解锁iOS手势密码的正确姿势

演讲者：姜若芾

平安科技 银河实验室成员

手势密码介绍

解锁姿势

加固手势密码锁

什么是手势密码？


4:37 下午
12月8日 周日
紧急呼救

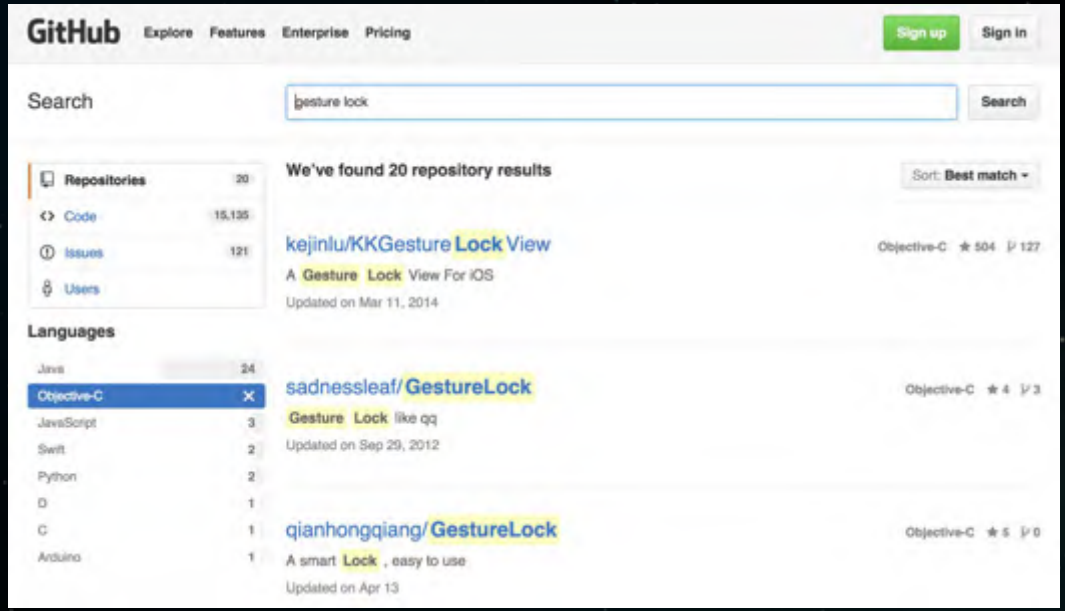

中国移动
下午6:13
19%
手势密码设置
手势密码
绘制解锁图案


6:12
CREATE A NEW PATTERN
Connect points to create a pattern!
Cancel
Next

传统密码 VS 手势密码

	数字密码	复杂密码	手势密码
组成	纯数字	字母、数字、部分符号	图形点位，可以映射成一串数字序列
位数	较少	可以很长	一般4~9位
安全性	较低	高	中
用户体验	中	差	好

实现原理


GitHub
Explore
Features
Enterprise
Pricing
Sign up
Sign in
Search
gesture lock
Search
Repositories 20
Code 15,135
Issues 121
Users
Languages
Java 24
Objective-C
JavaScript 3
Swift 2
Python 2
D 1
C 1
Arduino 1
We've found 20 repository results
Sort: Best match
kejinlu/KKGestureLockView
A Gesture Lock View For iOS
Updated on Mar 11, 2014
Objective-C ★ 504 ⑂ 127
sadnessleaf/GestureLock
Gesture Lock like qq
Updated on Sep 29, 2012
Objective-C ★ 4 ⑂ 3
qianhongqiang/GestureLock
A smart Lock , easy to use
Updated on Apr 13
Objective-C ★ 5 ⑂ 0

实现原理

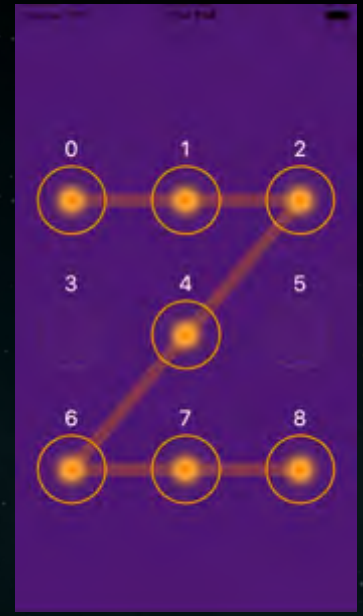
两个关键回调函数：

```
//开始绘制手势密码
- (void)gestureLockView:(KKGestureLockView *)gestureLockView
didBeginWithPasscode:(NSString *)passcode;

//手势密码绘制完成
- (void)gestureLockView:(KKGestureLockView *)gestureLockView
didEndWithPasscode:(NSString *)passcode;
```

实现原理

@”0,1,2,4,6,7,8”



市场现状

主要出现在带有金钱、用户隐私信息的金融、工具、社交类应用中

基本同时有两处以上安全漏洞

手势密码介绍

解锁姿势

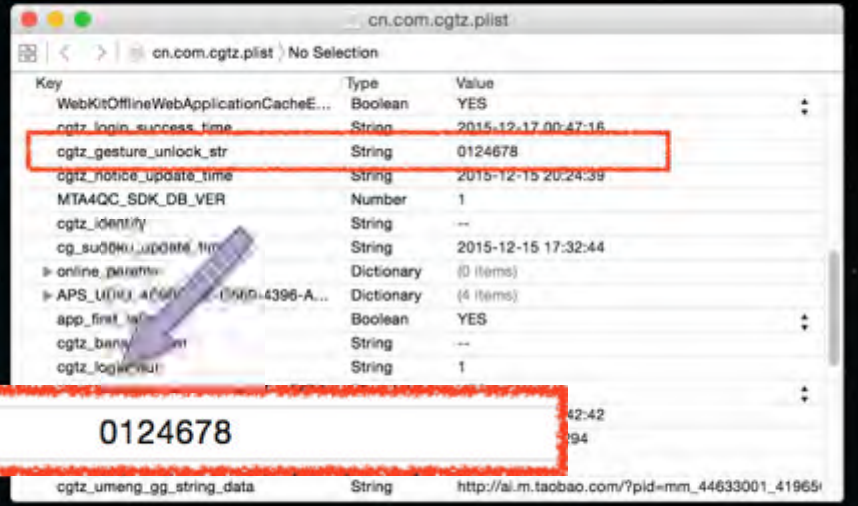
加固手势密码锁

姿势[0] – 飞行模式越过手势密码

- 飞行模式
- 连续输错5次
- 后台关闭应用

姿势[1] – 修改文件重置手势密码

- 本地配置文件
- 明文或单次MD5
- 剩余尝试次数



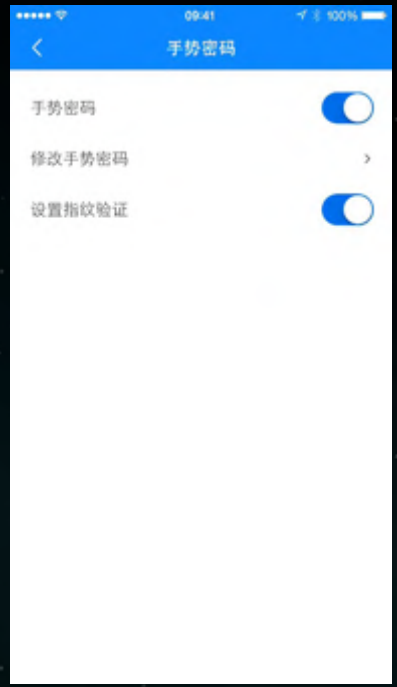
cgtz_gesture_unlock_str	String	0124678

姿势[2] – “偷窥”手势密码

- 控制类中某变量
- 还原后的明文密码
- 暴露在内存空间

姿势[2] – “偷窥”手势密码

- 控制类中某变量
- 还原后的明文密码
- 暴露在内存空间

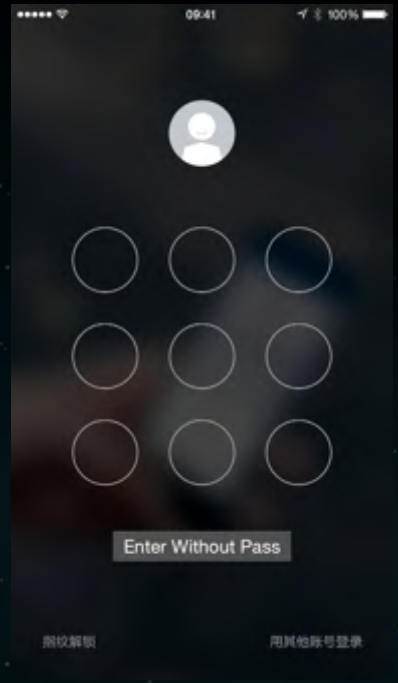


姿势[3] – 芝麻开门

- 校验密码成功的回调方法暴露
- 注入应用
- 调用成功回调方法

姿势[3] – 芝麻开门

- 校验密码成功的回调方法暴露
- 注入应用
- 调用成功回调方法



姿势[4] – 买通密码审判官

- 校验密码方法暴露
- 返回布尔值
- Hook后返回YES

姿势[4] – 买通密码审判官

- 校验密码方法暴露
- 返回布尔值
- Hook后返回YES

姿势[5] – 暴力破解手势密码

- 修改剩余尝试次数
- 密码可能性

$$P_9^9 + P_9^8 + P_9^7 + P_9^6 + P_9^5 + P_9^4$$

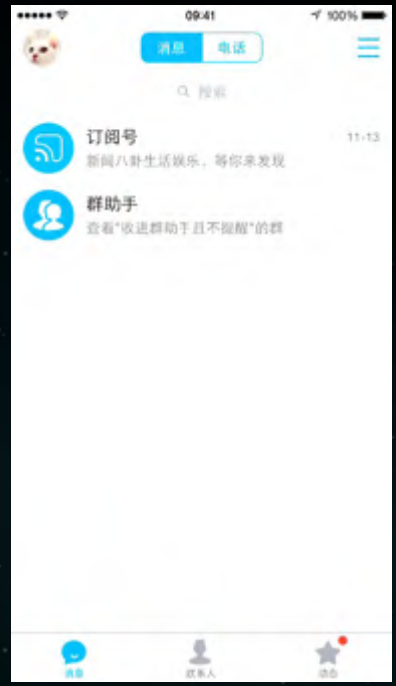
1,218,588

姿势[5] – 暴力破解手势密码

- 修改剩余尝试次数
- 密码可能性

$$P_9^9 + P_9^8 + P_9^7 + P_9^6 + P_9^5 + P_9^4$$

1,218,588



编号	应用		类别	本地存储	内存明文	方法暴露	校验Hook	暴力破解
1	京东金融		金融			✗		✗
2	QQ		社交				✗	✗
3	阿里钱盾		工具		✗			✗
4	QQ安全中心		工具			✗	✗	✗
5	阿里云		工具			✗		✗
6	借贷宝		金融	✗	✗	✗		✗
7	百度理财		金融	✗		✗	✗	✗
8	点融网理财		金融				✗	✗
9	草根投资		金融	✗		✗		✗
10	铜板街		金融	✗		✗		✗

手势密码介绍

解锁姿势

加固手势密码锁

加固手势密码 – 敏感信息处理

优化本地存储

优化密码校验逻辑

加固手势密码 – 应用层面

隐藏关键代码

代码混淆

反调试

加固手势密码 – 行为验证

绘制时间

屏幕触摸事件

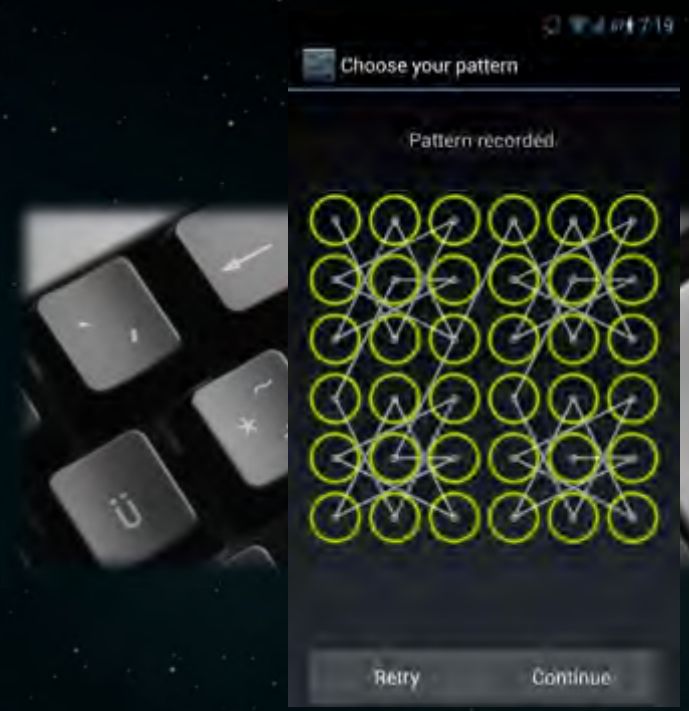
功能点日志分析

加固手势密码 – 反暴力

延时验证

联网验证

*添加节点



后记

模块化

越狱

本地认证的安全性

安全与业务的平衡

后记

模块化

越狱

本地认证的安全性

安全与业务的平衡

Thanks