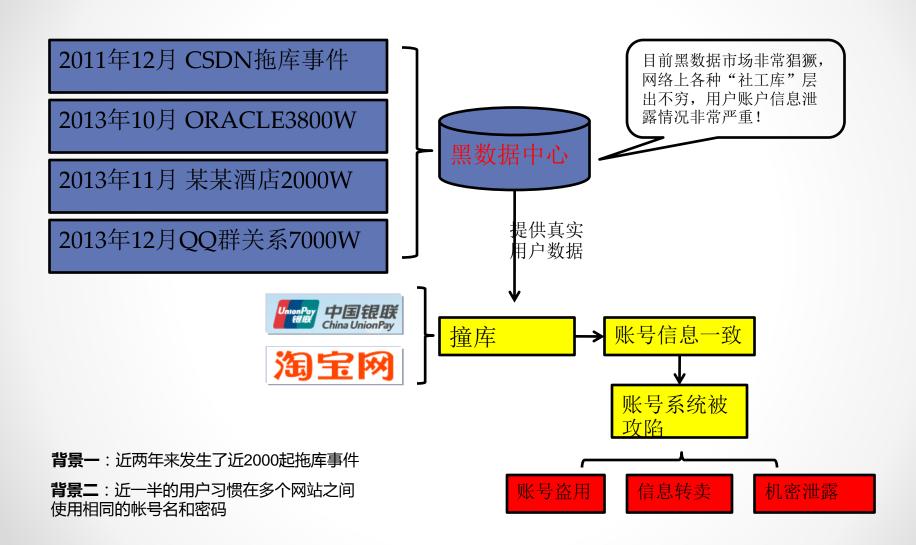
移动应用安全的新挑战

Sea Salt

目录

1	账号安全问题
2	移动安全问题
3	交易安全问题

账号安全:传统"账号-密码"体系脆弱



Are you a sheep

* 账号-密码泄露:

试试你的QQ关系是不是泄露了:

https://s3.amazonaws.com/qqqun/index.html

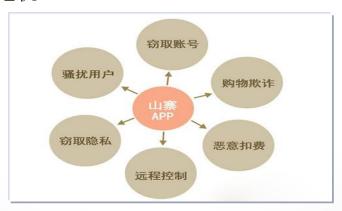
* 移动端问题更大:

支付宝客户端密码保护措施:

http://blog.csdn.net/androidsecurity/article/details/8666954

移动安全: Android平台成病毒温床

- 据去年的统计结果,仅2012年,CNCERT监测和网络安全企业通报的移动互联网恶意程序样本有162981个,较2011年增长25倍,其中约有82.5%的样本针对Android平台,已成为移动平台第一重灾区,这主要是缘于Android平台的用户数量快速增长和Android平台的开放性。
- * 而按照恶意程序的行为属性统计,恶意扣费类的恶意程序数量仍居第一位,占39.8%,流氓行为类(占27.7%)、资费消耗类(占11.0%)分列第二、三位。2012年,CNCERT组织通信行业开展了多次移动互联网恶意程序专项治理行动,所重点打击的远程控制类和信息窃取类恶意程序所占比例分别较2011年的17.59%和18.88%大幅度下降至8.5%和7.4%。
- * 目前一些APP大面积被山寨,存在泄露隐私的风险,同时由于APP山寨版和正版外观相似,要一眼分辨存在困难。其实,除了一些App被山寨外,还面临着被破解、二次打包、数据篡改、注入等危机。



移动安全:"梆梆"、"爱加密"看起来很美

- * 目前针对Android市场山寨APP众多的情况,应运而生了例如"梆梆加密"、"爱加密"等针对Android APP的安全服务商,为独立开发者和厂商提供APP加固方案,加固效果一度受到业界重视,看起来很美。
- * 但这些安全提供商却有着不能视而不见的弊端:
 - (1)返回给独立开发者和厂商的加固后APP,不提供反向验证手段,独立开发者和厂商不知道加固后的APP是否内置后门。
 - (2) 由于加固条件未做完备的限制,导致被病毒利用,目前已有多款病毒应用(例如最新的"支付宝大盗")利用梆梆加固进行安全加固,躲避杀毒软件的查杀。
 - (3) 单独的APP加固不足以实现真正的移动安全,易被攻破:

```
44:45:51
                                                            android.support.v4
                                                                                                 BuildConfig.class MainActivity.class
                                                            ii - ⊞ accessibilityservice
                                                                                                 package com.example.testbangbang;
群主号召一下,大家一起搭个服务器,自动解密梆梆
                                                            в врр
                                                             吧
                                                             database
                                                                                                   public static final class attr
                                                             graphics.drawable
                15:54:57
                                                             n hardware.display
                                                             media
支持時
                                                             net
                                                                                                     public static final int activity_horizontal_margin = 2130968576
public static final int activity_vertical_margin = 2130968577;
                                                            n ⊕ os
⊕ ⊕ print
                       15:55:08
                                                             ⊞-∰ text
                                                             util
6.3
                                                            ⊕-∰ view
⊕-∰ widget
                        15:55:23
                                                            com.example.testbangbang
                                                             BuildConfig
                                                            ⊕ ☑ MainActivity
⊕ ☑ R
最近发现大批用梆梆加固的病毒。
                                                                                                     public static final int action settings = 2131230720
梆梆这是要干嘛啊!!
                   15:55:23
可以搞一个自动化的工具 哈哈哈
                  15:55:25
                                                                                                     public static final int action_settings = 2131034113;
不支持的会被认为是梆梆的么。。 支持一下
                                                                                                      ublic static final int app_name = 2131034112;
ublic static final int hello_vorld = 2131034114;
      45:55:51
                                                                                                   public static final class style
免费提供解密梆梆技术支持。
```

移动支付,安全是关键!

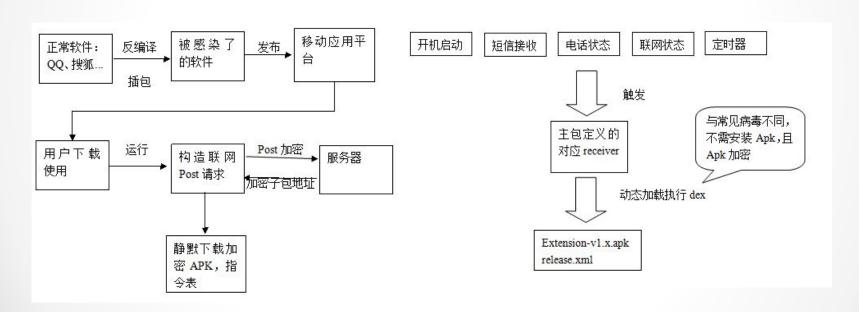
- * 移动支付属于 金融范畴。
- * 体系重点: 联 网通用、安全 可信
- * 需补充用户隐 私保护体系。



中国移动支付技术标准体系

"套餐窃贼"病毒

"套餐窃贼" (Extension)病毒于2012年9月规模性出现,在2013年1月后开始集中爆发,于2013年1月25日首先发现。套餐窃贼不同于以往的手机病毒,具有全面的控制能力,和极强的隐身能力,本身也具有联网升级的能力,还可以通过接受其他加密应用来不断扩展自身能力。该病毒已经进化到了一个新的高度,是里程碑式的手机病毒软件。



移动支付面临的挑战 - "套餐窃贼"类的智能病毒!

Thanks!