一种面向移动终端的抗肩窥图形密码方案

黄叶珏[1],郑河荣[2]
(1.浙江经贸职业技术学院 信息技术系,浙江 杭州 310018;
2.浙江工业大学 软件学院,浙江 杭州 310018)

摘 要:密码认证目前仍然是移动终端主流身份认证方式之一。移动终端由于其使用环境的复杂性,密码容易遭受肩窥攻击。针对这种情况,文中吸取Pass-Object经典图形密码方案加入干扰图形的设计思想并加以改进,提出了一种面向移动终端的抗肩窥图形密码方案,方案以字符和颜色为基础生成图形密码。方案的设计完全符合触摸式移动终端用户的使用习惯,整个认证过程用户只需在触摸屏上点击即可完成操作。安全性分析数据表明:方案在密码空间和抗意外登陆方面都安全性良好,而且可有效抵御登陆过程被多次录制的肩窥攻击。

关键词:图形密码;抗肩窥;移动终端;身份认证
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2015)07-0124-04
doi:10.3969/j.issn.1673-629X.2015.07.027

A Shoulder Surfing Resistant Graphical Passwords Scheme for Mobile Terminal

HUANG Ye-jue[1],ZHENG He-rong[2]
(1. Department of Information Technology,Zhejiang Economic & Trade Polytechnic,
Hangzhou 310018,China;
2. College of Software,Zhejiang University of Technology,Hangzhou 310018,China)

Abstract:Passwords authentication is still one of the main authentication modes for mobile terminal. Mobile terminal is vulnerable to shoulder surfing attack because of using in complex environments. Absorbing the design thought of adding interference graph from the pass-object graphical password scheme,a shoulder surfing resistant graphical passwords scheme for mobile terminal is proposed,in which the graphical passwords are generated by characters and colors. In the scheme,just by clicking the screen user can complete the whole log-in phase,the scheme design completely conforms to the use habit of touch type mobile terminal user. The security analysis shows that the scheme has good security in the password space and accidental login resistance,and can effectively resist the shoulder surfing attack in that the login process is recorded repeatedly.

Key words:graphical passwords;shoulder surfing resistance;mobile terminal;identity authentication

0 引 言

基于智能移动终端实现网上银行、网上股市等移动互联网应用日益普及,身份认证是移动互联网业务在应用中的第一道安全防线,而密码认证则是目前智能移动终端中主流身份认证方式之一。密码认证一直面临着易记性与安全性矛盾,特别是传统的文本密码。图形密码作为文本密码的潜在替代方案,日益受到关注,研究人员从不同层面对其展开了研究[1-6]。由于手机等智能移动终端的显示屏幕相对偏小,图形密码需要在小尺寸显示屏上保证用户的易用性,那么获得的密码空间是非常有限的。此外,移动终端用户的使用方式以触摸、点击等为主。因此,如何使得图形密码适用在移动终端并且符合移动终端用户的使用习惯都是需要研究的。文献[7]针对移动平台的特点,把图形密码和多点触控等技术相结合,设计了适用于移动平台的身份认证方案。文献[8-10]也为移动设备的应用设计了图形密码身份认证方案。

肩窥攻击是一种直接观察就可以得到所需信息的攻击技术。由于智能移动终端其使用环境复杂,可能

收稿日期:2014-08-18 **修回日期**:2014-11-21 **网络出版时间**:2015-06-23
基金项目:浙江省自然科学基金(Y1110781);浙江省教育科研项目(Y201327499)
作者简介:黄叶珏(1978-),女,副教授,研究方向为计算机图形图像、网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150623.1005.008.html

在人员拥挤或者视频监控的情况下使用,也可能被不怀好意的人安装上恶意软件,因此非常容易遭受肩窥攻击。文献[11]基于凸包图形算法提出了一种抗肩窥的图形密码方案。文献[12-13]也对抗肩窥攻击图形密码身份认证机制的设计与实现作了研究。而文献[14]提出了点击型图形密码综合性的评价方案。文中吸收典型图形密码 Pass-Object 方案的设计思想,设计了一种面向移动终端的图形密码方案,从抗肩窥分析数据可以看出,即使攻击者多次录制登陆过程,获取正确认证图形密码的概率也非常低。

1　Pass-Object 图形密码方案安全性分析

Pass-Object 方案是经典的图形密码方案。注册阶段,此方案允许用户选择一些图形物体。验证阶段,系统会显示出一个由许多图形组成的陈列(用户注册阶段选择的图形也包括在图形阵列中),用户需要识别出注册阶段选择的图形,并且移动一个固定框架的位置,使得注册阶段选择的图形落在框架之中,如图 1 所示。通过多次重复此过程来防止随机选中的可能。

图 1　Pass-Object 图形密码方案验证界面

Pass-Object 方案抗肩窥攻击安全性分析[15]:由于每次选中的框架中,除了包括注册阶段选择的图形(即图形密码)之外,还包括若干个干扰图形,所以即使整个登录过程被攻击者录制,攻击者也无法直接获得图形密码,但是由于选中的框架之中包含的干扰图形比较少,如果攻击者录制若干次登录过程,通过分析就有可能获得正确的图形密码。举例如下:假设选中的框架之中包含 8 个图形,而攻击者录制的某两次登录过程选中框架内包含的图形如下所示:“蝴蝶、小熊、小鸟、蜘蛛、书本、袋鼠、企鹅、月亮”;“方形、心形、圆形、小鸟、星星、闹钟、小花、兔子”,由于两次登录选中的框架内除了图形密码之外,其他的干扰图形都不一致,所以攻击者马上可以分析出正确的图形密码是“小鸟”。为了提高方案的安全性,Pass-Object 方案的设计者建设将图形阵列中的图形定义为 1 000 个,这固然可以扩大密码空间,但是上述攻击成功的概率也很大,而且不利用用户识别。

2　面向移动终端的抗肩窥字符图形密码方案

文中吸取 Pass-Object 方案中添加干扰图形来抵御肩窥攻击的思想,设计了面向移动终端的抗肩窥字符型图形密码方案。考虑到图形密码目前还没有被普遍的接受,字符型密码认证方式还是主流的方式。本图形密码方案采用 ASCII 码表的 34 到 126 之间的 93 个字符,搭配红色、绿色、蓝色三种显示颜色组成 279 个基本图形(基本图形采用 Pass-Object 方案所用的图形也是一样的)。

为了让用户能够接受这种图形密码方案,操作过程也足够的简单方便。本图形密码方案在注册和登陆阶段都只需在触摸屏上作“点击”操作即可完成整个操作,完全符合触摸屏的操作习惯。该方案中,基本字符空间和颜色类型空间可以根据不同的应用场景作扩大和缩小。

2.1　注册阶段

用户注册阶段与常规的注册类似,用户首先输入用户名、注册 Email 邮箱地址,这些信息通过移动终端标准的输入法来完成。接着用户在输入框中输入需注册的图形密码。由于在本方案中,图形密码的基本字符空间和颜色类型空间是固定的,所以设计了一个如图 2 所示的图形密码专用输入键盘。用户在密码输入框中输入字符长度大于等于 8 位的密码即可符合要求。在密码输入框中每输入一位字符由两步组成:用户首先在专用键盘的下方颜色类型键中选择颜色,然后再点击字符键来选择字符。只有颜色和字符都选定之后,该位密码字符才最终确定。确定之后相应颜色的字符就显示在密码框中,以便用户直观地确认密码是否是自己选定的内容,比如用户先选择红颜色,然后选择字符“%”,那么密码框中就会显示红颜色的“%”字符,这样用户就可以发现自己的输入是否正确。采用这种方式,用户输入了自己的字符图形密码之后,移动终端上的整个注册过程就完成了。系统会通过 SSL 或者 TLS 协议向用户的 Email 邮箱地址发送一封确认邮件,用户在邮箱中确认之后整个注册就生效。

图 2　图形密码专用输入键盘

(界面中颜色类型键的顺序是红色、蓝色和绿色)

2.2 登陆阶段

用户登陆阶段,系统根据用户注册密码的位数 N 自动生成 N 个选择字符图形密码的步骤。每个步骤中,系统根据 93 个基本字符和 3 种颜色类型的组合生成 279 个字符图形,这些字符图形每次都随机排列分布到 3 × 3 的格子中,因此每个格子都均匀分布着 31 个字符图形,这 31 个字符按照颜色分类显示,颜色一样的显示在一起,如图 3 所示。先显示所有的红色字符,接着是蓝色字符,最后是绿色字符,这样显示可加快用户识别出正确图形密码所在格子的速度,因为用户知道正确图形密码的颜色,只要在同色中查找即可。用户在该步骤中只要找到该位字符图形密码所在的格子,然后在触摸屏相应的位置作点击操作即可完成该位图形密码的输入,如果用户按错了格子位置,只要在正确的格子位置作点击操作即可选中正确的位置,同时前一个格子位置就作废。为了操作更加的人性化,触摸屏的下方放置了“前进”和“后退”按钮,当用户确定选择了正确的图形密码所在的格子位置之后,可以点击触摸屏右下方的“前进”按钮,系统就会生成下一位图形密码的认证步骤,用户可以采用相同的方式进行选择;如果用户想修改前一次认证步骤的内容,可以点击触摸屏左下方的“后退”按钮。

图 3 系统在登陆阶段某一步骤随机生成的字符图形密码选择界面

(界面中每个格子的 31 个字符按照颜色分类显示,颜色顺序是红、蓝、绿)

方案实现时,用户登陆认证的整个流程具体描述如下:

(1)用户请求系统进行密码认证。

(2)系统随机生成一个如图 3 所示的界面,并记录该界面对应的是用户图形密码第几位图形密码的输入,见图 3 界面下方的中间位置有一个显示框即指示当前界面用于认证图形密码的第几位,如图中显示的是 3,表示该界面用于认证用户图形密码的第 3 位密码的输入。

(3)用户根据自己记忆的该位字符图形密码,在界面中进行寻找,然后在该字符图形密码所在的格子位置上点击,选定该格子,选定之后,该格子就会被覆盖一层半透明的蓝色,以提醒用户选定了该格子。点击选择可以多次操作,每次点击之后系统只记录当前点击格子的位置,丢弃上一次点击格子的位置,并在当前点击的格子上覆盖一层半透明的蓝色,而上一次点击的格子则恢复原来的样子,这样可以方便用户操作,以防误点击。

(4)用户选定格子之后,点击触摸屏右下方的“前进”按钮,系统则记录该位用户字符图形密码的输入,并对下一位图形密码进行认证。如果用户的字符图形密码还没输入结束,则转步骤(2);如果用户图形密码已输入完毕,则转步骤(6)。

(5)如果用户点击触摸屏左下方的“后退”按钮,系统则丢弃当前步骤的认证内容,并判断当前是认证图形密码的第几位,如果不是第 1 位,则退到前一位进行认证,并转到步骤(2)。

(6)系统把用户输入的认证内容与用户注册时的图形密码进行比较,如果正确则系统登陆成功;如果错误,则判断是否已经出现三次错误,如果出现三次错误则发送一封提醒邮件到用户的注册邮箱,系统退出。如果不满三次则转骤(2)重新开始字符图形密码的输入。

3 安全性和易用性分析

3.1 易用性分析

系统的可操作性方面,该图形密码认证方案完全根据触摸屏用户操作习惯进行设计,用户在整个注册阶段和登陆阶段都只需作简单直观的点击操作即可完成。认证的步骤长度与用户注册时设定的字符图形密码长度有关,如用户注册时设置了 8 位长度的字符图形密码,则需要 8 个步骤来完成登陆。此外,系统图形密码的记忆方面,系统的图形密码是由文本字符和颜色的组合构成,延续了传统教育中用户对文本字符的记忆能力,而颜色用户可以根据自己的习惯自由选择,所以易记性方面比较符合用户习惯。登录过程中,为

了方便用户识别出正确的字符图形密码,每个格子的图形都按照不同的颜色分类显示,这样可加快用户的识别速度。因为虽然每个图形密码输入的界面中都包括 279 个字符图形,但由于每个格子的字符图形按照颜色分类显示,而用户知道正确图形密码的颜色,选择时可忽略其他颜色的图形,所以用户平均真正需要识别的字符图形为 93 个,经实验测试,用户可基本接受。

3.2　安全性分析

3.2.1　密码空间分析

本图形密码方案的图形由 93 个基本字符和 3 种颜色类型的组合生成 279 个字符图形,所以长度为 N 位的字符图形密码的个数为 279^N。假设密码长度 $N=8$,密码的个数约为 3.671×10^{19},假设本方案的密码长度为 8–16 之间,则整个密码空间为:

$$SP = \sum_{N=8}^{16} 279^N \approx 1.35 \times 10^{39} \tag{1}$$

3.2.2　抗意外登陆分析

登陆阶段,对于每一位字符图形密码的输入,用户需要在 3 × 3 的格子中选择包含该位字符图形的格子,直到每位图形密码都选择正确,系统才正常登陆。对于每一位图形密码的认证,用户意外选择正确的概率为 1/9,如果用户注册的图形密码的位数为 N,则意外登陆成功的概率为:

$$P_{acc}(N) = \left(\frac{1}{9}\right)^N \tag{2}$$

假设用户注册的图形密码长度为 $N=8$,则

$$P_{acc}(8) = \left(\frac{1}{9}\right)^8 \approx 2.323 \times 10^{-8} \tag{3}$$

如果用户注册的图形密码长度为 $N=16$,则

$$P_{acc}(16) = \left(\frac{1}{9}\right)^{16} \approx 5.396\ 6 \times 10^{-16} \tag{4}$$

可见意外成功登陆的概率是非常低的。

3.2.3　抗肩窥分析

假设有窥视者录制用户的登陆过程,经过多次录制,他可以对用户每次登陆选择的数据进行分析,从而根据其相关性来破解出用户的注册密码。在本方案的用户登陆过程中,用户在确认第 i 位图形密码时,选择的格子中包含 1 个用户注册的字符图形密码和 30 个干扰字符图形密码,所以窥视者猜测该位图形密码正确的概率为 1/31。如果是长度为 N 的图形密码,并且窥视者只录制一次用户的整个登陆过程,那么他猜测出完整的图形密码的概率为 $(1/31)^N$。

如果窥视者录制多次的话,那么根据注册用户在不同次登陆的相关性,也可以分析正确的图形密码。由于每个格子包含 31 个字符图形密码,如果该格子是用户选定的包含正确图形密码的格子,那么用户在下一次登陆的选择过程中,该格子也同样包含那个正确的图形密码。当两次选择时,格子中除了正确的字符图形密码相同,而其他 30 个字符图形密码在这两次登陆的过程中完全不同,那么窥视者就可以推断出该位正确的图形密码。所以本图形密码方案抗肩窥的能力可以通过窥视者正确猜测出密码的概率来表示:

$$P_{ss}(N,T) = \begin{cases} \left(\frac{1}{31}\right)^N & T = 1 \\ \left(\left(\frac{8}{9}\right)^{30} \times (T-1)\right)^N & T > 1 \end{cases} \tag{5}$$

式中,N 为用户注册的图形密码的位数,T 为窥视者录制次数。当 $T > 1$ 时,这里计算的是用户选择的格子中只包含一位相同的图形密码,而其他 30 位图形密码完全不同,这样窥视者就直接可以得到该位注册的图形密码。因为总共有 9 个格子,所以某位图形密码两次不落到同一个格子的概率是 8/9,这样的图形密码有 30 个。如果 $T=1$, $N=8$, $P_{ss}(N,T) \approx 1.17 \times 10^{-12}$;如果 $T=7$, $N=8$, $P_{ss}(N,T) \approx 3.05 \times 10^{-6}$。当然这样第二种情况表达的是直接可以得到注册密码的情况,这是一种最严格的情况。还可以采用同样的方式分析两次选择中有一半数据相同的概率,只要把式(5)的第二个式子中的 30 改成 14 即可计算得到。

4　结束语

针对智能移动终端使用环境复杂,身份认证密码输入时容易遭受肩窥攻击的特定问题,文中尝试性地结合文本密码和图形密码的技术,设计并实现了一个面向移动终端的抗肩窥字符型图形密码系统。从安全性分析可以得出:该方案可有效抵御肩窥攻击,即使整个认证过程被攻击者多次录制,正确图形密码被分析得到的概率也很低。

参考文献:

[1] Meng Yuxin. Designing click-draw based graphical password scheme for better authentication[C]//2012 IEEE 7th international conference on networking, architecture and storage. Xiamen: IEEE, 2012: 39-48.

[2] Wang Liming. Against spyware using CAPTCHA in graphical password scheme[C]//Proc of 2010 24th IEEE international conference on advanced information networking and applications. [s. l.]: IEEE, 2010.

[3] 蔡伟俊,杜晓荣,万　里. 推理型图形密码认证系统的设计与实现[J]. 计算机工程与设计,2010,31(12):2687-2690.

[4] 刘　杰. 基于图形密码的身份验证技术研究与实现[D]. 北京:北京大学,2010.

[5] Biddle R, Chiasson S, van Oorschot P C. Graphical passwords: learning from the first twelve years[J]. ACM Computing Sur-

(下转第 132 页)

安全防护,文中将智能 USIM 卡与 PKI 技术相结合,为移动终端提供一种安全可靠的安全认证方案,对众多的第三方移动应用提供身份认证,确保移动终端的信息安全。USIM 卡成为保存私钥、证书的理想载体,在安全存储了个人信息的同时,它的便携性也使它成为开展移动安全业务的理想媒介。

目前,信息技术的发展日益改变着人们传统的工作生活模式。智能手机、平板电脑等移动终端的功能不断加强,终端应用的大量开发使用,移动终端的信息安全正面临着越来越严峻的挑战。随着智能卡等一些安全芯片的处理能力的不断提高,PKI 技术的不断演进,移动终端的安全性一定会得到更大的提高[13]。

参考文献:

[1] Markovié M, Dordevié G. Secure mobile government and mobile banking systems based on android clients[M]//Securing electronic business processes. Fachmedien Wiesbaden: Springer, 2013: 263-273.

[2] 张 杨. 移动终端安全认证的设计与实现[D]. 北京:北京邮电大学,2012.

[3] EI Kettani M D E C, En-Nasry B. MIdM: an open architecture for mobile identity management[J]. Journal of Convergence, 2011, 2(2): 25-32.

[4] Toshikazu N. A distributed authentication mechanism for sharing an overlay network among multiple organizations[C]// Proceedings of the 12th international conference on information integration and web-based applications & services. USA: [s. n.], 2010: 813-817.

[5] 许喆明. 基于 PKI 的智能卡双向身份认证机制的设计与实现[D]. 长沙:国防科学技术大学,2006.

[6] 范亚军. 无线移动网络中的认证密钥交换协议及其应用研究[D]. 北京:北京邮电大学,2012.

[7] 刘百乐. 基于安全 SIM 卡的移动通信研究[J]. 计算机安全,2007(11): 26-29.

[8] Li M, Sandrasegaran K. A proxy based authentication localisation scheme for handover between non trust-associated domains[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2010(4): 47-50.

[9] Tsai Y R, Chang C J. SIM-based subscriber authentication Mechanism for wireless local area networks[J]. Computer Communications, 2006, 29(10): 1744-1753.

[10] 张李静. 智能卡在移动通信领域的应用:USIM 卡操作系统底层设计、移植与测试[D]. 天津:天津理工大学,2008.

[11] Firoozy-Najafabadi H R, Feizi-Derakhshi M. Multipurpose smart SIM card based on mobile database and location dependent query[C]//Proc of 2012 6th international conference on application of information and communication technologies. [s. l.]: IEEE, 2012: 1-5.

[12] Kuhn D R, Coyne E J, Well T R. Adding attributes to role-based access control[J]. Computer, 2010, 43(6): 79-81.

[13] 滕震方. 基于多属性的移动终端安全接入网络认证协议[J]. 计算机应用与软件,2013,30(8): 43-46.

(上接第 127 页)

veys, 2012, 44(4): 1-41.

[6] Biddle R, Mannan M, van Oorschot P C, et al. User study analysis and usable security of passwords based on digital objects[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 970-979.

[7] 胡 卫,张焕国,魏国珩,等. 面向移动平台的新型身份认证方案设计[J]. 计算机科学,2014,41(4): 99-102.

[8] Chang Tingyi, Tsai Cheng-Jung, Lin Jyun-Hao. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices[J]. Journal of Systems and Software, 2012, 85(5): 1157-1165.

[9] Cheong Soon-Nyean, Ling Huo-Chong, Teh Pei-Lee. Secure encrypted steganography graphical password scheme for near field communication smartphone access control system[J]. Expert Systems with Applications, 2014, 41(7): 3561-3568.

[10] 黄叶珏,褚一平. 基于多分辨离散模型的图形密码[J]. 计算机工程与设计,2012,33(12): 4493-4496.

[11] Wu Tzong-Sun, Lee Ming-Lun, Lin Hanyu, et al. Shoulder-surfing-proof graphical password authentication scheme[J]. International Journal of Information Security, 2014, 13(3): 245-254.

[12] 潘 源. 防肩窥攻击的图形密码的设计与实现[D]. 北京:北京大学,2013.

[13] 高晶元. 一种防肩窥攻击的图形密码的设计与实现[D]. 北京:北京大学,2008.

[14] Chinasson S, Stobert E, Foret A, et al. Persusive cued click-points: design, implementation and evaluation of a knowledge-based authentication mechanism[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(2): 222-235.

[15] 胡 卫,马常楼,廖 巍. 图形密码方案可用性及安全性分析[J]. 计算机应用与软件,2010,27(12): 55-57.

一种面向移动终端的抗肩窥图形密码方案

作者： 黄叶珏， 郑河荣， HUANG Ye-jue， ZHENG He-rong
作者单位： 黄叶珏,HUANG Ye-jue(浙江经贸职业技术学院 信息技术系,浙江 杭州,310018)， 郑河荣,ZHENG He-rong(浙江工业大学 软件学院,浙江 杭州,310018)

刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(7)