BlindLock：一种有效防范污迹攻击的图案锁系统

吴继杰 曹天杰 翟靖轩

（中国矿业大学计算机科学与技术学院 徐州 221000）

摘 要 现阶段，越来越多的智能手机使用图案锁作为身份认证机制。为解锁智能手机，用户需要将解锁图案绘制在屏幕上，这样就不可避免地留下油性残留物，又称污迹。敌手可以利用污迹重现解锁图案，使用户的隐私受到威胁。通过对现有图案锁的研究，提出了一种能在衣服口袋中进行解锁的系统：BlindLock图案锁系统。BlindLock图案锁利用覆盖原理抵抗污迹攻击，同时利用视觉闭塞原理抵抗肩窥攻击。用户研究表明：BlindLock可在不改变原有图形记忆方式和增加最少解锁时间的情况下显著提升系统安全性、可用性和密码空间。

关键词 图案锁，智能手机，污迹攻击，肩窥攻击，认证

中图法分类号 TP309，TP393.08 **文献标识码** A

BlindLock：An Effective Pattern Lock System Against Smudge Attack

WU Ji-jie CAO Tian-jie ZHAI Jing-xuan

（School of Computer Science and Technology，China University of Mining and Technology，Xuzhou 221000，China）

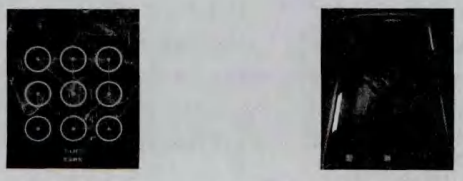
Abstract Recently，a growing number of mobile devices use pattern lock as the identity authentication mechanism. To unlock a smartphone，a user must draw a memorized graphical pattern with a finger on the touchscreen where the finger actually leaves its oily residues，also called smudges. The smudges can be exploited by adversaries to reproduce the secret pattern，so that the user's privacy is always revealed. Based on the research of the existing patten lock，we presented BlindLock as our main result. BlindLock can not only unlock in a pocket，but also use the cover principle to resist smudge attacks and use theory of visual occlusion to resist shoulder surfing attacks. Our user study also shows that BlindLock can significantly improve security，usability and password space of the pattern lock system while incurring minimal cost increase in terms of unlocking time and keeping the original graphics memory.

Keywords Pattern lock，Smartphone，Smudge attack，Shoulder-surfing attack，Authentication

1 引言

智能手机的快速发展改变了我们与手机进行交互的方式。我们经常用手指点击触摸屏来操作智能手机，使用各种互联网服务和应用程序等。因此，我们非常关心自己的智能手机的隐私问题。常见的身份验证方法有文本密码、PIN值和图案锁[1,2]。

Aviv等人提出污迹攻击，并提出图案锁易遭受污迹攻击[3-6]。Andriotis等人就智能手机的污迹攻击进行了具体阐述[7]：敌手利用污迹推断出解锁图案，从而达到破解图案锁的目的，如图1中的(a)和(b)所示，污迹攻击已经威胁到用户的隐私[8]。



(a)解锁图案 (b)解锁后屏幕上留下的污迹

图1 污迹攻击原理

图案锁的另一个安全问题是肩窥攻击[9-12]。用户经常在公共场所使用智能手机，敌手可以很容易地观察到用户的密码或使用相机等设备拍摄到，这种直接观察的攻击被称为肩窥攻击。我们需要更多的视觉闭塞来防范肩窥攻击。解锁操作通常是单手大拇指解锁，因为另一只手常占据主要或次要任务[13]。

回顾一些具有代表性的方案。(1)基于绘制的图案锁，例如Draw-A-Secret[14]和Passdoodles[15]。DAS要求用户在5×5的网格上验证图案，由于复杂的图案难于记忆和操作，使得DAS的可用性和实用性差。Passdoodles的解锁图案像我们触摸屏写字一样，没有网格约束，但解锁时间长且准确性差。(2)基于点击的图案锁，例如Passpoints[16]、GPI和GPIS[17]。Passpoints要求用户在一张图片上按顺序点击3个预设的像素点来解锁，缺点是准确性差和屏幕尺寸要求高。GPI和GPIS要求用户从许多小图片中选择出与解锁相关的图片，缺点是可用性差且难于记忆。

Android图案锁是现在最流行的图案锁，由谷歌在2010年开始推广。相对于其它密码，图案锁有着图案易于记忆和易于使用的优势[18]，事实也证明用户非常喜爱图案锁。

本文受江苏省"333工程"科研项目(BRA2014047)，江苏省"六大人才高峰"科研项目(2014-WLW-023)资助。

吴继杰(1988—)，男，硕士生，主要研究方向为信息安全，E-mail：756038169@qq.com；曹天杰(1967—)，男，博士，教授，主要研究方向为密码学与信息安全；翟靖轩(1982—)，男，博士生，主要研究方向为计算机安全和物联网安全。

Android图案锁采用3×3的网格作为用户认证界面，每个网格有一个网格点，用户需要精确的点击中心。用户需要用手指绘制出预设的图案，单向路径连接4～9个点。Android图案锁比4位PIN值安全性更高，据估计有389112种方案[3]。但容易受到污迹攻击和肩窥攻击。

在最近的工作中，Zezschwitz等人试图通过旋转和移动网格位置来抵御污迹攻击，但污迹攻击依然存在，只是改变了角度和位置[19]。Taekyoung Kwon等人提出了TinyLock是通过减小网格尺寸并涂抹操作区来抵御污迹攻击，小网格使得准确性下降，对应PIN值1到8的连线操作很难完成[20]。De Luca和Alexander等人提出的Back-of-device Shapes通过在手机背面的触摸屏上依次输入3个小图案，利用覆盖原理来防范污迹攻击。视觉闭塞使得系统很好地防范了肩窥攻击，但对硬件提出了要求(背面有触摸屏设备)，改变了图案的记忆方式且只支持双手操作[21]。

对于这些具有挑战性的问题，我们亟需一个满足视觉闭塞、扭曲污迹、单手大拇指操作和不改变图案记忆方式的、可用性高的解锁方案。鉴于此，我们提出了BlindLock图案锁。BlindLock系统无需复杂的软硬件，界面简单。根据Back-of-device Shapes的划痕覆盖原理来防范污迹攻击。对比Android图案锁手指的绝对移动操作，BlindLock图案锁手指的相对移动使得系统有着闭目解锁的优势，与许多研究者提出的移动设备eyes-free interaction相呼应[22]。视觉闭塞能有效防范肩窥攻击，例如在衣服兜里解锁给予完全的视觉闭塞。除此之外，还方便用户对手机的日常操作。

本文第3节介绍BlindLock系统，并对可用性和安全性进行简要分析；第4节将BlindLock图案锁与Android图案锁进行对比；最后总结全文。

2 威胁模型

在日常生活中，我们会频繁地使用智能手机，各种操作都会留下污迹，例如解锁、打电话、上网、使用应用程序和玩游戏。所以，污迹攻击在没有特定的设备和照明条件下很难完成[3]。在这里，评估一个最糟糕的情况，假设：(a)敌手拥有发动污迹攻击所需的设备和完美的照明条件；(b)在用户身份认证前触摸屏进行过清洁；(c)触摸屏上只留下解锁的污迹。

我们认为这是一个最好的执行污迹攻击的条件，就安全性来说，这是最糟糕的情况。

3 BlindLock图案锁系统

3.1 BlindLock概念

BlindLock又称“盲人锁”，这里指在视觉闭塞条件下进行解锁。将界面进行简单调整，如图2所示。网格区和周围的空白区域都可以进行用户操作，并且网格区会反馈用户图案绘制的情况。为了方便实验测试，在下面添加3个按钮，分别是设置密码、重置密码和校验密码。

图2(a)是BlindLock系统的解锁界面，光标处于起始位置。图2(b)和图2(c)是2个解锁图案。为了方便图形的记忆，将光标的走势约束在3×3的网格中，超出网格的部分将视为无效输入。允许的用户操作及网格中光标对应的走势见表1。

(a) (b) (c)

图2 BlindLock图案锁

表1 BlindLock系统的用户操作

允许的用户操作	网格中光标对应的走势
左划	←
右划	→
上划	↑
下划	↓
左上划	↖
右上划	↗
左下划	↙
右下划	↘
单击	光标不移动

注：用户操作的划痕可长可短。单击操作仅用于确定光标起始位置为图案起点，用⊙表示。

表2列出BlindLock的3个示例。每次进行解锁操作时，第一次的划痕都是起点，后续为绘制图案。示例1中，用户先左上划，选择最左上角的点作为起点，紧接着右划-右划-左下划-左下划，系统等待时间超过1s视为用户操作完成，系统将进行验证。示例2中，用户先单击屏幕，选择初始光标位置为起点，紧接着右上划-左划-左划-右划，同样地，系统等待时间超过1s视为用户操作完成，系统将进行验证。示例3所画的图案和示例2一样，但是划痕数不一样，将其视为与示例2不同的密码。示例1对应的图案如图2(b)所示，示例2和示例3对应的图案如图2(c)所示。

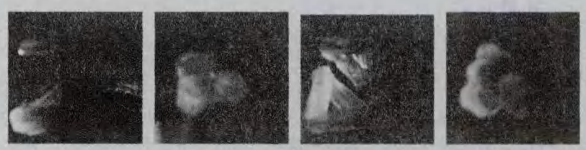
表2 BlindLock系统解锁示例

用户操作	选择图案起点	绘制图案
示例1	↖	→ → ↙ ↙
示例2	●	↗ ← ← →
示例3	●	↗ ← ← → → ↙

注：用户在触摸屏上的第一次划痕(或单击)是选择图案起点。

为了提高用户操作的准确率，满足各种用户需求，用户可以设置：是否反馈10ms短震动，是否显示网格区。

图3是Android图案锁和BlindLock图案锁在屏幕上留下的解锁污迹对比。



(a) Android-简单图案 (b) BlindLock-简单图案 (c) Android-复杂图案 (d) BlindLock-复杂图案

图3 Android图案锁和BlindLock图案锁在屏幕上留下的解锁污迹对比

图3(a)和(c)是在Android图案锁系统中留下的解锁污迹，可以很明显地辨别出解锁图案。图3(b)和(d)是相同图案在BlindLock图案锁系统中留下的解锁污迹，污迹已经模糊不清，很难重现解锁图案。

3.2 安全性分析

闭目解锁给予完全的视觉闭塞，有效地防范了肩窥攻击[15]。解锁操作通常是单手大拇指解锁，因为另一只手常占据主要或次要任务[7]，所以即便是把手机拿到眼前进行解锁，利用大拇指移动范围局限性的特点，留下的污迹区域也非常小。小的污迹区域在安全性方面有许多优点。首先，相比Android图案锁，BlindLock图案锁中手指挡住的有效绘图区更多，使得肩窥攻击更加困难。其次，BlindLock图案锁手指的移动范围小，保证BlindLock在解锁过程中手指仍然覆盖大部分有效绘图区。最后，移动区域范围小使得划痕覆盖得比较全面，使得污迹攻击更加困难。由此可知，小的污迹区域可以很好地提高可用性和安全性。从图3中得出，BlindLock的污迹已经被扭曲，图案越复杂，越难重现原有图案。

3.3 可用性分析

小的污迹区域在可用性方面也有许多优点。相比Android图案锁手指的绝对移动，BlindLock图案锁的相对移动可以减少手指的移动距离，支持闭目解锁，提高了系统可用性。在BlindLock系统中，用户可以继续利用最流行的3×3网格图形记忆，没有改变原来的图案记忆方式。用户可以设置显示网格反馈和短震动反馈，更好地帮助用户操作。考虑到用户在一个视觉闭塞的条件下进行解锁，例如从口袋里拿出手机需要一些时间，我们设置了1秒的认证等待时间，而不是通过单击来认证，使得系统更简单、更人性化。

3.4 BlindLock密码空间

BlindLock图案锁支持一点多次使用。图案采用最少3条划痕，最多8条划痕(不包括1个选点划痕或单击操作)。理论上的密码方案大概有3709750种，远比Android图案锁多。存储方案按照PIN值进行存储，例如图2(b)的存储用12357表示。

4 实验

将BlindLock图案锁和Android图案锁做比对，来评估BlindLock图案锁的性能。在整个实验过程中，记录了许多数据以供分析。注意：触摸屏在每次解锁操作前将进行清洁，并确保触摸屏上仅存在当前解锁操作留下的污迹。所拍摄的照片均是清晰的、高分辨率的，并且视角都是最佳状况。

4.1 实验环境

系统环境：谷歌Android 4.4平台；手机型号：联想S820(4.7英寸，1280 * 720像素)；相机：Canon HF S21。

4.2 实验设计

我们设计了一个组内重复测量的方案。第一步，评估BlindLock系统的可用性和安全性。第二步，评估BlindLock系统在长期使用下的可用性。下文中将用BlindLock和Android表示其对应的图案锁系统。

4.2.1 可用性设计

为了评估BlindLock的可用性，采用重复组内析因实验设计，独立变量为图案类型(简单图案和复杂图案)和图案锁系统(BlindLock和Android)。为了满足实验要求，对图案进行了筛选，使其满足上述的2种系统。复杂图案至少由6条划痕组成，简单图案由3或4条划痕组成。参与者的任务就是在各种独立变量组合下，输入正确的图案来解锁智能手机，每个组合至多尝试5次。各种独立变量组合顺序都被打乱，以减少学习效应。对于包含BlindLock的组合，将在后续两天重复第一天的实验来评估其在相同图案下长时间的可用性。

4.2.2 安全性设计

为了评估BlindLock的安全性，依然采用重复组内析因实验设计。独立变量依然是4.2.1节中的图案类型和图案锁系统。用户的任务是根据拍摄的照片来猜测其他用户绘制的图案。所拍摄的照片均是清晰的、高分辨率的，没有视角被遮挡和区域模糊的状况。照片上的污迹也都是当前解锁操作留下的污迹。假设有n个参与者，第i个参与者需要猜测第$(i \bmod n)+1$个参与者的关于Android系统的攻击照片和第$(i+1 \bmod n)+1$个参与者的关于BlindLock的攻击照片，其中$1 \leqslant i \leqslant n$。这样就避免同一个用户猜测相同图案下的污迹。同样地，模仿现实中的系统，每个变量组合最多猜测5次。

4.3 参与者

我们在当地大学请到19个参与者(10男，9女)。参与者都是正常视力，右手拇指操作手机。他们的年龄从19岁到47岁，平均为25.3岁，使用智能手机的平均时间为4.6年。其中了解图案锁的有19人，使用过Android图案锁的有18人。

4.4 实验步骤

4.4.1 评价程序的可用性

第一天，我们给参与者介绍了BlindLock和Android的使用方法，并让参与者熟悉系统。对于每个组合，参与者可以尝试3—4次，随后需要向我们展示一次成功认证。最后，参与者开始系统解锁，每个组合最多进行5次尝试。每完成一个组合，我们会对其成功解锁后留下的污迹拍照，记录解锁时间和认证结果。实验结束后，参与者将完成一个关于当前系统的问卷调查，问卷采用李克特量表。

第二天，重复第一天的实验，并且只告诉用户昨天绘制的图案，没有让其进行尝试，目的是看参与者是否记住了系统使用方法。

第三天，继续重复第二天的实验。

4.4.2 评价程序的安全性

为了让用户更好地填写调查问卷，给参与者详细介绍了污迹攻击和肩窥攻击的原理，并要求参与者通过污迹照片来猜测用户绘制的图案，每张照片至多猜测5次。参与者可以对照片进行任何操作。然后进行问卷调查，问卷依然采用李克特量表。

4.5 研究假设

我们进行了如下假设：

(H1)BlindLock解锁速度比Android慢。

(H2)BlindLock比Android更易出错。

(H3)BlindLock防范污迹攻击的效果比Android好。

(H4)BlindLock长时间使用解锁速度会变慢。

(H5)BlindLock长时间使用易出错。

4.6 实验结果

4.6.1 解锁时间

BlindLock的解锁时间从手指接触到触摸屏开始，一直到认证成功，BlindLock系统包括1s的认证等待时间。实验很好地模拟了现实中解锁所需的时间。图4展示了Android系统和BlindLock系统分别在简单图案和复杂图案下的解锁时间。表3中总结了数值结果。

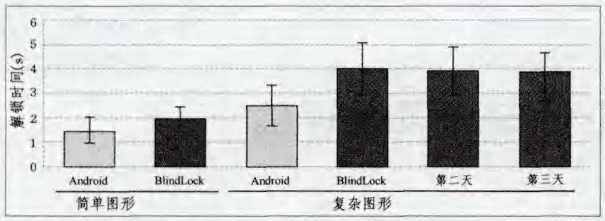


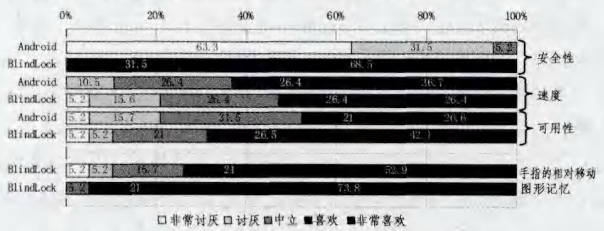
图 4　Android 图案锁和 BlindLock 图案锁分别在简单图案和复杂图案下的成功解锁时间

表 3　Android 系统和 BlindLock 系统在不同条件下的解锁时间(s)

组合	中值	平均值	最小值	最大值	标准差
Android-简单图案	1.414	1.432	0.965	2.030	0.310
BlindLock-简单图案	1.959	1.947	1.431	2.432	0.288
Android-复杂图案	2.359	2.492	1.667	3.337	0.467
BlindLock-复杂图案	3.813	4.035	2.931	5.084	0.628
BlindLock-简单图案-第 2 天	1.936	1.913	1.353	2.665	0.327
BlindLock-简单图案-第 3 天	1.884	1.887	1.371	2.365	0.262
BlindLock-复杂图案-第 2 天	3.861	3.914	2.921	4.882	0.512
BlindLock-复杂图案-第 3 天	3.759	3.904	2.684	4.653	0.533

最快的组合是 Android 简单图案(中值:1.414s;平均值:1.432s;标准差:0.310s),BlindLock 简单图案(中值:1.959s;平均值:1.947s;标准差:0.288s),Android 复杂图案(中值:2.359s;平均值:2.492s;标准差:0.467s)和 BlindLock 复杂图案(中值:3.813s;平均值:4.035s;标准差:0.628s)。通过 2×2(图案类型×图案锁系统)重复测量方差分析得出,比较大的影响因素有图案锁系统($F(1,18)=133.142$, n. s. $p<0.001$)和图案类型($F(1,18)=263.212$, n. s. $p<0.001$),图案锁系统和图案类型间之间的影响很小($F(1,18)=3.094$, n. s. $p=0.442$)。

根据图 5 中的调查问卷得出,参与者认为 Android(平均值:3.89;标准差:0.918)比 BlindLock(平均值:3.53;标准差:1.082)快。我们将其原因旧结于起始点选择和 1s 的认证等待耗费了时间。根据上述结果,我们认为 H1 成立。



问题:安全性-这个方法足够安全? 速度-认证速度足够快? 可用性-这个系统容易使用? 手指的相对移动对比 Android 的手指的绝对移动操作,你喜欢 BlindLock 的相对移动操作? 图形记忆-BlindLock 不会影响你对图形的记忆?

图 5　调查问卷得分率

4.6.2　出错率

我们测量了参与者是否可以在 5 次尝试中成功解开图案锁。

Android 系统中,大部分参与者在第一次尝试时成功解锁,有 2 位尝试了 2 次,而 BlindLock 全部在第一次尝试时成功解锁。我们认为其原因是 Android 网格距离大,大拇指的移动存在范围局限性,例如对角线这种远距离操作给手指的移动增加了难度。根据调查问卷,参与者认为 BlindLock(平均值:3.95;标准差:0.960)比 Android(平均值:3.47;标准差:1.082)更容易使用。我们认为原因是:手指更适合相对移动和小区域操作。

根据上述结果,我们认为假设 H2 不成立。

4.6.3　防范污迹攻击

在实验中,参与者分析污迹照片来猜测图案,每个组合尝试 5 次。实验结果表明,Android 系统的 48 个组合全部被猜测出来(破解率:100%),而 BlindLock 系统的 48 个组合全部错误(破解率:0%)。我们认为其原因是 BlindLock 支持 1 点多次使用、难以判断图案起点和大拇指的移动区域范围小使得步骤覆盖得比较全面。

根据调查问卷,参与者认为 BlindLock(平均值:4.68;标准差:0.456)的安全性优于 Android(平均值:1.42;标准差:0.561)。

根据上述结果,我们认为假设 H3 成立。

4.6.4　长期研究

在长期研究中,我们记录 BlindLock 的解锁时间数据。简单图案:第一天(中值:1.959s;平均值:1.947s;标准差:0.288s),第二天(中值:1.936s;平均值:1.913s;标准差:0.327s),第三天(中值:1.884s;平均值:1.887s;标准差:0.262s)。复杂图案:第一天(中值:3.813s;平均值:4.035s;标准差:0.628s),第二天(中值:3.861s;平均值:3.914s;标准差:0.512s),第三天(中值:3.759s;平均值:3.904s;标准差:0.533s)。利用 2×3 重复测量方差分析得:对于 BlindLock 系统,在相同图案下,长期使用对解锁时间没有明显的影响($F(2,36)=3.698$, $p=0.030$),相互之间也没有显著的影响($F(2,36)=0.753$, $p=0.474$)。图案类型是最大的影响($F(1,18)=216.267$, $p<0.001$)。

根据上述结果,我们认为假设 H4 不成立。

第二天,有一个人在第二次尝试的时候成功解锁,其余人全是在第一次尝试时成功解锁。第三天,所有人都在第一次尝试时成功解锁,时间上没有明显差别,我们认为假设 H5 不成立。

从而得出,BlindLock 在闭目条件下仍然有很快的解锁速度和很高的准确率。闭目解锁不仅能在日常中满足用户对手机的操作,更能有效抵御肩窥攻击。例如盲人使用屏幕锁保护自己的隐私,司机在行驶中解锁,以及公共场合中用户在口袋里进行解锁,来保护自己的隐私。

结束语　本文提出了一个称为 BlindLock 的新型模式锁机制,并且就安全性和可用性进行了评估。BlindLock 不仅能有效防范污迹攻击和肩窥攻击,更方便了人们的日常生活。在不改变原有图形记忆方式和增加最少解锁时间的情况下可显著提升系统安全性、可用性和密码空间。我们相信 BlindLock 可以应用于大多数的智能手机。

尽管 BlindLock 能有效防范污迹攻击和肩窥攻击,但它仍需要用户在闭目条件下(在口袋里或包里)解锁才能更好地抵御肩窥攻击。解锁时间有适当增加是让系统更具人性化。未来将继续研究更好的方法并将 BlindLock 系统改进运用在其它需要触摸的智能设备中。

参 考 文 献

[1] Suo X, Zhu Y, Owen G S. Analysis and design of graphical password techniques[M]// Advances in Visual Computing. Springer Berlin Heidelberg, 2006: 741-749

(下转第 385 页)

监控系统设计[J]. 农业工程学报,2013,29(S1):171-176

[7] Liu Jian-qi, Wang Qin-ruo, Wan Jia-fu, et al. Towards Key Issues of Disaster Aid based on Wireless Body Area Networks [J]. KSII Transactions on Internet & Information Systems, 2013,7(5):1014-1035

[8] 吕军,孙微涛,李彤. 基于栅格分簇的无线传感器网络路由协议[J]. 计算机工程,2014,40(2):97-101

[9] Ji Sai, Sun Ya-jie, Shen Jian. A Method of Data Recovery Based on Compressive Sensing in Wireless Structural Health Monitoring[J]. Mathematical Problems in Engineering, 2014, 2014(1): 1-9

[10] De Souza Evandro, Nikolaidis Ioanis. An exploration of aggregation convergecast scheduling[J]. Ad hoc Networks, 2013, 11 (8):2391-2407

[11] Liu An, Ning Peng, Wang Chun. Lightweight remote image management for secure code dissemination in wireless sensor networks[C]// IEEE the 28th Conference on Computer Communications. Rio de Janeiro, Brazil, 2009:1242-1250

[12] Weatherspoon H, Kubiatowicz J D. Erasure coding vs. replication: A quantitative comparison[C]// Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS 2002). MIT Faculty Club, Cambridge, MA, USA, 2002:328-337

[13] Gu Ren-tao, Zhang Lin, Ji Yue-feng. Secure and efficient metro-access network using network coding[C]// 2011 International Conference on Information Photonics and Optical Communications (IPOC). Jurong West, 2011:1-4

[14] Boykov Y, Kolmogorov V. An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2004, 26(9):1124-1137

(上接第 367 页)

[2] Suo X, Zhu Y, Owen G S. Graphical passwords: A survey[C]// 21st Annual Computer Security Applications Conference. IEEE, 2005:472

[3] Aviv A J, Gibson K, Mossop E, et al. Smudge attacks on smartphone touch screens[C]// Proceedings of the 4th USENIX Conference on Offensive Technologies. USENIX Association, 2010: 1-7

[4] Von Zezschwitz E, Koslow A, De Luca A, et al. Making graphic-based authentication secure against smudge attacks[C]// Proceedings of the 2013 International Conference on Intelligent user Interfaces. ACM, 2013:277-286

[5] Kim S, Yi H, Yi J H. FakePIN: Dummy Key Based Mobile User Authentication Scheme[M]// Ubiquitous Information Technologies and Applications. Springer Berlin Heidelberg, 2014:157-164

[6] Kim H W, Kang A, Barolli L, et al. Efficient locking scheme with OPOF on smart devices[M]// Advances in Computer Science and its Applications. Springer Berlin Heidelberg, 2014:369-378

[7] Andriotis P, Tryfonas T, Oikonomou G, et al. A pilot study on the security of pattern screen-lock methods and soft side channel attacks[C]// Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2013:1-6

[8] Airowaily K, Alrubaian M. Oily residuals security threat on smart phones[C]// 2011 First International Conferenceon Robot, Vision and Signal Processing(RVSP). IEEE, 2011:300-302

[9] Tari F, Ozok A, Holden S H. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords[C]// Proceedings of the Second Symposium on Usable Privacy and Security. ACM, 2006:56-66

[10] Schaub F, Deyhle R, Weber M. Password entry usability and shoulder surfing susceptibility on different smartphone platforms[C]// Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia. ACM, 2012:13

[11] Wu T S, Lee M L, Lin H Y, et al. Shoulder-surfing-proof graphical password authentication scheme[J]. International journal of information security, 2014, 13(3):245-254

[12] Chakraborty N, Mondal S. SLASS: Secure login against shoulder surfing[M]// Recent Trends in Computer Networks and Distributed Systems Security. Springer Berlin Heidelberg, 2014: 346-357

[13] Hirotaka N. Reassessing current cell phone designs: using thumb input effectively[C]// Extended Abstracts on Human Factors in Computing Systems(CHI'03). ACM, 2003:938-939

[14] Jermyn I, Mayer A, Monrose F, et al. The design and analysis of graphical passwords[C]// Proceedings of the 8th USENIX Security Symposium. 1999:1

[15] Wiedenbeck S, Waters J, Birget J C, et al. PassPoints: Design and longitudinal evaluation of a graphical password system[J]. International Journal of Human-Computer Studies, 2005, 63(1): 102-127

[16] Bicakci K, Atalay N B, Yuceel M, et al. Towards usable solutions to graphical password hotspot problem[C]// 33rd Annual IEEE International Computer Software and Applications Conference, 2009(COMPSAC'09). IEEE, 2009:318-323

[17] Shadmehr R, Brashers-Krug T. Functional stages in the formation of human long-term motor memory[J]. The Journal of Neuroscience, 1997, 17(1):409-419

[19] Von Zezschwitz E, Koslow A, De Luca A, et al. Making graphic-based authentication secure against smudge attacks[C]// Proceedings of the 2013 International Conference on Intelligent User Interfaces. ACM, 2013:277-286

[20] Taekyoung K, Sarang N. TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems[J]. Computers & Security, 2014(42):137-150

[21] De Luca A, Von Zezschwitz E, Nguyen N D H, et al. Back-of-device authentication on smartphones[C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013:2389-2398

[22] Li K A, Baudisch P, Hinckley K. Blindsight: eyes-free access to mobile phones[C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008:1389-1398