如何完成一份像样的互联网金融APP安全检测报告

2016年07月14日　朱易翔

移动互联网系统与应用安全国家工程实验室

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

关于移动互联网系统与应用安全国家工程实验室（1/2）

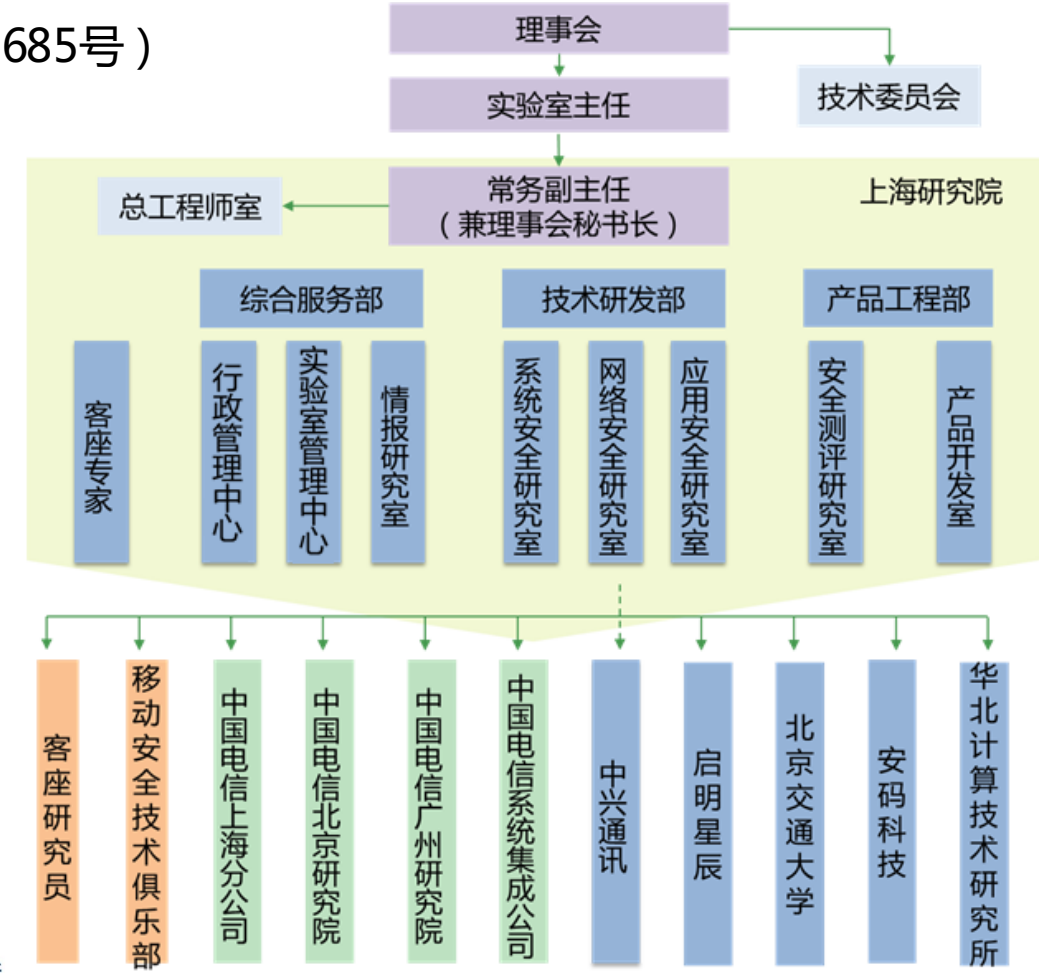
- 批复时间：2013年11月（发改办高技[2013]2685号）
- 建设地点：上海浦东、江苏南京
- 法人单位：中国电信集团公司
- 人员规模：100人

中华人民共和国国家发展和改革委员会

发改办高技〔2013〕2685号

国家发展改革委办公厅关于信息化领域
国家工程实验室项目的复函

教育部、工业和信息化部、公安部、人民银行、中国科学院办公厅，
北京市、深圳市发展改革委，中国电信集团公司，国家信息中心：
你们报来的信息化领域国家工程实验室建设项目资金申请报



中国电信 CHINA TELECOM　ZTE中兴　启明星辰 领航信息安全

北京交通大学　SA E-CODE 安码科技　CETC 中国电子科技集团公司第十五研究所

关于移动互联网系统与应用安全国家工程实验室（2/2）

移动互联网
系统与业务安全
研发实验平台
P1

端到端的
安全测评和仿真
试验平台
P2

移动互联网
安全技术应用
示范平台
P3

产业市场需求

企业自身保障

国家战略要求

新技术新业务安全监测响应

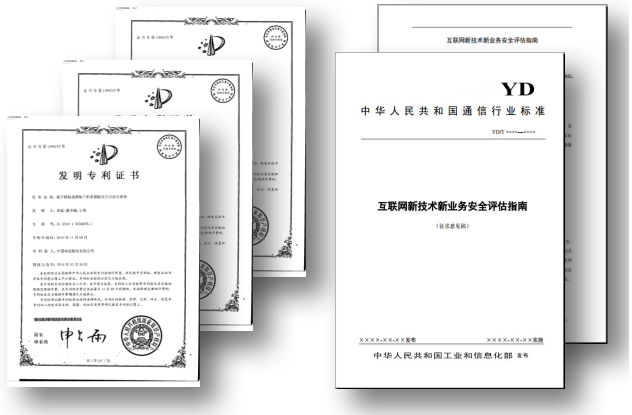
新技术新业务安全评估

基于运营商网络的反电子欺诈

基于运营商网络的
仿冒APP监测与拦截

大数据驱动的威胁情报分析

大数据驱动的攻击检测与溯源



关于我

- 2001年以前：ChinaNSL
- 2001年之后：信息安全从业者
- 2004：加入中国电信
- 2014年之前主要致力于为用户解决问题
  - 安全咨询、服务、解决方案
- 2014年3月：转到企业科研战线
  - 负责“移动互联网系统与应用安全国家工程实验室”的具体工作
  - 关注中国电信自身需求，更关注用户需求
  - 关注技术研究和突破，更关注解决问题和应用
- 其他
  - 程序员（C、C++、Python，etc.）
  - 安全技术细节及架构体系的长期实践者
  - 茶，书法，篆刻

引子——今天想分享点什么？

Content

问题提出的背景

- 2014年3月5日　互联网金融首度写入政府工作报告，国务院总理李克强在十二届全国人大二次会议政府工作报告中提出“促进互联网金融健康发展”、“严厉打击金融诈骗、非法集资”。
- 2015年9月　深圳 P2P 网贷平台融金所、国湘资本等相继被经侦调查。
- 2015年12月　“e租宝”涉嫌违法经营被调查。
- 2016年4月6日　上海市公安局发布信息，对“中晋系”相关联的公司进行查处。
- 2016年4月14日　国务院组织14个部委召开电视会议，在全国范围内启动有关互联网金融领域的专项整治，为期一年；当日，国务院批复并印发与整治工作配套的相关文件；在这份统领性文件之下，共有七个分项整治子方案，涉及多个部委，其中央行、银监会、证监会、保监会将分别发布网络支付、网络借贷、股权众筹和互联网保险等领域的专项整治细则，个别部委负责两个分项整治方案。由于此次整治涉及打击非法集资等各类违法犯罪活动，公安机关将密切配合参与其中。

- 根据第三方网贷资讯平台“网贷之家”的数据统计，自2011年有相关记录以来，截至2016年6月，国内累计成立的P2P理财平台达4127家，出现严重问题的互联网金融平台总数为1347个，占比高达32.64%。

问题的提出

- 从独立第三方的角度，选择一个合适的视角，探寻互联网金融当前的安全状况，发现主要安全问题、倡导并帮助行业提高APP应用的安全水平，确保APP安全可靠，为用户着想，保障用户利益。
- 视角：
  - ✧一个细分领域：网贷
  - ✧一个观察的切入点：APP客户端的安全性
  - ✧一定的范围：取样要有一定的规模，且具有典型的代表意义
- 一分钟目标设定
  - ✧在一个月时间内，完成对主流P2P产品Android移动客户端的安全检测，并出具一份专业的报告。

Content

思路：把目标分解成若干个小问题

- 选择检测对象
- 确定检测标准
- 讨论检测方法
- 组建检测团队（培训）
- 搭建检测环境（工具）
- 记录检测过程（迭代）
- 编写检测报告

面临哪些困难和风险

- 考虑到APP的更新太快，因此检测周期要尽可能短。
- 与传统APP安全检测的差异化：金融类的APP有什么需要特别关注的。
- 既要体现专业性，又要与单个APP的深度检测有所区别。

Content

工作计划

- 时间进度计划（4周）
  - ✧第一轮测试、问题提炼、方法改进：1周（18个）
  - ✧第二轮测试：1周（20个）
  - ✧第三轮测试：1周（25个）
  - ✧第四轮测试：1周（25个）
- 人力资源计划：3个检测小组（负责人制）+技术指导团队
  - ✧中国信息通信研究院信息产业通信软件测评中心
  - ✧移动互联网系统与应用安全国家工程实验室
  - ✧上海掌御信息科技有限公司
- 启动前的培训
- 工具保障计划
- 沟通计划：即时通信的群+例会+邮件组
- 尖刀班的作用：通过筹备组启动项目，做一些可行性的研究

如何挑选检测对象

- 行业细分，目标收敛：P2P
- 采样的代表性：2015年发展指数前100名P2P公司
- 对“网贷之家”站点“网贷评级” 栏目（http://www.wdzj.com/pingji.html）2015年我国移动互联网金融APP全年运营数据的统计中各月排名前100位的“发展指数”数据进行逐月采集，并进行算数平均、全年综合排名，最终得出年度前100位作为此次互联网金融APP金融信息安全现状检测的最终样本库。
- 其中具有APP的：共计88个（ Android应用）

排序	平台	发展指数												平均
		201501	201502	201503	201504	201505	201506	201507	201508	201509	201510	201511	201512	
1		70.97	66.08	65.06	67.08	69.8	72.18	72.92	72.21	71.94	71.15	73.68	72.72	70.48
2		69.46	64.76	64.23	64.12	67.91	67.95	67.86	67.93	68.56	64.93	67.84	68.6	67.01
3		69.18	59.06	59.09	56.15	58.51	62.82	65.06	65.34	65.64	64.3	69.12	68.61	63.57
4		60.42	53.63	52.99	54.43	58.22	63.71	64.72	64.96	65.8	63.92	66.84	65.96	61.30
5		61.63	54.31	53.76	55.83	58.19	62.65	60.53	60.8	58.67	61.07	63.05	63.37	59.49
6		61.6	54.17	53.78	56.25	59.34	64.06	60.98	60.85	59.78	58.55	60.72	60.37	59.20
7		61.98	57.34	56.91	53.74	57.47	61.18	60.87	60.5	59.42	56.81	59.4	60.26	58.82
8		62.78	53.18	52.12	51.62	54.5	58.99	55.7	58.27	58.26	57.1	60.79	60.34	56.97
9		53.66	46.59	50.57	51.14	54.65	58.79	59.49	59.28	60.04	58.31	59.19	59.44	55.93
10		54	51.05	51.63	51.28	53.04	58.69	55.1	54.21	57.06	55.96	58.84	59.07	54.99
11		58.92	51.98	51.54	51.04	53.04	53.9	51.11	51.56	52.35	50.51	55.45	54.21	52.97
12		59.21	53.97	51.49	48.07	50.69	52.79	52.22	52.54	53.41	52.68	54.15	54.3	52.96
13		54.48	49.78	50.52	48.5	51.65	55.53	55.04	55.62	54.37	52.43	52.57	52.35	52.74
14		57.06	48.92	47.43	49.42	52.56	54.03	50.97	51.29	52.46	50.04	53.14	54.28	51.80
15		53.58	47.35	46.49	45.55	46.8	50.52	51.55	53.5	53.45	55.23	58.55	57.84	51.70
16		51.52	46.98	47.2	47.81	49.87	54.5	53.32	53.9	53.68	52.83	52.41	51.92	51.33
17		46.82	43.81	46.13	48.06	50.5	52.86	52.84	53.04	53.15	51.47	50.1	50.12	49.91
18		50.91	44.5	45.12	46.03	48.3	52.76	51.9	52.32	52.17	49.47	51.64	50.82	49.66
19		51.57	46.96	46.31	45.05	46.34	50.49	50.92	50.4	50.06	48.36	51	50.08	48.96
20		48.77	43.78	43.71	44.45	47.23	51.92	50.72	50.11	49.11	48.75	52.38	53.39	48.69
21		46.74	44.26	43.5	44.99	47.71	50.59	51.62	52.34	53.11	50.07	49.4	49.99	48.69
22		47.06	44.51	44.66	45.54	46.98	52.65	51.72	51.34	51.1	50.83	47.8	46.8	48.42
23		50.09	45.65	45.69	45.23	47.42	51.66	48.4	48.83	48.48	48.41	49.09	48.79	48.15
24		44.48	43.29	44.7	44.77	47.6	51.9	50.75	50.94	50.8	49.49	49.28	49.22	48.10
25		45.26	40.77	41.94	44.8	46.36	51.62	49.48	50.4	51.06	48.91	50.16	50.91	47.64
26		49.82	47.04		44.68	47.85	52.7	51.97	53.4	53.98	52.98	57.25	58.59	47.52
27		45.58	41.26	42.41	44.12	46.71	49.69	50.52	50.36	51.12	49.17	49.78	49.18	47.49

如何定义检测标准（1/2）

- 本地数据安全
  - ✧敏感数据是否存放在外部存储器卡上，是否加密
  - ✧私有目录数据是否设置了正确的权限
  - ✧敏感数据是否以明文形式存储在私有目录中
- 数据传输方法和实现
  - ✧是否使用（HTTP）明文进行数据通信
  - ✧如使用HTTPS，是否验证证书以及绑定证书
  - ✧若使用自定义协议，是否有完善的密钥交换协议
- 服务器安全（N/A）

如何定义检测标准（2/2）

- 多方交易安全
  - ✧是否存在客户端信息泄漏
  - ✧是否存在身份验证机制的缺失
  - ✧信息提示是否完整
- 代码保护
  - ✧是否实现了完整性检查
  - ✧是否实现了防逆向分析
  - ✧是否实现了防进程注入

检测方法

- APP的下载和锁定
- 静态检测
- 动态检测
- 深度检测
- 危害性重现
- 评分
- 报告

人工分析方法示例

■ Android应用安全敏感行为审计

✧APP应用的敏感行为或者恶意行为主要体现在APP应用本身申请的权限、调用的应用接口APIs以及用于通信的IPC Intent事件；

✧基于静态分析方法，采用逆向分析和集成分析的手段，来查看APP应用申请的敏感权限Permissions以及APP应用调用的敏感应用接口APIs；

✧基于动态分析方法，采用沙盒分析和条件触发分析的手段，来跟踪分析APP应用动态运行的日志记录以及用于通信的IPC Intents事件。

■ 总结APP应用的敏感行为审计库

✧基于Adrienne.P.Felt Permission Map，统计总结APP应用的敏感行为如下：

敏感行为类型	敏感行为关注
短信行为	发送、拦截、监控、解析等
上网行为	访问网页、网络接入隐藏等
电话行为	获取电话状态信息等
联系人行为	通话状态监控行为、获取电话号码等
疑似隐私窃取行为	联系人获取、联系人删除、联系人添加等
疑似系统破坏行为	自启动行为、获取安装包列表行为等
疑似木马行为	静默安装、卸载程序、后台下载、自我隐藏等
疑似流氓行为	收藏主页、非用户确认操作等
疑似对抗行为	防止用户卸载恶意软件自身

■ Android应用安全设计分析

✧从6个维度评估应用本身的安全设计

✧基于静态分析方法，采用逆向分析和集成分析的手段，来分析评估APP应用是否存在权限滥用、Intent权限泄露、组件权限绕过漏洞的风险；

✧基于动态分析方法，采用条件触发分析和沙盒分析的手段，来评估Android框架中的Activity组件、Service组件、Broadcast Receiver组件、Content Provider组件是否存在暴露风险、劫持风险以及组件拒绝服务漏洞的风险；

✧基于静态&动态分析方法，采用取证分析和流量分析的手段，来评估Android设备中文件和敏感隐私数据是否存在被泄露的风险，其中数据泄露的途径有很多，包括通过存储文件、共享变量、数据库或者未加密的HTTPS数据通讯等多重方式来泄露。

脆弱性风险评估维度	风险评估方法
密码学误用维度	逆向分析、流量分析
权限滥用维度	逆向分析
组件安全维度	条件触发分析、仿真分析
数据传输维度	取证分析、流量分析
文件安全维度	逆向分析、取证分析
日志安全维度	逆向分析、取证分析

资源配套

- 场地
- 检测工具和设备
  - ✧APP样本采集和自动化检测平台
  - ✧Indroid
  - ✧apktool，androguard，JEB，Genymotion，signapk，Drozer，Burp，adb…
  - ✧基于Android＆iOS Fuzz漏洞挖掘系统
- 后勤保障

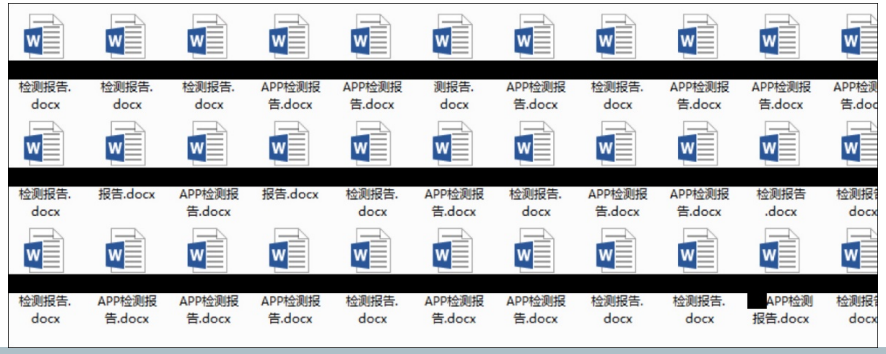
检测中踩过的那些坑...

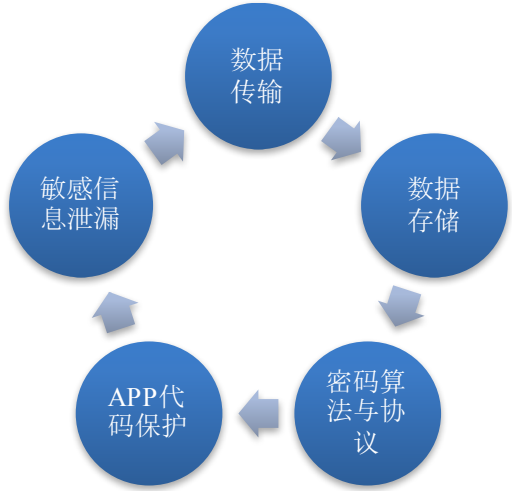
当然，收获也是颇丰☺

Content

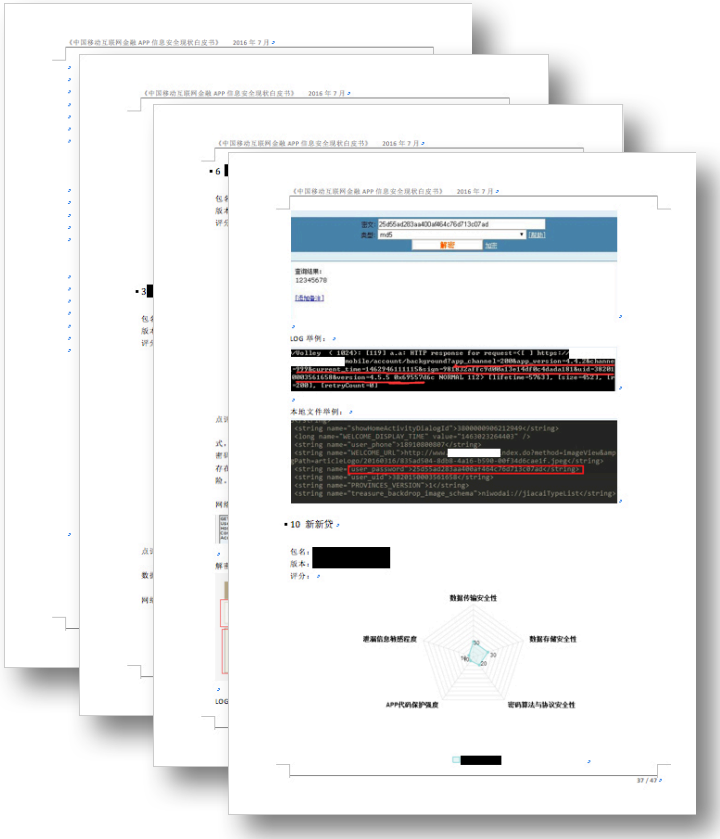
基本的结论

- 完成情况：按时完成了所有APP的检测（88个），形成了88份独立的检测报告（记录）。
- 统计、分析、汇总成完整的报告：科学 + 专业 = 像样。
- 从测试结果可以看出，目前互联网金融类APP的安全性并不高，每个APP都存在不同程度的安全问题。其中普遍存在的问题集中在加密算法的误用，网络传输保护不足，应用程序缺乏保护措施，本地文件及系统日志敏感信息泄漏等几个方面。
- 除此之外，个别APP还存在组件暴露漏洞，可数据备份漏洞，Webview远程执行漏洞，拒绝服务攻击漏洞，网络接口攻击漏洞等等其他安全问题。
- 移动互联网金融类APP的安全性严重不足，急需增强安全保护措施。





回到引子



致谢

2016阿里安全峰会
2016 ALIBABA SECURITY SUMMIT

CAICT
中国信通院

PALMIM
上海掌御

ESSENCE OF MEDIA

还有一件事

欢迎关注近期报告的正式发布
我们的实验室向大家开放
爱技术，更爱生活



感谢聆听！

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT