阿里安全
SECURITY OF ALIBABA

潘爱民，阿里巴巴集团安全部

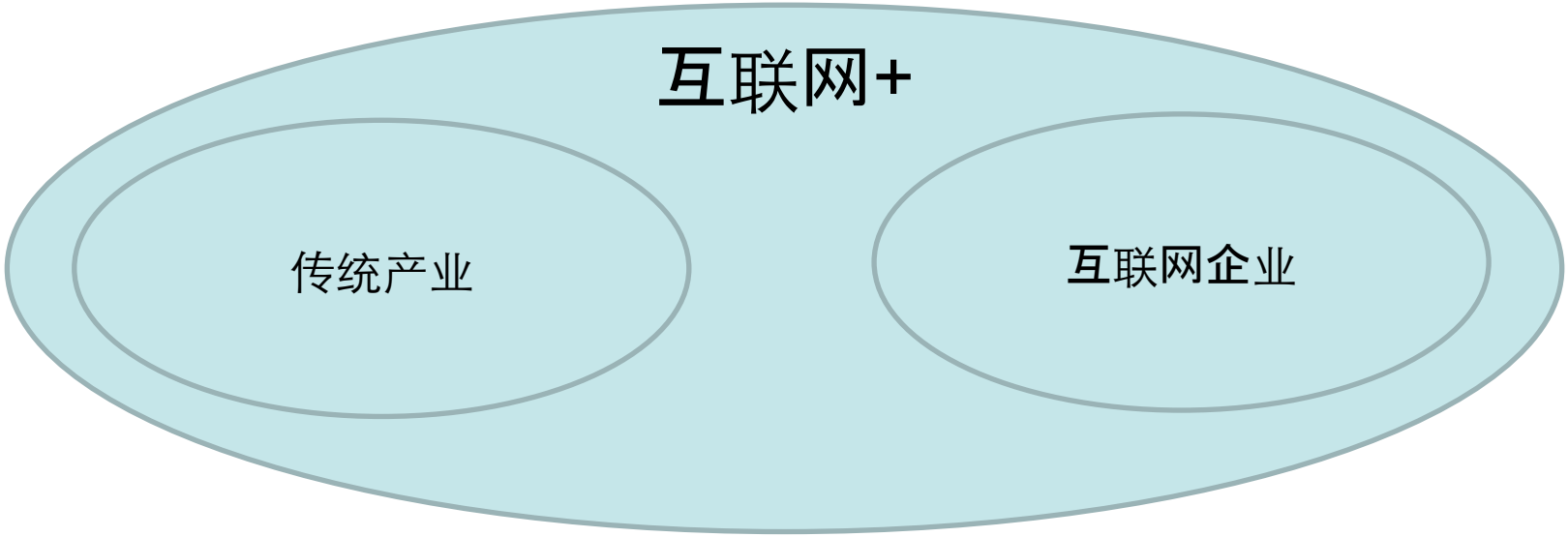
互联网+时代的移动安全实践

2015.7.9

提纲

- 互联网+时代的安全威胁
- 移动业务背景下的安全需求
- “云”+“端”的安全模型
- 阿里移动安全实践

从互联网到互联网+



大众创业，万众创新

互联网 -> 移动互联网

- 诞生:移动通信与互联网的结合
  - 手机上网带来了新一批互联网用户
  - 智能终端的普及

- 推动了创新
  - 用户体验被加强和重视
  - 应用和应用商店
  - 业务模式更趋精准
  - 直达用户的营销模式
  - 软硬件结合的产业链

IoT(物联网)

移动互联网的新安全威胁

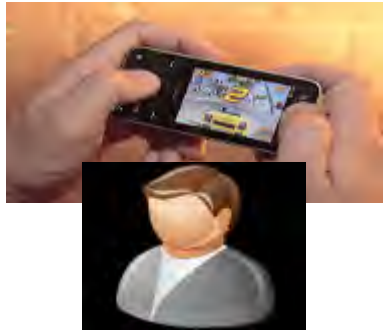
- 无线信号安全
  - 各种无线信号的保密和真伪
- 无线链路安全
  - 连接Internet
- 端的安全
  - 操作系统，厂商 ……
- 用户信息安全
  - 隐私信息泄露，欺诈，钓鱼 ……

移动互联网安全角色分布

芯片商

终端商

安全软件厂商



用户

移动OS厂商

应用软件厂商

骇客

灰产/黑产

移动业务面临的安全需求

- 系统不安全，缺乏基本的可信执行环境
- 应用分发渠道不可控，存在应用被假冒、篡改等
- 业务风险
  - 账号被盗，垃圾注册，信息泄漏
  - 虚假交易，营销作弊，信用炒作/刷量

移动互联网安全现状

病毒木马

100%

病毒木马的月均增长比例超过100%，严重威胁移动互联网的安全

应用漏洞

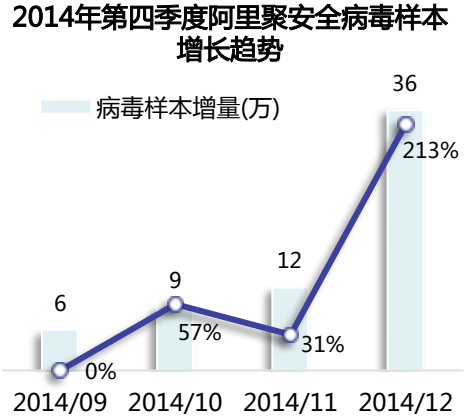
86%

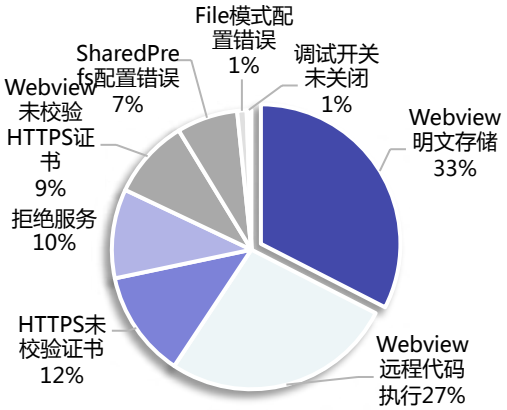
超过86%的应用存在漏洞，而开发者却没有足够的重视

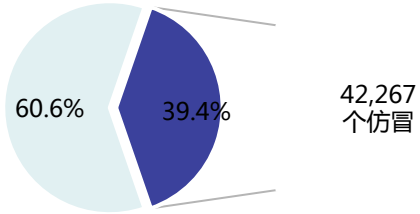
仿冒应用

40%

近40%的应用存在仿冒应用，热门的应用被仿冒几率越高







移动安全 – App模式+业务风险

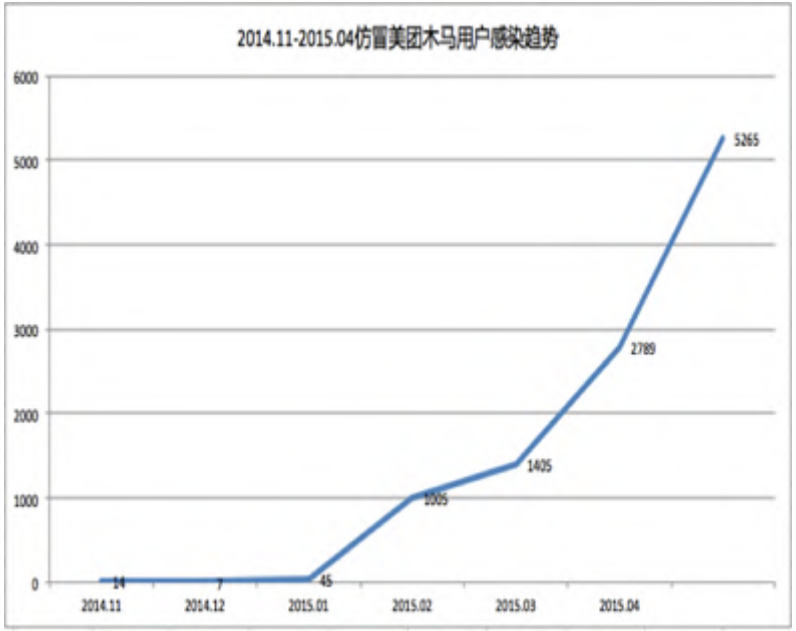
- App模式挑战
  - 目前尚处于漏洞频发阶段
  - 漏洞修复的到达率取决于用户升级意愿和场景
  - App版本长期处于新老并存的状态
- 业务欺诈
  - 根据支付安全报告，账户被盗导致资金损失的比例33.9%，交易过程中木马导致资损的比例为24%
  - 移动黑色产业链在不断渗透，涉及：
    账号被盗、垃圾注册、虚假交易、信用炒作/刷量、营销作弊，等等

实例1:某金融类恶意木马

- 木马行为:
  - 高度伪装支付宝客户端
  - 软件打开后要求用户输入账户信息登录
  - 木马把账号、密码发送到黑客手机
  - 恐吓用户账户支付宝账号存在异常消费
  - 引导用户申请冻结
- 危害性
  - 将支付宝账户、密码、支付密码、银行账号、开户行、信用卡账户等信息发送到黑客手机

案例2:美团红包仿冒

- 仿冒美团的App，也是一款木马，其行为：
  - 安装后根据不同的参数，向服务器传送数据，上报用户敏感信息，包括：手机号、手机硬件配置信息、银行卡号、身份证号、姓名等
- 危害性
  - 美团应用安装量大和使用广泛
  - 迷惑性强，用户容易被诱骗



移动攻防- 投入不对等

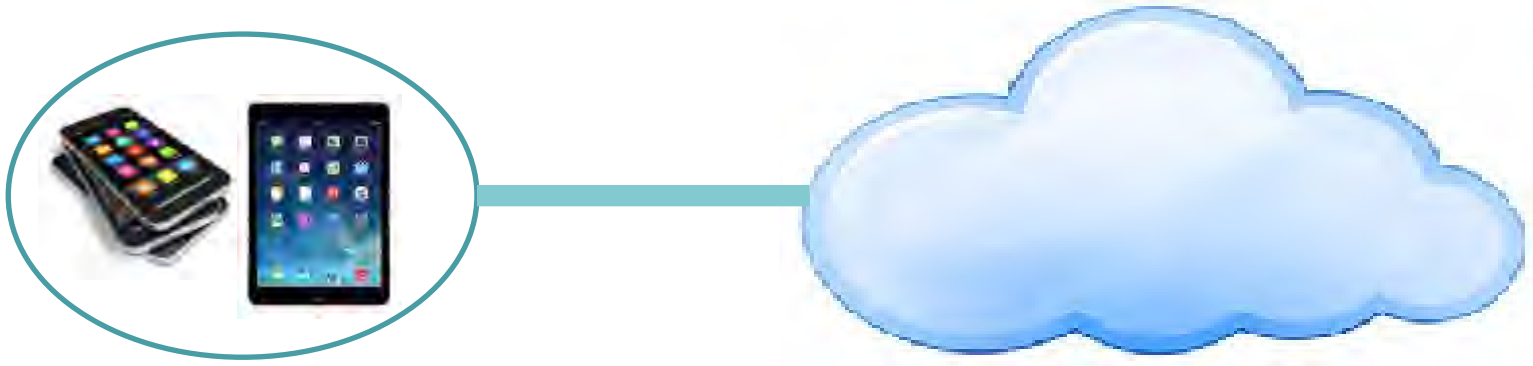
黑色产业

- 专业的应用攻防能力
- 100%的精力投入
- 完整的产业链结构与分工
- 各种先进的检测工具

应用开发

- 没有应用安全攻防经验
- 没有精力和时间投入到应用安全防护中
- 缺乏相应的防护工具

移动安全 – “云”+ “端”的平衡

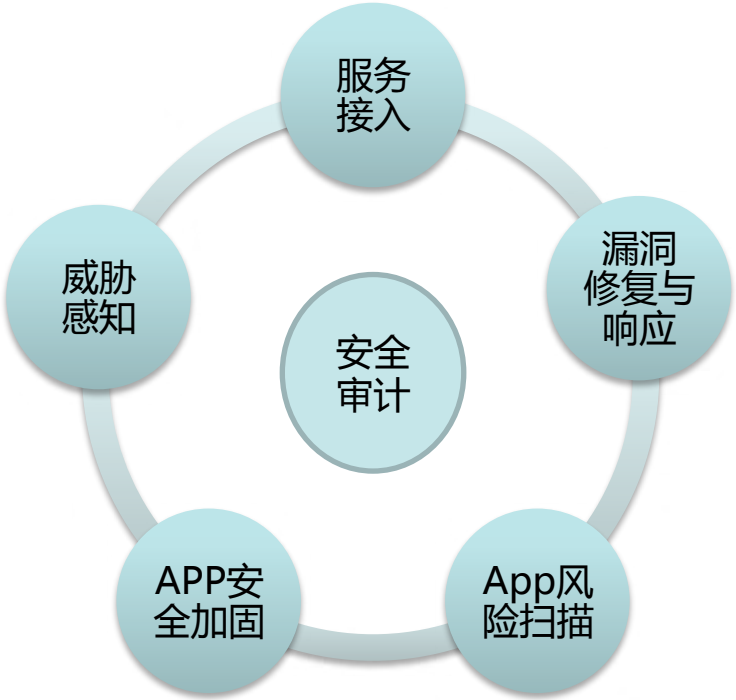


业务逻辑比重

风险控制

阿里移动安全实践

- 威胁感知
- App安全加固
- App风险扫描
- 漏洞修复与响应
- 服务接入层
- 安全审计

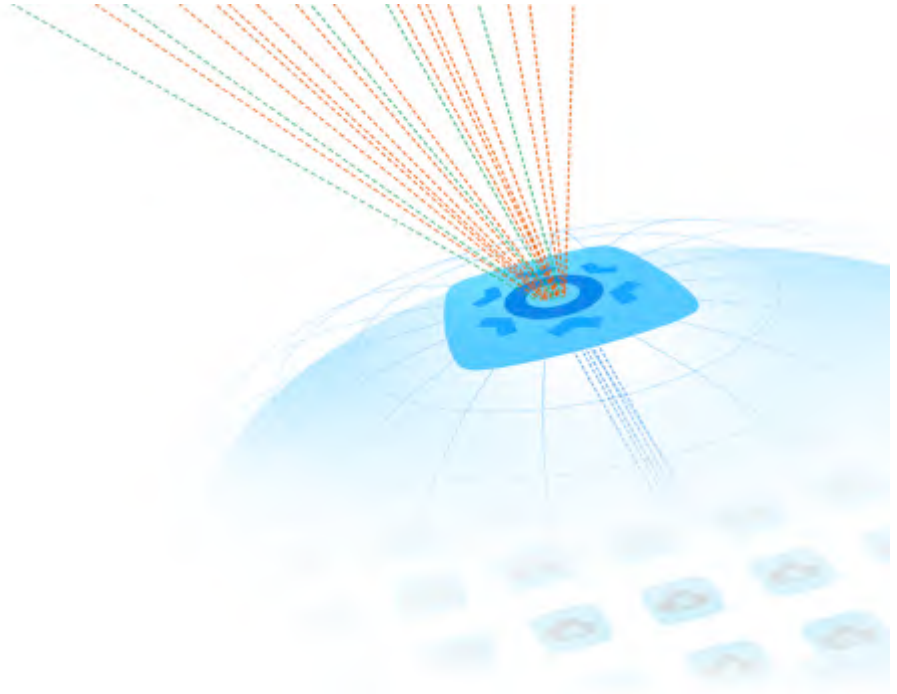


阿里移动安全实践:威胁感知

- ROOT检测
  - 手机ROOT（越狱）破坏了操作系统原有的保护机制,容易引发针对App的攻击和业务风险
- 模拟器检测
  - App运行在模拟器设备中，容易受到逆向破解、抓包分析等攻击，同时增加业务风险
- 重要数据的篡改检测
  - 攻击者对于客户端的用户数据、机密文件、网络数据、安全配置等进行篡改，如修改证书、JS代码等，从而威胁应用安全
- 恶意调试检测
  - 攻击者利用调试工具,对应用程序进行动态调试,分析程序逻辑与保管的核心数据，造成密码、业务逻辑、安全策略等信息外泄，威胁业务安全

威胁感知:优势

- **全生命周期监控**
  - 开发、测试、线上全周期监控，及时应对风险
- **风险可感知**
  - 应用运行环境、被攻击情况实时可见

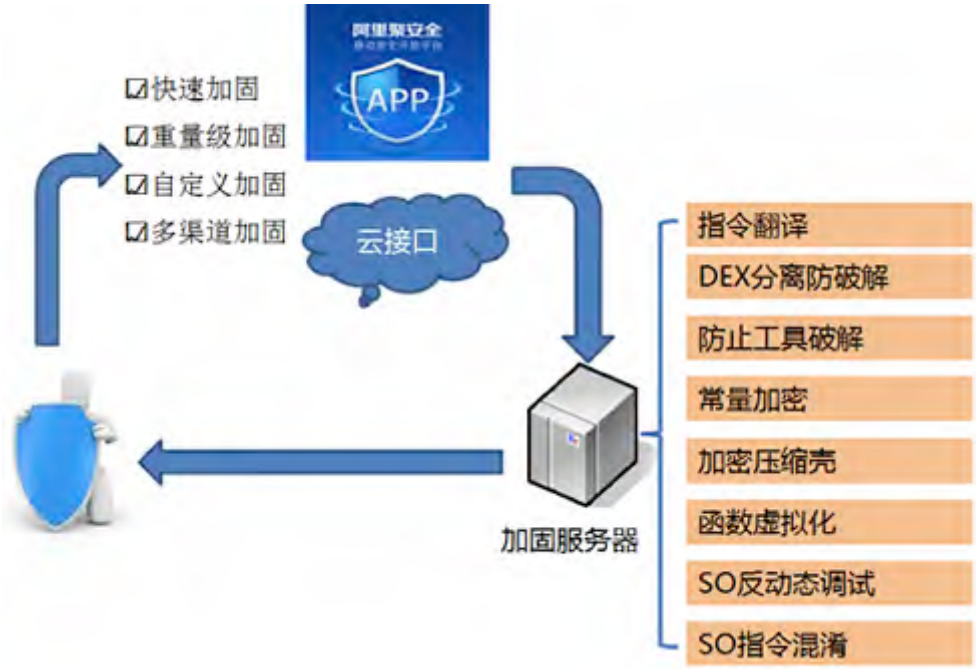


成功案例：某O2O应用(反欺诈服务)

- 协助客户解决的问题：
  - 通过阿里聚安全的持续监控功能，检测到客户端运行过程中存在外挂刷机等行为
- 效果
  - 2周内避免了数百万级的资损

阿里移动安全实践:App加固

- **低成本的安全防护方案**
  - 针对App安装包进行加固，无需修改源代码或者二次开发
  - 主要手段：加壳、加密、逻辑混淆、代码隐藏等应用加固方法
- **有效性**
  - 防止应用被逆向分析，反编译
  - 防止应用被二次打包嵌入病毒广告等恶意代码



成功案例:某游戏平台安全加固服务

- 客户服务类型
  - 游戏平台Android客户端
- 项目实施
  - 阿里的安全加固服务集成到该游戏平台的开发流程中
    - 保证开发效率
    - 通过高强度的加固服务，提高了客户端的安全能力
  - 另集成了阿里风险扫描及加固的API，为该游戏平台提供进一步的安全能力支持

阿里移动安全实践:App风险扫描

- 应用漏洞检测
  - 阿里自主研发的应用漏洞扫描引擎
- 恶意代码检测
  - 对APK进行可疑代码段静态分析，恶意行为动态分析，特征及黑名单匹配，查找隐藏在代码中的后门和恶意代码等
- App仿冒监测
  - 对全网应用渠道进行持续监测，收集仿冒应用、二次打包等各种威胁，为客户提供仿冒应用数、装机量、资产损失等数据

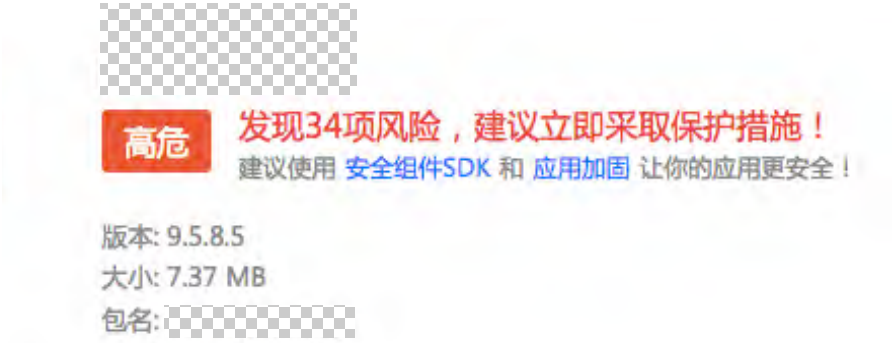
App扫描：优势

- 漏洞检测
  - 数百万级别（230万＋）的漏洞库
- 恶意代码检测
  - 千万级样本规模，识别能力强

- APP仿冒检测
  - 覆盖TOP应用渠道以及网盘论坛等非典型渠道，实现全网监控
  - 检测项精细，包括特征值、图像等高级匹配能力
  - 不仅监测到渠道及还能够获取到对应的安装量

成功案例:某金融应用的风险扫描服务

- 协助客户调查漏洞影响范围
  - Android 客户端的漏洞，恶意代码，以及仿冒应用检测
- 10分钟以内发现如下风险情况:
  - Android客户端34个安全风险，其中23个高危漏洞，甚至能够通过检测自动发现APP本地密钥。
- 针对相应的问题，为客户提供快速解决方案



阿里移动安全实践:漏洞修复与响应

- 移动App的安全现状
  - 漏洞不断被发现，连接的SDK也可能存在漏洞
  - App一旦发布，难以“召回”，或者禁止使用
- App每个版本的生命周期呈长尾效应
  - 意味着每个被发现的漏洞，都可能存在可适用的App版本

- 问题:
  - 新版本要尽快递交到用户手中，降低漏洞的影响
  - 残留的老版本会不会成为安全体系中最薄弱的环节？

针对移动漏洞的方案

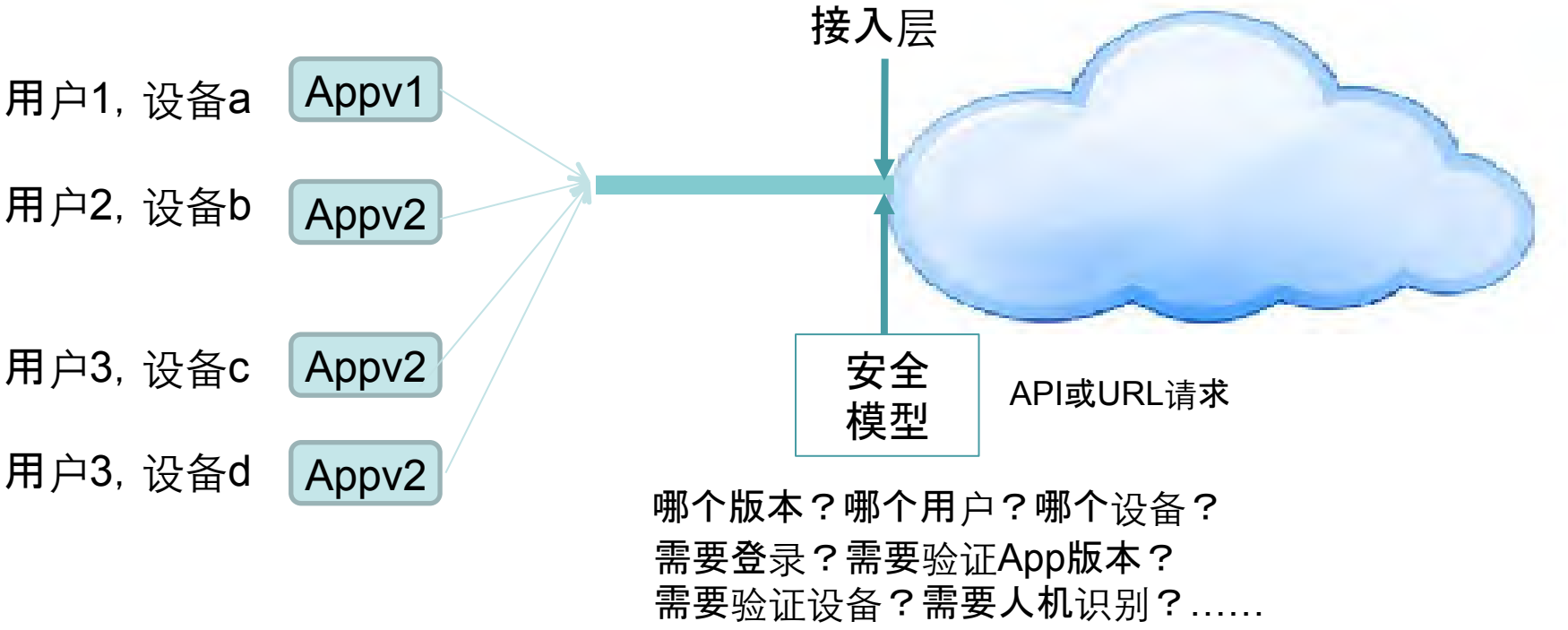
- **流程保障：安全测试，漏洞响应规范**

- **技术与架构**
  - 核心逻辑提供热补丁的能力 —— 适用于基础模块
  - 模块级的升级/隔离方案 —— 特别是第三方模块
  - 服务器端的逻辑控制 —— 适合于业务逻辑模块
  - 接入层控制 —— 适合于接口层/通迅层的逻辑

阿里移动安全实践:服务接入层

- 服务接入层:针对用户的一个重要控制点
- 对用户请求的安全认证，可以基于多个维度的标识信息
  - 账号体系
  - 设备可信度
  - 客户端软件的认证
- 实施的控制力
  - 对App软件版本的生命周期控制
  - 对业务风控的部署点
  - 减小漏洞影响的控制点

服务接入层:移动业务安全模型



阿里移动安全实践:安全审计(ASDL)

- ASDL标准
  - 安全编码
  - 安全架构审查
  - 安全测试/漏洞检测
  - App上下线安全规范
  - 漏洞响应与修复流程

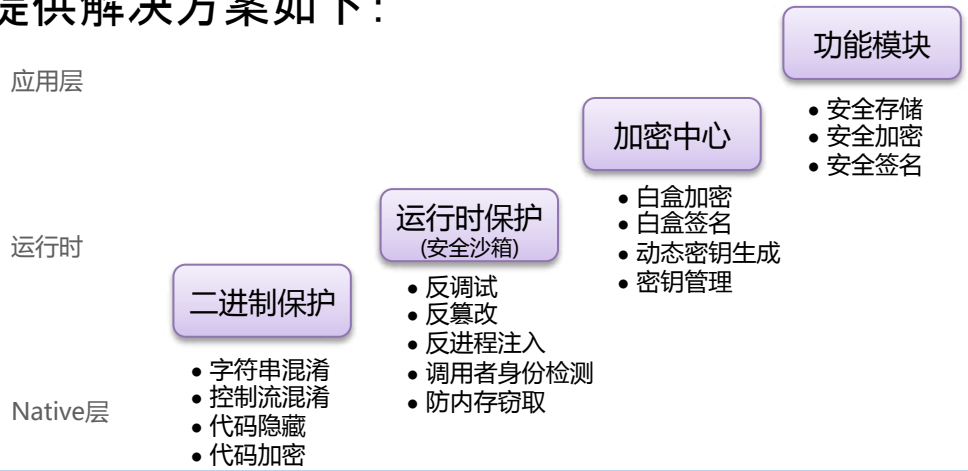
- ASDL安全培训
  - 进行安全流程与安全意识的培训

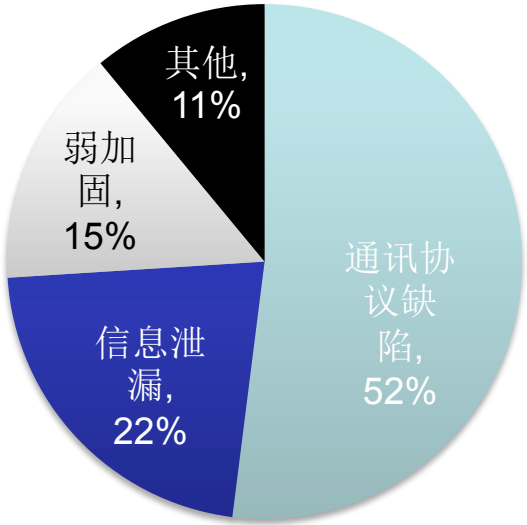
安全审计:优势

- **提高研发效率**
  - 基于互联网敏捷开发模式，很好地平衡了开发效率与安全之间的矛盾
- **有效预防实际的安全风险**
  - 阿里自身在进行最有效的安全实践
  - 阿里移动审计服务基本上覆盖了阿里集团所有业务（移动App）
- **审计服务标准化**
  - 把阿里的经验输出给同行

成功案例:某票务应用的安全评估

- **安全评估范围:**
  - 该应用iOS和Android 客户端的安全评估服务
- **漏洞扫描与挖掘:**
  - iOS客户端共发现15个安全风险，其中7个高危漏洞
  - Android客户端12个安全风险，其中7个高危漏洞
- **提供解决方案如下:**





阿里移动安全实践:业务风险控制

- **最全面的业务风控数据**
  - 阿里巴巴拥有全链路的账号、交易、信用等业务和风控数据，数据的范围和质量都具有领先的优势

- **业界领先的技术以及风控模型策略与实践**
  - 阿里移动安全的技术模型和策略在阿里巴巴电商业务、支付业务等得到了实际的历练和验证，具有非常强的实用性

- **全方位整体方案**
  - 覆盖PC、H5、Native全端的业务风控整体解决方案，为第三方提供了各种灵活的接入方案

业务风控:重要风险场景

账号安全

- 垃圾注册
- 账号被盗
- 撞库脱库

交易安全

- 营销作弊
- 交易刷单
- 三方欺诈

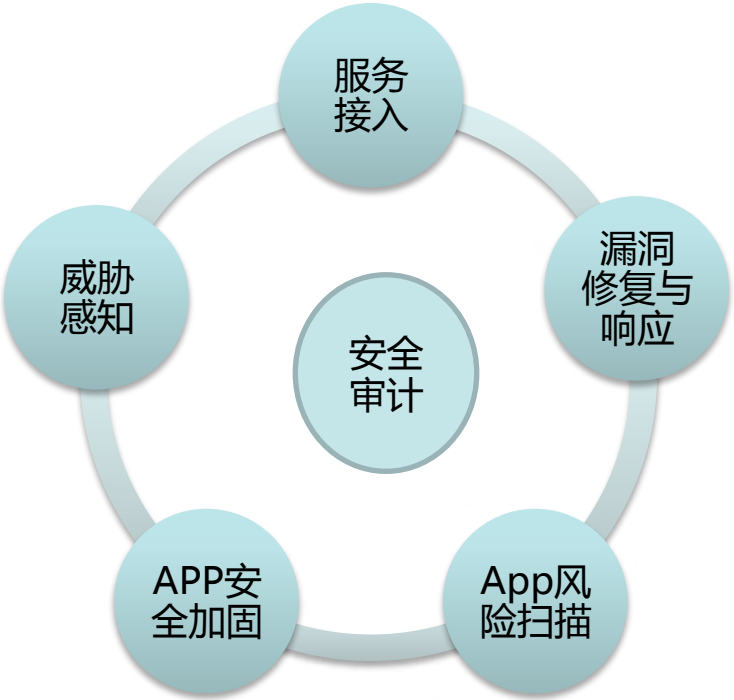
支付安全

- 银行卡盗用
- 套利套现

信用安全

- 渠道作弊
- 炒信刷信
- 信用支付欺诈
- 信用贷款欺诈

阿里移动安全能力输出:聚安全



谢谢！