是由耶鲁大学发起,之后由多所大学共同开发完善的。CAS主要为Web应用系统提供单点登录功能,采用集中式认证模型提供身份认证服务[6]。其在交互过程中使用https协议,通信过程具有很高的安全性。该协议使用了两种票据:TGT(Ticket Granting Ticket,票据授予票据),对用户的单次登录会话有效;ST(Service Ticket,服务票据),仅对用户本次访问的目标业务系统有效。CAS方案发源于高校,之后又由多所高校共同改进,能够更好地贴合高校应用场景。CAS的安全性与扩展性可满足智慧校园架构对于身份认证系统及认证模型的要求,本文将CAS作为统一身份认证的单点登录方案。

1.3 企业微信

企业微信是腾讯公司在2015年推出的企业级微信平台,具有与微信一致的使用体验,可为用户提供丰富的API(Application Program Interface)以及全面、可靠的安全保障[7-9]。基于企业微信生态构建《智慧校园总体框架 GB/T 36342-2018》标准中的应用平台层,可为智慧校园上层应用提供通讯录、消息会话及身份识别等基础功能。目前,国内已有较多高校结合自身实际情况,基于企业微信构建了管理服务与智慧教学相关应用[10-13]。企业微信在身份认证体系构建方面提供了以下基础功能接口[14]:

(1)通讯录管理接口。提供用户信息同步、组织架构同步等功能,基于该接口将数据中心中的教职工、学生、访客等信息同步至企业微信通讯录,从而构建实名制的通讯录。师生的学号、工号与企业微信通讯录的账号一致,用户登录企业微信即可使用企业微信的身份信息进行身份识别。

(2)身份验证接口。企业微信通过OAuth协议提供了网页授权登录与企业微信APP扫码登录两种身份验证方式。第三方应用可通过企业微信的身份验证接口获取当前登录企业微信的用户信息,从而免去了用户输入账号、密码的环节。企业微信采用OAuth授权码方式提供身份验证服务。企业微信身份验证流程如图3所示,具体流程为:①用户点击开发者构造的OAuth链接;②企业微信客户端从后台获取携带授权码(CODE)的链接;③企业微信后台检查用户请求的参数合法性;④企业微信后台返回携带有授权码的链接;⑤企业微信客户端将携带有授权码的链接重定向至开发者后台;⑥开发者后台使用授权码通过企业微信的开放API获取当前用户账号等信息;⑦开发者后台根据用户账号建立会话;⑧企业微信客户端将授权的内容呈现给用户。

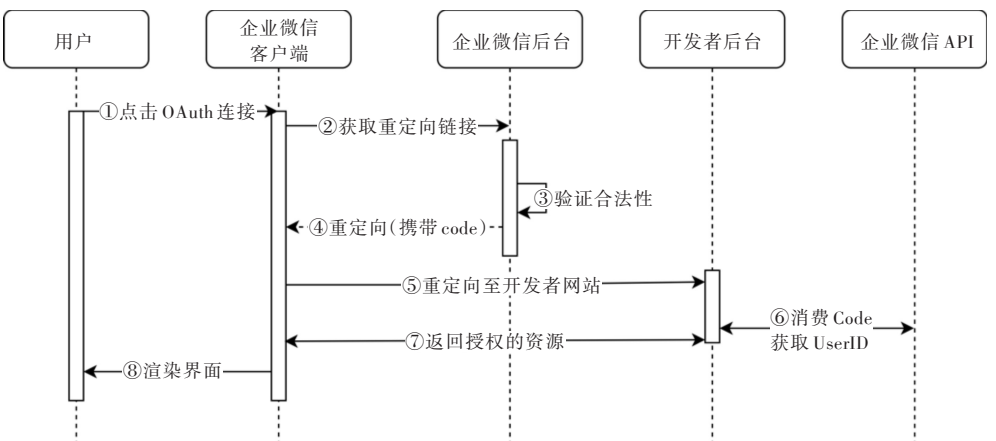

Fig. 3 Enterprise Wechat OAuth authentication process

图3 企业微信OAuth身份验证流程

通过以上流程,第三方应用即可通过企业微信的接口获取当前用户信息,从而完成系统登录。

2 方案设计

2.1 系统架构

基于“企业微信+CAS”的统一身份认证方案总体架构如图4所示,系统由运行环境层、数据存储层、业务逻辑层及表示层组成。

(1)运行环境层。系统采用Docker的Kubernetes集群进行部署,通过Docker运行时环境降低了异构环境下系统部署的难度,通过集群化系统部署提高系统的稳定性。

(2)数据存储层。采用MySQL主从部署架构作为数据库,记录用户账号、接入系统白名单及操作日志等信息,该数据库是统一身份认证系统的数据基础。采用MySQL作为数据层,相较于LDAP具有扩展性强、数据结构灵活及功能迭代效率高等优势。

(3)业务逻辑层。通过扩展CAS协议,为用户提供身份管理、认证、授权及审计服务,为终端用户提供统一身份认证账号的激活、密码重置等功能。

(4)表示层。系统通过表示层提供身份认证服务,以及CAS认证接口、Restful接口与LDAP认证接口。

系统在业务逻辑层与表示层的全生命周期中设计了用户操作的详细审计日志,以保证用户在系统中的所有操作都有痕迹,提高身份认证过程的安全性及认证结果的不可抵赖性。

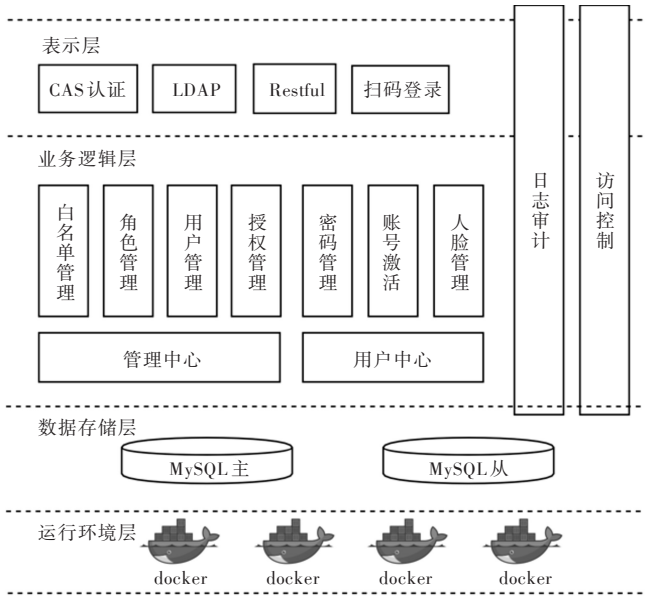

Fig. 4　System overall architecture

图 4　系统总体架构

2.2　“企业微信+CAS”统一身份认证方案设计

随着信息技术的不断发展,研究者不断尝试将新技术、新手段作为身份认证的双因子以提升登录的安全性。相关方法主要概括为3类:令牌(如手机短信验证码)、生物信息(如人脸、虹膜、体态等)、智能硬件(如U盾、校园卡等)[15]。企业微信APP作为一款具有极高安全级别的移动应用,在用户完成登录后能够长时间保持登录状态,且用户一般不会将具有高度私人属性的手机出借给他人。因此,可将企业微信作为身份认证的一种方式,用户可方便地通过企业微信扫码或企业微信内置浏览器完成身份认证。同时,借助企业微信很好的安全防护基础,在提升便捷性的同时,不会降低安全性。用户在非可信环境中通过企业微信扫码登录,能够有效降低用户通过键盘输入账号、密码导致密码泄露的风险。

“企业微信+CAS”的统一身份认证方案思路为:用户首次访问业务系统时,请求会被重定向至CAS服务器,CAS服务器通过判断用户当前访问的客户端User-Agent头信息来构造不同的企业微信登录链接。如图5所示,具体流程描述为:①用户首次访问业务系统A;②业务系统A将用户请求重定向至CAS服务器进行身份验证;③CAS服务器检查用户请求的Agent头部信息,如果User-Agent中包含wxwork,则构造企业微信OAuth2登录链接,否则构造企业微信扫码登录链接;④将用户请求重定向至构造好的链接;⑤用户通过企业微信APP完成扫码登录;⑥企业微信将Code返回CAS服务器,并向用户的企业微信推送一条账号登录提醒;⑦CAS通过Code从企业微信服务器获取当前用户身份信息;⑧CAS服务器针对业务系统A签发有效的TGT和ST;⑨CAS服务器将ST信息返回给用户;⑩用户携带ST信息访问业务系统A;⑪业务系统A通过CAS服务器验证ST的有效性;⑫业务系统授权用户完成系统登录,并返回会话票据;⑬用户后续使用业务系统返回的会话票据完成系统操作。

通过以上流程,用户通过企业微信的身份认证接口授权CAS获取其账号后完成系统登录。企业微信与CAS服务之间使用OAuth方式完成身份验证,业务系统通过CAS返回的ST完成身份验证。特别地,在步骤④中,用户使用企业微信客户端的内置浏览器进行身份验证时,系统会构造OAuth授权链接,免去了扫码操作,从而“无感知”地完成身份验证。当用户访问相同身份域中的业务系统B时,由于用户已携带了用于标识用户身份的TGC票据,CAS服务会直接签发用于业务系统B的ST票据,业务系统B直接通过ST票据验证用户的有效性,从而实现单点登录。

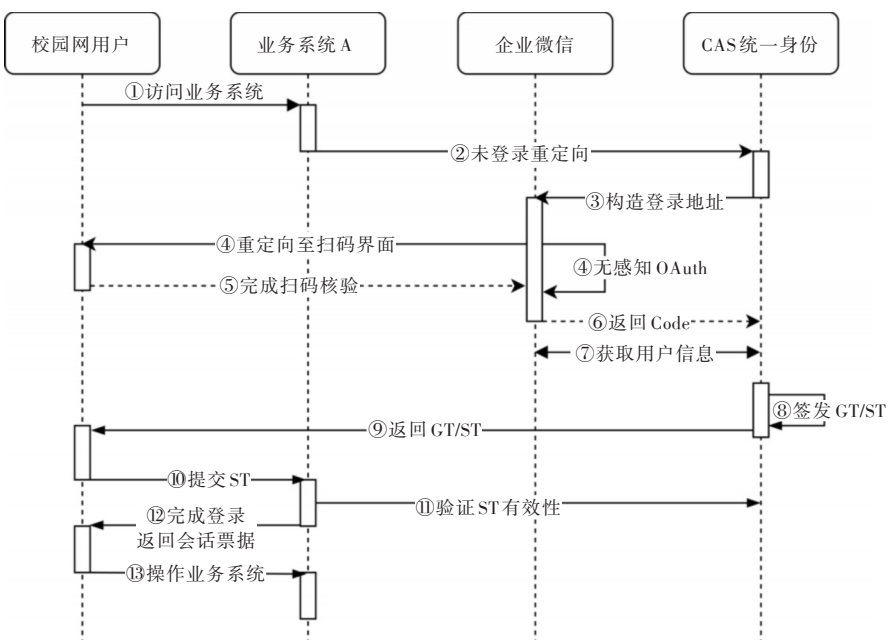

Fig. 5　Enterprise Wechat + CAS login process

图 5　企业微信+CAS登录流程

3 方案实施与分析

3.1 方案部署实施环境

方案部署环境配置信息如表2所示。

Table 2 Scheme deployment environment configuration information

表2 方案部署环境配置信息

用途	配置参数	数量
MySQL数据库(主/从)	磁盘300GB,主频2.10GHz,内存64G	2台
CAS服务器	磁盘100GB,主频2.80GHz,内存16G	2台
缓存服务器	磁盘100GB,CPU:2.80GHz,内存32G	1台
网络环境	1Gbps	-

本文通过设计两个实验验证方案的并发处理能力与系统性能,每个实验均执行10轮并取实验结果的平均值。实验采用账号、密码的方式进行认证。

(1)多客户端的并发实验。通过运行1~200个客户端对系统进行压力测试以验证系统的并发能力,每次实验时均并发运行客户端请求,每个客户端均独立对系统发送身份验证请求。

(2)单独客户端的性能实验。通过实验分析用户在短时间内频繁访问相同身份域内多个业务系统时的响应速度等情况。

3.2 应用效果

笔者所在单位将企业微信作为移动门户,在企业微信中置入了全员组织架构信息及用户基本身份信息,并分别与学籍信息库及人事系统库进行数据联动,企业微信日活人数覆盖在校总人数的98%以上。采用本文设计方案改造统一身份认证系统,并接入智慧校园中的全部业务系统。与之前LDAP统一认证登录方式相比,通过本文方案为Web应用提供身份认证与单点登录功能,通过Restful及LDAP接口层为学校VPN及网络登录提供身份认证功能,补充了用户登录系统的方式,提高了智慧校园环境下各业务系统登录入口的安全性。

采用更加标准、通用的CAS协议与企业微信开放接口,可减少第三方厂商对接的难度,提高对接效率。通过认证中心中的弱密码检测功能,在用户输入密码时检测密码强度,并通过企业微信的消息接口通知用户修改密码为符合要求的强密码。在笔者单位,用户访问统一身份认证系统时需经过入侵检测、防火墙、WAF防火墙等安全设备,并使用HTTPS协议加密交互全过程,结合企业微信完备的安全防护能力,全方位提升了业务系统登录入口的安全性。

图6的分析结果显示,“企业微信+CAS”统一身份认证系统方案上线一个月后,用户总体登录习惯由账号密码登录方式转变为企业微信登录方式(本方案占比80%以上)。其中,学生账号与总体习惯趋势一致,而教职工账号很大程度上保留了账号密码的登录方式(本方案占比20%左右)。通过对访问日志的进一步分析及用户调研后发现,教职工通常使用浏览器的记住密码功能以减少频繁输入账号、密码的频率,学生群体更容易接受使用企业微信授权登录方式完成身份认证。基于良好的用户反馈,一方面可加强企业微信登录方式在保障用户隐私、提高账号安全性优势方面的宣传,另一方面需进一步挖掘企业微信的用户身份鉴权相关接口,为用户提供更好的登录体验,以进一步提高用户对企业微信身份认证功能的使用率。

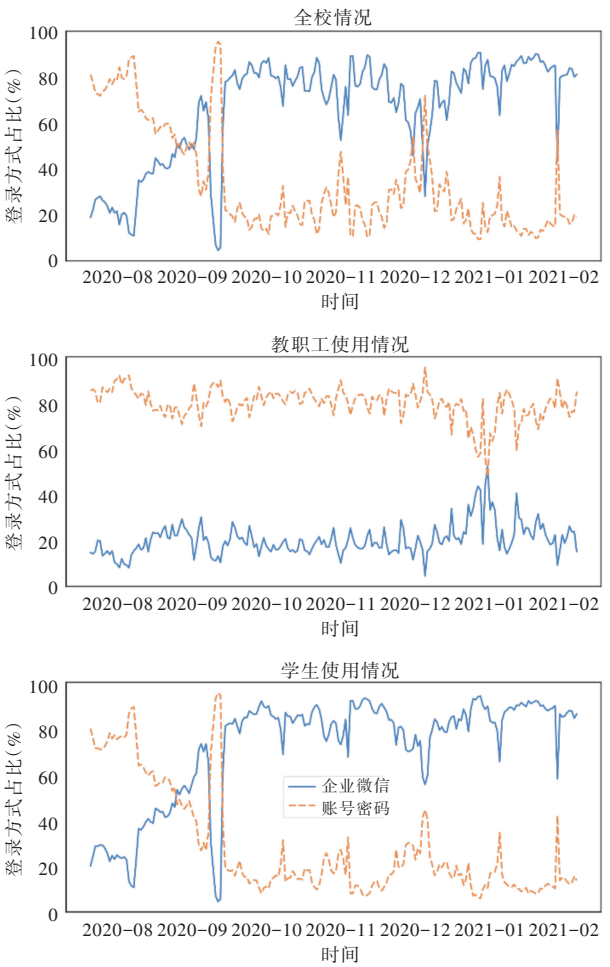

Fig. 6 Proportion of different login methods

图6 不同登录方式占比情况

3.3 系统安全性与响应时间分析

“企业微信+CAS”方案在安全性与便捷性之间取得了一定程度上的平衡,基于企业微信完善的安全防护体系,该方案具备了较高安全水平。笔者单位在实施本文方案后,通过弱密码检测功能识别出10 000余人使用了常见的弱口令,并锁定了5 000余个长期闲置的账号,以提前预防账号风险。利用企业微信结合CAS的账号安全机制,智慧校园下各个业务系统可具有统一的安全入口,使建设方能够更专注于自身业务的打磨,提升智慧校园建设的整体效能。通过分析用户登录日志后得出,用户在扫码完成或输入正确的账号、口令后到跳转到业务系统完成身份认证的响应时间在800ms以内(平均响应时间为498ms),具有较理想的响应效率。

4　结语

本文在智慧校园总体框架下,探讨了智慧校园中统一身份认证与单点登录相关概念及模型,提出“企业微信+CAS”的统一身份认证系统设计方案。通过融合应用广泛的CAS协议及具有可信身份环境的企业微信,实现校园内各业务系统的统一身份认证与单点登录功能,并通过企业微信扫码登录和“无感知”登录方式免去了用户记忆密码的烦恼,提升了校园网络环境的安全性及信息化水平。今后将进一步深入研究智慧校园框架下统一身份认证系统的优化运用。

参考文献:

[1] WANG Q, LI F J. A laboratory unified identity authentication scheme based on single sign on[J]. Experimental Technology and Management, 2020, 37(5): 219-223.
王群,李馥娟. 一种基于单点登录的实验室统一身份认证方案[J]. 实验技术与管理, 2020, 37(5): 219-223.

[2] GU N J. Cross domain SSO design and implementation of “all in one network” talent settlement system[J]. Computer Applications and Software, 2020, 37(5): 25-29.
谷宁静. “一网通办”人才落户系统的跨域SSO设计与实现[J]. 计算机应用与软件, 2020, 37(5): 25-29.

[3] GALLAGHER E A. Choosing the right password manager[J]. Serials Review, 2019, 45(1-2): 84-87.

[4] CARRETERO J, IZQUIERDO-MORENO G, VASILE-CABEZAS M, et al. Federated identity architecture of the European eID system[J]. IEEE Access, 2018, 6: 75302-75326.

[5] GUO H, WANG G C, LUO P. Design of a cookie based cross domain single sign on scheme[J]. Computer Engineering and Science, 2017, 39(7): 1295-1299.
郭豪, 王国才, 罗聘. 一种基于Cookie的跨域单点登录方案设计[J]. 计算机工程与科学, 2017, 39(7): 1295-1299.

[6] O'GORMAN L. Comparing passwords, tokens, and biometrics for user authentication[J]. Proceedings of the IEEE, 2003, 91(12): 2021-2040.

[7] Shibboleth Consortium.Shaping the future of shibboleth software [EB/OL]. https://www.shibboleth.net/.

[8] WANG W Q, CHAI L N, CHEN P, et al. Cross domain authentication integration model of shibboleth and CALIS unified authentication cloud service center [J]. Journal of the National Library, 2015, 24(4): 45-50.
王文清, 柴丽娜, 陈萍, 等. Shibboleth与CALIS统一认证云服务中心的跨域认证集成模型[J]. 国家图书馆学刊, 2015, 24(4): 45-50.

[9] LIU F, WANG Z, CAO H P, et al. Portal single sign on scheme based on CAS[J]. Computer System Application, 2011, 20(6): 77-80, 102.
刘峰, 王峥, 曹华平, 等. 基于CAS的门户单点登录方案[J]. 计算机系统应用, 2011, 20(6): 77-80, 102.

[10] HE J R, LIU M C, WANG H. Design and implementation of Shendong identity authentication and management platform based on CAS [J]. Scientific and Technological Innovation and Application, 2020(31): 68-70.
贺建荣, 刘明昌, 王欢. 基于CAS神东身份认证与管理平台的设计与实现[J]. 科技创新与应用, 2020(31): 68-70.

[11] Tencent.WeWork[EB/OL]. https://work.weixin.qq.com/.
Tencent. 企业微信介绍[EB/OL]. https://work.weixin.qq.com/.

[12] Tencent.WeWork Security[EB/OL]. https://work.weixin.qq.com/nl/index/security.
Tencent. 企业微信安全[EB/OL]. https://work.weixin.qq.com/nl/index/security.

[13] ZHANG M R, XU J W. Research on the construction of campus informatization based on enterprise Wechat[J]. Digital Technology and Application, 2020, 38 (12): 123-125.
张美茹, 徐建伟. 基于企业微信的校园信息化的构建探究[J]. 数字技术与应用, 2020, 38(12): 123-125.

[14] XIE P K, GUO W X, XU T, et al. Information demand collection and management platform based on enterprise Wechat[J]. Computer System Application, 2020, 29(11): 92-96.
解攀科, 郭伟秀, 许婷, 等. 基于企业微信的信息化需求采集管理平台[J]. 计算机系统应用, 2020, 29(11): 92-96.

[15] WU N, YU Y B, WANG J J, et al. Self built teaching platform for “enterprise Wechat” teachers based on social media —taking the course of computational materials as an example[J]. China Education Informatization, 2019(24): 86-89.
吴南, 于宜博, 王家佳, 等. 基于社会媒体“企业微信”教师自建教学平台——以《计算材料学》课程为例[J]. 中国教育信息化, 2019(24): 86-89.

(责任编辑:黄　健)