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

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

1. 移动平台-了然于心

关键词:现状　特点

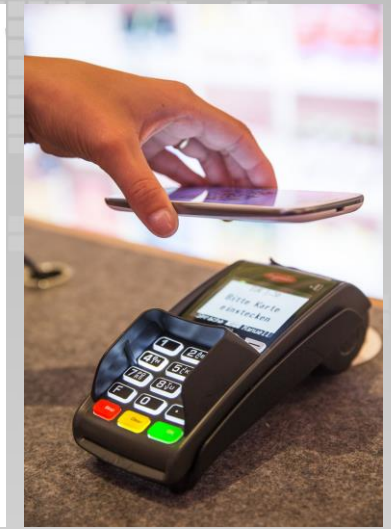
移动支付定义与要素

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，手机扫码支付
远程支付的典型场景：二维扫码

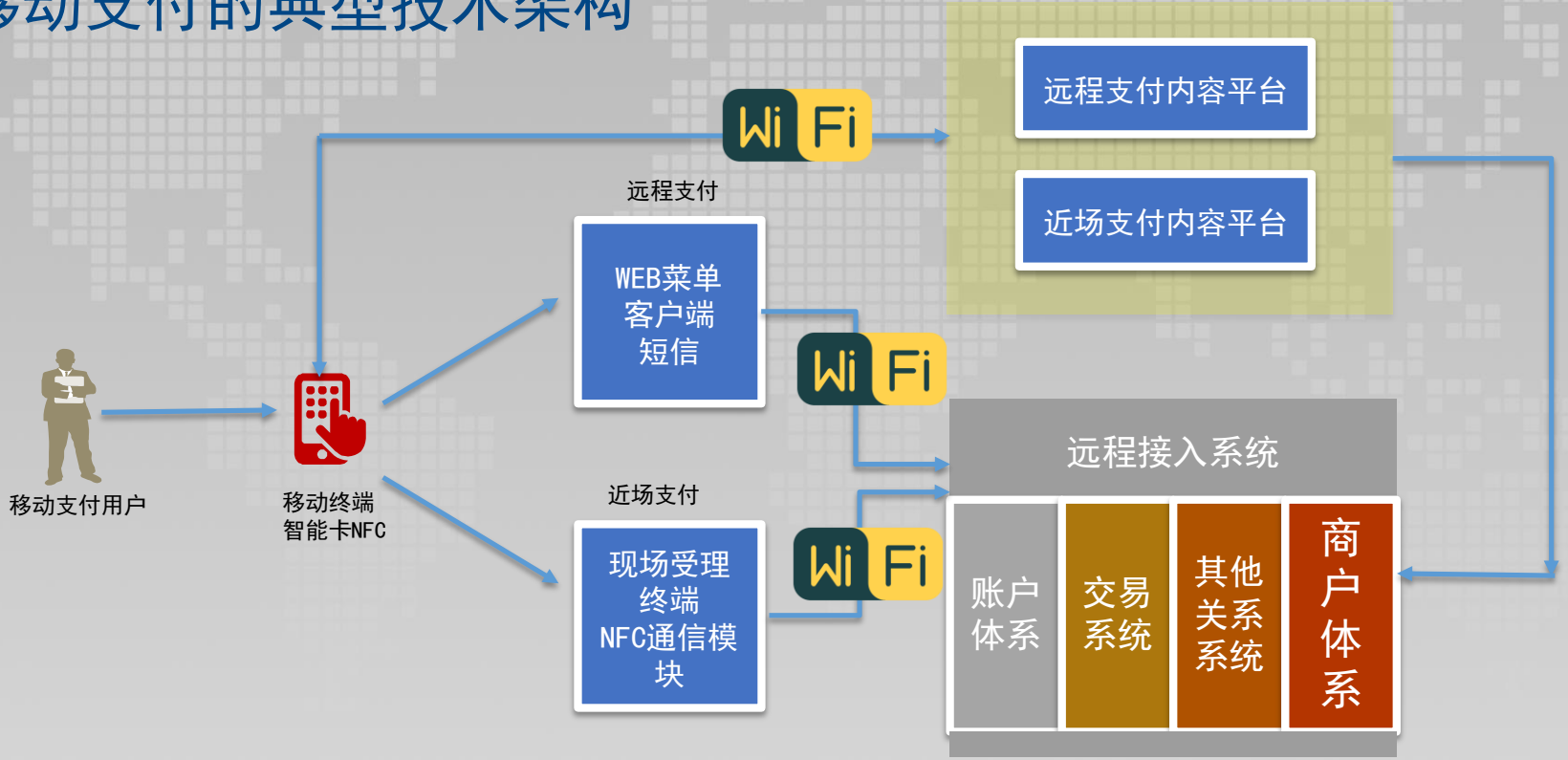
远程移动支付的关键要素：智能手机，APP客户端应用，APP应用服务器，网络通道（WIFI/3G/4G）
近场移动支付的关键要素：智能手机，智能手机NFC模块，APP客户端应用，APP应用服务器，网络通道（WIFI/3G/4G）

扫码支付



近场支付（NFC）

移动支付的典型技术架构



移动支付分布形态

- 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，虽没有支付通道，也建立了完整的支付链条
- 以电子商务企业为代表的企业，早期接入支付通道，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

跨境移动支付，中国银联拥有突出优势

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


黑客搭建钓鱼网站，控制用户手机
WiFi
黑客搭建钓鱼网站，控制内部员工电脑
外部用户
NFC模块
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
黑客搭建WIFI拦截网络通信，窃取敏感信息，同时尝试进行用户移动终端
黑客尝试本地拦截NFC通信模块与手机通信机制
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

移动支付安全风险汇总

功能要素	威胁分析
自然人客户	安全意识薄弱，受到欺诈，数据泄露
客户端APP	1. APP本身的代码安全问题，如SQL 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
客户手机	1. 手机操作系统的健壮性， 2. 手机是否root
网络通信	1. 中间人攻击 2. DDOS攻击
服务器端	1. 服务器操作系统安全问题。 2. 内部网络安全 3. 服务器端的应用安全问题 4. 与外部接口的安全问题，如第三方银行和支付机构
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

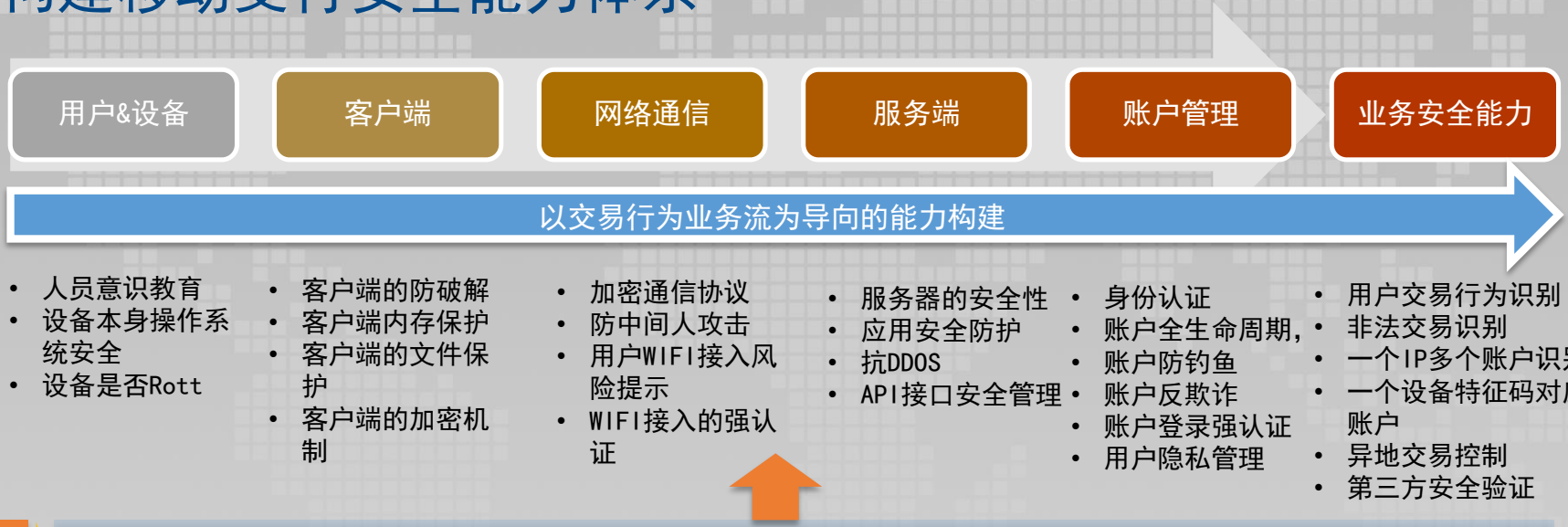
3. 跨越鸿沟-走向卓越

关键词：架构 安全 测试

移动支付安全规范

- 《信息安全技术 移动应用网络安全评价规范（征求意见稿）》 国标
- 《信息安全技术 金融信息保护规范（征求意见稿》行业标准
- 《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》
- ……

构建移动支付安全能力体系



常见移动支付安全技术分析

安全技术	必要性	实施要点
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件
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
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

手机APP安全开发的关注点

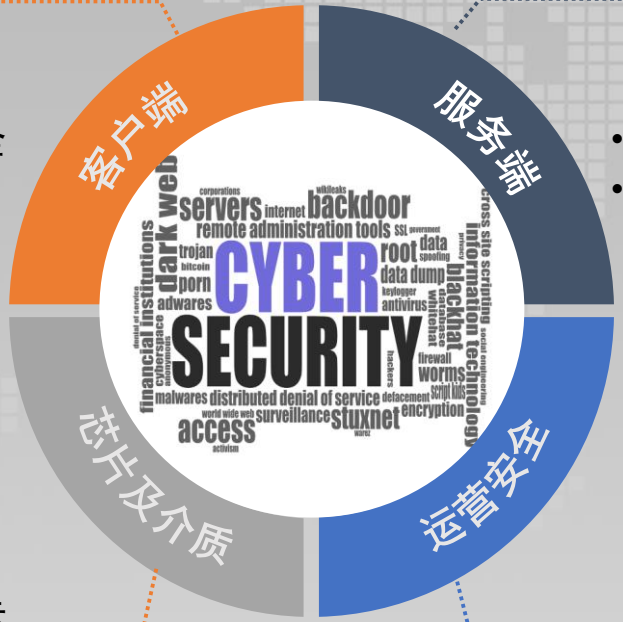
- 用户账户权限
- 数据文件、存储
- 网络通信
- 审计日志
- 用户身份认证
- 源代码安全
- 内核安全
- 外部资源调用
- 加密
- 用户隐私保护

Android安全开发指南https://developer.android.com/training/articles/security-tips.html

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

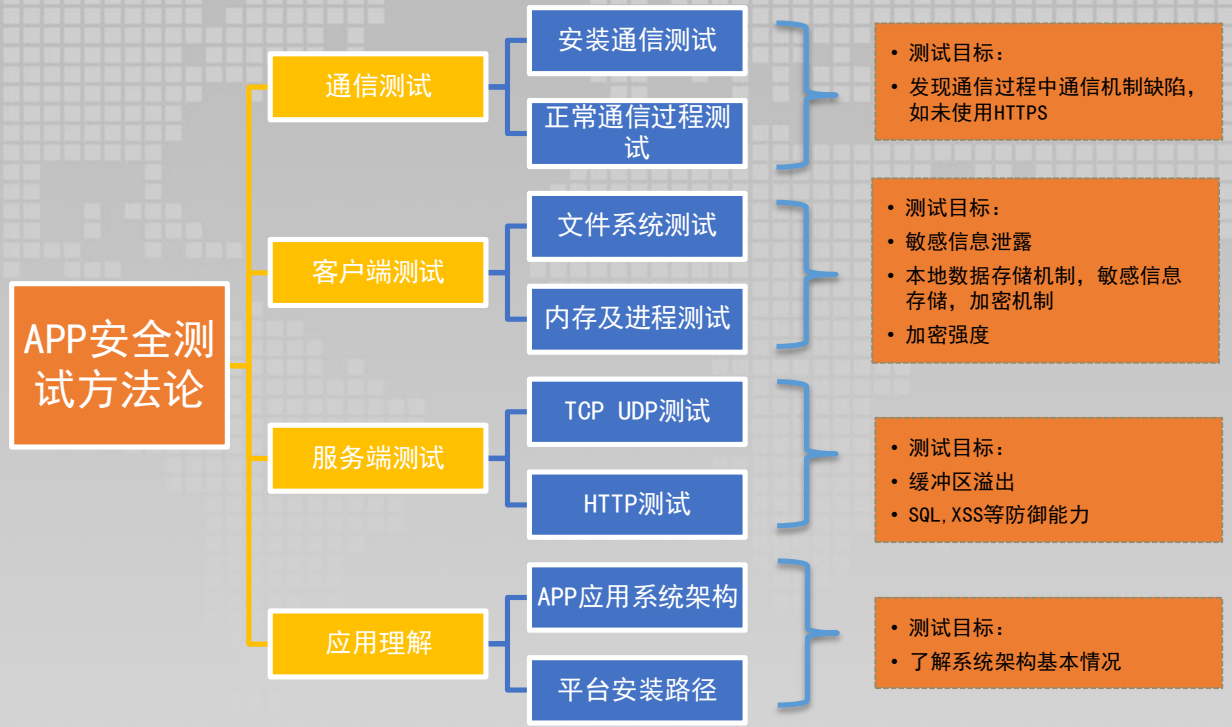
芯片及介质测试

- 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

运营安全

- 开发SDLC
- 运维流程管理
- 安全事件管理
- 业务连续性管理

APP应用安全测试关注点(参考)



OWASP参考指南https://www.owasp.org/images/1/1b/Mobile_App_Security_Checklist_0.9.3.xlsx

未来之路

了解他

业务结合

安全与风控的结合

Just Do It