**20170727分享主题“手机安全相关”整理**

# 1 分享背景

大家好，我是uniker，目前在华通银行从事APP和SDK相关产品的研发。前期群里面很多大牛给分享了很多干货，也在里面学习到了很多，今儿就由我来介绍下移动开发安全相关的内容，抛个砖。11年~13年左右我在某家从事金融服务的公司主要负责开发支付SDK产品、MPOS产品。今天就结合之前产品中使用到的技术来简单谈一下app安全的问题。

主要内容如下：

（1）信息安全介绍

（2）移动安全介绍

（3）实际应用中的一个简单流程探讨

# 2 分享内容

## 2.1信息安全介绍

信息安全这里主要介绍一下，加密相关的知识。目前加密主要分为对称加密和非对称加密两种方式。其中所谓对称加密简单说就是加密明文和解密密文使用同一个密钥串，就像我们家里的门锁，家庭成员每个人都有相同的一把钥匙，可以打开同一锁。当然你的钥匙如果丢失，就存在这被盗的风险。所以对称加密，密钥的分发和存储就比较重要了。

对称加密的优势就是加解密的速度较非对称加密高效，对我们服务端和app来说都没有什么压力。

目前对称加密常见的算法有DES，3DES，AES等。

除了对称加密，还有非对称加密的方式。非对称加密在数据加解密的时候分别用到了公钥和私钥。这里公钥和私钥是成对出现，仅有公钥要求在当前计算能力内很难或无法推测出私钥。其中公钥主要用于对外发布使用，允许一定范围内公开。

非对称加密的优势安全性较对称加密更高，但是非对称加密涉及到复杂的运算，导致效率上来讲比对称加密率差一下。非对称加密典型的算法就是RSA算法。

实际中，一般会将对称加密和非对称加密结合起来用。

上面是加密方式的简单介绍，除了对称、非对称，这里提一下散列函数。

散列函数（或散列算法，又称哈希函数，英语：Hash Function）是一种从任何一种数据中创建小的数字“指纹”的方法。散列函数把消息或数据压缩成摘要，使得数据量变小，将数据的格式固定下来。这是wiki上对散列函数的定义。

通过一定的算法，将任意长度的数据流散列成指定长度的字符串。散列函数要求通过值无法逆向推出源输入的数据。常见的散列函数有MD5，SHA256，SHA128等。

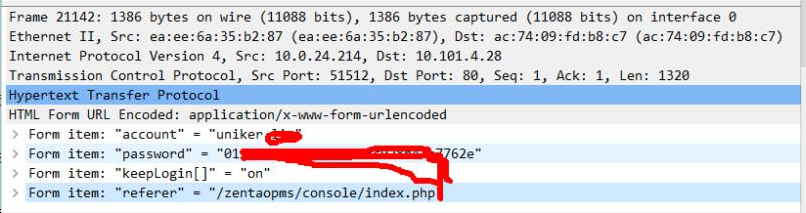
这里提一个人，[王小云](https://baike.baidu.com/item/王小云/29050?fr=aladdin)，当年震惊国内外的破解MD5第一人。还有就是今年Google已经可以通过计算破解SHA1。所以MD5和SHA1在使用中需要注意了。

上面是密码相关的基础知识点，大白话表述，应该可以理解。

## 2.2 APP安全介绍

app安全，我总结下来可以从3方面着重考虑：通信安全设计、应用安全设计、业务安全设计。

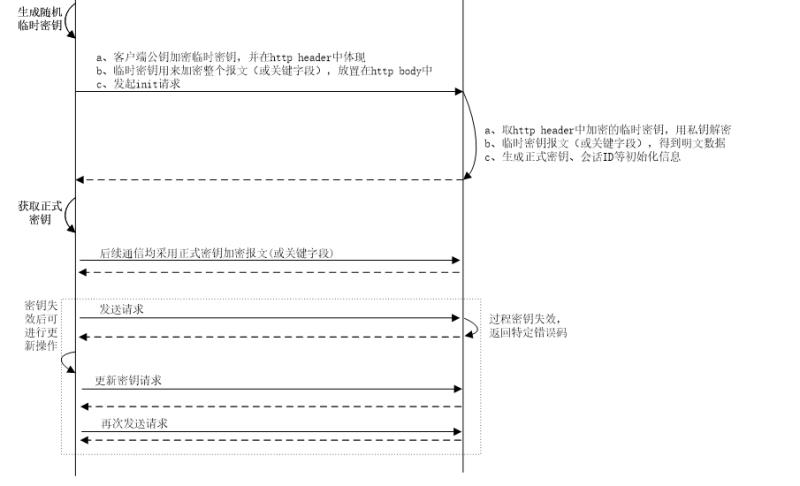
首先通信安全设计，目前APP和服务交互的方式绝大多数是基于HTTP方式。但是HTTP方式传输是明文传输，通过截取数据包，可以直接看到明文数据。



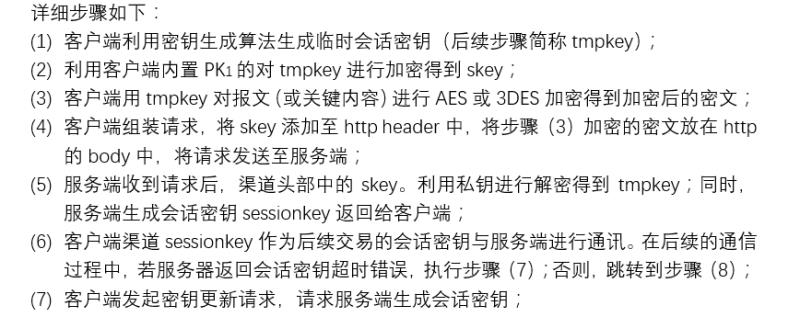
下午，我简单抓了一个包，里面有登陆用户名，密码hash值数据。

如果是普通应用，数据安全要求不高的情况下，http简单高效，没有问题。但是涉及到支付、账户等，http就显得苍白无力。所以，通信层安全在金融类、支付类APP里，至少应该是HTTPS方式来进行通信，这里建议HTTPS在应用实现上尽量要做单向认证

## 2.3 应用层安全设计



这个交互图左边是客户端，右边是服务端。里面结合RSA、DES/AES实现了密钥协商和密钥更新的逻辑。



上面截图是简单的说明，这里就不展开了。

应用层安全，还有so加固（Android需要重点考虑）、代码混淆。现在市场上很多安全公司提供成熟的方案，不展开。

在支付流程中，需要用户输入密码，这个太重要了，这里要重点摆一摆，对于做金融软件的人来说，看到密码，有点害怕，生怕没有保护好。密码这个东西，太重要了，重要到什么地步了，借用前领导一句话，不仅要防外贼，还要防内贼。要求除了用户知道，加密机知道，在整个业务流中不能出现密码的明文。所以现在有很多密码控件的厂商提供密码解决方案，这里简单介绍下之前实施的支付SDK中的密码键盘的思路。

1. 密码一次一密，用户每次输入密码，均在JNI层加密保存在内存中；

2.so文件要禁止调试；

3.一旦发起网络请求，6个密码解密后拼装PINBLOCK，立马用公钥（单独用于密码加密的公钥）加密，网络请求发出，密码所有相关数据清零；

4.密码要求做到防重放攻击，可以通过时间戳，特定业务码的方式来实现；

5. 防止截屏和监听点击事件，要求密码乱序展示及点按无状态。

上面是密码控件的一些实践。

## 2.4业务层安全设计

这里提一个事件，若干年前，某银行的登陆验证码被不法分子用来做了转账，并且成功的将客户的资金转走。这个要说明什么呢？就是我们在设计支付类业务的时候，要考虑到是否有空子被不法分子利用，导致客户的资金风险。业务层安全常用的方式就是接入一些自建或第三方的反欺诈平台。前期有大牛对反欺诈做过很精彩的分享，这里就不具体展开了。

## 2.5 结语

好，今天的移动安全大概就这些内容，最后说一句，安全无小事，对客户负责，对自己负责。感谢大家，如有问题，请多多指正。

## 2.6 Q&A

Q：Web端的密钥怎么存才安全呢？还有业务时序怎么控呢？

A：这个问题专业，我了解到的一种方案是通过后端生成密码图片，前端取坐标计算，但是这种方案密码要在server端落地一次。

Q： 请教下，现在市面常用互联网交易报文，一般什么加解密和签名方式？

A：现在native app已经有支持国密和国际两种了，但是web的主要还是国际

Q：加密机的原理和灌密钥的过程可以讲下？

A：加密机这块有专门的安全部门负责，一般我们接触不到，不过这里我可以问问有没有资料可提供

## 2.7 业务安全设计其他补充讨论

逻辑问题和权限绕过等业务设计缺陷造成的漏洞是最大的安全隐患，因为无法进行通用的防护，比如经典的密码找回漏洞。

密码找回凭证太弱，容易被爆破。如4位验证码

密码找回凭证可以从客户端、URL中直接获取。如短信验证码出现在返回的数据包中

密码找回凭证可以在网页源代码中直接获取

密码找回的邮箱链接易猜解，如时间的md5

密码找回凭证存并非只是与单个用户并绑定的问题

密码找回的手机或邮箱从页面获取，可以通过firebug修改，并可以重置作保用户的密码

Session紊乱

重置密码时返回的token没有与账号以及验证码绑定

服务器只验证了对应的验证信息是否存在，没有验证是否与账号匹配

提交新密码时的，只验证了部分可控的信息是否匹配

……

扩展阅读：《[**谈谈用户体验与风控的平衡性**](https://mp.weixin.qq.com/s?__biz=MzI0MjA1Mjg2Ng==&mid=2649867358&idx=1&sn=6959f35aba89ab107383acafc1255654&chksm=f1075e33c670d72504ed0afab51f68172a3713104e254b92dd2e0026fb50b249be873b2a9f31&mpshare=1&scene=1&srcid=07253MeuqxqPPgsQ12jSFJjW#rd)》

风控是用来保障业务发展的，而不是遏制业务发展的，风控会导致用户体验下降，这是必然的，但应该遵循一些保障用户体验的原则，比如渐进原则，比如防范策略友好度原则。要对风险容忍度有认识，寻求用户体验与风控的平衡点。比如自绘的随机键盘，安全性是高了，可体验不好

# 3 自由讨论

## 3.1 征信

Q：下下周我和领导去觐见人行征信司的领导，大家有没有什么尖锐问题要问的？

A：怎么看待乐视员工作用卡额度被降为一元？额度不是根据个人征信情况而来的吗？公司情况就决定个人征信了？

建行估计因为乐视断交社保了，又怕员工找不到工作，所以就一起全部降额度了

建行信用卡一元额度的问题，乐视不是第一家。

## 3.2 小额交易手续费收取方式

Q：请教一下，对于小额交易（没有保底手续费），乘以千分比之后也收不到手续费，如果一天所有的订单都是小额交易，即使汇总金额很大也收不到手续费。所以一般手续费计费的时候是逐笔计费，还是汇总计费呢？比如商户每笔都是1元，根本收不到手续费

A1：如果是10元 手续费也是几分 应该也是收得到阿

A2：现在的手续费有些就是银行自己补贴了，例如一分钱，扣除手续费2分还要负资8分，这样的规则就直接挂账了，银联那边是这样干的

A3：银联有保底手续费8分钱，收单机构对商户很多都不设保底手续费，这种情况下，比如1元的交易，0.2%手续费，收不到钱，如果这个商户一天有1000笔1元的交易，汇总后是能收到，但逐笔计算手续费收不到钱。

Q：一般收单机构手续费计算，是逐笔计费还是汇总计算呢？

A：微信是逐笔的