NSFOCUS TECHWORLD

智能 · 敏捷 · 可运营

TECHWORLD2015

绿 盟 科 技 技 术 大 会

暨第 3 届绿盟科技攻防大赛

NSFOCUS

移动互联网和移动支付的安全

闫绍华
系统架构部

密级：内部使用

目录

移动支付的总体概况

移动支付的总体概况

- 方便（Convenient）
- 便携（Portability）
- 高效（Efficiency）
- 易用（Usability）
- 安全（Security）

移动支付的总体概况

1. 移动支付（Mobile Payment）是用户通过手机等移动终端对消费的商品或服务进行支付的一种方式。

2. 移动支付技术将移动终端设备，互联网，应用提供商以及金融机构相融合，为用户提供货币支付、缴费等金融业务。

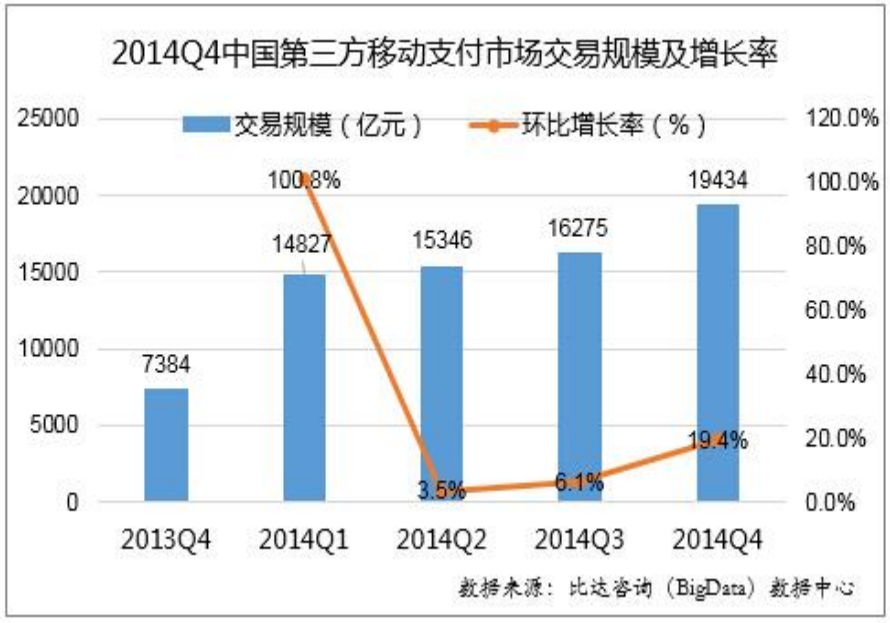
3. 与传统支付方式相比，移动支付具有"随时，随地，随身"，产业链长，行业跨度大，社会影响面广等特点。

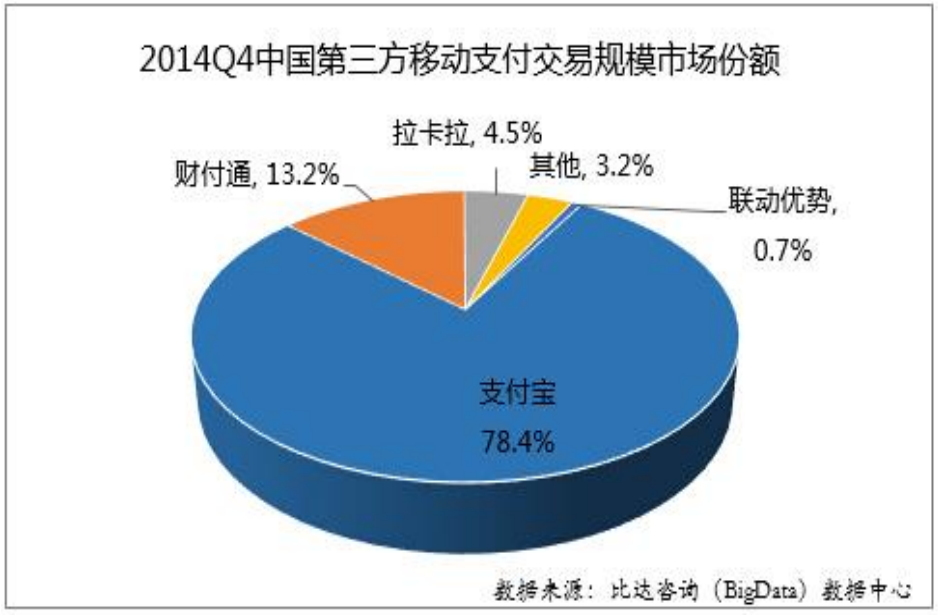
4. 随着我国移动支付业务的飞速发展，支付安全问题也成为全产业关注的最基本、最重要的问题之一。

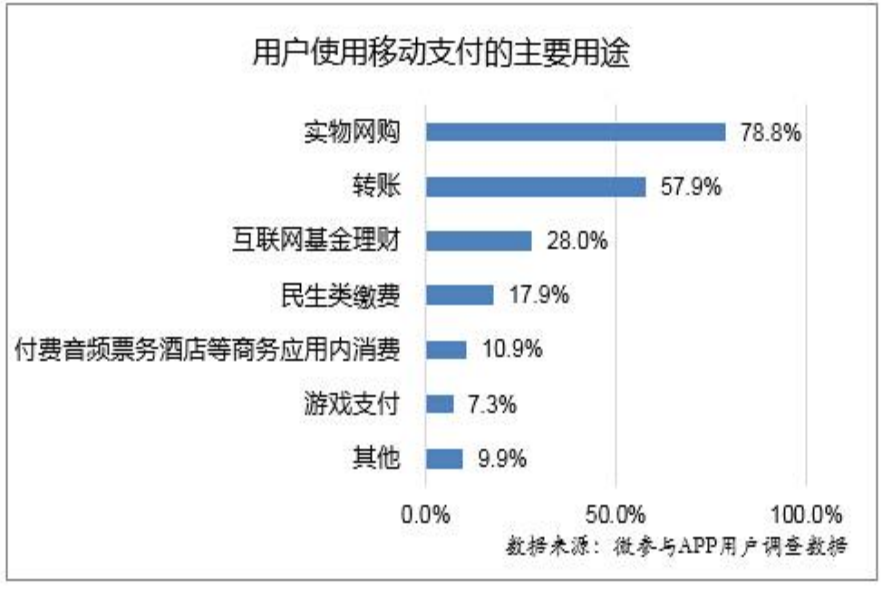
UnionPay 银联

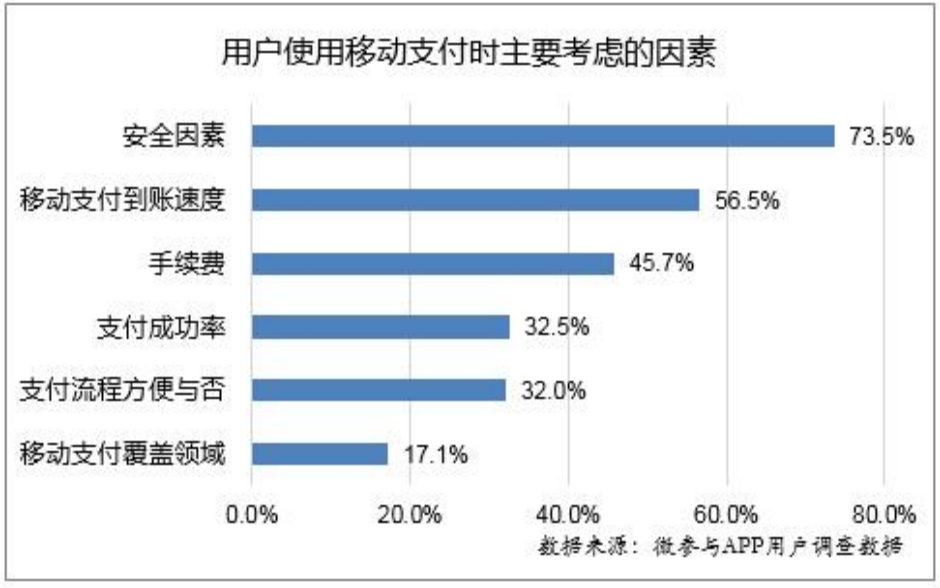
支付宝™

移动支付的总体概况


2014Q4中国第三方移动支付市场交易规模及增长率
交易规模（亿元）
环比增长率（%）
25000
20000
15000
10000
5000
0
120.0%
100.0%
80.0%
60.0%
40.0%
20.0%
0.0%
7384
14827
15346
16275
19434
100.8%
3.5%
6.1%
19.4%
2013Q4
2014Q1
2014Q2
2014Q3
2014Q4
数据来源：比达咨询（BigData）数据中心


2014Q4中国第三方移动支付交易规模市场份额
拉卡拉, 4.5%
其他, 3.2%
财付通, 13.2%
联动优势, 0.7%
支付宝 78.4%
数据来源：比达咨询（BigData）数据中心


用户使用移动支付的主要用途
实物网购 78.8%
转账 57.9%
互联网基金理财 28.0%
民生类缴费 17.9%
付费音频票务酒店等商务应用内消费 10.9%
游戏支付 7.3%
其他 9.9%
0.0%
50.0%
100.0%
数据来源：微参与APP用户调查数据


用户使用移动支付时主要考虑的因素
安全因素 73.5%
移动支付到账速度 56.5%
手续费 45.7%
支付成功率 32.5%
支付流程方便与否 32.0%
移动支付覆盖领域 17.1%
0.0%
20.0%
40.0%
60.0%
80.0%
数据来源：微参与APP用户调查数据

移动支付的实现方式

➢ 远程支付Remote Payment：

1. 使用SMS(Short Message Service)短消息业务
2. WAP(Wireless Application Protocol)无线应用
3. IVR(Interactive Voice Response)互动式语音应答
4. USSD(Unstructured Supplementary Service Data)非结构化补充业务数据

➢ 近距离支付Local Payment：

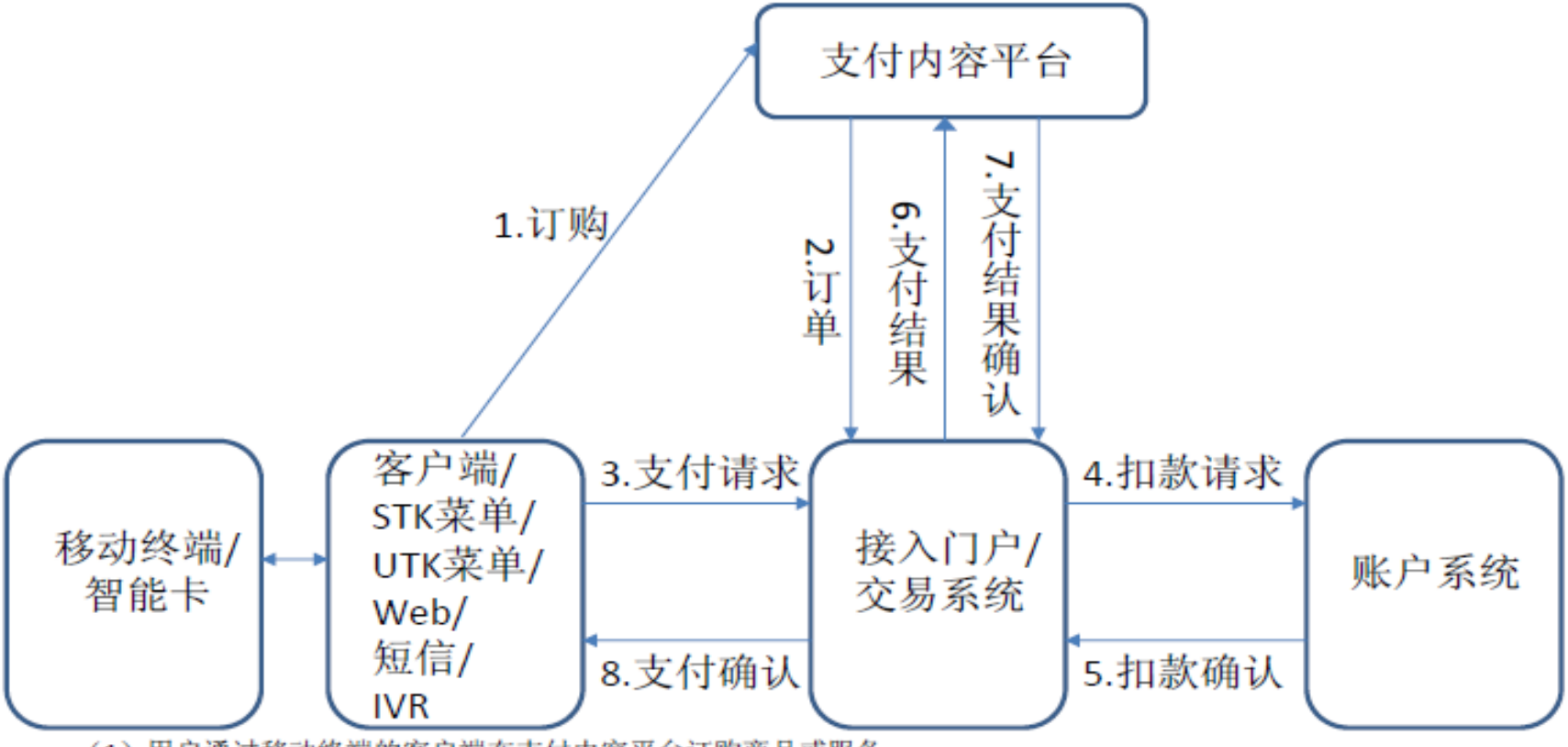
1. 双界面SIM卡技术（SIM-Pass）
2. RFID-SIM卡技术（基于2.4G Hz）
3. NFC（Near Field Communication）技术（基于*13.56M* Hz）

NFC技术架构

RFID的一种 | 距离10 CM | 非接触 | 速率几百Kbit/s

双向识别和连接 | 功耗低 | 成本低 | 安全性好

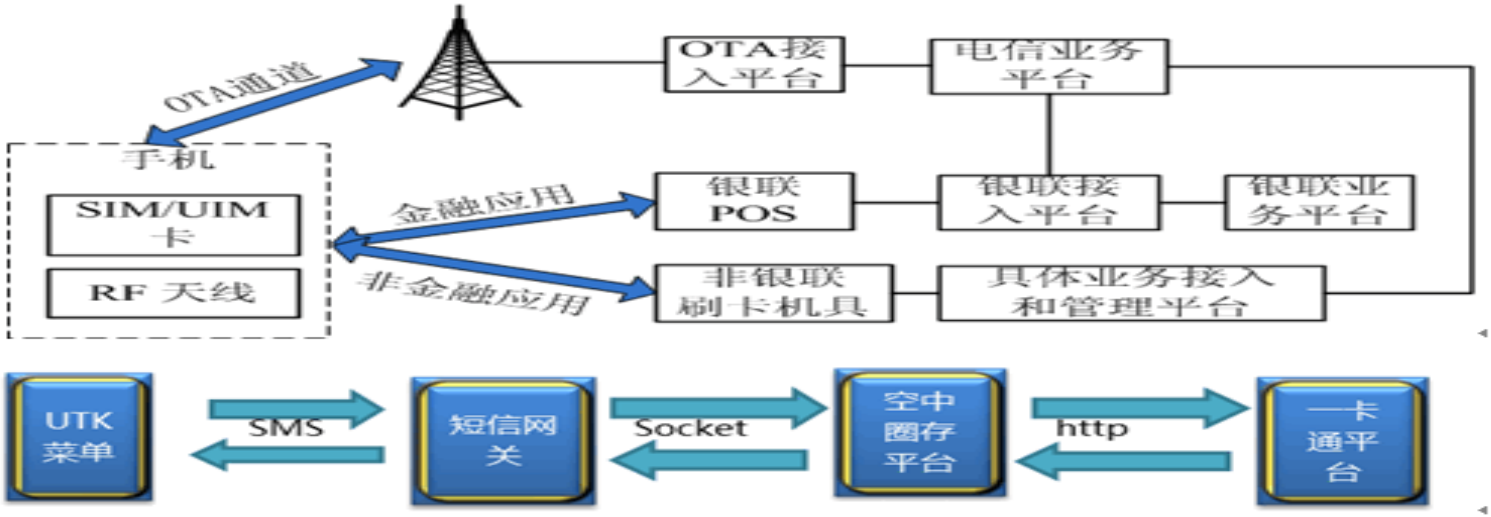
远程支付流程



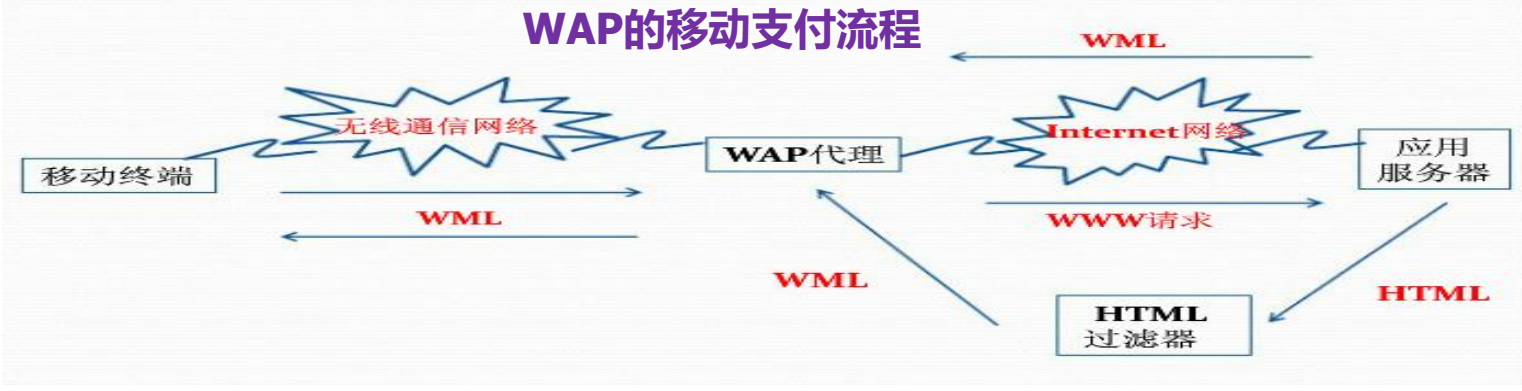
（1）用户通过移动终端的客户端在支付内容平台订购商品或服务
（2）支付内容平台向移动支付交易系统提交订单
（3）用户通过移动终端向移动交易系统发起支付请求
（4）移动支付交易系统接收用户支付请求，检查用户的订单信息，向账户系统发起扣款请求
（5）账户系统接收扣款请求并对用户账户信息进行鉴权，鉴权通过后完成转账付款并发送扣款确认信息给支付交易系统
（6）支付交易系统将支付结果通知支付内容平台
（7）支付内容平台向支付交易系统返回支付结果确认的应答
（8）支付交易系统为支付客户端返回支付成功确认，完成交易流程

远程支付流程

SMS和USSD的移动支付流程

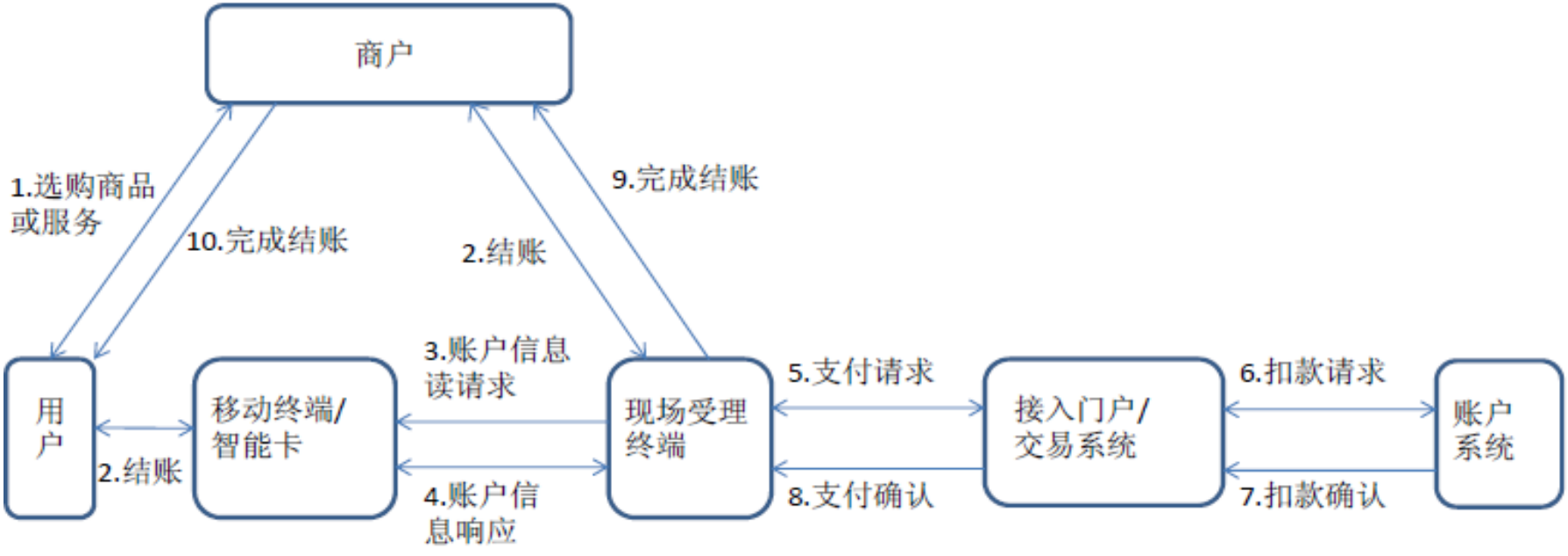


WAP的移动支付流程



SMS	基于GSM的SMS	非连接，非独立通道	交互性差，适合小额支持福
USSD	基于GSM的SMS	面向连接，独立通道	适合交易型业务
WAP	基于GSM的GPRS	面向连接，安全通道	适合交易型业务

近场支付（联机消费）流程



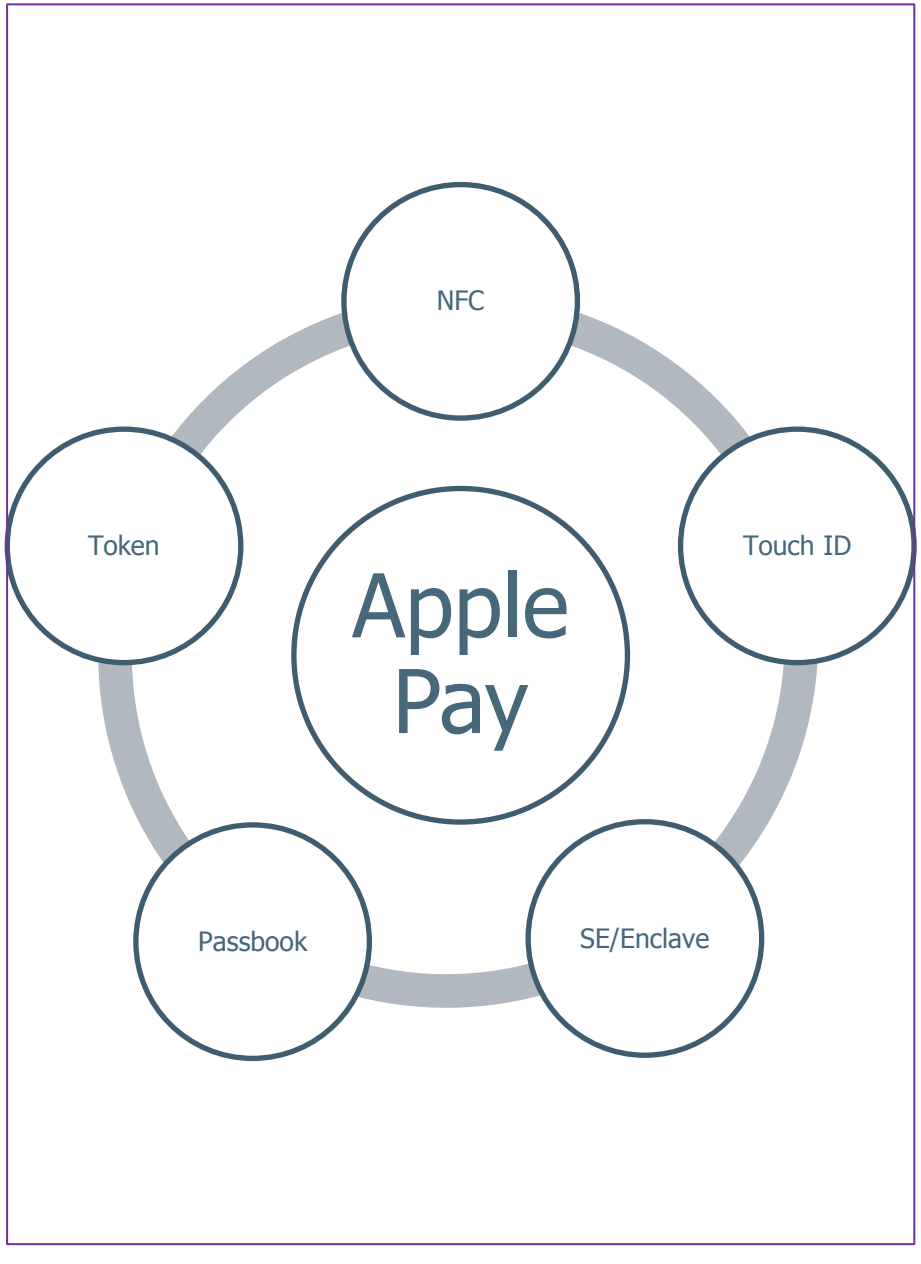
（1）用户在商户店内选择商品或服务
（2）用户到商户收银台结账
（3）商户在现场受理终端（POS）上输入消费金额，通过近场通信技术向移动终端/智能卡发起账户信息读取请求
（4）移动终端/智能卡将账户信息发现给现场受理终端
（5）现场受理终端发送支付请求指令给交易系统
（6）交易系统发送账户扣款请求给账户系统
（7）账户系统受到扣款请求后，进行用户账户鉴权，返回扣款确认信息
（8）交易系统返回支付确认信息给受理终端
（9）完成结账过程

移动支付的类型

基于APP的支付 Vs 基于OS的支付

- 第三方支付类
- 电商类
- 团购类
- 理财类
- 银行类

Apple Pay技术



NFC

- 近距离通信模块，和SIM卡分离
- 不支持读卡器和点对点模式
- Only Apply Pay

Touch ID

- 指纹识别，替代密码输入
- 存储安全

Passbook

- 电子钱包
- 管理银行卡

SE

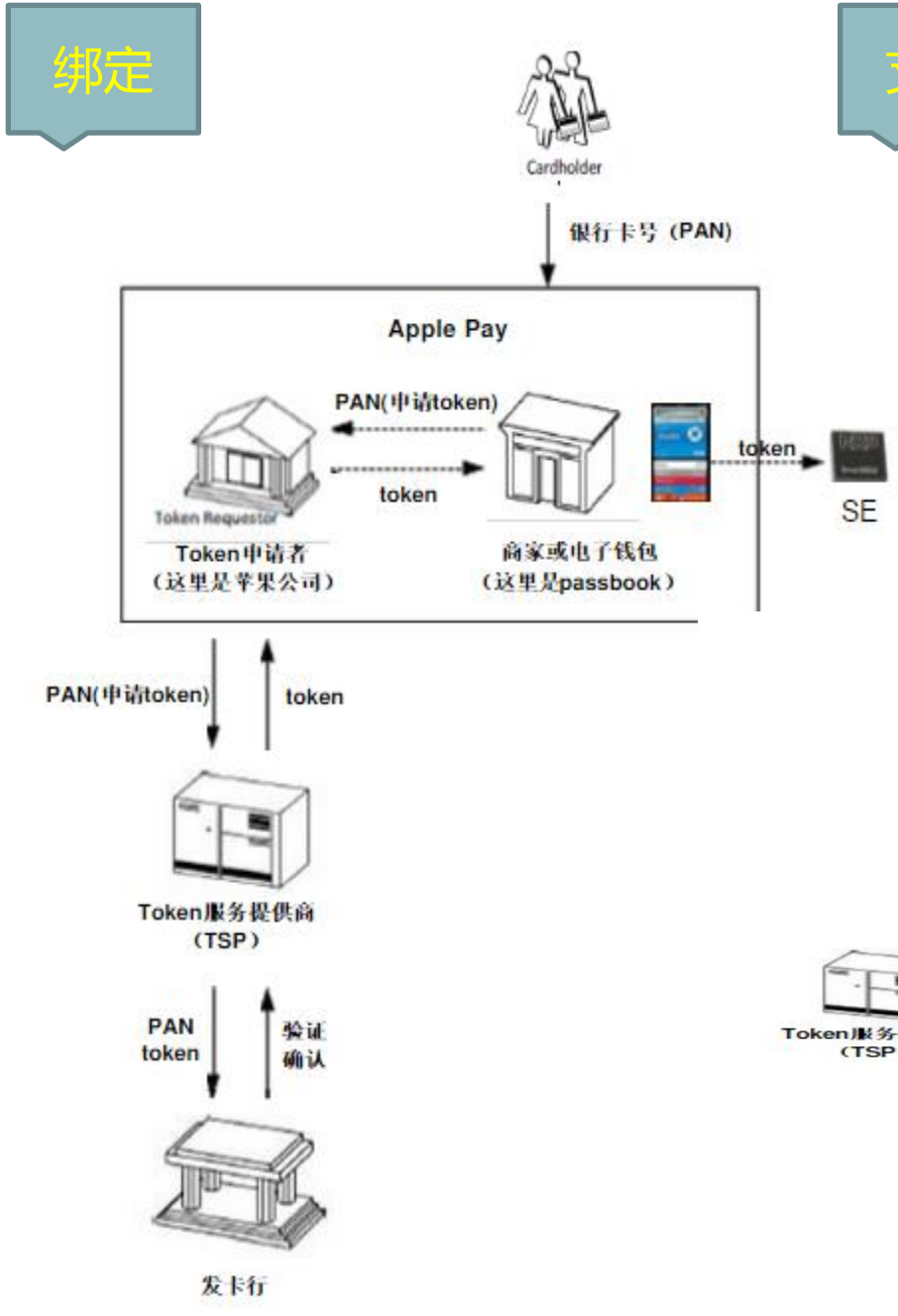
- 安全元件
- 存储Token和密钥

Token

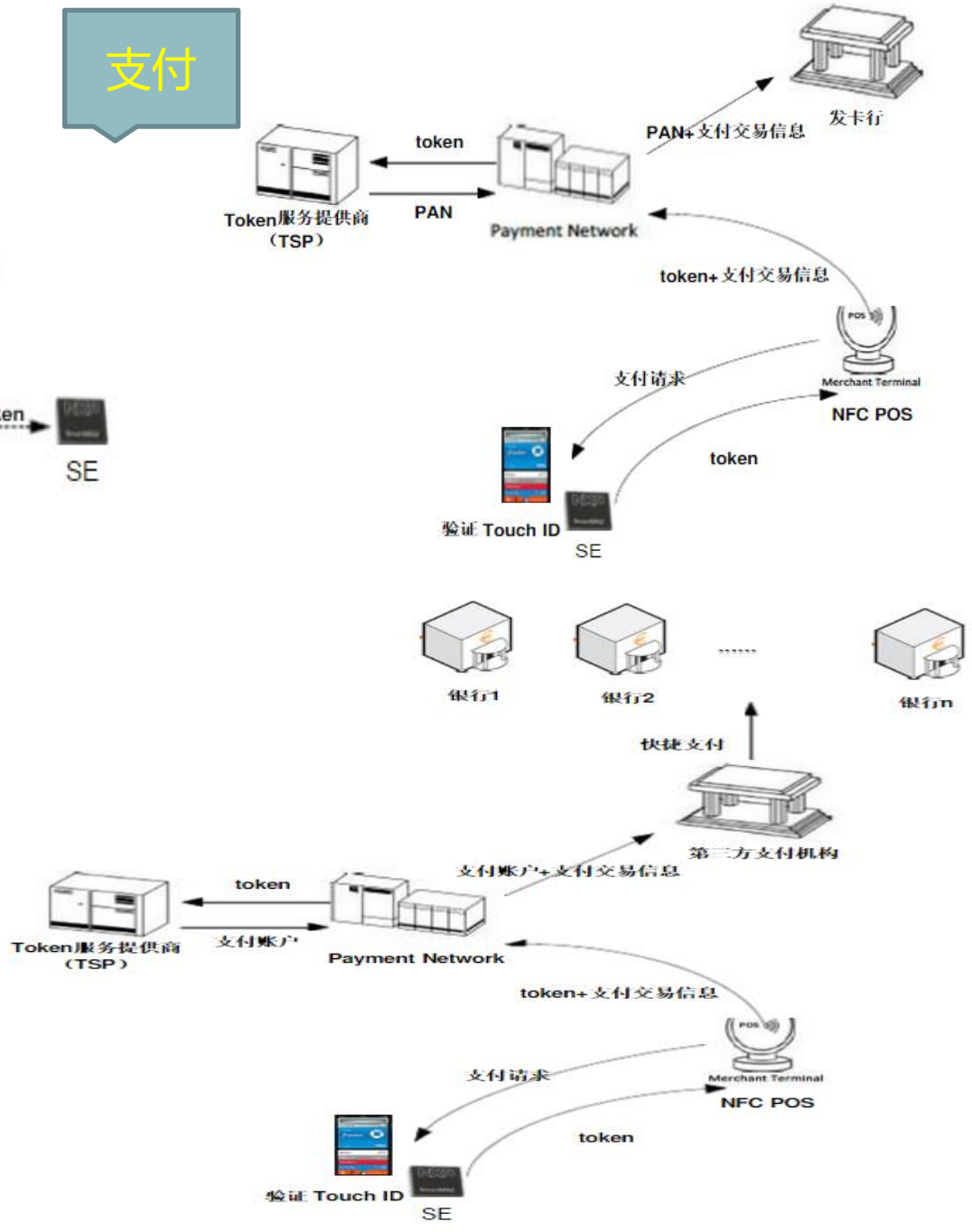
- 银行卡号的别名，避免敏感信息外泄
- 动态安全码

Apple Pay技术

绑定



支付



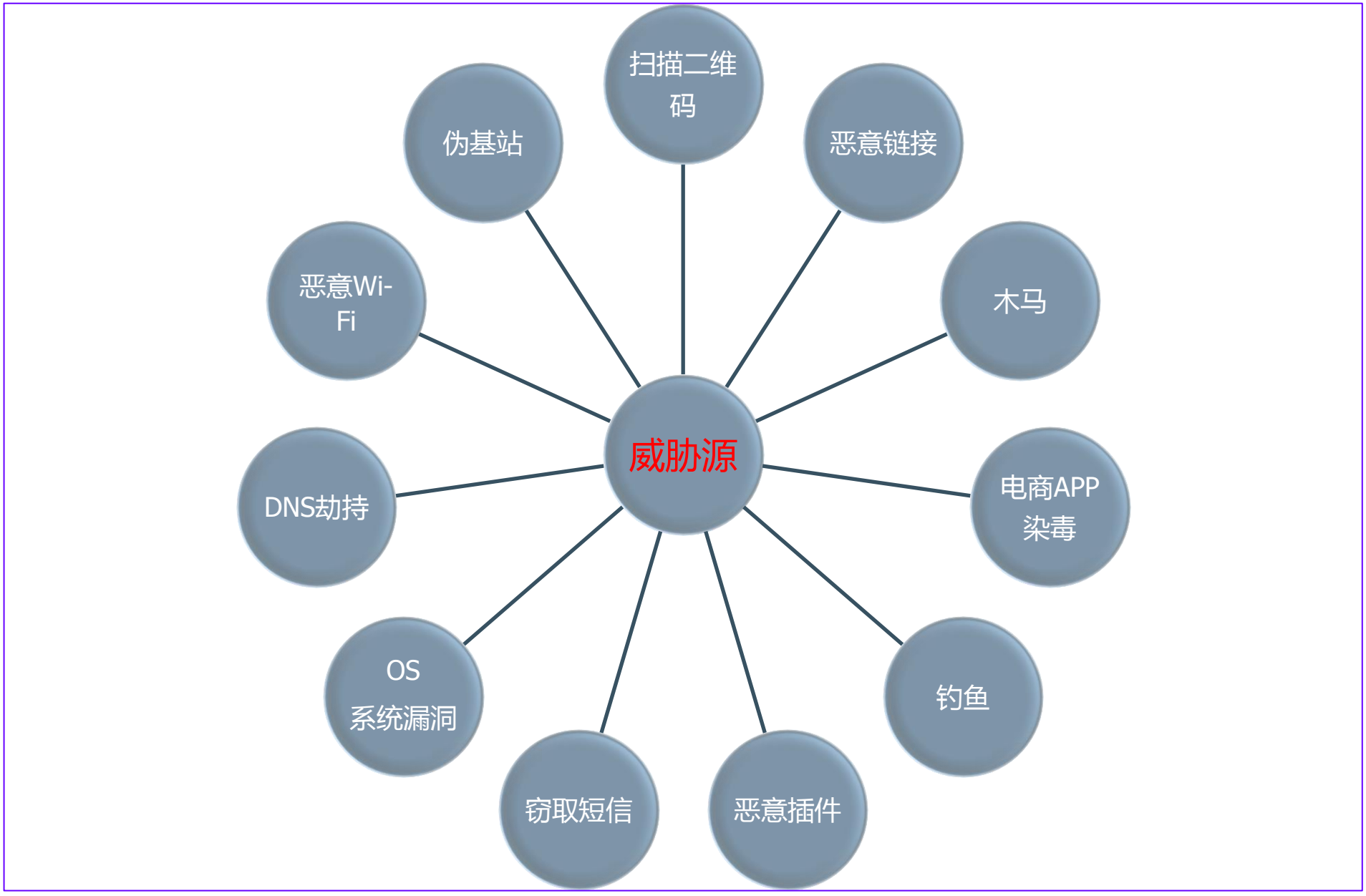
移动支付的安全威胁和目标

移动支付的安全威胁

- 被动攻击：
  1. 嗅探: Sniff
  2. 信息收集：Collection
  3. 无线截获：Interception

- 主动攻击：
  1. 假冒：Masquerading
  2. 重放攻击：Replay Attacks
  3. 修改：Modification
  4. 拒绝服务：Denial of Service
  5. 伪造：Fabrication
  6. 否认：Repudiation

移动支付的安全威胁


威胁源
扫描二维码
伪基站
恶意链接
恶意Wi-Fi
木马
DNS劫持
电商APP染毒
OS系统漏洞
钓鱼
窃取短信
恶意插件

网上已经明码标价开卖此类木马

WooYun.org

加关注 14万

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 乌云峰会 | 乌云招聘 | 知识库 | 公告

当前位置：WooYun >> 漏洞信息

漏洞概要

缺陷编号： **WooYun-2014-53947**

漏洞标题： 某移动支付产品存在远程命令执行漏洞

相关厂商： **某支付产品**

漏洞作者： **路人甲**

提交时间： 2014-03-18 14:02

公开时间： 2014-05-02 14:03

漏洞类型： 命令执行

危害等级： 中

自评Rank： 5

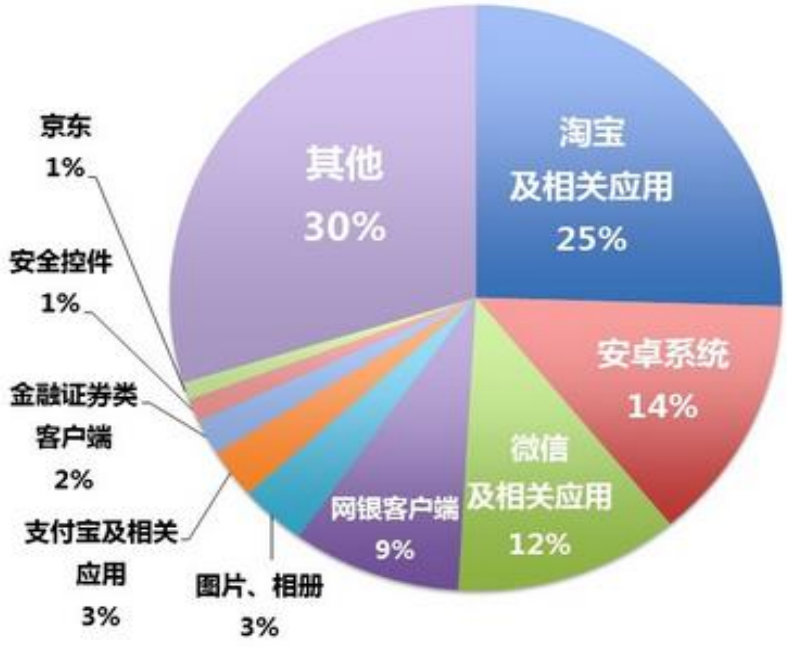
漏洞状态： 已交由第三方合作机构(cncert国家互联网应急中心)处理

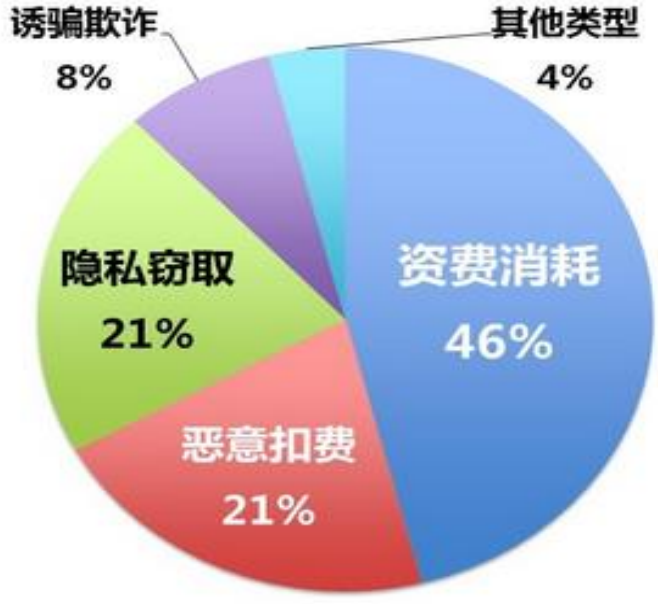
漏洞来源： **http://www.wooyun.org**

Tags标签： **struts**

分享漏洞： 分享到 0

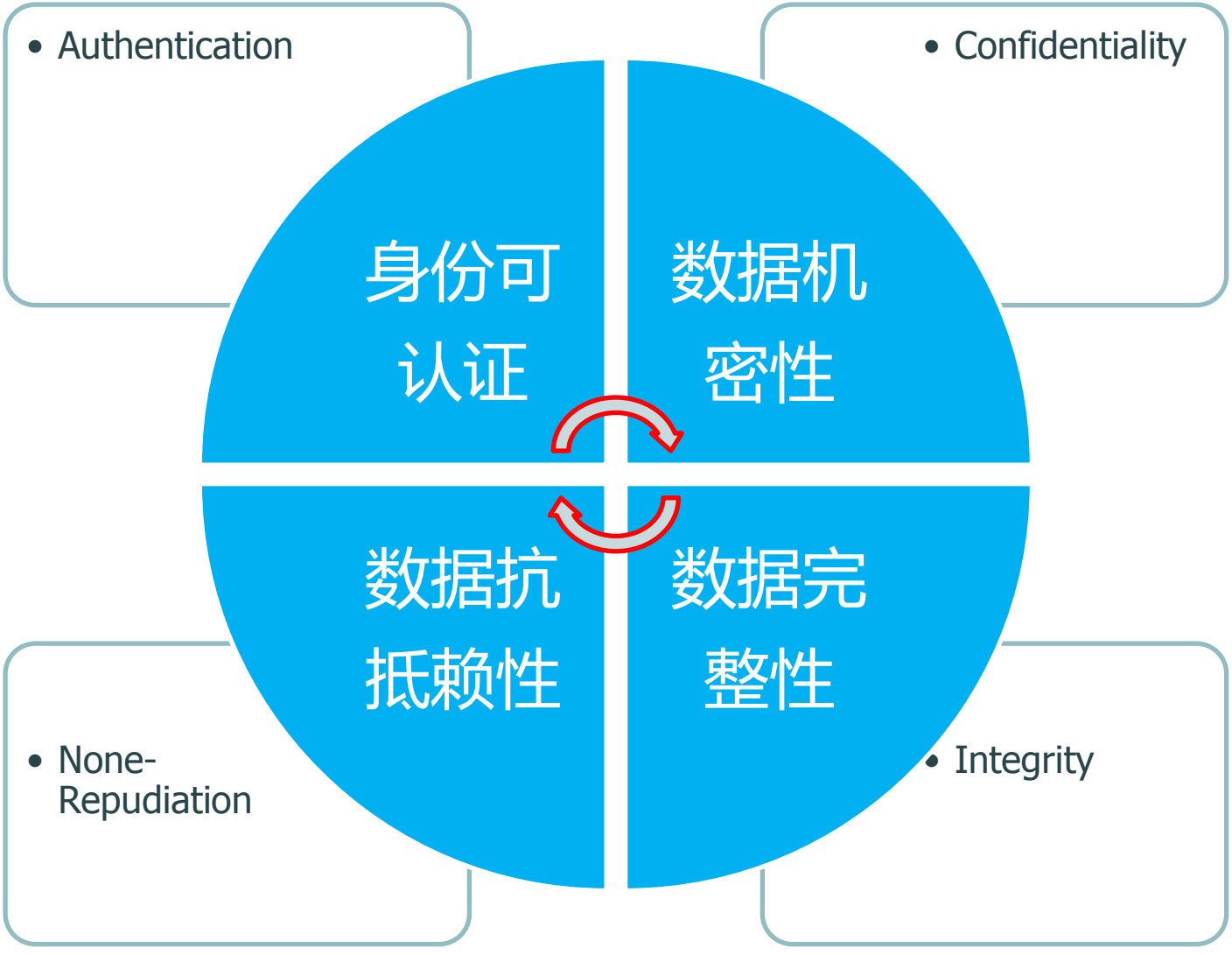
手机APP的安全威胁统计





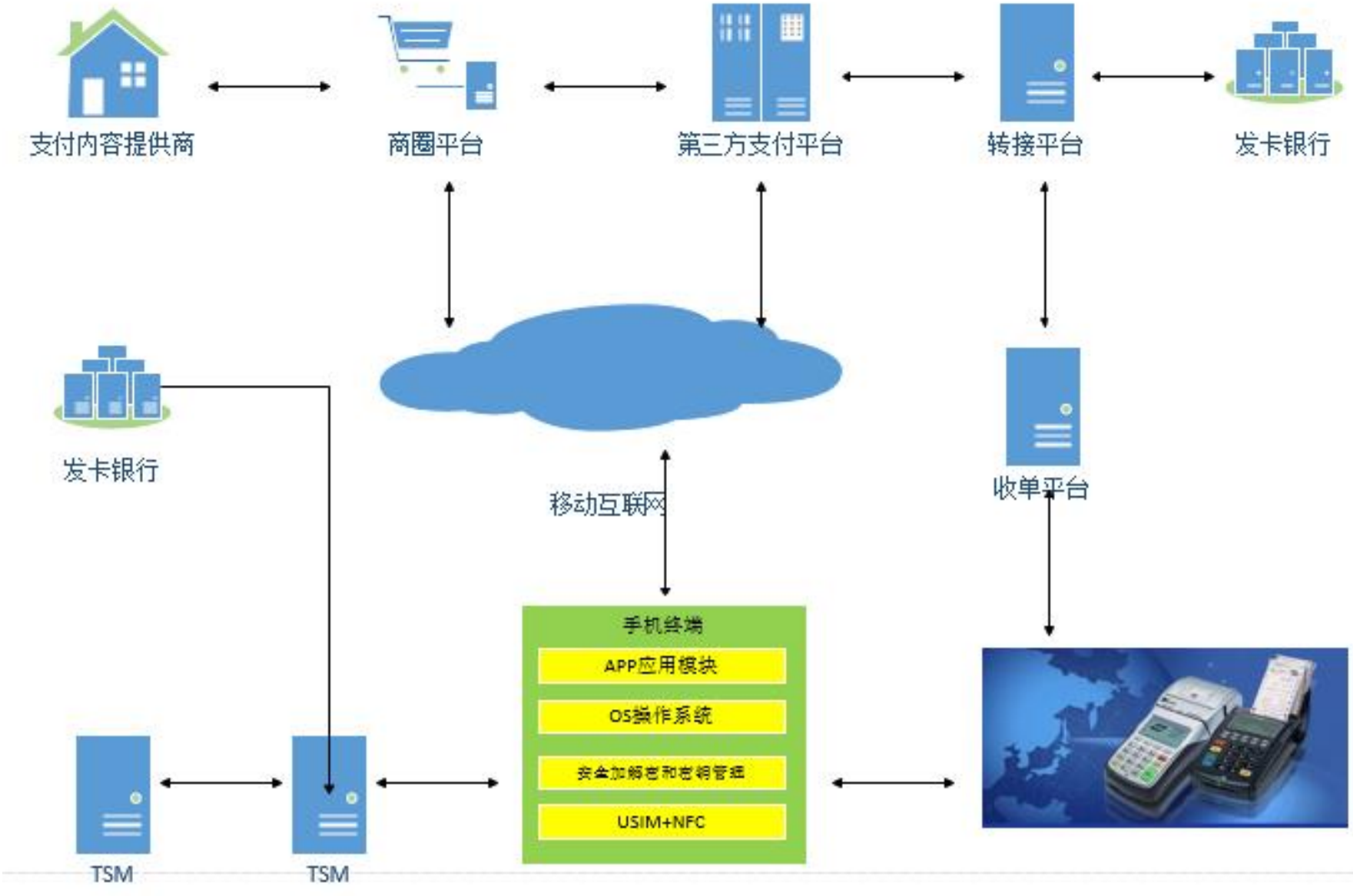
漏洞类型	漏洞危害
后台消息	恶意程序可在用户不知情的情况下在后台向指定号码发送消息
签名漏洞	恶意程序可在不改变正常程序签名的情况下篡改这些程序
短信欺诈	恶意程序可向机主手机发送欺诈短信
后台电话	恶意程序可在用户不知情的情况下在后台向指定号码拨打电话
清除数据	恶意程序可以恶意删除手机中的文件或信息
静默安装	恶意程序可以在后台静默安装，用户不知情。
静默联网	恶意程序在后台静默联网

移动支付的安全目标


• Authentication
• Confidentiality
身份可认证
数据机密性
数据抗抵赖性
数据完整性
• None-Repudiation
• Integrity

移动支付的体系结构和安全

移动支付的体系结构


支付内容提供商
商圈平台
第三方支付平台
转接平台
发卡银行
发卡银行
移动互联网
收单平台
手机终端
APP应用模块
OS操作系统
安全加解密和密钥管理
USIM+NFC
TSM
TSM

移动支付的安全

- USIM卡多业务安全域划分，电子钱包，电子信用卡，电子票据
- 加密算法，椭圆曲线算法ECC
- 加密密钥CK和完整性密钥IK
- 双向鉴权
- 用户访问权限控制
- 支持NFC的SIM卡
- Android系统安全
- IOS系统安全

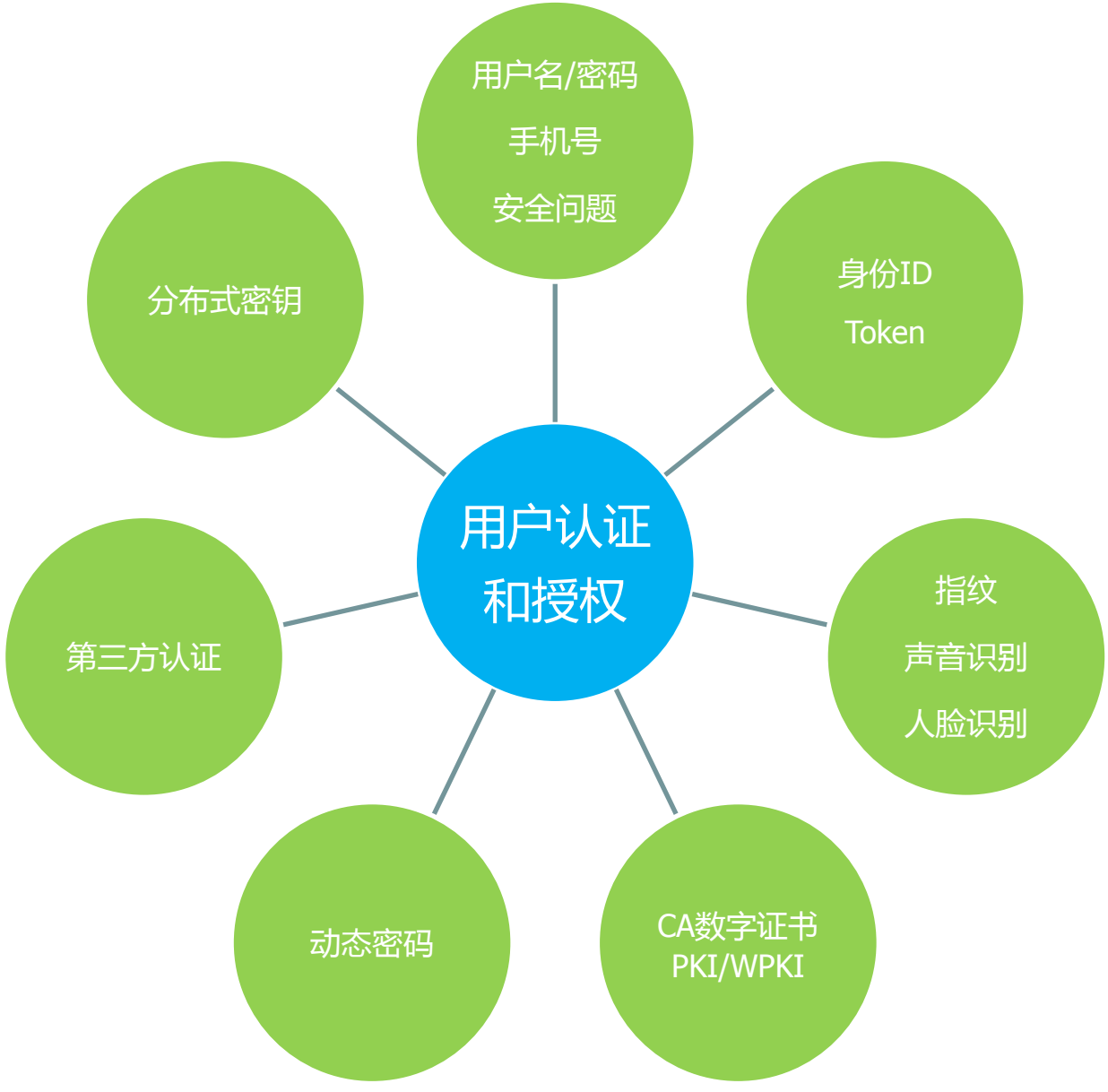
- 高可靠性
- 高性能
- 数据传输加密（HTTPS/SSL）
- 数据存储加密和访问控制
- 防火墙和入侵检测
- VPN

- 银行监管第三方支付平台，支付宝，信支付，财付通
- 用户和银行卡绑定安全
- 用户和第三方支付帐号
- 用户体验和安全的取舍
- 日志审计
- 保险制度

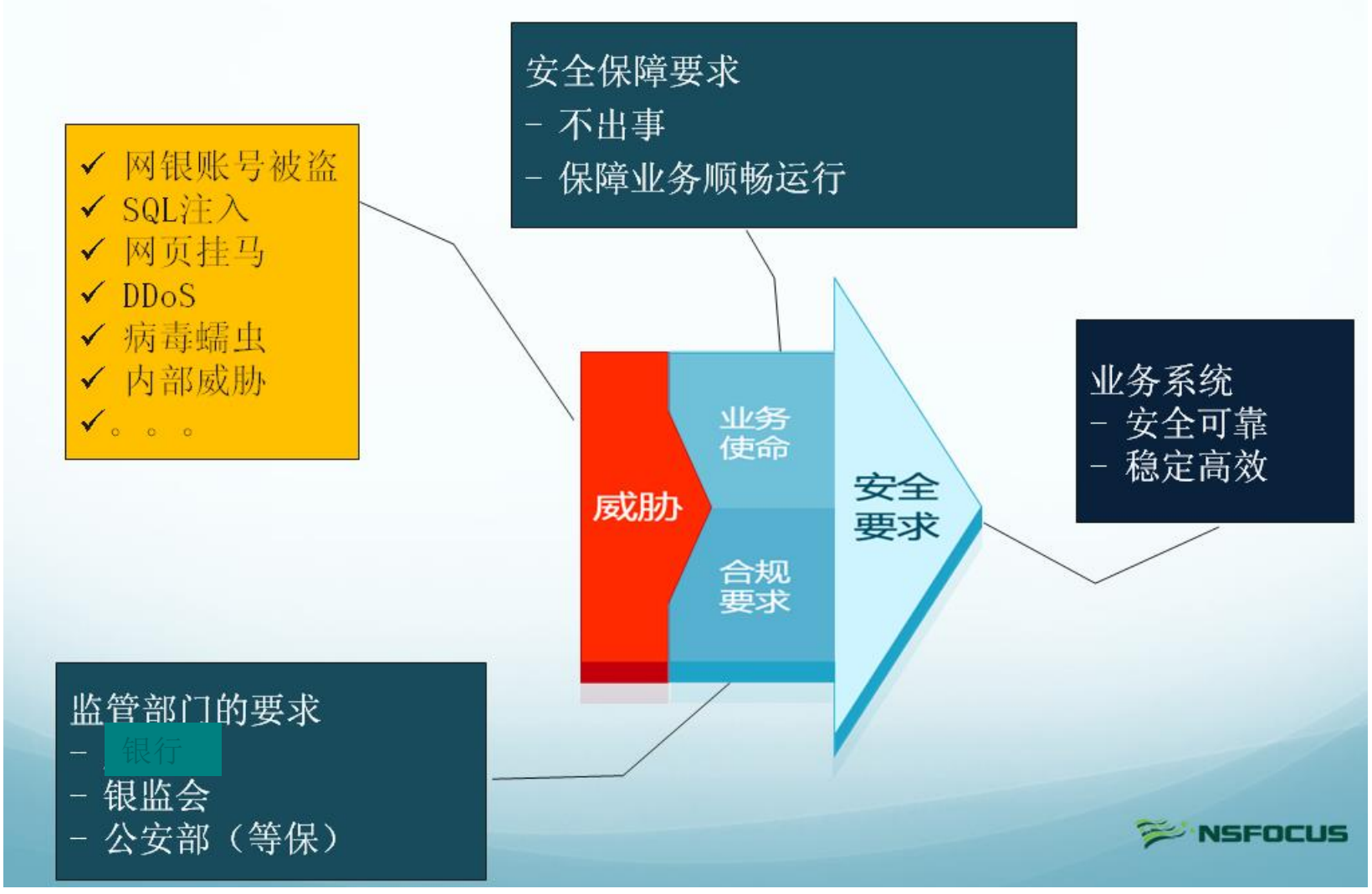
- 防止支付类APP病毒，挂马
- 反编译后钓鱼
- APP账号自身安全
- 防止二次打包
- 支付平台接口SDK的安全性
- 防止键盘和输入法攻击
- 防止界面截取

移动支付的安全

- 静态口令 → 动态口令
- 软件加密 → 硬件加密
- 单因子认证 → 多因子认证
- 加密密钥 → 生物特征识别



绿盟科技 NSFOCUS
您的专业安全服务顾问



绿盟科技 NSFOCUS
您的专业安全服务顾问

移动APP端	服务器端
证书验证	输入验证
组件安全	身份认证
数据保护	授权管理
代码保护	会话管理
键盘保护	异常处理
反编译保护	日志管理
进程保护	数据保护

谢谢！

NSFOCUS TECHWORLD

智能 · 敏捷 · 可运营

TECHWORLD2015

绿 盟 科 技 技 术 大 会

暨第 3 届绿盟科技攻防大赛

NSFOCUS