安全小课堂第八十一期【APP手势密码安全】

京东安全 京东安全应急响应中心 1月15日

越来越多的支付功能和手机绑定在一起。为了使用方便，手机APP上通常默认一次输入密码后，在相当长一段时间内就不会再需要输入密码，让不少人担心手机丢失后被人盗取信息、金钱，于是越来越多的APP推出了手势密码，比输入密码简单，又能防盗。但是，手势密码真的安全么？

JSRC **安全小课堂第八十一期**，邀请到**剑影**作为讲师就**APP手势密码安全**为大家进行分享。也感谢白帽子盆友的精彩提问与互动~

师傅能不能简单介绍一下手势密码？

京安小妹

剑影：

手势密码是一种保护机制，接触到最多的就是手机的开机解锁了，但APP也有手势密码，APP手势密码存在的目的就是为了保护用户的安全利益，在手机被他人操控的时候能够很好的保护用户自身的利益，手势密码方便快捷，安全性高，被广泛的运用在各类APP当中。

讲师

那手机APP中的手势密码与传统密码相比，具有哪些更好的安全优势呢？

京安小妹

剑影：

以前传统的手势密码是默认4位数字，现在有些是6位数字，传统的手势密码具有限制性，最低4位，最高6位，可被暴力破解，很久之前苹果不就被爆出了可被无限制爆破锁屏密码得问题嘛，而手机应用当中的手势密码一般最低4位，最高可9位，那么安全性得到保障，相比输入密码，滑动手势密码图案来解锁具有更高效性以及更安全性。

讲师

手机APP中，哪些手势密码是不安全的？

京安小妹

剑影：

密码简单，复制程度低等都是不安全的，而且如果用户的设备已经被ROOT过，那么也极有可能不安全。

讲师

手势密码绕过的思路有哪些？能否详细说一下

京安小妹

剑影：

分为两种环境：

①：普通权限环境

②：高权限环境

无需ROOT环境手势密码绕过的思路

0x01 利用APP广告绕过

本来打算想到网上找例子，但是没有找到。一般APP都会在启动页面时加载广告，此时，如果验证不当，当你点击广告后直接返回一下，就可以绕过手势密码。

0x02 利用多重启动绕过

这个多重启动也是我之前很早发现的思路，之前发现以为必须要ROOT环境，后来发现完全不需要，直接打开APP，停留在APP手势密码输入页面，此时我们按Home键返回到桌面，随便打开个应用市场，再搜索这个APP，此时由于你已经下载了这个APP，那么它显示的就是打开，这时你点击打开，它会又重新启动一次APP，如果验证不当，可导致直接绕过手势密码，进入到APP。

0x03 利用退出绕过&爆破

这个问题也是我在很久之前测试中发现的，当然，现在这种问题很多APP还是存在的，希望尽快修复这方面的问题。一般手势密码允许输入的错误次数为5次，当错误次数达到了5次了，就会需要重新登录，而这时这个超过次数的信息可能会以弹框来提醒，或者直接显示在TextView，也就是直接显示在手势密码界面上，这都不是问题，不要点击任何界面，比如它弹出了手势密码次数超过限制框框，信息框下方会有个确认的按钮，不要点击，我们直接返回到桌面，然后清理掉后台的APP，有时候会清理不干净，导致还是在后台运行着，这可能会导致失败，所以，为了测试成功起见，到设置里找到相关的应用，然后选择强制停止，然后再次打开APP，这时如果验证没做好，就会直接进到主页面，或请输入新的手势密码页面，或者会再次跳出手势密码验证界面，这时跳出的手势密码验证页面就存在爆破的问题，因为现在你又有5次机会输入手势密码，以此思路循坏，可造成对手势密码的暴力拆解。

0x04 利用清理不当绕过

一些APP会这样储存手势密码，把手势密码储存在本地文本信息里，把账户的登录状态信息储存在本地数据库里，当清理掉这个本地数据后，实际上它并没有清理掉登录信息也就是并没有清理掉本地数据库信息，而是清理掉了本地文本信息，这就导致了清理掉了手势密码，而登录状态还是保持的，就导致了绕过问题。另一个思路比如你直接卸载再安装同样是这个原理。

0x05 利用显示不当绕过

一些APP当你启动APP的时候，它会在短时间内进入到或者说可以点击到APP内的某些功能，此时你只要一直点击这个页面，只要够快，就可以绕过手势密码，到达这个功能界面。

0x06 利用APP自带提示绕过

一些APP会自带提示，比如在状态栏内时不时推送一些信息，如果验证不当，直接点击推送的信息，就可以直接绕过手势密码，直接进入到主页面。

0x07 利用显示不当绕过

这个我从来就没遇到过，APP手势密码验证界面会出现设置按钮，直接设置没有加以验证从而绕过。

0x08 利用清理缺陷绕过

跟刚刚那个说的很像，也是手势密码跟账户信息储存在不同处，而最后只清理掉手势密码没清理掉登录信息的问题，在需要手势密码验证的界面点击忘记手势密码，此时会跳转到登录界面，直接返回到桌面，清理掉后台运行的APP，再次打开就直接进入到主界面，并且是登录状态。

0x09 利用界面设计缺陷绕过

以前看到过相关问题，问题是出现在IOS下的，所以我就列出来了，当进入到手势密码界面，可以左右滑动，从而滑动到主页面，绕过手势密码，这个问题可能已经很少软件存在了。

总结：

以上思路有些是我自己测试过程中所发现的，有些是网上的，以上思路都是在无需ROOT环境下或越狱下实现的，但是IOS下的软件这里面的思路基本很少可以实现，因为这些思路主要是android 下的APP问题。现在很多大型APP有一半都存在这个问题，希望各大厂商下的SRC尽快去修复或者白帽子发现了尽快提交，避免对用户以及自身产品造成影响。

以上是无需各种环境的，下面这些是需要高权限的环境下的绕过思路。

ROOT权限下绕过手势密码的思路

(修改时所需要的软件：RE管理器、Sqlite编辑器)

0x01 利用拒绝服务绕过

通过分析APP，找到跟手势密码相关的组件，利用拒绝服务攻击可直接绕过手势密码到达主页面，因为都是不同的Activity，当这个Activity停止后，就会跳转到下个Activity，而下个Activity就是主页面，从而绕过了手势密码，这类问题可利用ADB命令进行测试。

0x02 修改shared_prefs目录下的文件从而绕过的思路总结

我为了省略一些不必要的分类，就把所有关于这个目录下的绕过方式归类到这第二种思路内，方便大家阅读吸收。在我挖掘这方面问题的这么久以来，我把容易出现的点尽可能详细的描述出来。在这个文件夹内我们只看XML，有些备份的文件就没必要看了，在这么众多的文件内怎么找到关于这个手势密码相关的文件内， 这里我就给大家说下我的技巧吧，我的技巧其实很简单，比如你修改手势密码时过1分钟后再修改，因为你进入APP时会加载信息，此时文件时间会同步变动，等在设置手势密码那里我们停住，等过1分钟再修改，这时，就可以筛选出相对来说比较精确的文件了，这时再一一查看，全都是一大串加密的值就没必要去看，参数相对来说很少且基本都是time值，也没必要去看，后面可以通过相同的方法再来一次筛选。

经过如上你找到了储存手势密码的文件后，就可以开始修改了，这里我说下相关的思路。

第一种思路：修改文件权限

你可以把它的读权限去掉，只留下写入权限，如果APP验证不当，当你启动APP后它便会调用设置手势密码的界面，因为你没有读权限，那么只有写，误以为你需要设置手势密码，然后就调用设置手势密码的界面，从而绕过了手势密码验证。当然也可以把所有权限全部去掉，不让它加载手势密码，那么直接启动就行。

第二种思路：修改文件内容

当修改权限这种思路无用时，就得需要修改内容了。在文件内找到手势密码，看手势密码是否加密，如果加密看能否得知加密方式以及明文信息，比如是base64或MD5等一些常见加密，那就去解密，便可得到密码，直接输入密码就行。如果加密方式无从得知，可以测试当关闭手势密码后手势密码的值，如果这时这个参数内的值被清空或者这个参数被删除了，就可以利用这种方式清空这个参数或参数值，如果当手势密码关闭时这时还是存在值，可以复制这个关闭时产生的值用在另一个账户当中，看能否强制关闭，如果没有做校验那么就可以直接强制关闭另一个账户的手势密码，达到绕过目的。

这里我说下我的一个小技巧，可能这个问题会困扰到很多挖掘这方面问题的白帽子，在你修改这个文件时，你可能会发现你明明修改了，但是APP无任何变化，比如你都禁用了任何权限了但是却还是没有任何变化，都修改了文件内容但是又恢复到原来的内容了，此时问题不是APP做了什么验证和限制，而且你没有彻底的清理掉后台运行的APP进程，当你修改时，其实它一直在运行着，运行着是不能修改文件的，就好比你修改电脑上正在运行的软件的文件一样，只不过在手机上你修改文件时看不到任何关于APP正在运行无法修改文件的提示，而电脑上就会提醒，所以你应该到设置内或快捷方式找到对应APP，选择强制退出，然后再修改文件，再打开，就可以了。网上我实在是找不到这相关的例子，找到了一个但是也只是很简单的明文显示问题，这让我很无奈。

第三种思路：修改目录权限
当你发现修改对应的文件没有作用的时候，可能是你找错了或者修改有问题，这时你可以尝试修改这个shared_prefs目录权限，把读写权限全部去掉再运行APP，这时就可以绕过手势密码。
0x03 修改databases目录下的文件从而达到绕过
同样是利用上面的方法找到相关手势密码所存放的数据库文件。当你找到了储存手势密码的相关文件，我这里就说下相关思路。
提前说下，如果你打开数据库文件出现这个：打开数据库发生错误（code：14）提示
其实有很多思路，你可以修改权限，具体是修改哪里的权限我忘记了，好像是修改这个数据库文件的权限，或者数据库目录权限，把执行权限都勾上，具体请自己去测试下。
也可以直接把这个数据库文件复制到本地目录也就是sdcard目录下，就可以正常打开，因为权限允许，然后修改后再覆盖回去，再修改好相关权限即可。
第一种思路：修改数据库文件内容
如果手势密码是明文存放在数据库文件内，可以通过Sqlite编辑器找到对应的数据库文件，修改里面内容，同样，如果加了密可以尝试解密，如果不行，进行不断测试，看当无手势密码时这个数据库里的值得内容变为什么，如果为空，那么就可以直接清除掉当前的内容就可以绕过，如果是其它值同样复制下这个关闭下的值去替换到另一个账户不同的数据库当中看能否关闭手势密码，如果能，那么问题就存在。
第二种思路：修改数据库文件权限
当第一种思路不行时，你可以尝试修改当前数据库文件权限，把所有权限去掉，看能否绕过。
第三种思路：修改数据库目录权限
如果都不行，那么可能是你找错了文件或者修改出错，可以直接修改目录权限，把所有权限去掉或者只去掉执行权限，看能否绕过
0x04 修改files目录的文件从而达到绕过
这个也是我在测试中发现的问题，有时候这个目录下会存放着手势密码相关的文件，在这里你可以根据我上面说的思路找出具体是哪个文件，然后不停开关手势密码查看其内容已经其它文件是否跟着变换，也可以尝试修改文件权限或者目录权限。
如何找到手势密码存放在哪里？关键就是我上面说的方法，不断修改观看其目录和文件时间是否同步变换跟随，这里说下，有些目录时间跟你修改时间不同步但是其目录里的文件是同步了的，比较隐蔽，比如你修改了手势密码，根据修改时间找相关的目录以及文件，但是一些目录它时间还是以前的时间，不细心的可能就会直接不看，但是我都会去看的，然后里面的文件最近修改的时间就是我刚修改手势密码的时间，所以细心很重要，如果不注意这个问题，你可能就找不到这个问题的存在或者需要花费很久的时间才能找到了。 ：

讲师

有哪些手势密码绕过的案例？

京安小妹

剑影：

这里是乌云漏洞库的镜像，我收集了一些案例：
①：http://wooyun.jozxing.cc/static/bugs/wooyun-2016-0177256.html
②：http://wooyun.jozxing.cc/static/bugs/wooyun-2015-0127528.html
③：http://wooyun.jozxing.cc/static/bugs/wooyun-2013-036972.html
④：http://wooyun.jozxing.cc/static/bugs/wooyun-2013-040714.html
⑤：http://wooyun.jozxing.cc/static/bugs/wooyun-2012-014456.html

：
讲师

防止APP手势密码绕过的防御方法有哪些？

京安小妹

剑影：

要时常的更新APP和手机系统，手机不要去ROOT，保持良好的上网行为，设置的密码程度要复杂点。 ：

讲师

白帽子提问：

有没有一些开发建议，即以上种种的绕过，能不能从开发层面去防护？

剑影：

1.合理的启动方式 2.手势验证码加校验 3.若手势密码被修改，自动清除登录状态信息

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心