基于情景感知的低交互移动双因素认证系统

刘 冬[1,4],陈 晶[1,2],杜瑞颖[1,3],何 琨[1]
(1. 软件工程国家重点实验室,武汉大学计算机学院,湖北武汉 430072;2. 保密通信重点实验室,四川成都 610041;
3. 地球空间信息技术协同创新中心,湖北武汉 430079;4. 北方自动控制研究所,山西太原 030006)

摘 要: 针对传统双因素认证缺乏可用性的问题,本文提出了一种基于情景感知的低交互移动双因素认证系统.用户通过本系统登录网站时,除输入用户名和口令外,只需点击令牌程序的认证键即可完成认证,平均登录时间不超过5秒.同其它可用性加强的移动双因素认证系统相比,本系统能够抵抗同一环境下的攻击者,而且支持用户手机浏览器进行网站登录.最终安全分析和实验结果证实了本方法的有效性.

关键词: 移动双因素认证;WiFi指纹;设备指纹
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)05-1056-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.05.005

A Low Interaction Mobile Two-Factor Authentication System Based on Context Awareness

LIU Dong[1,4], CHEN Jing[1,2], DU Rui-ying[1,3], HE Kun[1]
(1. *State Key Laboratory of Software Engineering, School of Computer, Wuhan University, Wuhan, Hubei* 430072, *China*;
2. *Science and Technology on Communication Security Laboratory, Chengdu, Sichuan* 610041, *China*;
3. *Collaborative Innovation Center of Geospatial Technology, Wuhan, Hubei* 430072, *China*;
4. *North Automatic Control Technique Research Institute, Taiyuan, Shanxi* 030006, *China*)

Abstract: Aiming at the problem of usability for traditional two factor authentication (2FA), we propose a low interaction mobile 2FA system in this paper. In our system users only need to enter the usernames and passwords in the browser and press the confirm button on the mobile app for authentication. The average login time for users is no more than 5 seconds. Compared with the current usability enhanced 2FA systems, our system can resist attackers in the same environment and support users to login website with phone browsers. The experimental and analytical results shows the effectiveness of our system.

Key words: mobile two-factor authentication (2FA); WiFi fingerprint; device fingerprint

1 引言

用户名和口令是现有网站系统中普遍采用的身份认证方式,这种方式虽然简单、有效,但存在着很多安全风险.首先用户为了方便记忆口令会设置的很简单.这使得攻击者能够通过在线猜测攻击或离线字典攻击的方式得到用户的口令,进而冒充用户的身份窃取信息[1].其次,用户往往会在多个网站中采用相同的口令,当它们不小心访问了钓鱼网站或者注册的某个的安全级别较低的网站受到攻击也会导致自己的口令泄漏[2,3].为了解决该问题,人们提出了双因数的认证方法,即用户通过浏览器登录自己的在线账户时,不仅要输入他所知道的信息,如口令,而且还要提供他拥有的某物的证明,如令牌.这样攻击者即使获得用户口令后也很难登录成功.

传统的令牌主要基于特殊的硬件设备,如USB Key,动态口令牌等.近年来随着智能手机的普及,人们设计出了基于智能手机的软件令牌,如Google身份认证器[4].相比硬件令牌,软件令牌的优点在于生产成本低廉,便于用户携带,并且支持多个网站.尽管有着诸多优势,但基于软件令牌双因素认证系统在用户在线账户的保护方面应用的并不普遍.其主要原因在于它们需要输入用户名和口令之外的信息,增加了用户的操作负担,影响了用户登录的速度.为了解决该问题,近年来人们提出了可用性加强的移动双因素认证方案[5~7].在这些认证方式中,

收稿日期:2017-01-22;修回日期:2017-06-11;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61572380,No.61772383);国家973重点基础研究发展规划(No.2014CB340600)

第二重认证对用户而言是透明的,用户只需输入口令即可完成认证. 可用性加强的移动双因素认证虽然减少了用户操作,但是却带来了其它问题:(1)它们无法抵抗同一环境下攻击者的攻击. (2)这些方法只适用于用户通过计算机浏览器进行登录,不支持用户通过手机浏览器对账户访问. 鉴于以上原因,本文设计了一种基于情景感知的低交互移动双因素认证系统,达到了用户身份认证的可用性,安全性和健壮性.

2　相关工作

这一节,我们对近年来提出的一些可用性加强的移动双因素认证方法进行介绍,并分析了这些方法的优、缺点.

文献[5]给出了一种消除用户和手机交互的双因素认证方法. 该方法充分利用了 google 浏览器提供的蓝牙 API,借助该 API 浏览器和手机能够实现自动的通信,从而为服务器和手机之间建立了一条信道. 虽然该方法具有良好的可用性,但是它取消了用户参与的蓝牙配对过程. 导致同一环境下的攻击者可以直接向手机发送蓝牙请求来获取手机中保存的认证信息,进而冒充用户的身份. 此外,该方法也不支持用户通过手机浏览器来访问账户.

文献[6]提出了基于混合带宽的移动双因素认证方法. 用户可以通过手动输入,扫码,蓝牙或 WiFi 的方式在计算机和智能手机间建立四种不同带宽的信道来传递认证信息. 其中手动输入和扫码的方式虽然能够保证信道安全,但是需要用户进行额外的操作,而且传递的信息量小. 蓝牙或 WiFi 的方式虽然传递的信息较大,减少用户交互,但是它面临着和文献[5]同样的问题.

文献[7]给出了一种基于声音比较的双因素认证方法,当服务器验证完用户通过计算机浏览器提交的口令后,会通知计算机和智能手机同时采集周围的声音信息,然后计算机借助服务器将声音信息传递给智能手机. 最终由智能手机来判断用户身份的合法性,如果声音信息足够相似,则返回給服务器成功的确认信息,否则返回给服务器失败的确认信息. 该方法的优点在于不需要用户与智能手机进行交互. 但是它只能抵抗异地的攻击者,无法防范同一环境下的攻击者. 而且不支持手机浏览器登录.

综上所述,可用性是移动双因素能否被用户广泛采用的关键因素,但如何在加强可用性的同时,保证其安全性以和健壮性是亟待解决的问题.

3　假设和目标

这一节,我们定义攻击者所具有的能力,同时给出本系统最终要达到的目标.

3.1　假设

假设攻击者得到了用户的用户名和口令,同时假设攻击者有可能与合法用户位于同一环境,使用相同型号的手机.

我们进一步假设攻击者无法攻陷用户的智能手机,如果攻击者能够获得软件令牌运行的平台的控制权,则任何的双因素认证方案降低成为了仅仅依赖于口令的单因素认证方案.

我们还假设用户计算机和手机的浏览器是安全的,攻击者无法实施针对 SSL 协议的中间人攻击.

3.2　目标

安全性　防止异地或同一环境下的攻击者在窃取受害人的用户名和口令后,冒充用户的身份登录用户的账户.

可用性　用户在登录时系统不需要改变其原有的基于口令认证的习惯,额外的操作就是开启手机的应用程序,点击认证键.

健壮性　系统应支持用户采用计算机或者手机浏览器进行登录,不能只适用于计算机登录.

4　系统结构

本文中提出的双因素认证方案包括注册过程和认证过程.

在注册程中,用户首先通过浏览器访问注册页面,然后在返回的页面填写用户名、口令等个人信息,并提交. 服务器端在收到用户传来的注册信息后首先对其进行验证,如果数据库中不存在同名用户,则生成公、私钥对,其中公钥连同用户的个人信息一起保存,而私钥和用户名则以二维码的形式返回给浏览器. 用户启动智能手机令牌程序,扫描该二维码,并将取得的信息保存至手机.

图 1 描述了认证过程,用户通过浏览器登录要访问的网站,然后在返回的页面中输入帐户名和口令信息,并提交. 服务器收到浏览器发来的消息后,首先验证用户提交的用户名和口令是否正确,如果正确,返回双因素认证界面. 否则返回口令重新输入界面. 浏览器在加载双因素认证界面的时会与服务器自动建立 Websocket 连接,并提交用户名,浏览器类型和程序类型. 服务器在收到消息后,首先根据程序类型判断是浏览器,还是令牌程序,如果是浏览器则返回“请点击令牌程序的认证键”的消息. 用户看到消息后启动手机令牌程序,并点击认证按钮,触发令牌程序向服务器发送 Websocket 连接请求. 服务器在收到令牌程序发来的消息后,首先根据程序类型判断是消息来自于浏览器,还是令牌程序,如果是令牌程序,则进一步根据用户名判断浏览器是否登录,如果未登录,则返回浏览器先登录的消息. 如果已登录,则根据浏览器类型做进一步判断,如果是计算

机浏览器,则通知浏览器和令牌程序采集 WiFi 信息,如果是手机浏览器,则通知浏览器和令牌程序采集设备指纹信息,除此之外还向智能手机发送随机数. 最终浏览器将采集到的认证信息发送给服务器,智能手机用保存的私钥对随机数进行签名,然后将签名信息和采集到的认证信息发送给服务器. 服务器在收到浏览器和智能手机令牌程序发来的消息后,首先验证签名是否正确. 如果正确,则会进一步检查浏览器和手机提交的认证信息是否相似,如果在规定阈值之内,则返回成功登录页面,否则返回拒绝登录的页面.

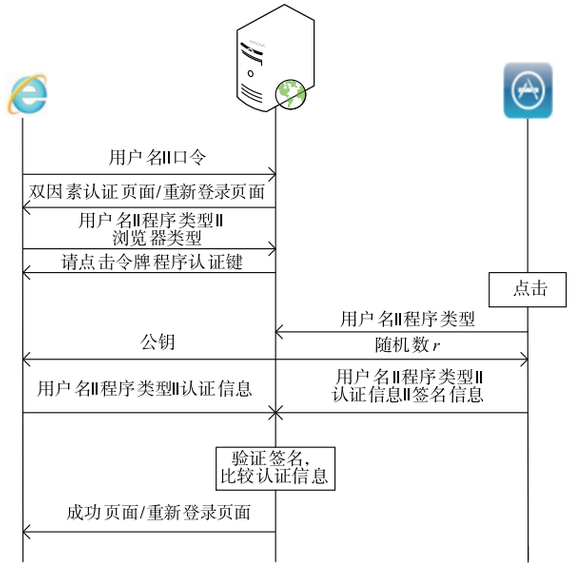

图1 认证过程

5 关键技术

5.1 基于 WiFi 的近邻检测技术

随着配备各种传感器的个人设备的普及,人们对基于 WiFi 的近邻认证技术展开了研究[8,9]. 他们希望不依赖用户的参与,两个设备通过自动比较所采集到周围的 WiFi 信号是否相似性来确定双方是否邻近,本文的方案中也采用了这种技术.

5.1.1 基本定义

设 WiFi 访问点的形式为(m,s),其中 m 是该访问点的标识,s 为该访问点对应的信号强度. 设 W_c和 W_p分别表示计算机和智能手机在一定时间内扫描到周围 WiFi 访问点的集合,n_c和 n_p分别表示计算机和智能手机在该时间段内检测到不同访问点的个数. 我们定义了如下集合:

$$W_c=\{(m_1^{(c)},s_1^{(c)}),(m_2^{(c)},s_2^{(c)}),\cdots,(m_{n_c}^{(c)},s_{n_c}^{(c)})\}$$

$$W_p=\{(m_1^{(p)},s_1^{(p)}),(m_2^{(p)},s_2^{(p)}),\cdots,(m_{n_p}^{(p)},s_{n_p}^{(p)})\}$$

$$W_c\cap W_p=\{(m_{\cap,1},s_{\cap,1}^{(c)},s_{\cap,1}^{(p)}),(m_{\cap,2},s_{\cap,2}^{(c)},s_{\cap,2}^{(p)}),\cdots,(m_{\cap,n_\cap},s_{\cap,n_\cap}^{(c)},s_{\cap,n_\cap}^{(p)})\}.$$

$$W_c\cup W_p=\{(m_{\cup,1},s_{\cup,1}^{(c)},s_{\cup,1}^{(p)}),(m_{\cup,2},s_{\cup,2}^{(c)},s_{\cup,2}^{(p)}),\cdots,(m_{\cup,n_\cup},s_{\cup,n_\cup}^{(c)},s_{\cup,n_\cup}^{(p)})\}.$$

$W_c\cap W_p$ 表示计算机和智能手机在一定时间内检测到相同访问点的集合,$W_c\cup W_p$ 表示计算机和智能手机在一定时间内检测到所有访问点的集合.

5.1.2 相似性度量

本文采用了杰卡德相关系数以及自定义的信号强度相似性分数来衡量两个设备采集 Wifi 信号的相似程度. 考虑到这两种判断结果有可能不一致,我们需要对判断结果进行融合. 目前融合可以在特征层[10],匹配分数层[11]和决策层[12]上进行. 本文的方案建立在匹配分数层,并采用了基于求和规则的融合方法给出最终判断.

杰卡德相似系数:

$$J(W_c,W_p)=\frac{\|W_c\cap W_p\|}{\|W_c\cup W_p\|}=\frac{n_\cap}{n_\cup} \tag{1}$$

信号强度的相似性分数:

$$S(W_c,W_p)=1-\frac{\sum_{i=1}^{n_\cup}\|s_i^{(c)}-s_i^{(p)}\|}{n_\cup*\max\|s_i^{(c)}-s_i^{(p)}\|} \tag{2}$$

其中 $s_i^{(c)}-s_i^{(p)}$ 表示相同访问点间信号的差异.

基于求和规则的融合公式:

$$s_{fus}=w_1s_1+w_2s_2 \tag{3}$$

其中 s_1表通过公式(1)求得的相似性分数,s_2表示采用公式(2)求得的相似性分数,w_1,w_2表示权重值,且 $w_1+w_2=1$.

关于权重的选择,我们参考了文献[11],其中

$$w_1=\frac{EER_2}{EER_1+EER_2},w_2=\frac{EER_1}{EER_1+EER}$$

EER_1 与 EER_2 分别表示通过采用公式(1)和公式(2)求得的等错误率.

5.2 设备指纹技术

设备指纹有许多名称,例如机器指纹,浏览器指纹,用户指纹等,它是以识别的目的而收集的远程计算设备的信息[13].

本方案中为了保证用户采用手机上网时也能够进行双因素认证,比较了浏览器和令牌程序都能直接获取的手机指纹信息,例如:设备型号,操作系统版本,耗电量级别等设备信息. 如果浏览器和令牌程序采集的这些信息全部相等,我们认为用户合法,否则认为用户非法.

6 安全性分析

在我们的安全模型中,假设攻击者无法攻陷用户的计算机和智能手机,而且攻击者无法实施针对 SSL 协议的中间人攻击,在这种情形下,攻击者获取用户的用

户名和口令后,如果想要登录受害人的账户,他可以采取如下方法:

(1) 猜测私钥

由于攻击者无法启动令牌程序,他可以猜测受害人手机中私钥,并以此来伪造响应值. 然而私钥对每个用户而言是随机的,且长度至少为 1024 位,所以想要通过猜测出正确的私钥是很困难的.

(2) 等待用户启动令牌程序

攻击者可以在浏览器中输入受害人用户名和口令,然后等待受害人启动令牌程序后认证通过. 本文方案中受害人会先进行浏览器登录,再启动令牌程序. 当受害人采用浏览器进行登录时,会收到请勿重复登录消息,因此他不会启动令牌程序. 其次,攻击者不能长期采用浏览器进行登录,它必须在输入用户名和口令后,30s 内启动令牌程序,否则会被服务器强行关闭. 最后即使合法用户启动了令牌程序,攻击者还必须提供和智能手机相似的 WiFi 信息或相同的设备指纹信息才能认证通过.

(3) 猜测 WiFi 信息

设 $W_p = \{(m_1^{(p)}, s_1^{(p)}), (m_2^{(p)}, s_2^{(p)}), \cdots, (m_{n_p}^{(p)}, s_{n_p}^{(p)})\}$ 表示手机令牌程序采集到 WiFi 访问点的集合,其中 m_i 表示访问点的标识,s_i 表示该访问点的信号强度. 由于 m_i 是很长的二进制随机数,攻击者需要执行 $n_p * 2^{|m|}$ 次的尝试才能猜测出所有的标识. 除此之外,攻击者还要猜测出于每个地址相对应的信号强度,而信号强度是随时间不断变化的. 在只允许有限次错误尝试的情况下,攻击者想要猜测出与合法用户手机相似的 WiFi 信息是很困难的.

7　实验评价

7.1　WiFi 数据采集

当用户采用计算机浏览器进行登录时,服务器通过比较计算机浏览器和智能手机令牌程序提交的 WiFi 信息的相似程度来确定经过口令认证后的用户身份的合法性. 为了验证该方法的可行性,我们进行了一系列实验. 实验中我们选择计算机实验室,图书馆和寝室三个位置来采集数据. 其中在同一环境下,每次采样时手机和计算机之间的距离在 1m 之内,采样的持续时间为 1s,采样频率为每秒 5 次,采样结果为这 5 次的平均值,最终得到 900 个样本. 在不同环境下,我们分成了两种情况,一种是两个设备相距较近,我们将计算机和智能手机放在了实验室,寝室和图书馆的不同房间来采集 WiFi 信号,另一种情形是设备相对距离较远,我们将手机和计算机分别放置于实验室和图书馆,实验室和寝室,以及寝室和图书馆来采集数据,其中每种情形下每次采样的持续时间为 1s,采样频率为每秒 5 次,采样结果为 5 次的平均值,最终在这两种情形下各获得 900 个样本.

7.2　WiFi 信息的采集与相似性分析

图 2 展示了两个设备在同一房间,同一大楼以及不同大楼内通过杰卡德相似系数求得的相似性分数. 图 3 展示两个设备在同一房间,同一大楼以及不同大楼内通过信号强度相似性计算公式求得的相似性分数. 图 4 展示了两个设备在同一房间,同一大楼以及不同大楼内通过融合公式求得的相似性分数.

假设同一环境下的两个设备是合法的,位于同一大楼以及不同地点的设备是非法的,根据不同的相似性分数计算结果,在设定不同的阈值下,我们能够得到不同的等错误率曲线. 图 5 展示了对杰卡德相似性分数计算结果设定不同阈值求得的等错误率曲线. 图 6 展示了对信号强度相似性分数计算结果设定不同阈值求得的等错误率曲线. 图 7 展示了对融合公式求得的相似性分数计算机结果设定不同的阈值下求得的等错误率曲线. 对比图 5,图 6 和图 7,我们可以发现融合后的等错误率要低于前两者. 这表明融合后的判断结果更优.

7.3　设备指纹采集与分析

当用户采用手机浏览器进行登录时,服务器通过比较手机浏览器和令牌程序所提交的设备指纹是否相同来确定用户的合法性. 为了寻找合适的指纹,本文选

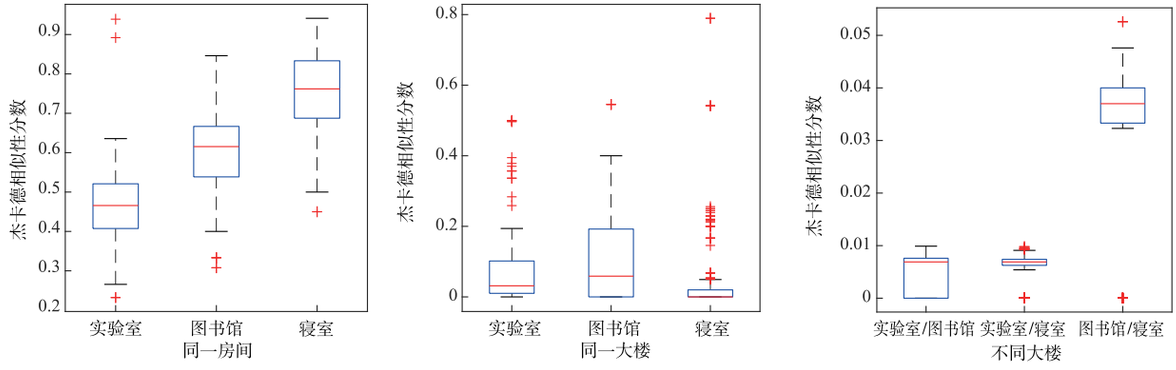

图2　同一房间、同一大楼和不同大楼内利用杰卡德系数求得的WiFi相似性分数

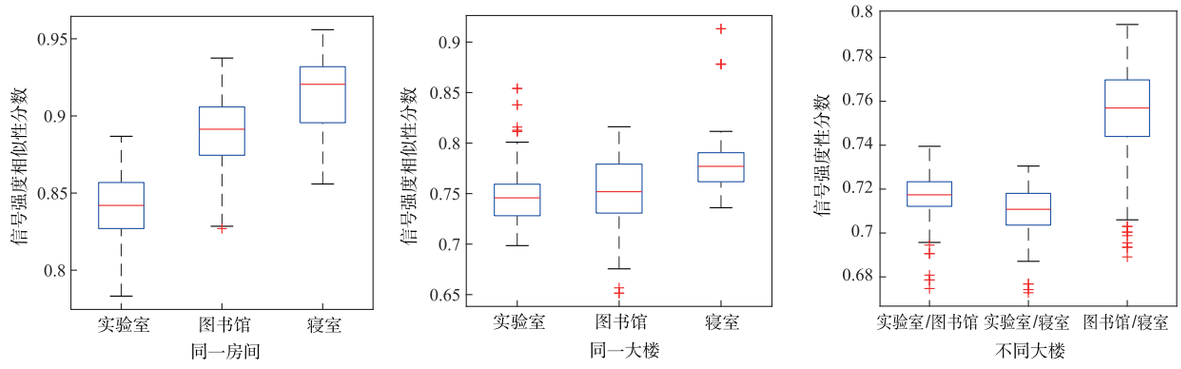

图3 同一房间、同一大楼和不同大楼内利用信号强度相似公式求得的WiFi相似性分数

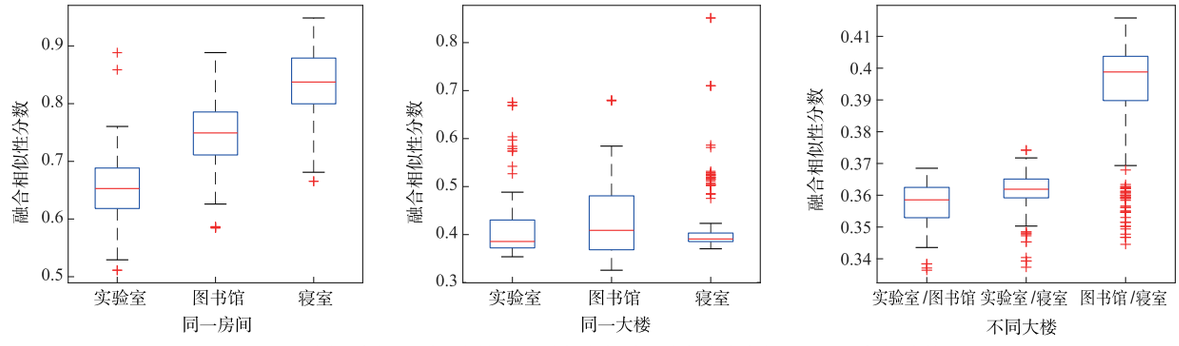

图4 同一房间、同一大楼和不同大楼内利用融合公式求得的WiFi相似性分数

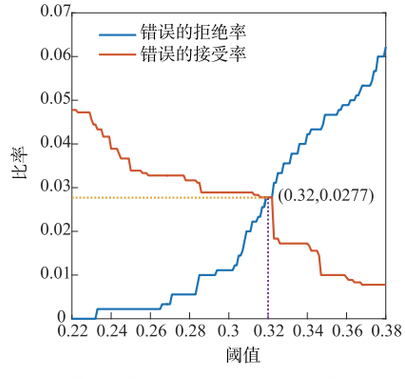

图5 根据杰卡德公式计算结果得到的错误率曲线

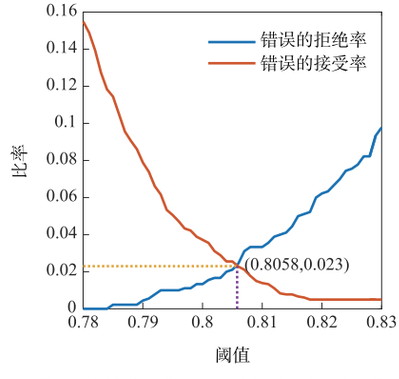

图6 根据信号强度相似公式的计算结果得到的错误率曲线

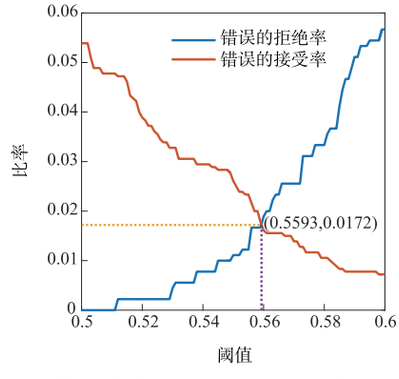

图7 根据融合公式公式计算结果得到的错误率曲线

择了如表1所示的5种不同的个人设备进行实验,其中前4种为智能手机,最后一种为平板电脑. 从该表可以看出不同类型的手机型号会不同,手机当前电量会随时间进行变化,它可以作为区分是否是同一手机的重要指标. 用户采用的操作系统版本有也会有较大的差异. CPU核心数通常和设备型号绑定,同一款手机,具有的CPU核心数相同. 不同的手机也有可能具有相同的CPU核心数.

7.4 时间成本分析

我们还进行了一系列实验来验证双因素认证所花费的时间. 其中计算机和手机位于学院的实验室,服务器位于学院的机房. 在进行基于计算机浏览器的双因素认证实验时,计算机和手机都采用了无线WiFi进行联网. 在基于手机浏览器的双因素认证实验时,手机采用了WiFi和移动网络两种方式. 在每种方式下分别进行了100次登录实验,计算的时间为用户从点击令牌程序的认证按钮到浏览器收到成功登录页面. 表2展示了实验结果,在采用计算机浏览器进行登录时,平均的验证时间为4.1s. 在采用手机浏览器进行登录时,如果联网方式为WiFi,平均的验证时间为3.9s. 如果联网方式为移动网络,平均的验证时间为5.2s. 然而不论哪种认证方式,时间都比较短. 相信

随着技术的将来网络性能的提高,认证的时间会进一步缩短.

表 1　不同手机的设备指纹

	设备型号	电量级别	操作系统	CPU 核心数
1	SM-G5700	1	Android 6.0.1	8
2	NEM-AL 10	0.77	Android 6.0	8
3	TCL P316L	0.43	Android 5.0.2	4
4	H60-L02	0.66	Android 4.4.2	8
5	GT-P3110	0.09	Android 4.4.4	2

表 2　采用不同的登录方式和手机联网方式认证的时间成本

浏览器类型	手机联网方式	期望(ms)	方差
计算机浏览器	WiFi	4133	512
手机浏览器	WiFi	3916	330
手机浏览器	移动网络	5208	573

8　结论

本文给出了一种用户友好的移动双因素认证方案,用户在浏览器中输入完用户名和口令后,只需按照提示,点击令牌程序的认证键即可完成认证. 同 Google 身份认证器,短信验证码等传统双因素认证系统相比,本文方案简化了用户操作,提高了登录的速度. 同基于蓝牙、声音等用户友好的双因素认证相比,它不光支持用户采用计算机浏览器进行登录,还支持用户采用手机浏览器进行登录. 而且相比这两种双因素认证方案具有更高的安全性,能抵抗同一环境下攻击者攻击. 在下一步的工作中需要将计算机端采集 WiFi 的程序做成插件的形式,方便用户进行部署,其次寻找更加强健的设备指纹特征用于手机浏览器登录时的认证.

参考文献

[1] Kelley P, Komanduri S, et al. Guess again (and again and again): Measuring password strength by simulating password cracking algorithms [A]. 33rd IEEE Symposium on Security and Privacy[C]. USA: IEEE, 2012. 523 – 537.

[2] hackers-target-google-users-advanced-phishing [DB/OL]. http://www.nbcnews.com/, 2014-5-13.

[3] China Software Developer Network (CSDN) leaked 6 Million user data [DB/OL]. https://www.rcesecurity.com/, 2012-12.

[4] Google 2-Step Verification [DB/OL]. https://www.google.com/landing/2step/, 2017

[5] CZESKIS A, DIETZ M, et al. Strengthening user authentication through opportunistic cryptographic identity assertions [A]. ACM Conference on Computer and Communications Security (2012) [C]. USA: ACM, 2012. 404 – 414.

[6] SHIRVANIAN M, JARECKI S, et al. Two-factor authentication resilient to server compromise using mix-bandwidth devices [A]. The Network and Distributed System Security Symposium (2014) [C]. USA: Internet Society, 2014.

[7] Karapanos N, Marforio C, Soriente C, et al. Sound-Proof: Usable two-factor authentication based on ambient sound [A]. USENIX Security Symposium (2015) [C]. USA: USENIX, 2015. 483 – 451.

[8] Krumm J, Hinckley K. The near me wireless proximity server [A]. International Conference on Ubiquitous Computing (2014) [C]. Brelin Heidelberg: Springer, 2004. 283 – 300.

[9] Truong T, Gao X, Shrestha B, et al. Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication [A]. International Conference on Pervasive Computing and Communications (2014) [C]. USA: IEEE, 2014. 163 – 171.

[10] 何国辉,甘俊英,李春芝,等. 人脸与虹膜特征层融合模型的研[J]. 电子学报,2007,35(7):1365 – 1371.
HE Guo-hui, GAN Jun-ying, et al. A model study for face and iris feature fusion and recognition[J]. Acta Electronica Sinica, 2007, 35(7): 1365 – 1371. (in Chinese)

[11] Horng S J, Chen Y H, Run R S, et al. An improved score level fusion in multimodal biometric systems[A]. Parallel and Distributed Computing, Applications and Technologies. (2009)[C]. USA: IEEE, 2009. 239 – 246.

[12] Prabhakar S, A. K. Jain, Decision-level fusion in fingerprint verification[J]. Pattern Recognition, 2002, 35(4): 861 – 874.

[13] Device fingerprint [DB/OL]. https://en.wikipedia.org/wiki/Device_fingerprint, 2017

作者简介

刘　冬　男,1984 年生于山西太原. 现为武汉大学计算机学院博士研究生. 研究方向为移动互联网络安全.
E-mail: liudong0503@126.com

陈　晶(通信作者)　男,1981 年生于湖北武汉. 武汉大学计算机学院教授、博士生导师. 研究方向为网络安全、无线网络.
E-mail: chenjing@whu.edu.cn