软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2017,28(2):361−371 [doi: 10.13328/j.cnki.jos.005023]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

# 一种随机剔除点的安卓图形解锁方案*

熊思纯, 杨 超, 马建峰, 张俊伟

(西安电子科技大学 网络与信息安全学院,陕西 西安 710071)

通信作者: 杨超, Email: chaoyang@xidian.edu.cn

**摘 要**: 安卓图形解锁(Android unlock pattern,简称 AUP)作为目前移动终端上使用最广泛的图形密码方案,实际应用的密码在理论空间上分布很不均匀,导致其实际安全性远低于理论安全性,所暴露出的巨大安全隐患极易被攻击者利用以加快字典攻击与暴力破解的速度.提出一种随机剔除点的安卓图形解锁方案(Android-unlock-pattern scheme through random points exclusion,简称 AUP-RPE).在设置密码阶段通过对原界面作一系列改动以规避用户具有安全隐患的使用习惯,并组织了 1 100 余人次的用户测试以收集实际应用的图形密码.建模分析发现,在保证与 AUP 相近的可用性前提下,AUP-RPE 的安全性提高了 3 个以上数量级,证明了该方案具有更高的安全性.

**关键词**: 图形密码;安全性分析;马尔可夫模型;猜测熵;安卓

**中图法分类号**: TP309

中文引用格式: 熊思纯,杨超,马建峰,张俊伟.一种随机剔除点的安卓图形解锁方案.软件学报,2017,28(2):361−371. http://www.jos.org.cn/1000-9825/5023.htm

英文引用格式: Xiong SC, Yang C, Ma JF, Zhang JW. Android unlock pattern scheme through random point exclusion. Ruan Jian Xue Bao/Journal of Software, 2017,28(2):361−371 (in Chinese). http://www.jos.org.cn/1000-9825/5023.htm

## Android Unlock Pattern Scheme Through Random Point Exclusion

XIONG Si-Chun, YANG Chao, MA Jian-Feng, ZHANG Jun-Wei

(School of Cyber Engineering, Xidian University, Xi'an 710071, China)

**Abstract**: As the most widely used graphical password scheme on mobile terminals, Android unlock pattern (AUP) is not quite uniformly distributed in its theoretical password space when in practical use, which exposes a tremendous hazard that can be easily exploited by the attacker to expedite dictionary attack or violence crack. To address this issue, this paper proposes a new scheme, Android-unlock-pattern based on random point exclusion (AUP-RPE), which helps the user to avoid habitual choices by the new interface arrangement. In addition, patterns in real-life use are collected by performing a large-scale user study with over 1 100 people. Modeling based on those patterns shows the entropy of AUP-RPE increases over 3 orders of magnitude than the entropy of AUP, which means that AUP-RPE has a much stronger security.

**Key words**: graphical password; security analysis; Markov model; guessing entropy; Android

长久以来,由数字字母构成的文本密码(text-based password)[1]是身份认证[2]的主要途径.心理学研究表明[3],人脑对图形化信息的记忆优于文字信息.此外,随着智能手机、平板电脑等设备的日益更新,图形化设备已成为人们生活中不可替代的通信工具,这使得采用图形化信息的认证方案——图形密码(graphical password)[4]成为一种更适合在图形化设备上使用的身份认证方案,其安全性研究已成为当前热点课题[5].现有的图形密码系统,按其认证过程的不同,大致可分为 3 大类.

1) 基于识别型(recognition-based):用户从由各种图片组成的网格中按顺序选出图片.比较具有代表性的有

* 基金项目: 国家自然科学基金(61672415, 61472310, U1405255)
Foundation item: National Natural Science Foundation of China (61672415, 61472310, U1405255)
收稿时间: 2015-09-07; 修改时间: 2015-12-02; 采用时间: 2015-12-27

RealUser 公司设计的 PassFaces[6].该方案通过识别网格中的人脸图片进行认证,文献[7]验证了其良好的可用性,但文献[8]指出 PassFaces 方案的图片选择受到性别、种族、肤色等特征的极大影响,难以建立一个图形密码设置的安全标准.所以,此类型的图形密码并没有投入到实际应用中.

2) 基于线索的回忆型(cue-based recall):利用图形化的提示信息降低用户回忆密码的难度.典型的有 CCP (cued click point)[9],在一组图片中点击每张图片的特定位置以完成认证.然而,图片信息显示的清晰度与屏幕大小、精度有很大关系,而且,此方案需存储大量图片以获取足够大的密码空间,这将占据不小的存储空间.因此,CCP 不能普遍应用于移动终端设备.

3) 基于回忆型(recall-based):要求用户重复以前的密码设定过程以通过认证.此类图形密码不需存储大量图片,对设备屏幕大小和精度要求也不高,有广泛的适用性,代表性的有 Jeymyn 等人设计的 DAS(draw a secret)[10].该方案设置阶段,用户在一个 2D 栅格上画出图形密码;认证阶段,DAS 根据画出的图形经过单元格的坐标顺序判断正确与否.文献[11]指出,DAS 尺寸限制了密码长度,且依赖于使用者所画的东西,易记性较差,并对 DAS 方案进行改进,提出了 Pass-Go 方案.与 DAS 不同的是,Pass-Go 方案利用 2D 栅格中网格线间的交点而不是单元格,通过给交点设置感应区域,用户划过感应区域即选择了该点,使栅格上的图形密码设计更加灵活,不再局限于水平方向与垂直方向,还可以连接对角线上的两点.通过对 167 人进行调查发现,用户使用 Pass-Go 的认证成功率达 78%,验证了 Pass-Go 方案良好的可用性.现今最常见的安卓图形解锁(Android unlock patterns,简称 AUP)[12]就是 Pass-Go 适应智能手机的一种具体应用,在 3×3 的九宫格形状的基础上,以网格线之间的交点为圆心形成 9 个感应区域(sensitive areas),并隐去网格线,使图形界面简单化以更适应人脑记忆,用户在此点阵上按照一定规则设置图案.

然而,近期 AUP 却被发现存在巨大的安全隐患.文献[13]对实际应用中 AUP 的密码强度以猜测熵(guessing entropy)的形式进行了测量.通过用户实验收集到近 2 900 个图形密码,在此数据上建模并发现这些图形的密码强度远低于理论上对应的密码强度:从密码熵值计算结果来看,理论上其安全性应与随机 5 位 PINs 相当,但在实际应用中安全性却低于随机 3 位 PINs.此外,用户使用习惯在很大程度上影响了实际应用中图形密码的安全性:高达 40%的用户选择左上角点作为密码的起始点;图案设计时笔划相对简单,如以直线形式连接水平、垂直或对角线上的 3 点;图案近似于某一特定形状,如字母、数字或几何形状等.这些使用习惯存在很大的安全隐患,极易被攻击者利用,从而提高攻击成功率.虽然文中给出了 4 种替代方案,但实验证明这 4 种方案并没有明显提高实际应用中图形密码的熵值:其中 3 种方案的熵值明显低于原方案,另一种方案的熵值也仅略高于原方案.而从人机交互角度看,这 4 种方案在可用性上均低于原方案.因此,这里并没有给出一种能够替代安卓图形解锁且行之有效的解决方案.

针对上述问题,本文提出一种随机剔除点的 AUP 认证方案——AUP-RPE(random-points-exclusion authenticating scheme based on android unlock patterns).我们将 3×3 点阵规模扩大到 4×4,在密码设置阶段,鉴于原方案四角处的点作为起始点的概率偏高或偏低,故将 4×4 点阵四角处的 4 点剔除,作为固定不可选点;为增大密码设置的随机性,在每次设置密码时,在剩余的 12 点中随机剔除两个点,即随机不可选点,因而每次可设置的点数为 10.由于两点是随机剔除的,故等价于在 12 个点中选取 4 个~10 个点设置密码,这在密码空间上要远大于 AUP 从 9 个点中选取 4 个~9 个点的情况.同时,为了测试评估实际使用过程中 AUP-RPE 的安全性,我们组织了 200 人模拟用户,收集到 1 169 个图形密码,在此基础上采用 5 折交叉验证(5-fold cross-validation)并建立三元的马尔可夫模型(3-gram Markov model),依此得出理论密码空间的图案在实际使用中出现的概率,计算出 AUP-RPE 的猜测熵:当攻击者按照此概率由大到小的顺序发起攻击时,达到某一攻击成功率所对应的攻击次数.结果表明,AUP-RPE 所做的改进,不仅保证了与原方案几乎相同的可用性,而且极大地提高了安全性,具有比安卓图形解锁更高的密码强度.

目前来看,在大规模的实际调查数据的基础上建模分析一种新方案的安全性是非常少见的,这使得 AUP-RPE 的安全性评估具有极大的现实意义.

## 1 AUP-RPE 图形密码方案

### 1.1 AUP-RPE方案设计思路

文献[11]通过对实际应用中的AUP进行实验分析发现,由于用户的使用习惯问题,实际应用中AUP的密码强度远低于其理论上的密码强度.具体表现有以下几点.

(1) 在起始点的设置上,40%以上的用户严重偏向于选择左上角点.

(2) 相邻点的选取,偏向于连接水平或垂直方向而不是对角线方向上的点.

(3) “三点一线”,以直线连接同一直线上的3点.

(4) 形似于特定符号,将图案设置成近似于某一特定字母、数字或符号的形状.

这一系列的使用习惯问题导致实际应用中的图形密码在理论密码空间上分布过于集中,利用率并不高,被攻击者利用后可显著提高攻击率.

因此,我们从两个方面考虑增强图形解锁方案的安全性.

(1) 在尽量不影响用户习惯的前提下,对密码设置界面做改动以强制用户改变可导致密码强度降低的使用习惯.方案的设计思想是在 AUP 的基础上做相应的改动,以规避用户设计出具有安全隐患的图形密码,将四角处的 4 点作为固定不可选点,再设置两个随机的不可选点,限定用户只能在剩余的 10 点中设置出图形密码.这样可避免四角处点使用过多或过少的情况的出现,打乱用户特定的使用习惯.

(2) 在尽量不影响用户使用方便性的情况下,增大密码空间,让攻击者的攻击难度成指数增加.主要措施是将AUP的3×3点阵规模扩大至4×4,且由于两点是随机剔除的,故等价于在12个点中选取4个~10个点设置密码,这在密码空间上要远大于在9个点中选取4个~9个点的情况,使密码空间增大了3个以上数量级.

### 1.2 AUP-RPE具体方案

针对用户的使用习惯问题,本文在原 3×3 点阵的基础上,通过对点阵布局做一系列调整以便能够在一定程度上使用户改变其原有的使用习惯,从而提出了一种 4×4 点阵的基于安卓图形解锁的改进方案——AUP-RPE.用户使用此方案设置密码仍遵循安卓图形解锁的规则.密码认证阶段采用的是一个普通的 4×4 点阵,如图 1 所示;密码设置阶段,如图 2 所示,在 4×4 点阵上做一些变动.

(1) 剔除四角处的点,使其不参与密码的设置,将其作为固定不可选点.

(2) 从剩余的12个点中再随机剔除两个点不参与密码的设置,将其作为随机不可选点.

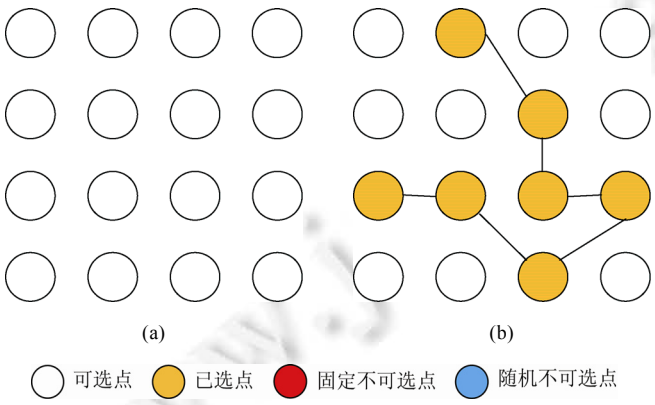



Fig.1 Loading interface

图 1 登录认证界面 可选点

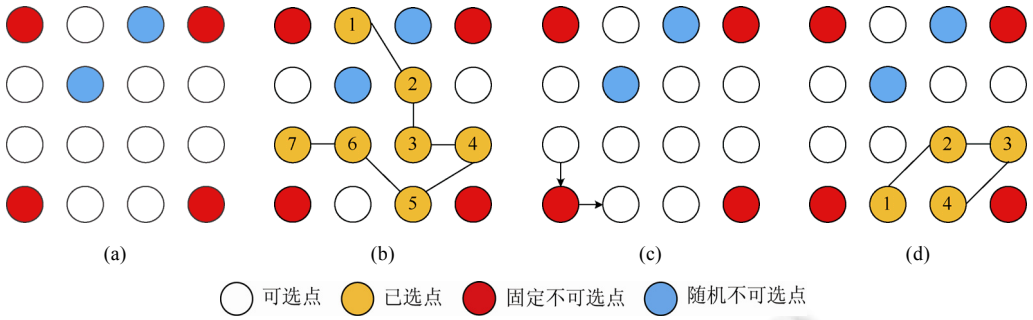



Fig.2 Pattern setting interface

图 2 图形密码设置界面 63

AUP 理论上可设计出的图形密码数目,即密码空间的大小为 389112≈$2^{19}$,若用户设置的图案在此密码空间上服从均匀分布,理论上的密码空间能够得到充分利用,则此方案的密码空间大小是足够的.然而,由于用户设置密码自身的使用习惯,使得实际应用到的图形密码在理论密码空间上分布得并不均匀.密码设置主要有以下两步.

(1) 进入图形密码设置的初始界面,如图 2(a)所示.

(2) 选定某一可选点作起始点,再在剩余的可选点中按使用规则设置图形密码,如图 2(b)所示.此时,若手指脱离屏幕,则黄色点的路径即为所设置的图形密码.

此外,若在密码设置过程中选取了固定或随机不可选点,则原已选择的路径将被系统认定为无效.例如,若在图 2(b)中的黄色点 7 后继续选择了左下角的红色点,此时界面恢复成图 2(a),继续往右如图 2(c)所示,选择路径如图 2(d)所示,此时又形成新的有效路径,如此,直至在可选点中设置一个路径长度在 4~10 的图案即为系统认定的合法图形密码.

尽管在设置密码时可供选择的点仅有 10 个,但由于两个随机不可选点是不固定的,在每次进入密码设置界面时都会改变,因而从 66 种不同密码设置界面中来看,这相当于实际可供选取的仍有 12 个,即在 12 个点中选取 4 个~10 个点,密码空间约达到 $2^{22}$.显然,此方案的理论密码空间远大于安卓图形解锁方案.

在输入密码进行认证时,展示给用户的是一个 16 个点均可选的点阵,尽管攻击者可能知道位于四角处的点并未参与密码设置,但由于每次用户设置密码时随机不可选点都不固定使攻击者无从知晓,因而在剩余的 12 个点中对密码实行攻击的难度明显高于 AUP 从 9 个点中进行猜测.

### 1.3 AUP-RPE方案实现

在 Android 4.3 平台上对 AUP-RPE 进行编码实现,为了实现对用户输入的图形密码进行记录以便建模分析,我们分别对 4×4 点阵中的 16 个点进行了编码,如图 3 所示,使每一个输入的图形密码能够转换成字符串的形式.

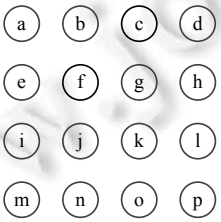
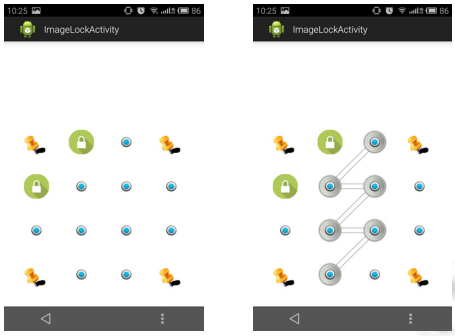



Fig.3 Encoding

图 3 编码

图 4(a)为图形密码设置界面,输入欲设置的密码,记录过程为从手指接触屏幕到脱离屏幕,如图 4(b)所示,则

记录下来的密码为“cfgjkn”.这里,密码的长度必须不小于 4,且被选择点必须是可选点,这样才能将字符串写入到指定的记录文件中.




(a) (b)

Fig.4 Implementation

图 4 实现

## 2 AUP-RPE 方案性能测试

为了验证 AUP-RPE 的可用性,我们进行了用户实验;为了评估 AUP-RPE 在实际应用环境下的安全性,对此次实验收集到的数据建模,并计算出一个衡量密码强度的值——猜测熵,并根据此熵值对 AUP-RPE 的密码强度进行分析与评估.

### 2.1 用户测试方案

为了在实际应用环境下对 AUP-RPE 与 AUP 的性能进行比较,我们在手机上分别实现了这两种方案,并组织了 200 名用户参与新方案的测试评估:参与者模拟用户设置密码,再模拟攻击者交叉猜测对方的密码.

首先,将 AUP-RPE 方案的使用规则介绍给参与者,参与者模拟用户,在手机上用 AUP-RPE 设置图形解锁密码,这是一种具有抵御攻击性质的密码,称为 Defensive AUP-RPE.此类密码要求“用户”设置的密码具有较高安全性,即在设置完成后能够抵御来自其他参与者的攻击;而又具有可用性,使用户在 30 分钟后仍能记住密码从而解锁成功.然后,在“用户”设置完密码到再次认证的 30 分钟内,参与者模拟“攻击者”,对其他“用户”设置的密码进行猜测以试图破解,这个过程所用到的密码具有“攻击性”,称为 Offensive AUP-RPE.

由于密码的设置与攻击都是在参与者中交叉进行的,因而,可分为以下 4 步.

(1) 设置一个密码(defensive AUP-RPE).

(2) 猜测他人的密码 2 次~5 次(offensive AUP-RPE).

(3) 等待 30 分钟以供“攻击者”猜测密码.

(4) 再次认证登录.

对于 AUP 方案,采取同样的步骤进行测试,得到 Defensive AUP 与 Offensive AUP.

一般而言,具有“防御性”的 Defensive AUP-RPE 安全性应高于具有“攻击性”的 Offensive AUP-RPE,故训练集与测试集均取自 Defensive AUP-RPE,而 Offensive AUP-RPE 将作为附加数据添加到训练集中去.这会带来两种不同的作用:训练集越大,求取的近似值就越精确.由于这两种数据来自不同的分布(Defensive AUP-RPE 来自安全性较强的分布,Offensive AUP-RPE 来自安全性较弱的分布),Offensive AUP-RPE 的加入会使计算得到的色熵值低于仅有 Defensive AUP-RPE 时的结果.

实验过程中,由于仅要求“用户”设置一个能够在 30 分钟内不被“攻击者”破解且 30 分钟内仍能记住的图形密码,即时易记性使得“用户”设置的密码强度比实际应用密码的强度更高.此外,参与此次实验调查的成员均为来自理工科院校的在读研究生,年龄在 20 岁~30 岁之间,男女比例约为 3:1,由于专业、年龄等限制,使此次收集

到的密码比一般情况下更专业化,安全性将略高于一般情况.尽管此次实验数据采集所面向的人群偏单一化,但采集的数据对于评估一种新方案来说仍然具有相当大的参考价值.

实验共收集到 defensive AUP-RPE 200 个,offensive AUP-RPE 769 个,defensive AUP 189 个,offensive AUP 569 个.

### 2.2 AUP-RPE方案建模

根据收集到的 AUP-RPE 与 AUP,在此基础上建立模型以分析安全性,具体细节如下所述.

#### 2.2.1 *n* 元马尔可夫模型(*N*-gram Markov model)

马尔可夫过程是具有马尔可夫性质的随机过程:在时刻 $t_i$ 所处的状态已知时,过程在时刻 $t(t>t_i)$所处的状态仅与过程在 $t_i$ 时刻的状态有关,而与过程在 $t_i$ 时刻以前所处的状态无关,也称为无后效性.

$$P(X_{t_{n+1}}=x \mid X_{t_1}=x_{t_1}, X_{t_2}=x_{t_2}, ..., X_{t_n}=x_{t_n}) = P((X_{t_{n+1}}=x \mid X_{t_n}=x_{t_n}).$$

在语音识别、概率文法等自然语言处理时,常根据当前字母的前几位来预测当前字母的出现概率.例如,在一个英文单词中,字母 *t* 后所出现字母为 *h* 的可能性明显大于 *q* 出现的可能性;而在安卓图形解锁的九宫格中,与当前的点距离越近,被选择的概率就越大.

基于这个相似之处,我们在计算图形密码的出现概率时采用这种 *n* 元马尔可夫模型[14],即某一位的出现取决于它的前 *n*–1 位.给定一个 *m* 位序列 $c_1c_2\ldots c_m$,用 *n* 元马尔可夫模型表示:

$$P(c_1c_2...c_m) = P(c_1c_2...c_{n-1}) \cdot \prod_{i=n}^{m} P(c_i \mid c_1c_2...c_{i-1}),$$

其中, $P(c_1c_2...c_{n-1})$ 为初始概率(initial probability), $P(c_n|c_1c_2...c_{n-1})$ 为转移概率(transition probability).由这两个概率可计算得出密码的出现概率.我们用从样本数据得出的频率来估计初始概率和转移概率.

#### 2.2.2 建立模型

从攻击者的角度考虑,在猜测用户密码时,对于理论上可能出现的密码,根据系统中实际用户的样本数据计算其出现概率,并将密码按出现概率由高到低进行排序,攻击者按此顺序对这一系统的用户密码进行攻击,即出现概率最高的密码将被最先用来进行攻击.在基于安卓图形解锁的改进方案中,根据给出的 4 条使用规则,可以用枚举的方法列出符合规则的可能设计出的所有图案.因此,利用一个训练集(training set)和一个测试集(test set),模型建立的实现算法如下:

(1) 选取训练集中出现频率较高的图案,使其在测试集中的出现频率也较高.

(2) 从训练集计算得出初始概率和转移概率.

(3) 根据 *n* 元马尔可夫模型计算所有图形密码的出现概率.

(4) 将所有图形密码按照出现概率由大到小进行排列.

(5) 在测试集上评估猜测次数.

对采集到的数据集进行 5 折交叉验证(5-fold cross-validation):将数据集平均分成 5 个互不相交的子集 $S_1,\ldots,S_5$.选择其中一个子集 $S_{i_0}$ 作为测试集,则训练集即为剩余 4 个子集的并集.这样,5 个子集中的每一个都做一次训练集,剩余 4 个子集的并集即为对应的训练集,最终结果取这 5 次的平均值.我们所取的样本容量约为 200,因此测试集的容量大小约为 50,而测训练集的大小约为 160.

#### 2.2.3 *n* 的选取

一般而言,当训练集中的数据足够多时,*n* 的取值越大,建模估算的结果就越准确.在我们的改进方案中,4×4 点阵中只有四角处的点始终不参与图形密码的设置,数据集大小为 300 且这些图形密码的平均长度为 5.59.因此,当 *n*=2 时,理论上有 12×11=132 种二元排列,实际的二元两点排列有 300×5.89–300=1377 个,即理论上的一种二元排列对应于实际的 1377/132≈10 个排列;当 *n*=3 时,理论上有 12×11×10=1320 种三元排列,实际的三元排列有 300×5.89–300×2=1077 个,即理论上的一种三元排列对应实际的 11671320≈0.88 个;当 *n*=4 时,理论上一种四元排列对应实际的 0.66 个.由于当 *n*=3 时,理论上每种排列与实际的比值更近似于 1,因此,*n*=3 时建立马尔可夫模型的效果最好.

2.2.4 密码强度计算

密码空间的大小衡量的是 AUP-RPE 在理论上的安全性,因而具有现实意义的密码强度分析应基于实际应用中的用户数据.猜测熵(guessing entropy)[15,16]正是基于用户数据来衡量密码强度,即当攻击者处于最佳状态时(按密码出现概率的降序进行猜测),破解全部密码所需要的攻击次数.熵值越大,密码就越复杂,密码强度也就越高;反之,熵值越小,密码就越简单,密码强度也就越低.

在实际应用中,要攻破系统中所有账户的密码难度很高,攻击者往往对攻破系统中账户达到某个百分比时所需的攻击次数更感兴趣,即部分猜测熵(partial guessing entropy)[17].也就是说,当某一系统中用户的密码被攻击者破解达到一定百分比时,所需攻击的次数.

设百分比为$\alpha$,满足 0≤$\alpha$≤1;攻击率达到$\alpha$时所需的攻击次数为$\mu_\alpha$,有:

$$\mu_\alpha=\min\left\{i_0\left|\sum_{i=1}^{i_0}p_i\geqslant\alpha\right.\right\},$$

这里,$p_i$表示第 $i$ 次猜测时破解密码的百分比.

攻击了$\mu_\alpha$次后,攻击成功率为

$$\lambda_\alpha=\lambda_{\mu_\alpha}=\sum_{i=1}^{i_0}p_i\geqslant\alpha,$$

根据上述条件,便可计算出部分猜测熵:

$$G_\alpha(X)=(1-\lambda_\alpha)\cdot\mu_\alpha+\sum_{i=1}^{\mu_\alpha}i\cdot p_i,$$

其中,$(1-\lambda_\alpha)\cdot\mu_\alpha$表示没有被攻击到的部分,$\sum_{i=1}^{\mu_\alpha}i\cdot p_i$表示被攻击到的部分.

然而,当面对许多密码时,我们希望用信息位来表示部分猜测熵[7]:

$$\tilde{G}_\alpha(X)=\log\left(\frac{2\cdot G_\alpha(X)}{\lambda_\alpha}-1\right)+\log\frac{1}{2-\lambda_\alpha},$$

其中,$\log\frac{1}{2-\lambda_\alpha}$用来使得到的熵值均匀分布.

这种用数学模型的方法计算的密码强度具有明确的意义,在某种程度上来说也是最佳的,因为它以数学的方法表示出密码对攻击的耐受能力,充分提供了一个对实际安全性的估计值.

## 3 测试结果评估

让参与此次实验的 200 名用户分别使用 AUP-RPE 和 AUP,先完成图形密码设置操作(包括首次输入设计的密码与再次确认密码两个阶段),然后交由他人来模拟攻击者猜测密码,再由原用户进行登录认证操作,最后对收集到的图形密码进行可用性与安全性分析与评估.

### 3.1 可用性评估

如表 1 和图 5 所示,对于 AUP-RPE 和 AUP 这两种方案,分别统计了参与者在图形密码设置阶段的所需时间分布情况,所有用户均在 60s 内完成密码设置,其中 60%以上的用户所需时间不超过 40s,而超过 90%的用户在 50s 内完成操作.图 6 显示了两种方案下,参与者进行密码设置与登录认证所需时间的平均情况,显然,尽管 AUP-RPE 在平均时间上仍然略多于 AUP,但两者的平均时间仍然十分相近.因而,AUP-RPE 进行密码设置与登录认证所需的时间,明确地体现了其具有良好的可理解性与易接受性.

**Table 1** Statics of password setting time and people counted

**表 1** 设置密码所需时间与人数统计

| 所需时间 | | ≤20s | ≤30s | ≤40s | ≤50s | >50s |
|---|---|---|---|---|---|---|
| 人数 | AUP-RPE | 6 | 26 | 121 | 188 | 12 |
| | AUP | 10 | 33 | 146 | 196 | 4 |

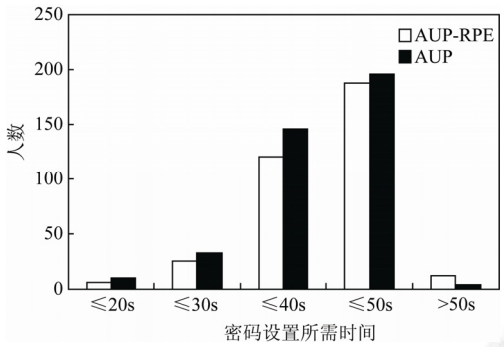



Fig.5 Distribution of password setting time and number of people

图 5 设置密码所需时间与人数分布

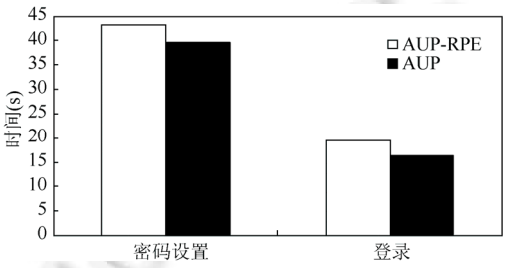



Fig.6 Average time needed for password setting and login

图 6 密码设置与登录成功所需平均时间

图 7 显示出参与者使用两种方案认证成功时所需尝试的次数与成功率的关系.显然,80%以上用户首次尝试即通过认证,超过 90%的用户在 3 次尝试内即通过验证.鉴于 AUP-RPE 方案的复杂性,两种方案的认证成功率非常相近.尽管 AUP 的认证成功率略高,但两者相近的较高认证成功率表明,AUP-RPE 充分保持了良好的易记性.

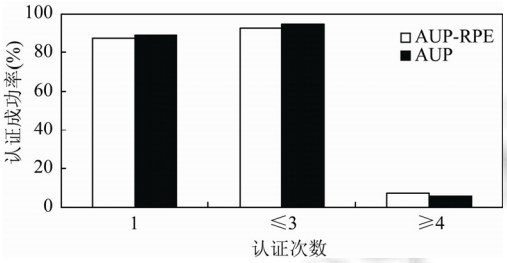



Fig.7 Login time and its success rate

图 7 登录次数及成功率

考虑到作为 AUP 的改进方案,AUP-PRE 在设计原理上复杂于 AUP,密码空间也远大于 AUP,因而在密码设置与登录认证所需时间、认证成功所需尝试次数与成功率等用户友好性测试结果中,AUP-RPE 与 AUP 的偏差均在合理范围内.两者非常相近的测试结果说明,对用户而言,AUP-RPE 方案仍具有与 AUP 相近的良好的可用性.

### 3.2 安全性评估

如图 8 所示,对收集到的图形密码建立如第 2.2 节所述的 3-gram 马尔可夫模型,由此计算出理论上所有图形密码的出现概率,如图 9 所示,并将这些图形密码按概率的降序排序.当攻击者按照理论上密码的出现概率由

高到低的顺序对系统中的用户密码进行猜测时,能够使其攻击效率达到最高.

| | | | | |
|---|---|---|---|---|
| cgfjkieb | hlkjef | fghlonie | iefgklhc | cfeghko |
| lgfeinkoc | knjfgh | fghjn | fegckolb | jgkolhn |
| fghjnb | bfgkjnl | gcko | ijkofbc | gjolhkn |
| ifbcgklho | ejkghlo | hgfjkonc | iecgkl | jfbn |
| ijkgchln | hlonjief | bfgkjn | jgokhln | jklfbch |
| jgklhbei | jklhoief | jnolh | fjkgclho | ifgjno |
| fokglhcbej | ejkgol | njfgh | njgkohl | efgkjil |
| ifjnok | efghkol | olhgfe | ifjgk | hgflkjno |
| ifbcgko | cghlon | njfkh | ifjgh | bfjkgo |
| ifjglob | hgfkol | njfkhc | ifcgkol | bfeijkln |

Fig.8 Graphical passwords in the form of string

图 8 以字符串形式记录的图形密码

| | |
|---|---|
| ejkgol | 0.000905091 |
| efghkol | 0.000209512 |
| cghlon | 0.000419024 |
| hgfkol | 0.000628536 |
| cfjokg | 7.85669e-005 |
| hgfjnkl | 0.000235701 |
| feijb | 0.000235701 |
| flhg | 7.85669e-005 |
| fjnkgol | 2.99303e-005 |
| einokh | 2.99303e-005 |

Fig.9 Probability of graphical password

图 9 图形密码的出现概率

如表 2 所示,分别计算当攻击者对 AUP-RPE 与 AUP 的攻击率$\alpha$达 10%,20%,50%时的猜测熵,并进行比较.由于用户为自己设置的抵御他人攻击的密码安全性高于其“攻击”时所使用的密码,因而 Defensive AUP-RPE 在用户密码安全性上更具代表性.同理,Defensive AUP 的安全性高于 Offensive AUP.故我们主要将 Defensive AUP-RPE 与 Defensive AUP 做比较:当攻击率$\alpha$为 10%时,两种方案的安全性相近,AUP-RPE 的熵值略低于 AUP;当攻击率$\alpha$为 20%时,AUP-RPE 的熵值高于 AUP,则改进方案的安全性高于原方案;当攻击率$\alpha$达到 50%时,AUP-RPE 的熵值明显高于 AUP,这表明 AUP-RPE 在安全性上有非常显著的提高.

**Table 2** Entropy comparison of two schemes

**表 2** 两种方案的熵值比较

| Schemes | $\alpha$=0.1 | $\alpha$=0.2 | $\alpha$=0.5 |
|---|---|---|---|
| Defensive AUP-RPE | 8.67 | 9.33 | 14.95 |
| Offensive AUP-RPE | 8.48 | 9.15 | 13.48 |
| Defensive AUP | 8.72 | 9.10 | 10.90 |
| Offensive AUP | 8.44 | 8.78 | 9.16 |

图 10 更详细地显示出攻击率的增长(纵坐标)与猜测次数(横坐标)的增长关系.总体来看,当攻击率在 0~20%时,AUP-RPE 与 AUP 所对应的猜测次数非常相近;当攻击率超过 20%以后,两种 AUP-RPE 的熵值曲线均明显位于 AUP 熵值曲线的下方,这表明当达到相同的攻击率时,AUP-RPE 的熵值更高,所需的攻击次数更多.此外,两种方案的图形密码中具有 Defensive 性质的密码熵值曲线均高于具有 Offensive 性质的密码熵值曲线,更直观地说明了用户为保护自身隐私而设置具有 Defensive 性质的密码,其安全性高于其用以攻击他人账户的密码,即当攻击率相同时,具有 Defensive 性质的密码所需的攻击次数更多.

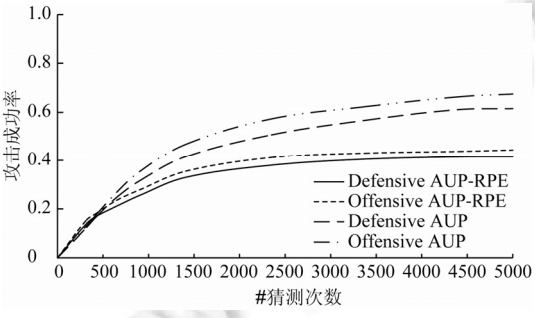



Fig.10 Diagram of the relation between attack rate and attack frequency

图 10 攻击率与攻击次数的关系示意图

图 11 显示出向原 Defensive AUP-RPE 训练集中分别加入 50,100,200 个 Offensive AUP-RPE 后,攻击率的增长(纵坐标)与猜测次数(横坐标)的关系.不难发现,当加入的 Offensive AUP-RPE 使训练集样本容量逐渐增大时,计算得到的图形密码所对应的出现概率更近似于实际概率,从而更有利于攻击率的提高;然而,由于加入的

Offensive AUP-RPE 均来自比 Defensive AUP-RPE 的密码强度更低的分布,可能导致最终计算得到的图形密码出现概率偏离于实际率.因此,当满足相同分布的训练集容量逐渐增大时,相同的猜测次数将达到更高的攻击率,也即同一性质的训练集样本容量越大,攻击者获得的信息就越多,也就越有利于提高攻击效率.

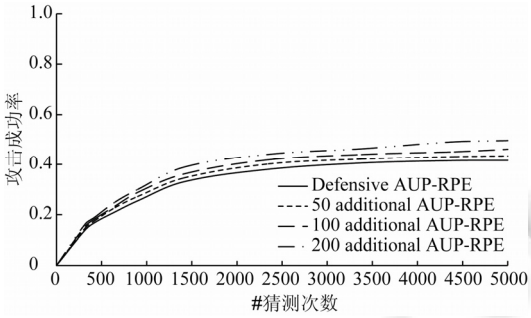



Fig.11 Impact of training set upon attack rate and attack frequency

图 11 训练集对攻击次数与攻击率的影响

综合以上分析,AUP-RPE 在图形密码设置所需时间、认证所需时间及成功率上都与 AUP 十分相近,在安全性分析中更具有远远大于 AUP-RPE 的密码熵值.这表明新方案在保持了与原方案几乎一致的可用性的基础上,极大地提高了图形密码的安全性,充分说明了 AUP-RPE 的良好实用性.

## 4 讨论与结论

AUP-RPE 是进行较大规模调查,基于用户数据建模并以熵值形式计算实际应用中密码强度的安卓图形解锁改进方案.它在认证阶段是普通的 4×4 点阵,在密码设置阶段,剔除 4×4 点阵四角处的点,剩余的 12 个点在每次设置密码时随机剔除其中两点,即每次参与密码设置的仅有 10 个点,这既保证了密码空间大于原方案,又在一定程度上规避了用户原具有安全隐患的使用习惯,避免了 AUP 中用户使用四角处点过多或过少的问题,而且 AUP-RPE 方案在攻击率达到 20%后,熵值明显大于 AUP,攻击者在攻击 AUP-RPE 时达到相同攻击成功率时通常比 AUP 需要更多的攻击次数,因而,AUP-RPE 的攻击难度更高,具有比 AUP 更高、更强的安全性.

AUP-RPE 着重于通过改变图形密码设置界面的布局,使用户规避具有安全隐患的使用习惯,所设置出的密码在密码空间上分布更均匀,使攻击者难以利用用户的使用习惯来加快字典攻击和暴力破解.因此,攻击者对某一系统用户密码了解得越少,实行字典攻击或暴力破解的难度越高,从而达到提高图形密码的熵值与安全性的目标.如果将 AUP-RPE 的大小再扩展到 5×5,6×6,那么,尽管密码空间越来越大,但设计出的图形也越来越多,密码强度也将随之增大,但考虑到手机屏幕的大小以及用户难以记住复杂的密码,如何在提高安全性的同时兼顾可用性又是一个值得探究的问题.AUP-RPE 在提高安全性的同时兼顾了可用性,具有良好的实用性.

**References**:

[1] Spafford EH. Opus: Preventing weak password choices. Computers & Security, 1992,11(3):273−278. [doi: 10.1016/0167-4048(92)90207-8]

[2] Hu XX, Zhang ZF, Liu WF. Universal composable password authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2011,22(11):2820−2832 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3910.htm [doi: 10.3724/SP.J.1001.2011.03910]

[3] Standing L, Conezio J, Haber RN. Perception and memory for pictures: Single-Trial learning of 2500 visual stimuli. Psychonomic Science, 1970,19(2):73−74. [doi: 10.3758/BF03337426]

[4] Biddle R, Chiasson S, Van Oorschot PC. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 2012,44(4):No.19. [doi: 10.1145/2333112.2333114]

[5] Qing SH. Research progress on Android security. Ruan Jian Xue Bao/Journal of Software, 2016,27(1):45−71 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[6] Passfaces Corporation. Passfaces. http://www.passfaces.com

[7] Brostoff S, Sasse MA. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In: People and Computers XIV—Usability or Else! London: Springer-Verlag, 2000. 405-424. [doi: 10.1007/978-1-4471-0515-2_27]

[8] Davis D, Monrose F, Reiter MK. On user choice in graphical password schemes. In: Proc. of the 13th Conf. on USENIX Security Symp., Vol.13. USENIX Association, 2004.

[9] Chiasson S, van Oorschot PC, Biddle R. Graphical Password Authentication Using Cued Click Points. Berlin, Heidelberg: Springer-Verlag, 2007. [doi: 10.1007/978-3-540-74835-9_24]

[10] Jermyn I, Mayer AJ, Monrose F, Reiter MK, Rubin AD. The design and analysis of graphical passwords. In: Proc. of the Usenix Security. 1999.

[11] Tao H, Adams C. Pass-Go: A proposal to improve the usability of graphical passwords. Int'l Journal of Network Security, 2008, 7(2):273−292.

[12] Tafasa. Patternlock. 2010. http://www.tafasa.com/patternlock.html

[13] Uellenbeck S, Dürmuth M, Wolf C, Holz T. Quantifying the security of graphical passwords: The case of android unlock patterns. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. ACM, 2013. 161−172. [doi: 10.1145/2508859.2516700]

[14] Castelluccia C, Dürmuth M, Perito D. Adaptive password-strength meters from Markov models. In: Proc. of the NDSS. 2012.

[15] Cachin C. Entropy measures and unconditional security in cryptography [Ph.D. Thesis]. Swiss Federal Institute of Technology Zürich, 1997.

[16] Massey JL. Guessing and entropy. In: Proc. of the IEEE Int'l Symp. on Information Theory. IEEE, 1994. No.204. [doi: 10.1109/ISIT.1994.394764]

[17] Bonneau J. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2012. 538−552. [doi: 10.1109/SP.2012.49]

**附中文参考文献**:

[2] 胡学先,张振峰,刘文芬.标准模型下通用可组合的口令认证密钥交换协议.软件学报,2011,22(11):2820−2832. http://www.jos.org.cn/1000-9825/3910.htm [doi: 10.3724/SP.J.1001.2011.03910]

[5] 卿斯汉.Android 安全研究进展.软件学报,2016,27(1):45−71. http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

**熊思纯**(1992－),女,湖南娄底人,硕士生,主要研究领域为网络与信息安全.

**马建峰**(1963－),男,博士,教授,博士生导师,CCF 会士,主要研究领域为网络与信息安全,密码学.

**杨超**(1979－),男,博士,副教授,CCF 专业会员,主要研究领域为网络与信息安全.

**张俊伟**(1982－),男,博士,副教授,CCF 专业会员,主要研究领域为密码学,网络安全.