OWASP

Open Web Application Security Project

金融企业如何构建安全的移动支付平台

演讲人：陈绍良　普华永道

演讲者介绍

陈绍良先生，普华永道风险管理资深专家

拥有超过十二年的风险管理从业经历

其在信息安全、信息科技治理及服务管理

内部控制及合规性检查，商业连续性管理等领域能力突出

业内知名的金融行业风险管理专家

参与国内外金融机构的风险管理体系建设

对于交易风险控制有着独到见解

同时信息安全领域有着丰富的实践经验

带领团队多次高质量地完成项目实施

主要服务于金融、互联网、运营商领域

目录

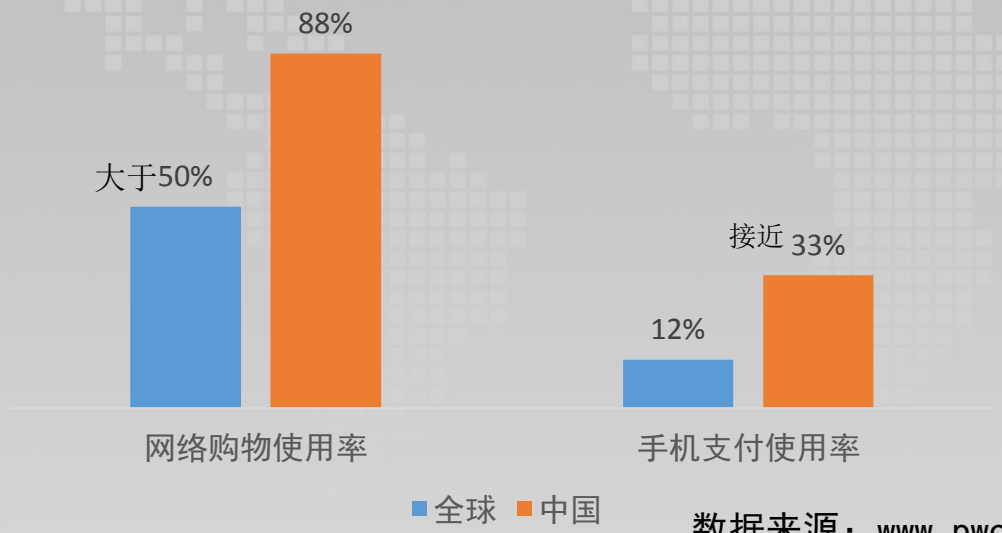
移动支付平台现状与生态
移动支付的主要风险分析
移动支付安全风应对之道

1. 纵观全局-了然于心

关键词:现状　特点

一组统计数据

普华永道2016年一份全球零售消费分析报告显示中国引领全球网络购物革新，手机在网购中的作用愈加重要。据国外数据显示2019全球移动支付收入达到10800亿美元



全球超过一半的消费者已通过手机进行网络购物，在中国这一比例高达*88%*

全球有12%以及中国有近三分之一消费者在网购时选择使用手机支付。

数据来源：www.pwccn.com　　www.statista.com

移动支付定义与要素

移动支付是指允许用户使用移动支付终端对所消费的商品或服务进行账务支付的一种服务方式，主要分为近场支付和远程支付两种。

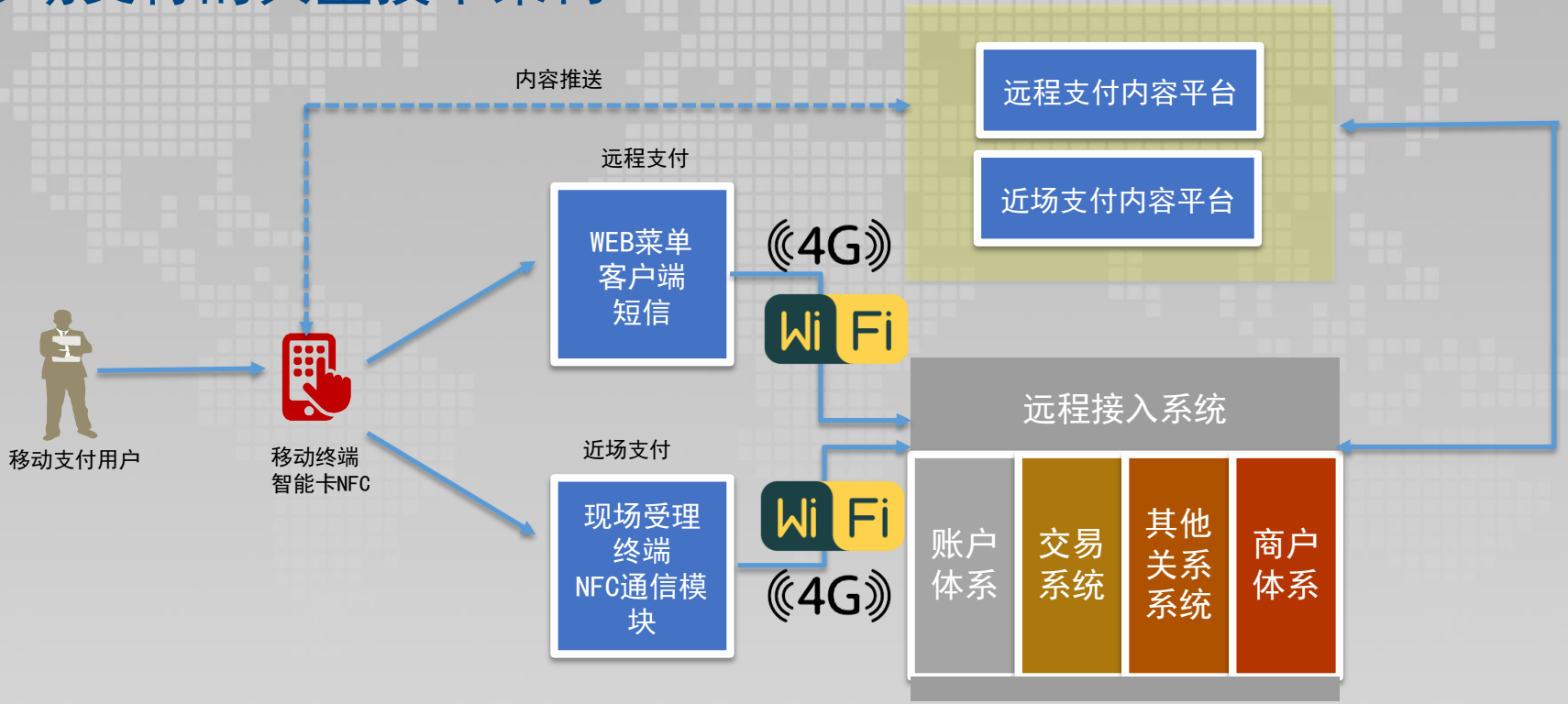
近场支付的典型场景：NFC消费
远程支付的典型场景：手机扫码支付，二维扫码

远程移动支付的关键要素：智能手机，APP客户端应用，APP应用服务器，网络通道（WIFI/3G/4G）
近场移动支付的关键要素：智能手机，智能手机NFC模块，APP客户端应用，APP应用服务器，网络通道（WIFI/3G/4G）

远程支付（扫码）

近场支付（NFC）

移动支付的典型技术架构



移动支付运营分布形态

- 以传统商业银行金融机构为代表的构建的自有移动支付平台 如中国的四大银行和商业银行，同时也尝试接入各类商户或自建购物平台。
- 拥有跨国支付通道的机构，如PayPal、VISA、中国银联，构建的移动支付平台，同时也尝试接入各类商户或自建购物平台。
- 拥有第三方支付平台的互联网金融或互联网企业，通常自建各类消费场景，同时提供给各类企业的支付通道，代表公司阿里支付宝、腾讯微信、Apple Pay。
- 互联网金融企业，如互联网理财，互联网保险等，部分拥有支付通道，也建立了完整的支付链条和生态体系。
- 以电子商务企业为代表的一支力量，早期外部接入各类支付通道，目前多购买支付通道，打造自身移动支付平台。
- 以提供聚合各类支付通道的公司，多为后起之秀。

目前国内市场支付宝和微信占具领先地位

目前跨境移动支付，中国银联拥有突出优势

移动支付安全规范和要求

- 《YD/T 2502-2013 移动终端安全技术要求》
- 《YD/T 2502-2013 移动终端安全测试办法》
- 《中国银联移动支付技术规范》
- 《移动终端支付可信环境技术规范》
- 《中国金融移动支付 安全单元 第1部分：通用技术要求》
- 《中国金融移动支付 安全单元 第2部分：多应用管理规范》
- 《中国金融移动支付 远程支付应用 第6部分：基于安全单元（SE）的安全服务技术规》
- 《中国金融移动支付 应用安全规范》
- 《中国金融移动支付 联网联合 第6部分：安全规范》
- 《中国金融移动支付 检测规范 第2部分：安全芯片》
- 《中国金融移动支付 检测规范 第3部分：客户端软件》
- ……

可参考工信部 中国银联 支付清算协会等网站

2. 正视风险– 运筹帷幄

关键词：风险分析

移动支付典型风险场景


钓鱼网站
水坑攻击
访问
黑客搭建钓鱼网站，控制用户手机
消费者
商户
社会工程
黑客通过地下产业链获取用户的敏信息，进而对用户采取更进一步的窃取资金的行动
NFC模块
边缘信道攻击
黑客尝试本地拦截NFC通信模块与手机通信机制
4G
Wi Fi
1黑客搭建Fake WiFi拦截网络通信，中间人攻击，窃取敏感信息
2. 黑客搭建基站
钓鱼网站
鱼叉攻击
黑客搭建钓鱼网站，实施鱼叉攻击，控制内部员工电脑
鱼叉攻击
内部员工
洪水攻击
僵尸网络
黑客直接攻击服务器，如利用SQL注入，或者DDOS攻击直接使网站瘫痪

移动支付安全风险分析

要素	脆弱性分析	安全威胁	风险影响
自然人客户&设备	1. 安全意识薄弱，受到欺诈， 2. 手机操作系统的健壮性， 3. 手机是否root	网络钓鱼 电话诈骗 越权控制	数据泄露 资金受侵害 手机被控制 隐私泄露
客户端APP	1. APP本身的代码安全问题，如SQL注入 2. APP源代码保护，反破解 3. APP文件管理，加密管理 4. 外部接口的调用的安全问题	APP源代码破解 黑客攻击	数据泄露 客户端手机被控制
网络通信	1. 通信未加密 2. 密钥管理不严	1. 中间人攻击 2. NFC通信攻击 3. 蓝牙攻击	信息泄露，交易金额被篡改
服务器端	1. 服务器操作系统&内部网络安全问题 3. 服务器端的应用安全问题 4. 与外部接口的安全问题，	1. 黑客攻击 2. DDOS攻击	服务瘫痪 服务器被控 APT攻击

移动支付安全风险分析

要素	脆弱性分析	安全威胁	风险影响
数据安全	1. 数据安全存储风险 2. 数据的脱敏 3. 用户隐私的保护	黑客嗅探攻击 黑客社工	数据泄露 隐私泄露 社会影响
账户管理	1. 账户权限划分不严 2. 账户认证不严 3. 内部监管不严	越权访问 绕过认证机制访问 内部人员犯罪	1. 系统被控 2. 用户资金受损 3. 数据泄露
交易安全	APP安全逻辑设计 业务逻辑问题	用户黑客欺诈 商户欺诈	交易受损 用户受损

事件高发原因

- 金融风险隐蔽性、传染性、广泛性和突发性的特点；
- 同时金融广泛采用互联网和新型技术；
- 属性导致面临的威胁是多维度的、多层次的。

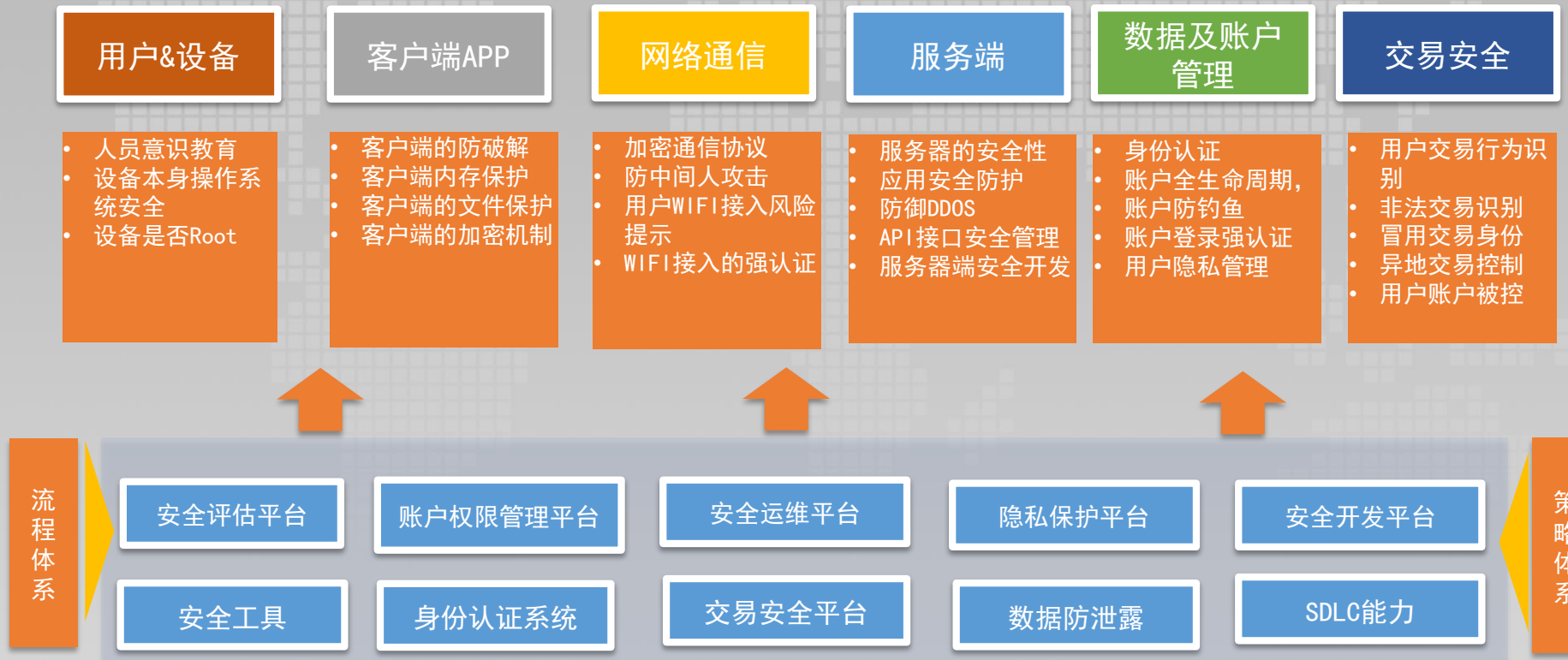
- 普遍缺少有效的数据及隐私保护措施；
- 自身安全投入不足；
- 采用的防御理念也较落后，头痛医头，脚痛医脚，缺少纵深防御，整本防御理念；
- 内部人员泄露；
- 内部人员安全意识不足；
- 缺少内部开发与安全人员的知识交互

- 攻击者趋利明显
- 地下黑色产业链的形成，体系化、集团化网络攻击日趋增多；
- 攻击过程的自动化、以及攻击工具、手段的快速更新，使得攻击者能在攻防对抗处于相对优势，同时当前采用安全防御机制的更新速度普遍慢于攻击者的更新速度，导致应对新型威胁乏力。

3. 跨越鸿沟-走向卓越

关键词：架构 安全 测试

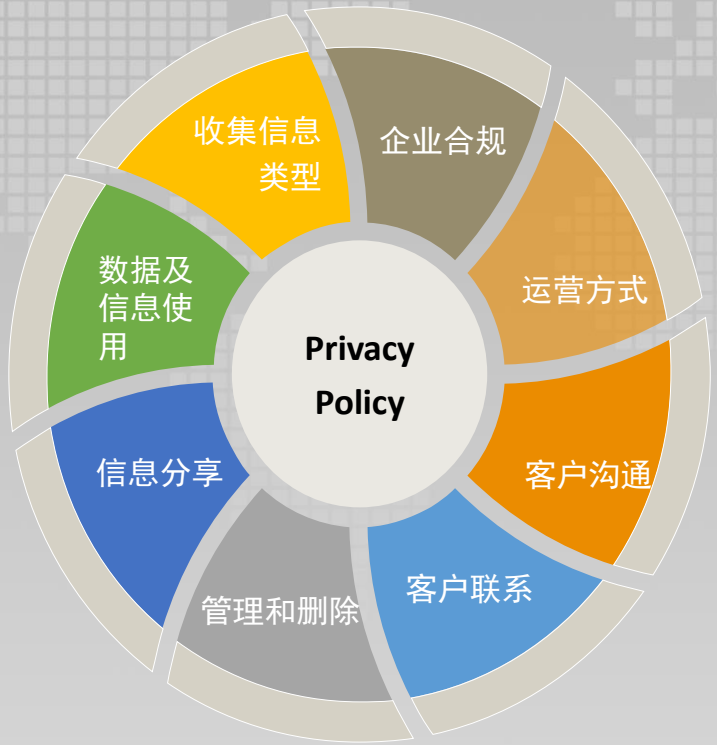
构建移动支付安全体系



客户端APP安全的一些实践

- 用户账户权限
- 数据文件、存储
- 网络通信
- 审计日志
- 用户身份认证
- 源代码安全
- 内核安全
- 外部资源调用
- 加密技术
- 用户隐私保护

用户隐私策略实践



- **收集哪些数据**
  - 人际关系网络（ 如IM，或交友类软件）
  - 设备信息，如IMEI等
  - 来自第三方或关联公司的信息
- **如何使用这些数据**
  - 提供、完善用户体验，广告服务等
- **这些数据如何被分享**
  - 网站使用、第三方使用、广告，推广等
- **如何管理和删除这些信息**
  - 如何保存，删除数据，用户可以采取的删除方式
- **如何管理和删除这些信息**
  - 如何保存，删除数据，用户可以采取的删除方式
- **如何应对法律的要求**
  - 适用何国何地法律
  - 有无美国，欧盟地区的法律条款的要求
- 运营的方式
  - 全球数据管理方式
  - 全球数据移动方式

对于隐私保护可参见我原创的金融云隐私挑战与应对的材料

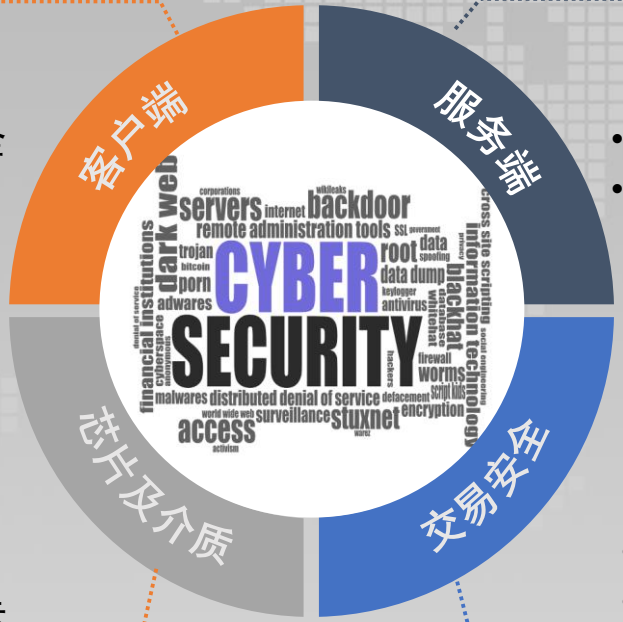
账户身份管理之常用安全技术分析（供参考）

安全技术	特点	应用关注点
实名认证	便于进行用户识别	需要第三方配合，如接入相应认证系统
支付控件	增加安全性，特别针对链路级风险时能够增加安全性	加密算法的选择，密钥动态调整
代码加密	反编译，防止敏感文件及信息泄露	建议考虑成熟的代码加密商用软硬件产品
短信验证	二次验证	但需要风控反欺诈结合，分析用户行为异常
数字证书/key	信息强加密，身份可确认	要构建密钥管理体系，同时要确保密钥的安全
额度设置	根据实际消费设定不同额度，有效止损	需要进行账户体系改造，识别高风险用户，需要双维设定
用户口令复杂度要求	有效增加用户口令被破译的难度	一定程度上要改变用户习惯，需要对用户进行意识培养
生物识别	较高的辨识率，识别用户相对唯一	需要考虑永久泄露的风险，对自然人身财产的影响较大 需考虑隐私保护、法律合规等方面。建议目前慎重选择使用。

移动支付安全评估关键范围

移动应用客户端

- 移动应用的源代码
- 移动应用的数据安全
- 算法安全
- 协议安全
- 日志审计



移动应用的服务端

- 支撑平台安全性
- 后台处理的健壮性
- 应用系统的安全性
- 数据加密
- 认证机制

芯片及介质测试

- NFC芯片安全测试
- 移动支付IC卡测试
- 移动支付SWP-SIM卡
- 移动支付双界面卡

交易安全

- 开发SDLC
- 交易场景安全测试
- 反欺诈体系结合度
- 安全事件管理

移动支付安全评估之APP测试关注点

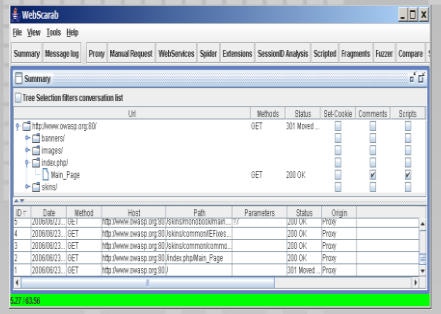
- APP安全测试关注点
  - 通信测试
    - 安装通信测试
    - 正常通信过程测试
  - 客户端测试
    - 文件系统及代码测试
    - 内存及进程测试
  - 服务端测试
    - 网络层协议测试
    - 应用层协议测试
  - 逻辑测试
    - 身份假冒
    - 验证机制绕过

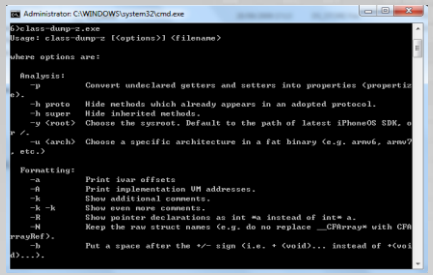
- 发现通信过程中通信机制缺陷，如未使用HTTPS
- 通信协议稳定性，如丢包率

- 敏感信息泄露
- 本地数据存储机制，敏感信息存储，加密机制
- OWASP十大安全漏洞

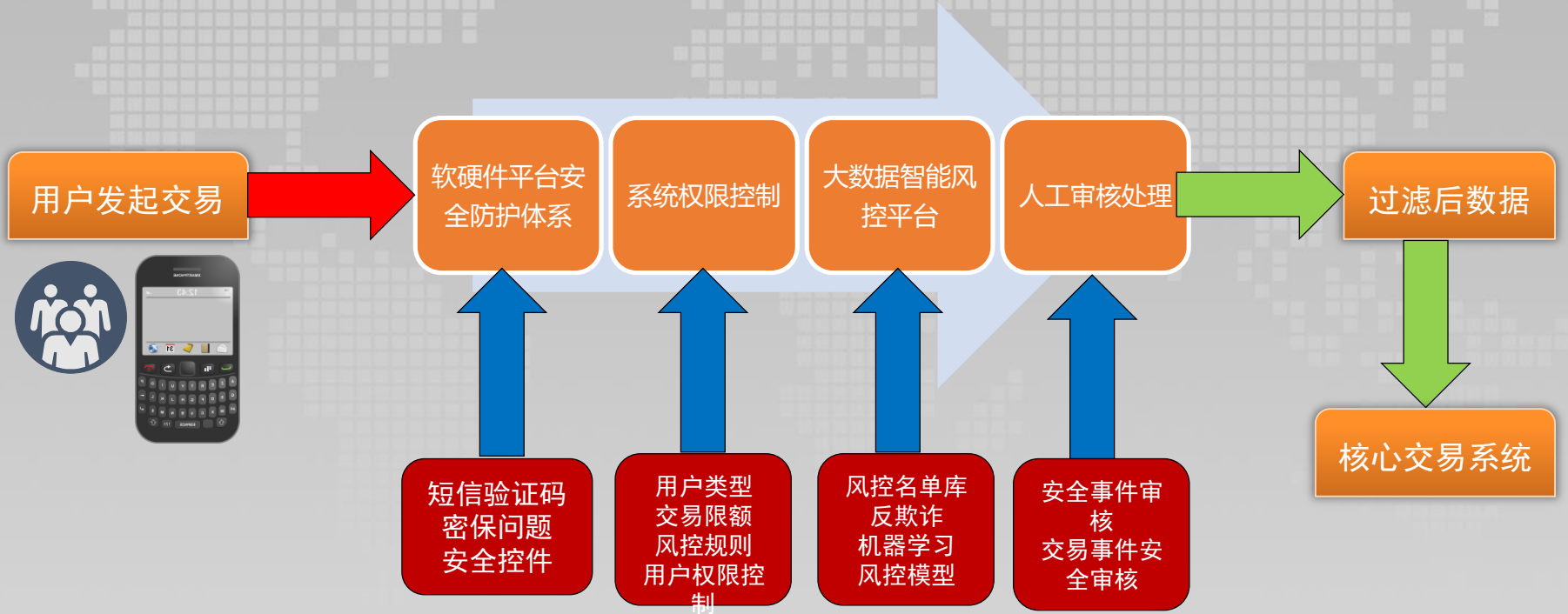
- TCP,UDP指定端口安全测试：
- 防御DDOS能力
- 缓冲区溢出防御能力
- 应用层协议安全测试SQL,XSS等防御能力,OWASP

- 正常用户Cookie冒用
- 正常用户账户的非法使用
- 二次验证渠道验证绕过测试
- 机器码等验证机制绕过测试





移动支付安全与交易风险控制结合



移动支付安全生态系统

未来之路

了解他　　业务结合

安全与风控的结合　Just Do It

普华永道2017年全球信息安全调查

根据PwC的2017全球信息安全调查，本次报告的主题为

《Moving forward with cybersecurity and privacy》

其中关于隐私、数据的安全调查成为本次报告的重点

报告地址：http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

Q&A

个人微信号