



“沃互联”统一认证技术研究

刘 镝¹, 张云勇¹, 张 尼¹, 张曼君²

(1. 中国联合网络通信有限公司研究院 北京 100032;

2. 中国联合网络通信有限公司技术部 北京 100033)

摘 要:近年来,网络用户信息泄露事件愈演愈烈,为保障网络用户个人数据安全,研究了网络场景下用户电子账户所面临的安全风险与威胁,分析了网络用户账号相关安全需求,提出了一种网络强身份认证方式——“沃互联”统一认证方案,该方案是以手机号码为用户唯一身份标识,为网络业务提供商提供统一的安全认证能力,使用户获得安全、便捷的用户认证和授权体验。

关键词:沃互联;身份认证;卡认证应用;信息安全

doi: 10.11959/j.issn.1000-0801.2015156

Research on “Wo Connect” Uniform Authentication Technology

Liu Di¹, Zhang Yunyong¹, Zhang Ni¹, Zhang Manjun²

(1. Research Institute of China United Network Communications Group Co., Ltd., Beijing 100032, China;

2. Technology Department, China United Network Communications Group Co., Ltd., Beijing 100033, China)

Abstract: Recently, many web user data leak incidents outbreak. In order to protect web user personal information, an analysis was made on security threats for web user, emphasizing security requirements. And a web-based strong authentication scheme, “Wo Connect” uniform authentication solution, was proposed. Based on user mobile phone number identifier, this solution provides the third party website uniform security authentication ability, enabling user to enjoy security and convenience authentication and authorization user experience.

Key words: Wo Connect, identity authentication, card authentication application, information security

1 引言

随着信息通信技术的不断演进,云计算、大数据等新技术的引入,人们可以利用 PC、移动终端开展网上冲浪、资源访问、电子商务、移动支付、社交网络等各种网络业务。虽然各种网络业务方便了用户,但网络用户隐私安全形势愈加严峻。近年来,一系列网络信息泄露事件层出不穷。

国际方面,全球用户隐私安全形势堪忧。2013 年,爆

发了“棱镜门”事件,已在全球范围内引起轩然大波,全球隐私信息遭到美国监控。事件背后的“元凶”美国国家安全局和联邦调查局,发起了代号为“棱镜”的秘密项目,搜集情报、监控互联网用户、窃听互联网用户隐私信息,并对别国实施网络攻击等恶意行为。2014 年,爆发了苹果 iCloud “艳照门”事件,黑客暴力破解 iCloud 用户设置的弱口令,入侵账户,100 余位好莱坞女星私密照片被公布于互联网。

收稿日期:2015-01-28;修回日期:2015-06-12

论文引用格式:刘镝,张云勇,张尼等.“沃互联”统一认证技术研究. 电信科学,2015156

Liu D, Zhang Y Y, Zhang N, et al. Research on “Wo Connect” uniform authentication technology. Telecommunications Science, 2015156



国内方面,我国用户隐私泄露事件也频有发生。2011年12月,爆发了“泄密门”事件,多家大型互联网网站及论坛用户数据库遭到攻击,黑客采用“拖库”、“撞库”等技术手段窃取用户隐私,造成将近1亿户互联网用户数据泄露。2013年12月,我国电商领域爆发用户信息泄露事件,泄露总量达2500万条。2014年12月,12306网站大量用户信息遭泄露,已公开传播的数据库涉及用户数据超过13万条,泄露信息包括用户账号、明文密码、身份证、邮箱等。以上一系列安全事件的爆发,已引起了网民对个人隐私安全的重点关注。

针对个人隐私保护问题,各国政府、国际组织均引起重视,采取相应措施。国际方面,欧美国家相继出台用户信息保护法案,如美国的《隐私法》、《隐私保护法》,德国的《联邦数据保护法》等。著名国际组织GSMA于2013年底提出GSMA Vision 2020个人数据项目,目的是号召全球运营商、厂商联合起来,拟构建一种基于mobile ID的新型统一认证方式,取代传统用户、密码网站登录、授权认证方式,以便更好地保护用户个人数据。国内方面,国家对个人数据安全高度重视。2012年12月,我国全国人大常委会颁布了“关于加强网络信息保护的決定”,以保护我国网络用户信息安全,保障公民合法权益。2013年8月,工业和信息化部发布了第24号令“电信和互联网用户个人信息保护规定”,旨在保护电信和互联网用户的合法权益,维护网络信息安全。2014年2月27日,网络安全与信息化领导小组成立,小组组长国家主席习近平主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话,强调网络安全是国家发展的重大战略问题。总之,国内外政府、业界均在致力于个人数据保护的研究,以寻求更加完备、安全的解决方案。

2 用户个人数据保护需求

随着国内外各种个人数据泄露事件的频繁爆发,业界普遍认识到传统的用户上网登录模式存在弊端。

(1) 数据库用户信息泄露问题

用户为了登录各种网站,首先要注册个人信息到第三方网站,而不少网站的安全防护工作不到位,一旦黑客发起“拖库”、“撞库”攻击,将造成大量用户信息泄露的严重后果。由于越来越多的个人数据泄露事件爆发,用户越来越不信任第三方网站,注册时不愿意将自己的真实信息录入。

(2) 弱口令问题

传统的输入用户名、密码的网站用户认证方式越来越不适应人们的日常需要,用户登录方式的便捷性与安全性

相互矛盾,相互制约。从用户便捷角度考虑,由于用户日常登录的各种网站繁多,为了方便记忆,往往为众多的网站赋予相同的账户与密码,即设定弱口令密码,一旦遭到黑客、恶意软件、间谍软件的攻击,用户账户、密码极易被窃取。从用户安全的角度考虑,用户可为不同网站设定不同的用户密码,这样会造成用户需要记忆大量不同的用户名、密码,极大地降低了用户体验。有些用户甚至会放弃访问那些需要用户注册的网站。

(3) 认证信息易被截取

传统的网络用户登录方式将认证信息与业务数据在同一信道传输,若传输过程中信道被境外势力监听,则大量认证信息将被窃取。

为维护国家安全和社会公共利益,保障用户个人数据安全,有必要研究新型、更加安全的网络强身份认证方式,使用户获得安全、便捷的用户体验,应具备以下安全能力:

- 用户无需设置多套账号和密码,使用移动终端实现强认证方式,解决弱口令问题;
- 第三方网站无需存储用户信息,改由运营商存储、管理用户身份数据,便于国家监管,减少网站信息泄露事件的发生;
- 用户与第三方网站之间只传输网站交互信息,认证数据在用户与运营商之间传输,实现认证信息与业务数据相分离。

3 “沃互联”统一认证方案

根据第2节提出的强认证安全需求,提出“沃互联”统一认证技术方案,将网络用户个人身份数据存放在比普通第三方网站更为可信的机构——运营商的基础设施中,并通过充分开放运营商业务层面的认证、鉴权能力,利用移动终端SIM卡绑定的个人移动ID(手机号),为第三方网站、大型企业,甚至银行、政府的用户登录、关键操作(支付)过程提供用户身份验证能力。

该方案具备两方面优势。

第一,对于用户而言,首先,更为可信,个人隐私、财务相关信息可以存放至更为安全的运营商基础设施中,用户与运营商直接交互完成第三方网站的认证、支付等关键操作。其次,更为便捷,用户借助运营商认证、鉴权能力完成第三方网站的认证流程,代替第三方网站传统的输入用户名、密码的认证方式。PC端场景下,仅需点击支持该业务的网站登录页面上的手机认证登录按键,然后根据弹出新

界面输入手机号码,即可借助用户移动终端自动弹出的 SIM-Applet 界面进行登录确认,完成第三方网站登录过程。移动终端场景下,用户仅需在浏览器中输入第三方 URL,然后即可以 SIM 卡绑定的第三方网站账号身份实现自动登录。再次,更为安全。在用户允许的情况下,运营商可以合理、合法地安全使用自身存储的大量个人用户数据,可以有效地防止用户数据被非可信的第三方滥用。

第二,对于第三方网站而言,可降低网站用户账户、认证系统设计的复杂性,减少投资成本。此外,在用户允许的情况下,可与运营商开展适当形式的合作,与运营商共同分享分析、挖掘好且经过脱敏处理的用户个人数据,经营智能营销、广告推送以及其他新业务。

3.1 总体架构

“沃互联”统一认证方案依托 SIM 卡应用认证、远程管理能力,为内容提供商(第三方网站)提供统一业务认证服务,使用户获得安全、快捷的用户体验。方案总体架构如图 1 所示。

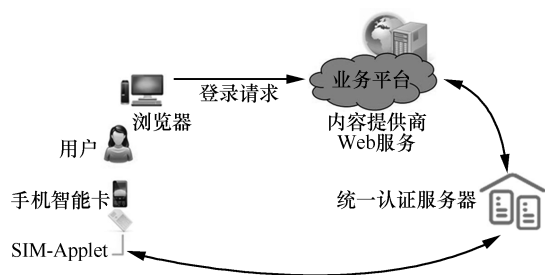


图 1 “沃互联”统一认证方案总体架构

该方案总体架构由用户终端 SIM 卡认证应用、认证管理 App、用户 PC(浏览器端)、业务平台(第三方网站)、统一认证服务器等组件构成。

- 卡认证应用(SIM-Applet):用户移动终端作为“沃互联”统一认证方案的核心认证工具,通过事前预装在用户终端 SIM 卡上的卡认证应用实现登录认证。
- 认证管理 App:具备两大功能,管理 SIM 卡认证应用;为卡认证应用与统一认证服务器提供数据通道,实现两者之间的认证交互。
- 用户 PC(浏览器端):当用户使用 PC 浏览某个第三方网站申请登录时,若用户采用统一认证方式登录,输入唯一身份标识手机号,将向统一认证服务器发起登录请求;当统一认证服务器反馈认证结果至第三方网站时,网站页面将呈现认证结果,即登录成功或失败。
- 业务平台:用户需要访问各种第三方网站,例如各种门户、金融网站、社交网站等。
- 统一认证服务器:用来与用户、第三方网站进行认证交互,由运营商构建,与用户终端 SIM 卡上的卡认证应用共同完成认证功能。

其中,认证管理 App、SIM 卡认证应用与运营商统一认证服务器为统一认证方案核心组件,帮助用户完成强认证服务,可取代传统用户网站登录方式。

3.2 技术模块

“沃互联”统一认证方案的核心组件具体技术模块如图 2 所示。

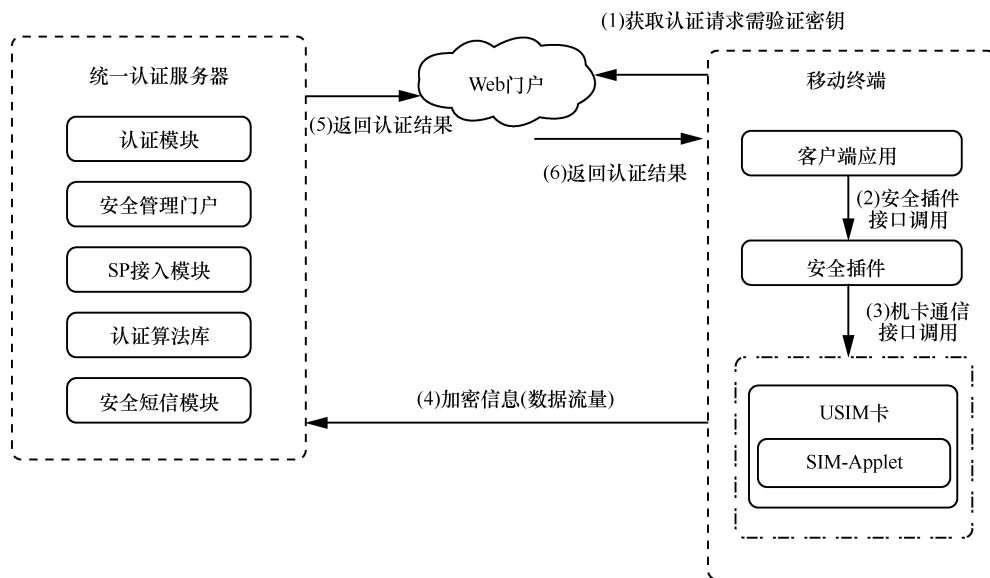


图 2 “沃互联”统一认证方案模块



(1) 统一认证服务器

认证用户身份的签名数据,并向第三方网站提供认证数据结果、组装数据报文和安全处理方案,包括以下模块。

- 业务接入模块:实现与第三方网站及内容提供商交互用户认证数据。
- 用户接入模块:使用短信或数据流量等传输方式与用户终端、卡认证应用进行数据交互。
- 认证算法库:管理各种不同安全等级认证算法,并根据业务需求,提供相应安全等级的认证算法。
- 用户身份认证模块:根据算法库提供的认证算法,与卡认证应用协同认证用户身份相关信息。
- 安全管理门户:系统管理员可通过访问该安全管理门户,管理、监控、维护统一认证服务器。

(2) SIM 卡认证应用

负责实现终端用户身份验证,具备以下功能。

- 卡与终端的交互指令。
- PIN 码管理、存储。
- 认证时负责向用户提供交互界面。
- 负责卡信息与统一认证服务器之间的数据交互。

(3) 手机 App

负责管理 SIM 卡认证应用,提供卡认证应用与统一认证服务器之间的数据通道。

- 注册时负责向用户提供交互界面。
- 负责读取卡信息并完成与统一认证服务器之间的数据交互。
- 负责展示用户访问 SP 的记录。

3.3 业务流程

将“沃互联”统一认证方案业务流程分为两部分,即用户注册流程与用户认证流程。

当用户第一次使用该业务时,需要进行用户注册,注册流程如下。

第 1 步,用户 PC 端在统一认证业务门户网站注册并登录。用户可利用运营商客服网站用户名(手机号)、密码实现直接登录。

第 2 步,用户统一认证业务门户网站登录后,进行统一认证业务初始化设置,激活统一认证业务服务,并页面提示用户下载统一认证 App 客户端。可设计多种下载方式:

- 手机扫描页面二维码下载、安装 App 方式;
- 移动终端 Web 登录本地下载、安装 App 方式;
- 短信网关发送下载地址短信链接至手机,告知下载、安装方式。

第 3 步,统一认证业务门户与运营商 SIM 卡接入管理平台联动,远程向用户 SIM 卡无感知推送卡认证应用。

第 4 步,实现与运营商签约的第三方网站进行 ID 绑定。用户需登录至第三方网站,用户设置页面输入手机号进行绑定。输入手机号过程中,可设计各种验证方式:

- 发送验证码至 App,将验证码输入第三方网站页面验证处;
- 发送验证码短信至用户移动终端,将验证码输入第三方网站页面验证处;用户将验证码输入 ID 绑定页面后,第三方网站弹出提示,显示后台绑定成功。

当用户注册完毕后,登录已绑定的网站可以实现统一认证方式,认证流程如图 3 所示,具体介绍如下。

第 1 步,用户登录某第三方网站,进入主页。

第 2 步,用户点击网站主页上的“沃互联”统一认证键。

第 3 步,用户在提示框中输入手机号码,点击确认。

第 4 步,用户移动终端弹出登录确认窗口,用户点击确认(低安全级别)或输入密码(高安全级别)完成用户认证流程。

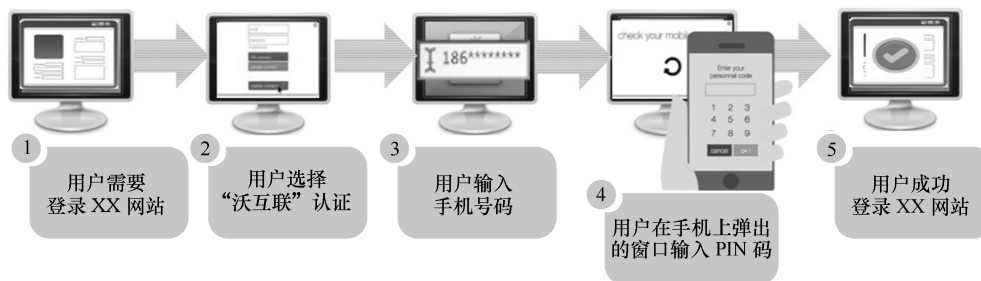


图 3 “沃互联”统一认证方案业务流程

第 5 步,待用户终端确认后,成功登录该网站。

3.4 与传统认证方案比较

将“沃互联”统一认证方案与其他几种常见认证登录方案进行比较,比较结果见表 1。

综上,“沃互联”统一认证方案,较其他传统认证方案可为用户提供更安全、便捷的用户体验,同时也便于网站、运营商集中管理身份账号体系。

4 方案部署关键问题

本节讨论“沃互联”统一认证方案部署关键问题及相关问题。

4.1 App+SIM-Applet 与 SIM-Applet 认证方式比较

由于“沃互联”统一认证方案可采用两种技术方式实现,即本文所采用的 App+SIM-Applet 认证方式与纯 SIM-Applet 认证方式。这两种方式之间的区别如下。

(1)卡认证应用初始化下载

- App+SIM-Applet 认证方式可实现通过 App 数据通道、3G、4G、Wi-Fi 通道下载卡认证应用至用户终端 SIM 卡内,通道稳定,下载快捷。
- SIM-Applet 认证方式需要通过短信网关发送数据短信远程推送卡认证应用至用户 SIM 卡内,由于数据短信存在短信分组丢失的情况,且一般卡认证应用需要 20~30 条数据短信,一旦某条短信发送失败,需要全部重新发送,下载成功率较 App+SIM-Applet 方案低。

(2)卡认证应用与统一认证服务器交互通道

- App+SIM-Applet 认证方式下,用户终端上的卡认证应用与统一认证服务器之间的交互是通过 App 与

统一认证服务器之间建立的数据通道实现的,例如 3G、4G、Wi-Fi 通道实现且建立通道连接相对稳定,响应速度快。

- SIM-Applet 认证方式下,卡认证应用与统一认证服务器之间的交互是通过短信网关与卡认证应用之间相互发送数据短信实现,由于短信通道存在短信数据分组丢失的可能性,可能会导致用户认证流程无法实现。

(3)两种方式终端、卡适配问题

- App+SIM-Applet 认证方式适用于 Andorid NFC 终端(其他 OS 终端暂不支持)以及支持 NFC 功能的 SIM 卡,因为 App 与卡的数据信息交互通过 OMA(Open Mobile API)完成。
- SIM-Applet 认证方式适用于 feature phone (功能手机)、3G/4G 终端,适用终端范围较广,对 SIM 卡要求为 128 KB 以上的 Java 卡。

4.2 实际运营负载考虑

当统一认证方案大规模推广后,运营商侧的统一认证服务器将面临各种不同第三方网站用户的登录压力。例如,具备 1 000 万甚至更多的活跃用户,面临每小时平均访问量可达到 40 万~50 万、访问峰值 100 万等状况。这就需要运营商考虑完备的资源性能部署方案,以满足实际运营压力需要。需要考虑的设备涉及业务服务器、数据库服务器、备份服务器、磁盘阵列、负载均衡器、交换机、防火墙等多种设备。可根据实际情况,持续进行扩容。

4.3 用户换卡或换号问题

用户换号时,统一认证服务器如何更新管理用户卡相

表 1 与传统认证方案的比较

认证方案	安全性	可信度	便捷性	管理
“沃互联”统一认证方案	安全级别高,可杜绝弱口令、“拖库”、“撞库”	可信度高,运营商验证用户真实身份,只有用户本人能通过身份验证	采用手机号作为唯一用户名,实现快捷登录	易管理,不同第三方网站共用运营商认证基础设施
二维码认证方案	存在扫描后,植入恶意软件、病毒的隐患	用户移动终端丢失后,他人(拾到手机的人)可实现仿冒身份盗登	扫码后,实现快捷登录	不同网站采用不同身份账号体系,不可实现统一管理
短信验证码认证方案	存在短信被恶意软件拦截的隐患	用户移动终端丢失后,他人(拾到手机的人)可实现仿冒身份盗登	存在收不到短信验证码的情况	不同网站采用不同身份账号体系,不可实现统一管理
用户名+密码认证方案	存在弱口令、“拖库”、“撞库”等隐患	可信度低,账号、密码易被破解	不同网站需要设置不同账号、密码,较繁琐	不同网站采用不同身份账号体系,不可实现统一管理



关信息,如 ICCID、MSISDN 等,需要进一步考虑,并设计用户换卡、换号具体业务流程方案。

4.4 账号绑定问题

如何进一步提高用户手机号与第三方网站现有 ID 账号绑定的问题,也需要进一步完善相关方案。用户可能需要利用统一认证方案访问众多第三方网站,如何实现便捷的新网站 ID 与手机号绑定问题,需要进一步深入研究。

5 结束语

本文提出一种网络强身份认证方式——“沃互联”统一认证方案,该方案是以手机号码为用户唯一身份标识,为网络业务提供商提供统一的安全认证能力,使用户获得安全、便捷用户认证、授权体验。为进一步推进方案的部署落地,后续可采用 App+SIM-Applet 与 SIM-Applet 认证方式并举的方案,迅速扩大用户群体,以便顺利开展与各种第三方网站的合作,实现运营商统一业务认证,确保广大网络用户隐私信息安全。

参考文献

- 1 CPAS06 Identity Gateway Functional Architecture V1.0. <https://infocentre2.gsma.com/gp/pr/V2020/PDATA/Core%20Product%20and%20Solution/Core%20Products%20and%20Solutions/CPAS06%20Identity%20Gateway%20Functional%20Architecture.docx>, 2015
- 2 CPAS08 SIM Applet Authentication Specification V1.0. <https://infocentre2.gsma.com/gp/pr/V2020/PDATA/Core%20Product%20and%20Solution/Core%20Products%20and%20Solutions/CPAS08%20SIM%20Applet%20Authentication%20Specification.docx>, 2015
- 3 卢煜,孔令山.移动互联网安全挑战与应对策略.通信世界, 2011(17): 38~39
Lu Y, Kong L S. Security challenge and countermeasure of mobile internet. Communications World Weekly, 2011(17): 38~39
- 4 胡启平,陈震.试析社交网络环境中个人隐私保护.信息网络安全, 2010(8): 43~44
Hu Q P, Chen Z. Analysis of personal privacy protection on social network environment. Netinfo Security, 2010(8): 43~44
- 5 景笑梅.统一身份认证平台技术开发与应用.信息安全与保密通信, 2010(6): 60~62
Jing X M. Development & application of unified identity

authentication platform. China Information Security, 2010 (6): 60~62

- 6 董昭.门户网站的统一认证与单点登录技术.电信工程技术与标准化, 2010(5): 59~64
Dong Z. Uniform authentication and single sign on of portal website. Telecom Engine Technics and Standization, 2010 (5): 59~64
- 7 容晓峰,苏瑞丹,崔树鹏等.基于 SIM 卡的双因素认证方案.计算机工程与应用, 2004(3): 147~149
Rong X F, Su R D, Cui S P, et al. A SIM-based dual-factor authenticated scheme. Computer Engineering and Applications, 2004(3): 147~149

[作者简介]



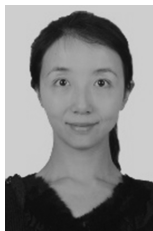
刘镒,男,博士后,中国联合网络通信有限公司研究院云计算实验室工程师,主要研究方向为认证安全、终端安全、云计算安全等。



张云勇,男,博士后,中国联合网络通信有限公司研究院副院长,中国通信学会、电子学会、计算机学会高级会员,主要研究方向为下一代开放网络、移动互联网及业务、云计算、智能终端等。



张尼,男,博士后,中国联合网络通信有限公司研究院云计算实验室高级工程师,主要从事移动互联网安全、云计算安全、信息安全等领域研发工作。



张曼君,女,博士后,现就职于中国联合网络通信有限公司技术部,主要研究方向为信息安全、网络安全等。