黑客眼中的移动安全

梆梆安全高级安全咨询师 赵磊

lei.zhao@secneo.com

移动互联网威胁分析

你手机真的安全吗?

可以被恶意ROOT

应用程序代码逻辑、和服务器交互逻辑可被轻易分析

运行环境可被完全控制
（CPU,寄存器、内存）

本地证书、密钥可被探知
资源文件可被轻易替换

二进制完全可见
（反编译、静态分析）

完全控制可执行程序
（修改、调试、动态分析）

移动互联网和传统互联网的差别

环境变化

抛开冗余而沉重的传统IT架构，越来越多的移动终端出现在办公场所，BYOD正在普及。

效率提升

没有人会时时刻刻守在自己的电脑旁，但现在的人们绝不会丢弃掉自己的体外器官-手机。在移动互联时代，每个人都被改造成一台高效的计算节点。

载体变化

智能终端作为现代人的“体外器官”，让我们对信息的收集、反馈、流转的效率成倍增长

数据导向

数据导向道出了企业运营的变化原因：加入更多更高效的载体、媒介，是为了更高效的为主体——数据来进行服务

Android平台威胁分析

终端厂商机型众多
硬件无统一行业安全标准

开源系统源码公开
底层漏洞响应修补滞后

任何开发者随意签发安装
任何应用随意提权ROOT

安卓发布市场混乱
缺少安全校验和必要监管

IOS平台威胁分析

所有的安全机制
都可以被越狱绕过

封闭的生态环境
0day漏洞众多

第三方厂商
引入不可预知的风险

开发环节
引入不可控风险

OWASP十大移动风险（2016）

- 平台使用不当：应用程序未遵循安全控制原则滥用平台提供的功能
- 不安全的数据存储
- 不安全的通信：如缺乏证书校验、明文传输数据
- 不安全的身份验证
    - 会话管理中存在漏洞、没有对用户身份进行识别，没有保持对用户身份信息的确认
    - 如可预见的会话标识符，仅客户端登出等
- 加密不足：弱密码，差密钥算法。可预测的密钥，容易伪造的完整性检查
- 不安全的授权：用户可执行他们本不能执行的创建、读取、更新和删除等操作
- 客户端代码质量问题：缓冲区溢出、字符串格式漏洞等
- 代码篡改：包括二进制修补、本地资源修补，hook，方法调整，动态注入和调试
- 逆向工程：利用IDA等工具对核心代码进行逆向分析
- 无关的功能

移动端单点攻击手段总览

- 通过移动端篡改内容
- 获取用户敏感信息
- 插入广告，赚钱广告费
- 木马病毒攻击
- 窃取账户，发起中间人攻击
- 从脆弱的移动端入侵系统服务端的风险

黑产、灰产-新的安全挑战

01 攻击产业化

从原有的孤胆英雄到成规模、成体系的黑色产业链

移动应用新业务

02资金套现渠道隐蔽

多种方式可以实现非法资金的套现，如比特币，虚拟装备

03从黑产到灰产

攻击往往利用业务缺陷，很难被界定为非法，游走于法律边缘

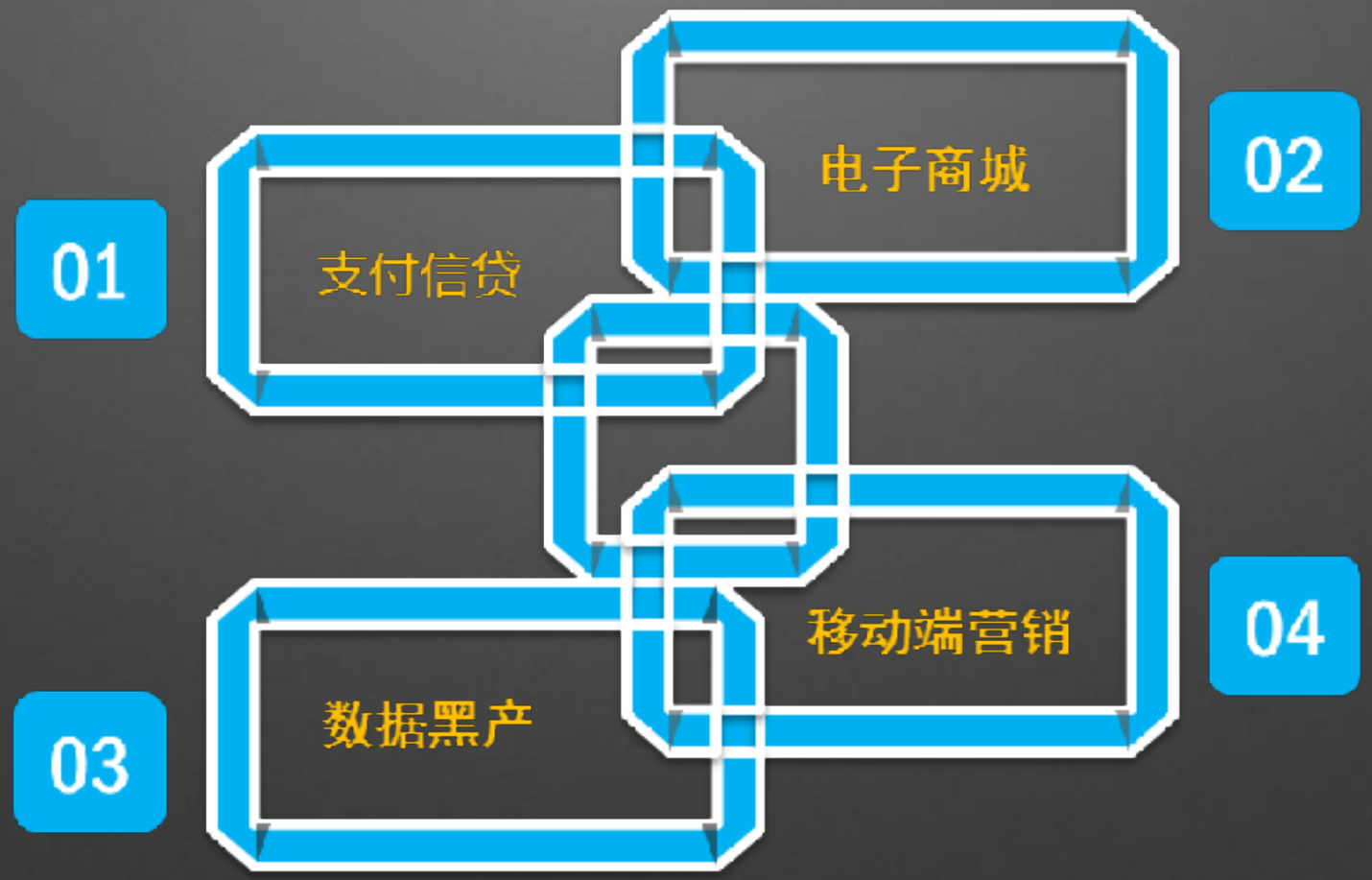
04 单点技术失效

面对有组织有计划的攻击，单点技术很容易被绕过突破

05 完整而不可或缺

专业的移动应用安全服务已经从锦上添花变为不可或缺

黑产、灰产-新的安全挑战

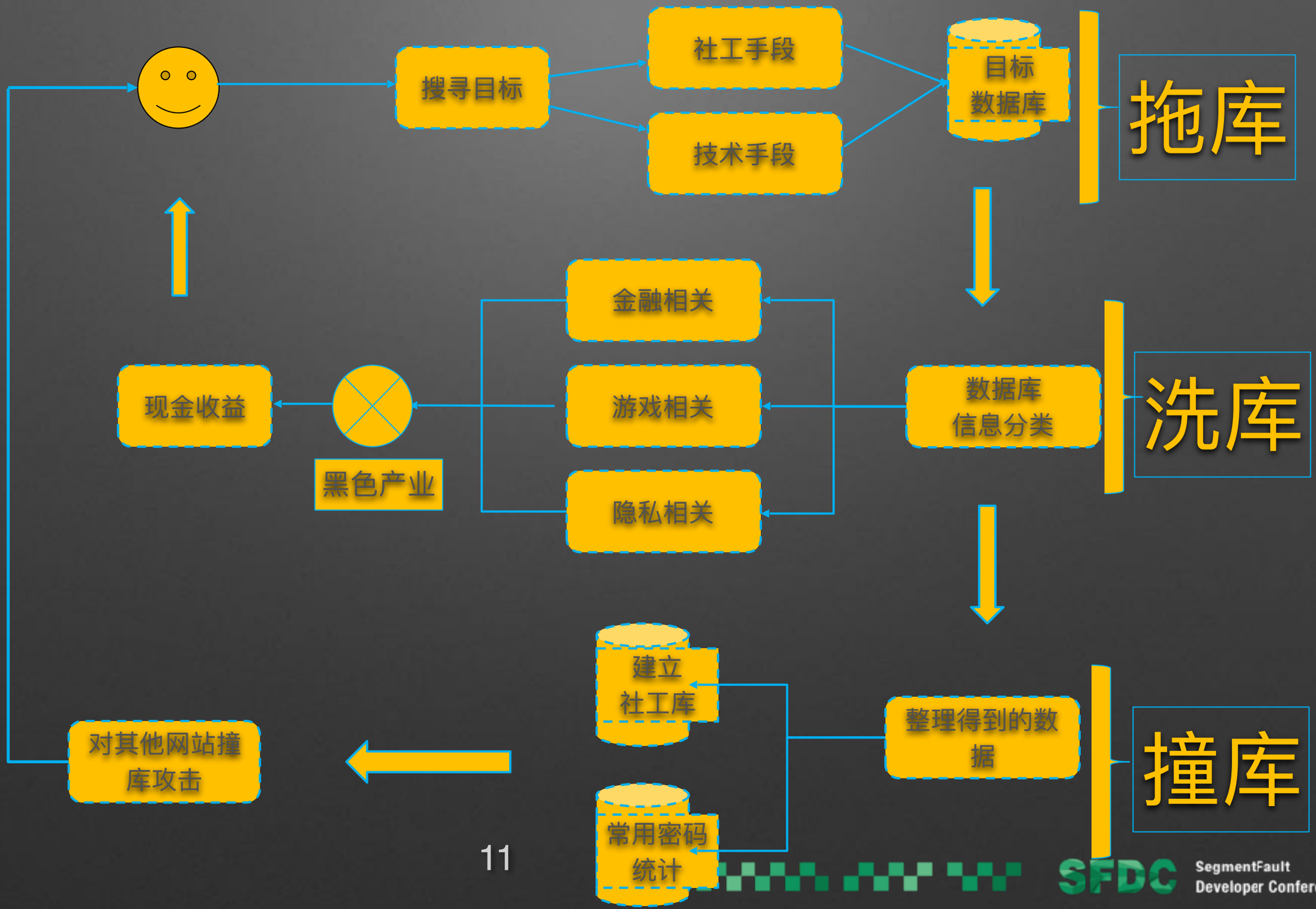


- 欺诈交易
- 钓鱼欺诈

- 刷单
- 刷积分
- 刷优惠

- 拖库
- 洗库
- 撞库

黑产基础-数据黑产



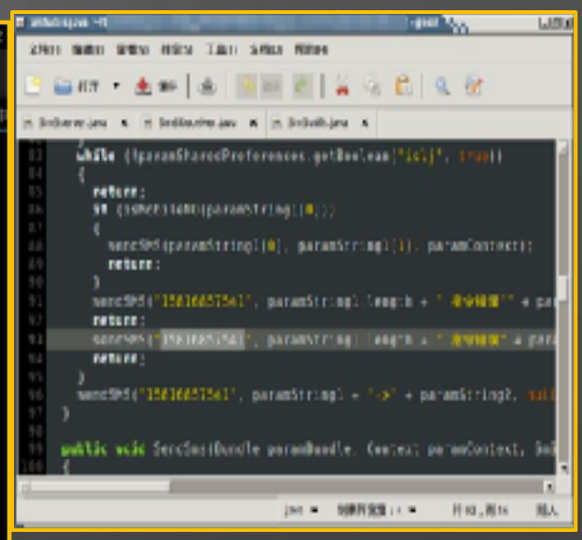
黑产基础-数据黑产的冰山一角

2015年2月	2015年4月	2015年5月	2015年5月
优步5万司机信息泄漏	中国社保系统5279万条个人信息泄漏	支付宝大量账户被撞库异地登陆	网易邮箱用户信息泄漏导致iphone用户遭远程锁定勒索

01 ..... 02 ..... 03 04

钓鱼过程中黑客技术的组合运用

A 伪基站 钓鱼短信 ------ B 钓鱼APP 诱导下载 ------ C 钓鱼APP潜伏、获取权限 ------ D 作恶



APP会向黑客手机号码发送短信报到从此中招手机变为受控制的肉鸡。

受害手机的短信记录不会保存那些控制指令，所以机主感知不到

控制者可以用任意手机号向受害手机发送控制指令

平常APP处于潜伏状态，当收到特定短信后，开始启动并作恶。

控制者尝试偷取受害手机里的X.509证书文件

APP尝试阻止被卸载并欺骗用户卸载成功

羊毛党黑产

- 刷单软件
- 账户批量注册
- 短信对接软件
- 打码平台工具

刷单准备阶段

- 秒杀
- 0元
- 优惠券
- 实物奖励

活动刷单阶段

- 资金转移

利益套现阶段

羊毛党黑产相关工具

批量账号注册工具

百度账号批量注册软件 金兰知道账号注册机

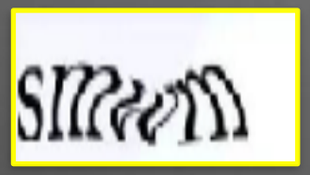
京东账号注册工具 小米账号全自动注册机

4399注册机下载(4399账号注册软件)

京东账号注册软件

验证码绕过

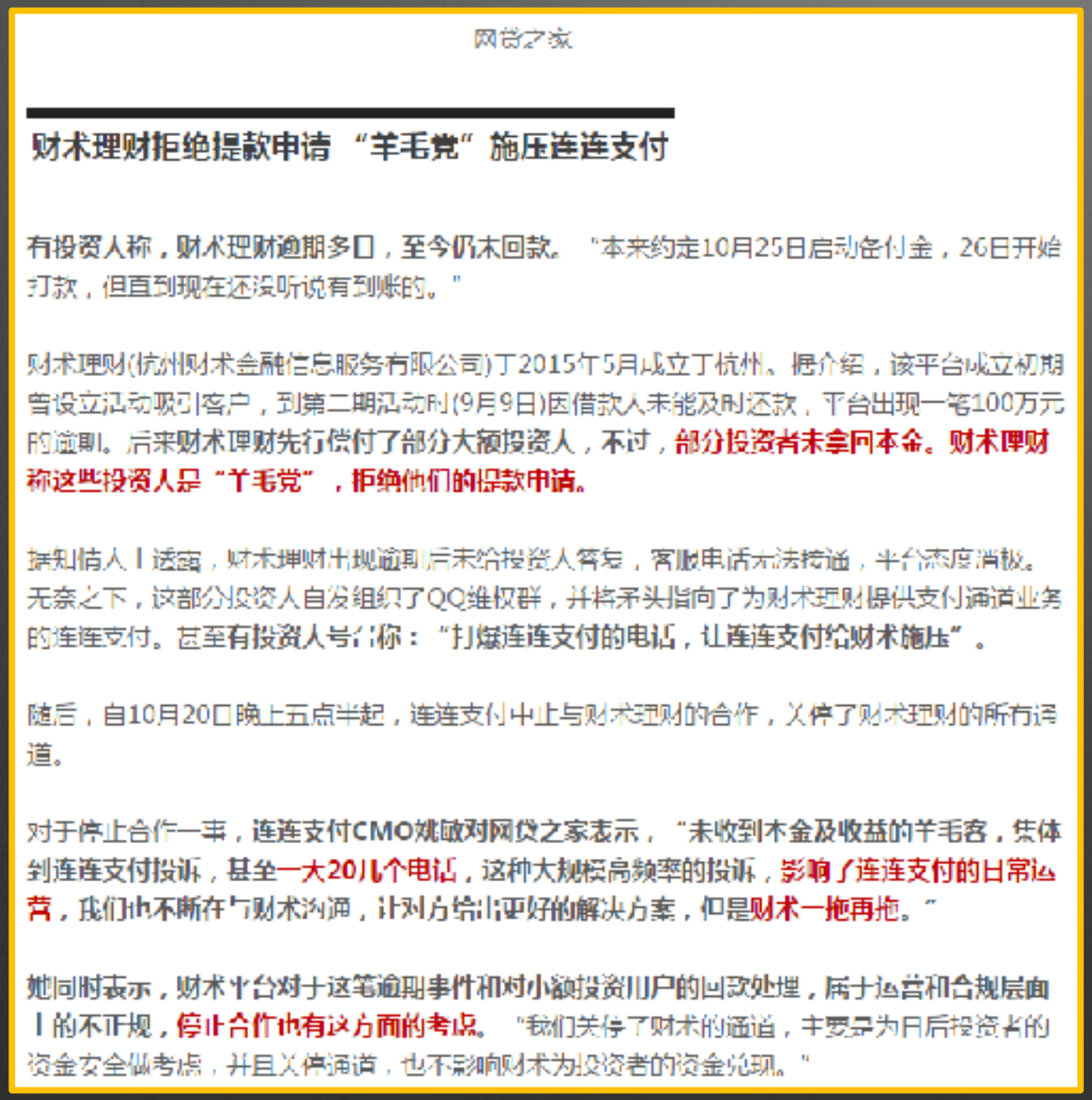
图像自动识别、人工打码



模拟操作、人工打码

短信验证码绕过

羊毛党黑产行为分析



网贷之家

财术理财拒绝提款申请 “羊毛党”施压连连支付

有投资人称，财术理财逾期多日，至今仍未回款。“本来约定10月25日启动备付金，26日开始打款，但直到现在还没听说有到账的。”

财术理财(杭州财术金融信息服务有限公司)于2015年5月成立于杭州。据介绍，该平台成立初期曾设立活动吸引客户，到第二期活动时(9月9日)因借款人未能及时还款，平台出现一笔100万元的逾期。后来财术理财先行偿付了部分大额投资人，不过，**部分投资者未拿回本金。财术理财称这些投资人是“羊毛党”，拒绝他们的提款申请。**

据知情人士透露，财术理财出现逾期后未给投资人答复，客服电话无法接通，平台态度消极。无奈之下，这部分投资人自发组织了QQ维权群，并将矛头指向了为财术理财提供支付通道业务的连连支付。甚至有投资人号召称：“打爆连连支付的电话，让连连支付给财术施压”。

随后，自10月20日晚上五点半起，连连支付中止与财术理财的合作，关停了财术理财的所有通道。

对于停止合作一事，连连支付CMO姚敏对网贷之家表示，“未收到本金及收益的羊毛客，集体到连连支付投诉，甚至**一大20几个电话**，这种大规模高频率的投诉，**影响了连连支付的日常运营**，我们也不断在与财术沟通，让对方给出更好的解决方案，但是**财术一拖再拖**。”

她同时表示，财术平台对于这笔逾期事件和对小额投资用户的回款处理，属于运营和合规层面的不规，**停止合作也有这方面的考虑**。“我们关停了财术的通道，主要是为日后投资者的资金安全做考虑，并且关停通道，也不影响财术为投资者的资金兑现。”

“羊毛党”行为分析

- 通过购买的个人身份信息，在平台大量注册账户
- 利用平台投资奖励计划，每个账户投资100元
- 从单个账户获取投资奖励，此类奖励收益率远远高于资金收益率
- 单个“羊毛党”可通过技术手段，同时控制数千个账户

移动安全防护体系构建

新趋势下的安全思考

- 从单点防御走向立体防御
- 从架构设计、安全流程、可信执行和安全响应四个维度入手
- 覆盖软件开发全生命周期
- 移动应用“泛安全”视角

- 重视数据的价值
- 数据驱动的安全感知、情报触发的安全防护

纵深防御理念

1 架构设计

从设计层面出发的安全架构，包括设计开发安全、可升级性、可扩展性

2 安全流程

完整的安全质量管理和控制流程、包括安全需求、安全建模、渗透测试、持续集成和发布审核

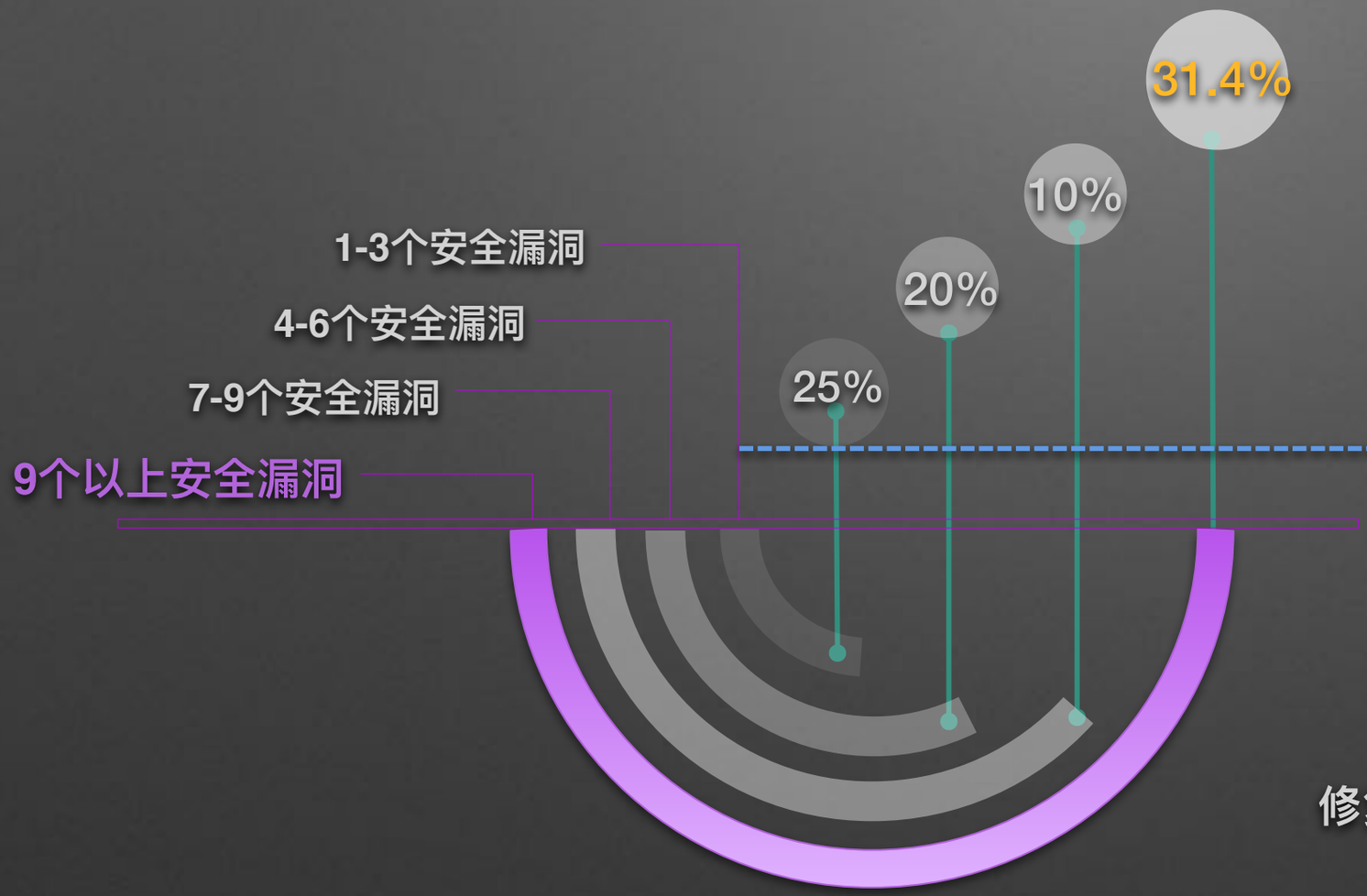
3 可信执行

- 白盒环境假设
- 基于应用加固技术和各类安全组件实现可信执行保障
- 可信执行的目标：数据可信、代码安全、通讯可信、执行可信和认证可信等

4 安全运维

- 安全是个过程不是结果
- 构建移动应用程序泛安全运维理念和目标
- 可视化、可追溯、可处理

安全架构—设计



设计层规避

- 安全需求分析（ST）
- 威胁建模（PP）
- 安全设计及编码（SDF）
- 安全测试（ST）

修复及更新能力

- 动态更新机制
- 强制升级及版本禁用机制
- 数据采集分析机制

安全架构—实施

1 安全目标

网络传输层的帐号密码安全

2 威胁建模

威胁建模
流量未加密
证书伪造窃取
对称密钥破解窃取
钓鱼窃取

3 安全设计

安全设计
通讯数据加密
双向证书校验
本地密钥白盒处理
流量加密与证书绑定

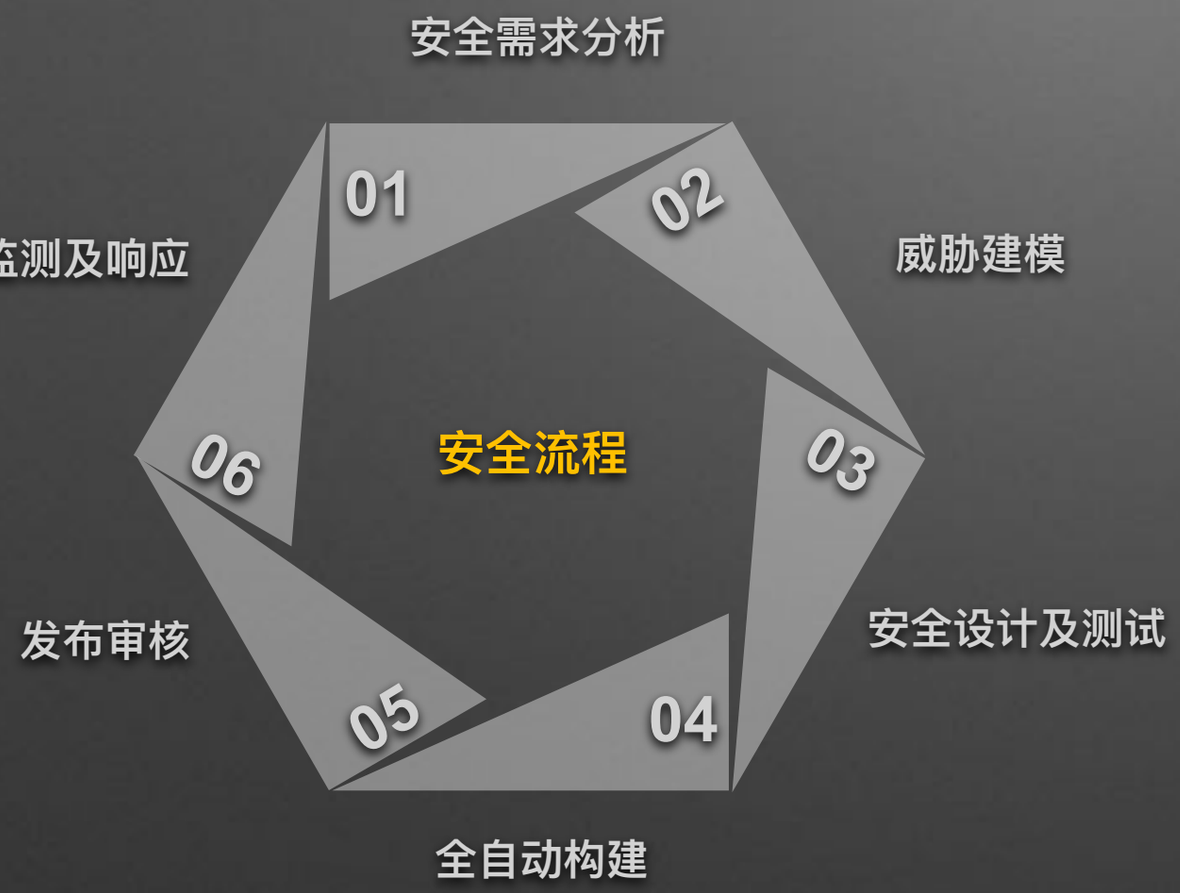
4 安全测试

安全测试
TS1:验证……
TS2:验证……
TS3:验证……
TS4:验证……

残留风险处理

- 接受风险
- 运维手段处理
- 第三方解决方案

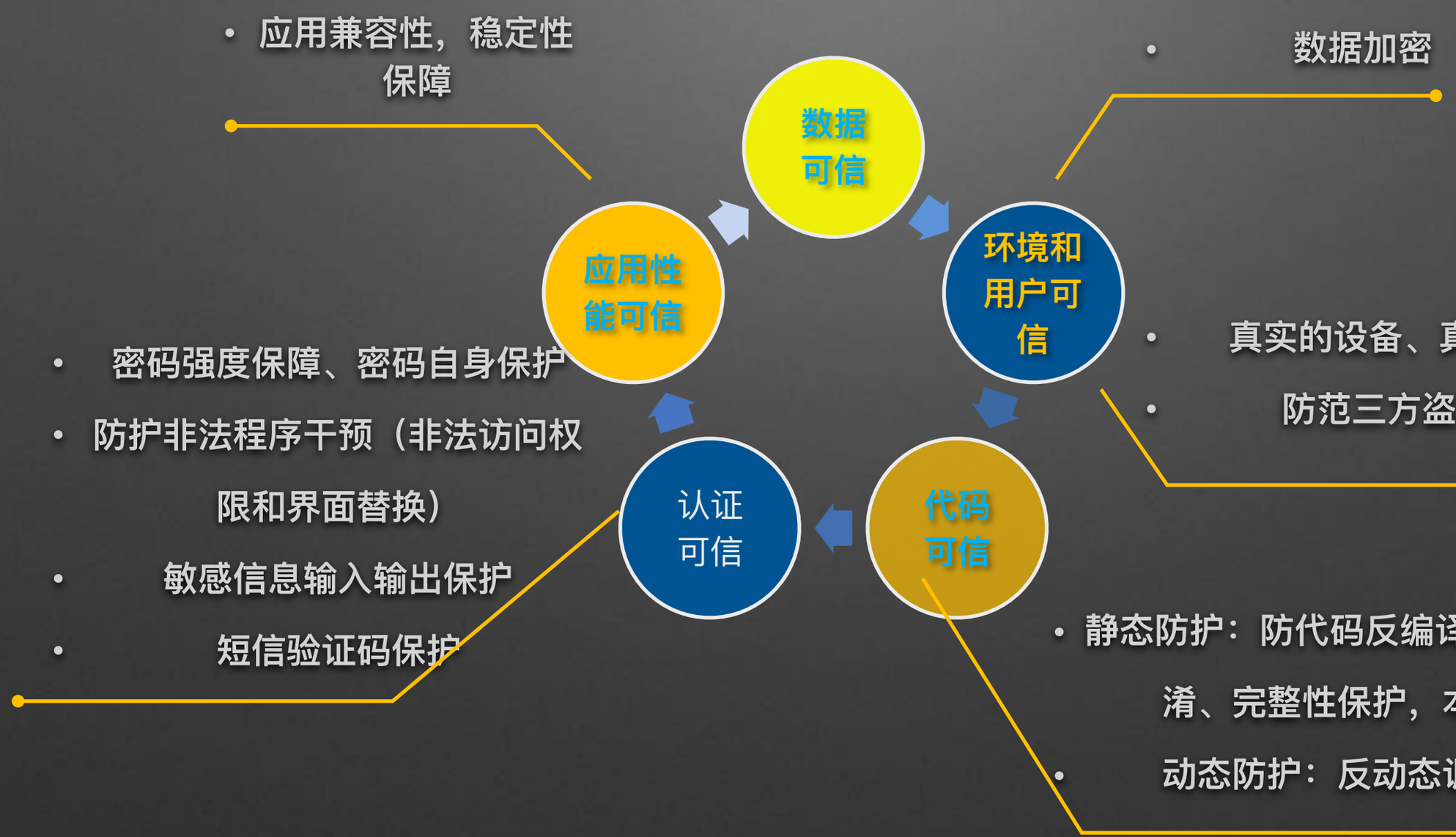
安全架构—流程



大部分的安全问题，都是人的问题

通过把安全贯穿到整个应用生命周期当中，借助于流程化的安全控制手段，实现从源头到运维的安全控制能力，减少因人的因素导致的安全缺陷及风险威胁

安全策略—可信执行



安全策略—安全运维

- 在软件全生命周期的安全和运维单点上都需要采取主动化的流程、工具
- 典型如应用更新和升级维护机制

应急响应流程构建

可视化运维

主动运维

- 可视化是运维的基础，是安全体系必备的配套体系
- 用于评价效用、发现问题
- 包含安全可视化、应用性能可视化等

- 承认安全事件的必然性
- 讲求规范性和实效性

安全策略—数据驱动安全

必然攻击路径：从所有攻击的必然技术节点布置探针，从基础技术原理上检测各类交易欺诈信息

A 安全指数基础

威胁情报

C 基于威胁模型生成威胁指数：用户可信度、环境安全可信度、交易行为可信度

B 威胁分析

1、结合业务特点的威胁模型构建
2、利用决策链分析、图论分析等技术应对复杂场景的威胁模型构建

D 溯源管控

控制攻击比例：基于从威胁情报贡献的安全指数；基于不断训练提升的系统可信度，对接威胁指数到其他控制体系实现管控

大数据风控系统架构

溯源管控

移动威胁管控中心

威胁报警、管控

移动威胁展示中心

威胁溯源

生成情报

设备威胁库

应用威胁库

账户威胁库

IP威胁库

威胁分析

规则自定义系统

异常规则定义

大数据分析系统

关联分析、决策树分析

数据采集

在线威胁采集系统

在线移动威胁攻击数据，含系统、应用、业务威胁数据

后台数据采集系统

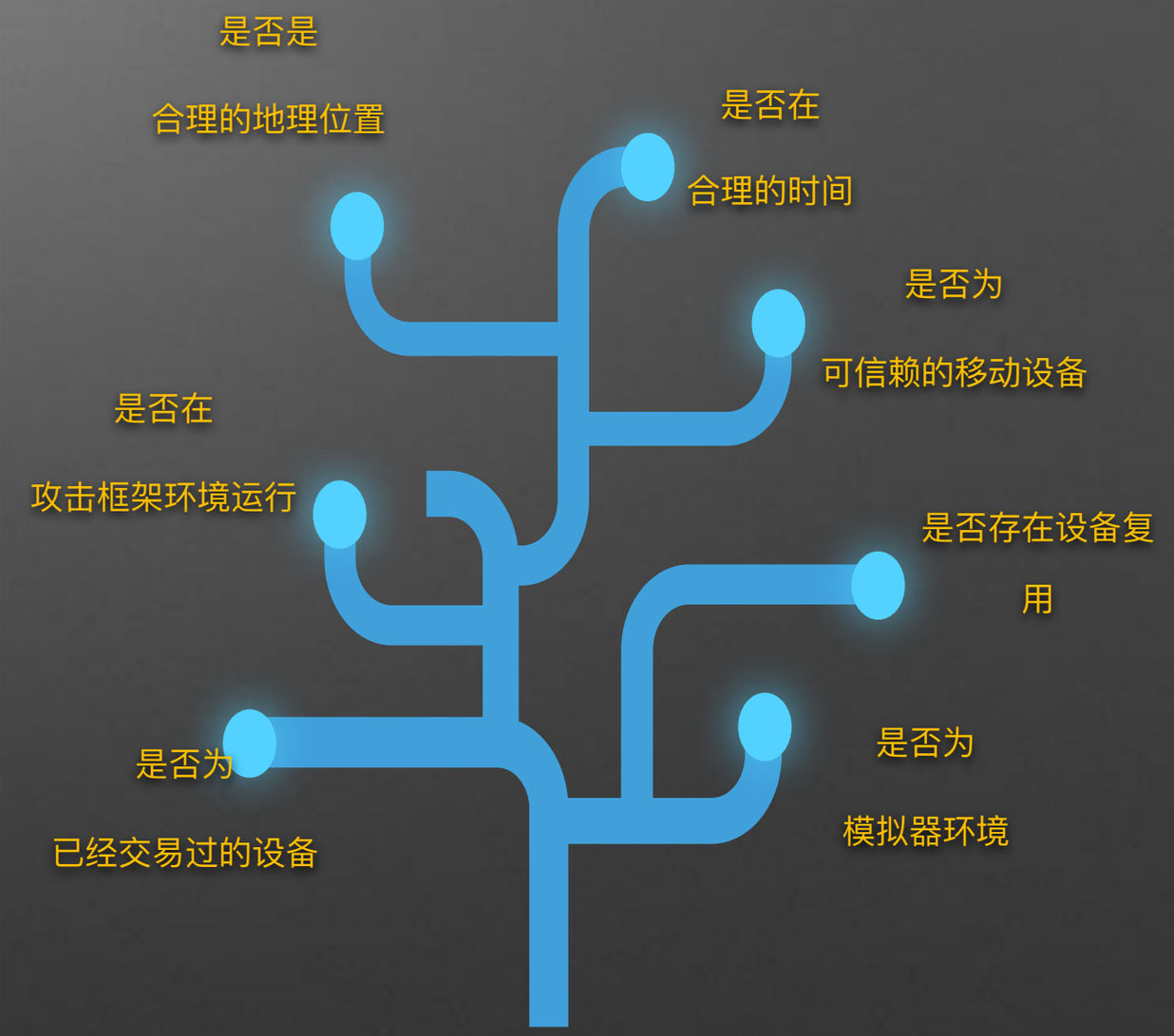
从日志报文中采集业务数据

第三方威胁采集系统

从域名、网络服务提供商、其他第三方安全中心等采集网络威胁数据

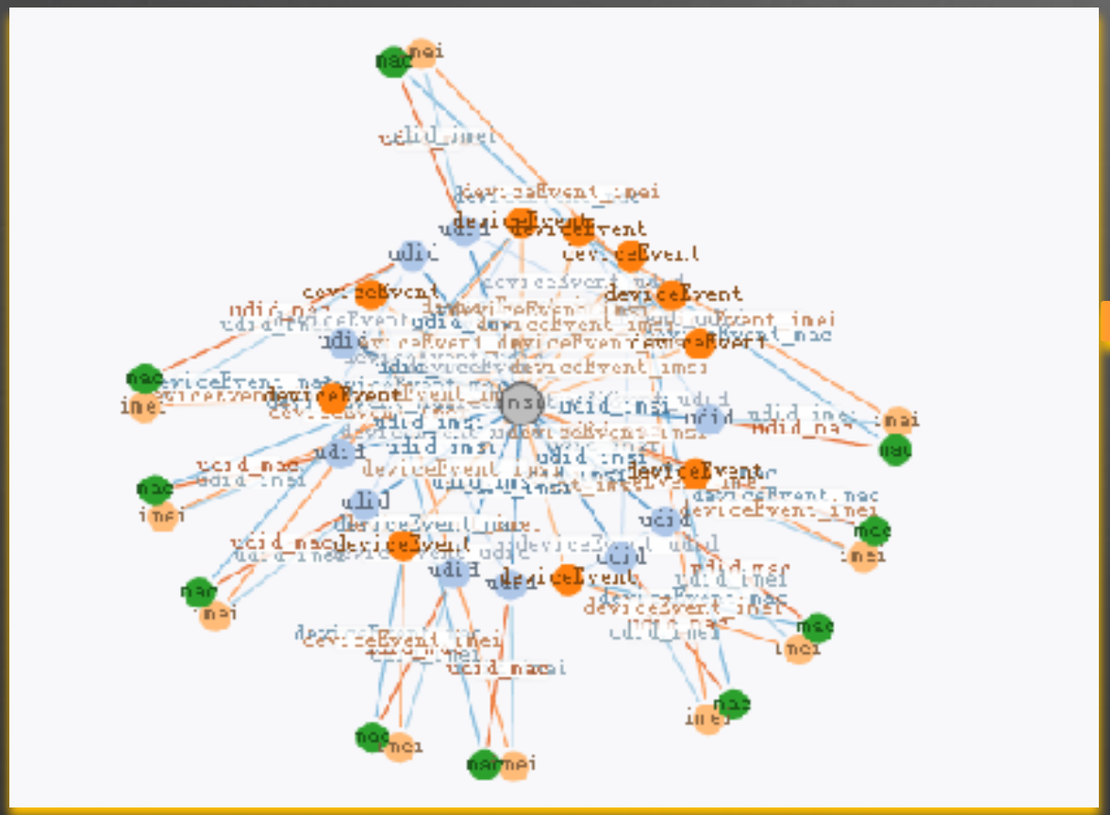
安全策略—威胁感知

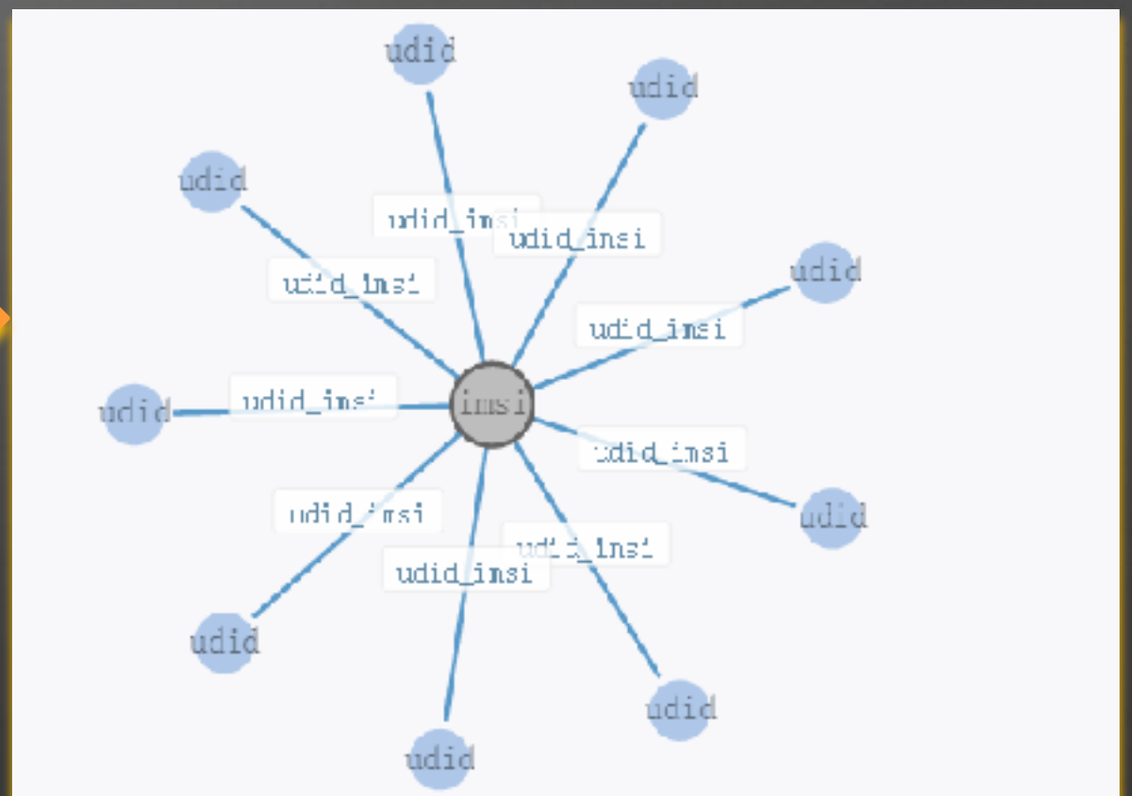
模块名称	采集的数据说明
设备复用检测	硬件信息、系统信息、应用信息、位置信息、函数劫持信息、系统root信息等
模拟器检测	硬件信息、系统信息、应用信息、配置信息、指令结果信息
加速器检测	时间信息、指令结果信息
攻击框架检测	Zygote信息、函数劫持信息
修改器检测	内存修改信息、文件修改信息、调试信息、注入信息
地理位置造假检测	地理位置信息、指令信息、函数劫持信息
本地域名劫持检测	本地域名信息、函数劫持信息
外挂检测	外挂修改的文件信息、外挂特征信息
应用崩溃检测信息	应用启动信息、堆栈信息、崩溃日志



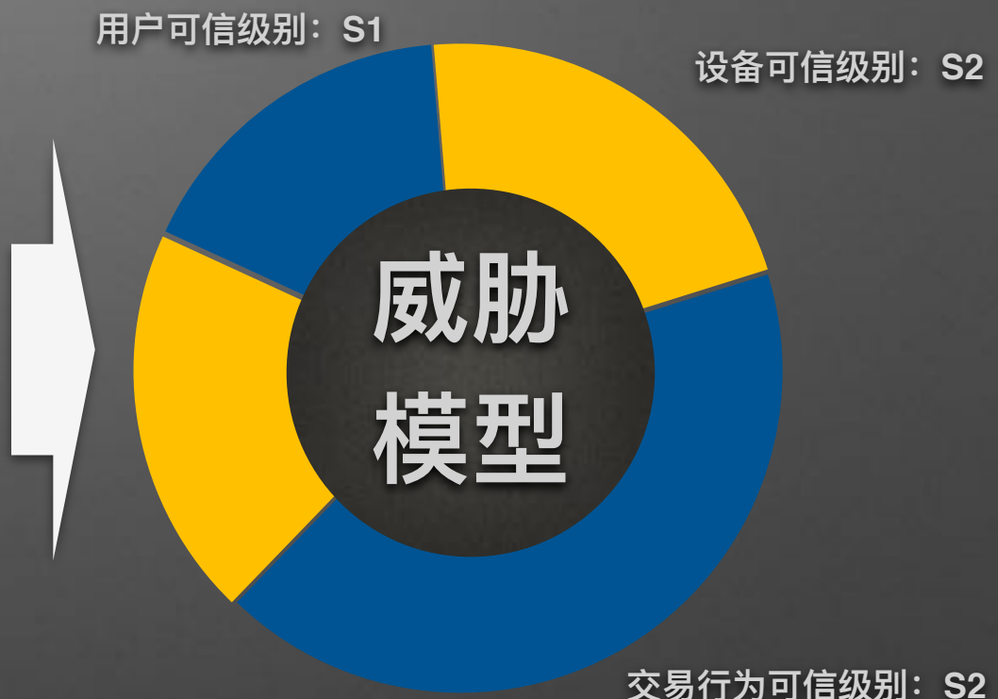
安全策略—威胁感知图论分析

图论分析方法能够提供更复杂场景下的建模和威胁分析





安全策略—威胁分析用户画像



以上信息会被赋予从0%～99.9%的可信率，然后综合计算出一个基于相似度的设备指纹，而设备指纹的确认不再基于是否一致，而是基于相似度。针对不同的设备指纹相似度，后台业务风控可采取不同等级及不同手段的控制措施：如拒绝登录、强制身份验证等。

数据驱动安全的最佳实践

数据驱动的安全感知

- 把分离抽象的数据提取成形象的［人］
- 通过机器学习，建立针对［好人］和［坏人］的行为模型
- 通过决策链条及实时收集的数据，建立每个［人］的安全威胁等级
- 建立不同等级的威胁指数，通过数据驱动指数变化
- 通过跨平台，跨客户的数据共享，建立同守同防的安全体系

梆梆安全

BANGCLE

保护智能生活