



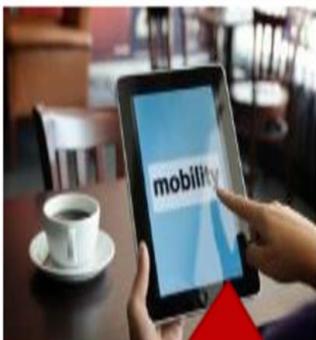
OWASP

Open Web Application  
Security Project

# 如何构建多维立体的移动信息 安全体系

苏鹏 CIW/CISA/ISO 27001 LA

# 全面普及的移动办公



58.7%  
已经或正在部署  
移动办公



20%+  
企业已经将移动办公  
导入正常办公

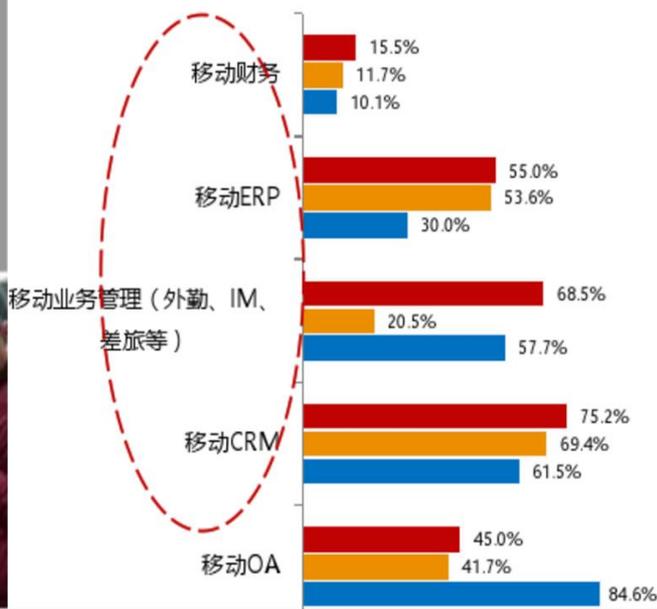
93%  
CIO非常认可  
移动办公



47.1%  
CIO表示移动办公极大  
推动业务的进展



### 企业移动应用首次部署情况

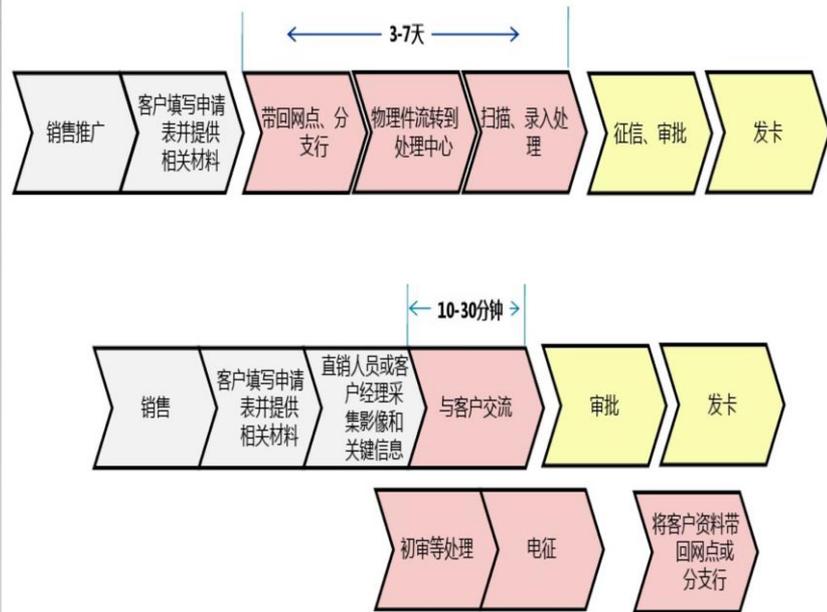


# 移动业务提高生产力：移动展业、移动政务

## 某银行信用卡开卡工作流程



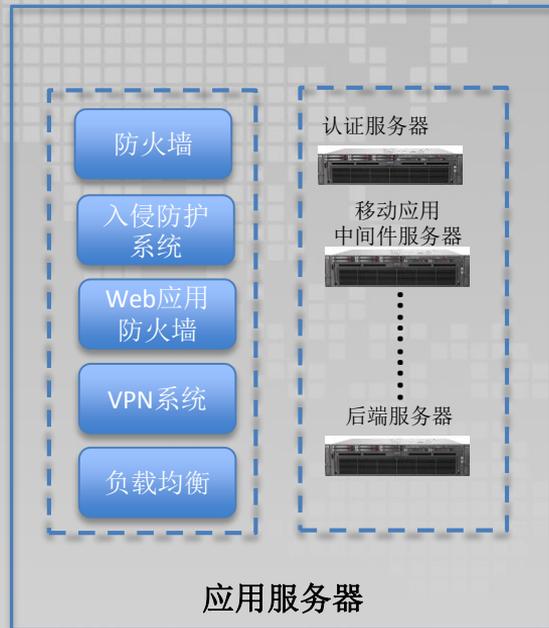
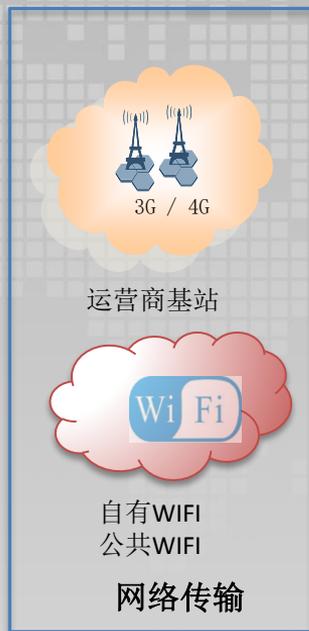
## 极大提高工作效率



# 移动支付业务全球首位

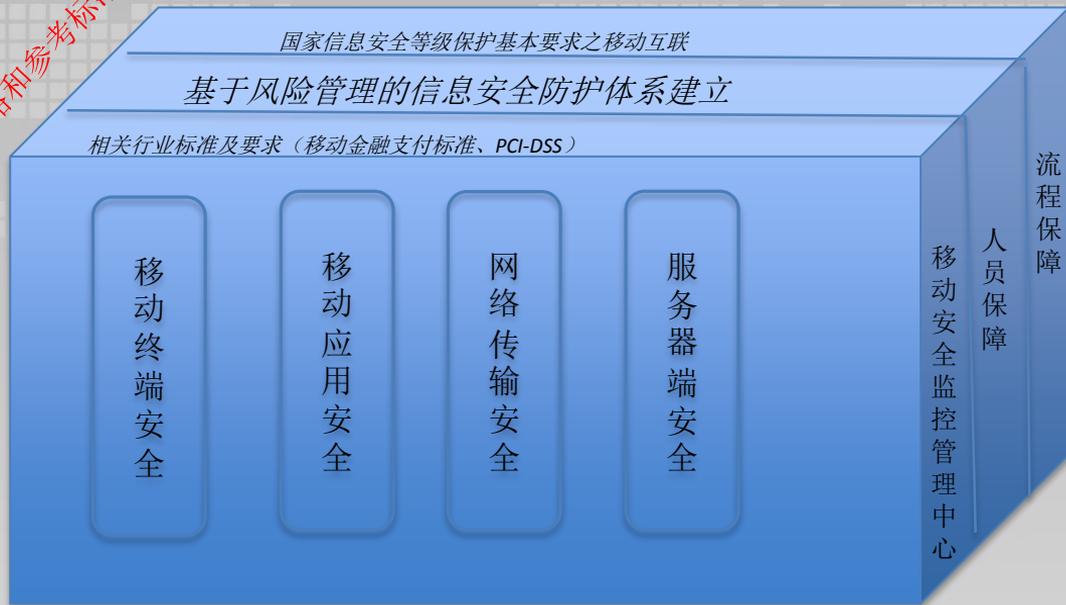


# 移动信息化系统模型



# 构建多维立体防护体系的思路

思路和参考标准



信息安全技术防护体系

信息安全监控和保障体系



# 风险分析-移动终端

物理层：容易丢失、被盗

系统层：

- 1、Android系统漏洞非常严重
- 2、Android系统缺少补丁统一更新机制
- 3、iOS系统漏洞其实很多
- 4、缺少企业级的安全策略，比如锁屏、密码复杂度等

数据安全：

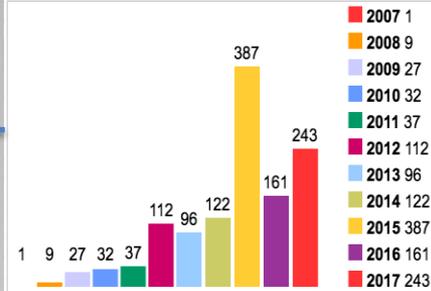
- 1、个人数据和企业数据混合存储带来的风险
- 2、企业数据的使用、存储缺少DLP策略保护

移动设备

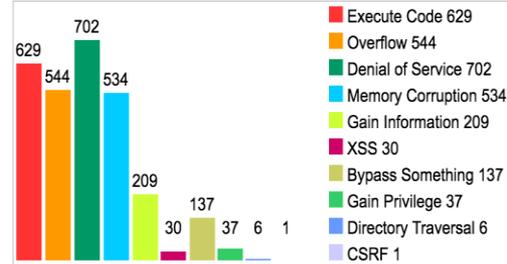


iPhone漏洞：CVE 统计数据

Vulnerabilities By Year



Vulnerabilities By Type

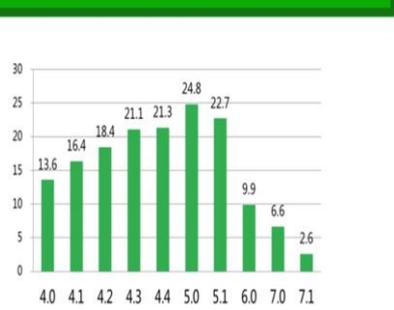


Android手机漏洞：国内机构统计数据

接受检测的42个安卓系统漏洞的危害类型分布及其影响设备比例



不同安卓系统版本的手机平均漏洞数



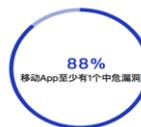
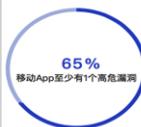
# 风险分析-移动应用APP

序号	脆弱性	风险
1	M1: 平台使用不当	可能造成数据暴露、允许连接到不受信的主机、或实现欺诈付款
2	M2: 不安全的数据存储	通过移动设备中所含的恶意软件、被篡改的应用程序或调查分析工具, 提取应用程序中的敏感信息
3	M3: 不安全的通信	传输的敏感信息会被恶意监听、窃取
4	M4: 不安全的身份验证	向未识别身份的用户暴露数据或提供服务
5	M5: 加密不足	使用加密技术保护的数据可能会被暴露; 可猜测的或可预测的加密令牌则可能导致虚假的交易。
6	M6: 不安全的授权	未经授权用户可以调用服务, 或使用凭据本没有授予他们的服务。
7	M7: 客户端代码质量问题	有害代码可以允许攻击者利用业务逻辑, 或绕过设备上执行的安全控制。代码级的错误可能以意外的方式暴露敏感数据。
8	M8: 代码篡改	这类攻击可以改变应用程序的隐性或显性逻辑: 被植入恶意代码、用来攻击后端服务器等
9	M9: 逆向工程	攻击者可以枚举或绕过业务逻辑、绕过安全控制、促进源代码盗用和篡改代码
10	M10: 无关的功能	通过这些额外的能力, 有窃取敏感数据或访问未经授权功能的高风险

在这些漏洞类型中, 排名前10 (测试App出现最多的漏洞) 的分别是

- 1 Activity公开组件暴露
- 2 Broadcast Receiver组件调用漏洞
- 3 Service组件任意调用漏洞
- 4 运行其它可执行程序漏洞
- 5 应用反编译
- 6 硬编码敏感信息泄露漏洞
- 7 本地拒绝服务漏洞
- 8 外部存储设备信息泄露漏洞
- 9 PendingIntent包含隐式Intent信息泄露漏洞
- 10 Android App allowBackup安全漏洞

“ 用户很乐观, 现实很骨感。从统计结果来看, 65% 的移动App至少存在1个高危漏洞; 平均每1个App就有7.32个漏洞。 ”



# 风险分析-网络传输

iOS



移动设备端

未加密或加密强度不够的数据传输被恶意监听、窃取敏感数据

伪基站和不安全的公共WIFI造成数据被恶意监听、窃取

不安全的身份认证，容易遭受劫持攻击

```
POST https://
User-Agent: Spay_Business3.1.3.apk/3.5 (Linux; Android 4.4.4; LGE Bu11d/KTU84P)
fp-lang: zh_cn
sp-AndroidId-353490069872493: 2,cgb_and,zh_cn,4.4.4,2017-06-07 14:37:46,Android
Accept-Encoding: gzip
Content-Length: 281
Content-Type: multipart/form-data; boundary=tpsJuf-9juGTDArTWek7kcdgGgLOk2Qh
Host: spay3.swiftpass.cn
Connection: Keep-Alive
Cookie: gtpid=75631d744e4835807c8a8cfa9e4f3fc7; kaptchaId=52b59ce4-a307-40cd-8c03-481f9b5c8430
Cookie2: $Version=1
--tpsJuf-9juGTDArTWek7kcdgGgLOk2Qh
Content-Disposition: form-data; name="data" 包含明文帐号、密码
{"pushCid":"75631d744e4835807c8a8cfa9e4f3fc7","username":"13666666667","client":"SPAY_AND","password":"1j1am123","androidTransPush":"1","bankCode":"cgb_and"}
--tpsJuf-9juGTDArTWek7kcdgGgLOk2Qh--
```

明文的登录请求数据包

包含明文帐号、密码

Find... (press Ctrl+Enter to highlight all)

View in Notepad

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching

Cookies Raw JSON XML

```
{
  "code":
  "message": "用户名或密码不正确"
  "reqFeqTime": 0
  "result": 400
}
```

明文的返回值



服务器端

服务器端没有对客户端的证书做认证



OWASP  
Open Web Application  
Security Project

# 风险分析-服务器端



# 基于终端的安全防护技术

## To 企业内部的基于MDM的强管控

### 设备层安全防护

- 1、设备丢失后的紧急处理：定位、远程锁屏、远程擦除数据
- 2、强制执行锁屏策略，并执行设定的密码策略
- 3、设备认证，设备和用户绑定，支持企业级认证体系

### 系统安全

- 1、目前还没有移动设备补丁统一管理功能
- 2、通过APP以及数据层面安全来弥补
- 3、通过对I/O进行管控

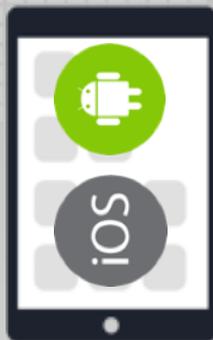
### APP管控

- 1、内部企业商店，只有通过认证设备才能获取并安装APP
- 2、APP黑白名单技术
- 3、单一APP/多APP模式，kiosk模式 / single模式

### 数据安全防护

- 1、容器化技术将企业数据进行保护
- 2、通过APP层面的安全保护来实现，通过app实现关键数据加密保护：关键数据、数据库sqlite以及其他文件

## To 最终用户的弱保护模式（威胁感知）



1

MDM客户端不适用安装

1

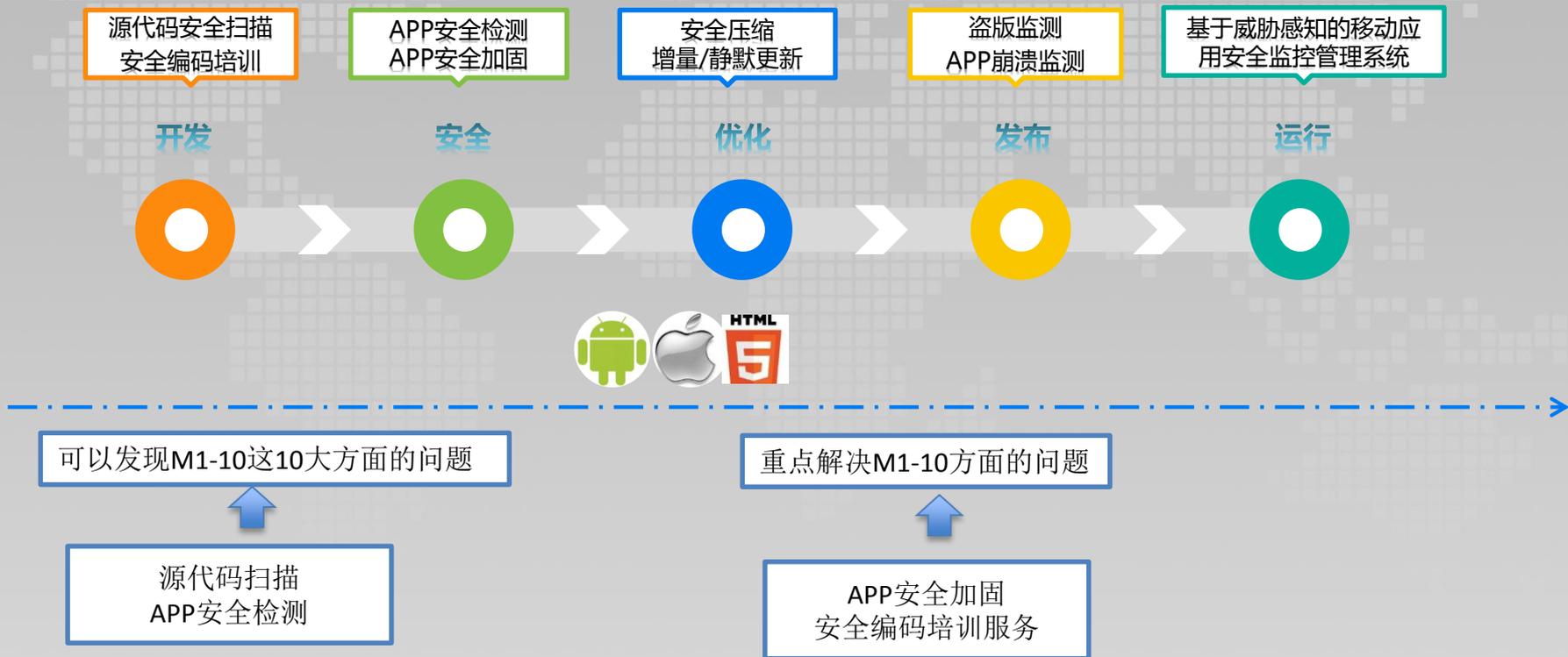
通过在APP集成安全检测SDK:

- 1、具备恶意程序检测能力
- 2、具备拦截各种恶意攻击：注入攻击、动态调试等
- 3、检测Root / 越狱



**OWASP**  
Open Web Application  
Security Project

# 基于APP的安全防护技术



# 源代码安全扫描（APP和服务端）



- 1、支持多种语言，支持字节码；
- 2、支持对接SVN、GIT等代码管理系统
- 3、支持单机版 / 群集版 / 云服务
- 4、支持自动任务

- 1、可以自定义引擎和规则库
- 2、代码扫描效率
- 3、支持漏洞库数量

- 1、参考标准：OWASP、CVE
- 2、最好有中文，阅读简单
- 3、自定义报告模版



# Android安全加固

## 防逆向

### DEX文件保护

DEX VMP

DEX整体加壳

DEX函数分离

多个DEX加密

### SO库保护

ELF VMP

SO文件加壳

SO库混淆  
(LLVM编译级)

## 代码防篡改

DEX代码防篡改

SO库文件防篡改

H5代码防篡改

## 资源文件防篡改

Assets防篡改

AndroidManifest配置  
文件防篡改

Res资源防篡改

## 防篡改

签名  
防篡改

防动态调试

防进程调试

防内存代码注入

防内存DUMP

防模拟器

防HOOK攻击

## 数据防泄漏

数据传输加密

防日志泄漏

本地文件加密

本地数据保护

## 页面数据保护

应用防截屏

应用防劫持

安全键盘



# iOS和H5安全加固

iOS加固

方法名高级混淆

程序结构混排/  
URL编码加密

字符串加密

Xcode 8

支持最新的Xcode 8编译器

H5  
混淆  
和  
加密

JS  
混淆  
和  
加密

爱加密H5安全加固平台

加密

混淆

压缩

原H5文件

加固后的H5文件

浏览器

执行  
JavaScript

调用

解密算法

解密

加密、压  
缩的文件



OWASP  
Open Web Application  
Security Project

# 移动端威胁感知技术（设备+应用APP）



模拟器运行感知  
终端Root/越狱感知  
终端病毒APP感知  
终端系统签名内核机制破坏感知  
终端设备信息篡改感知  
终端系统LIBC内核破坏感知

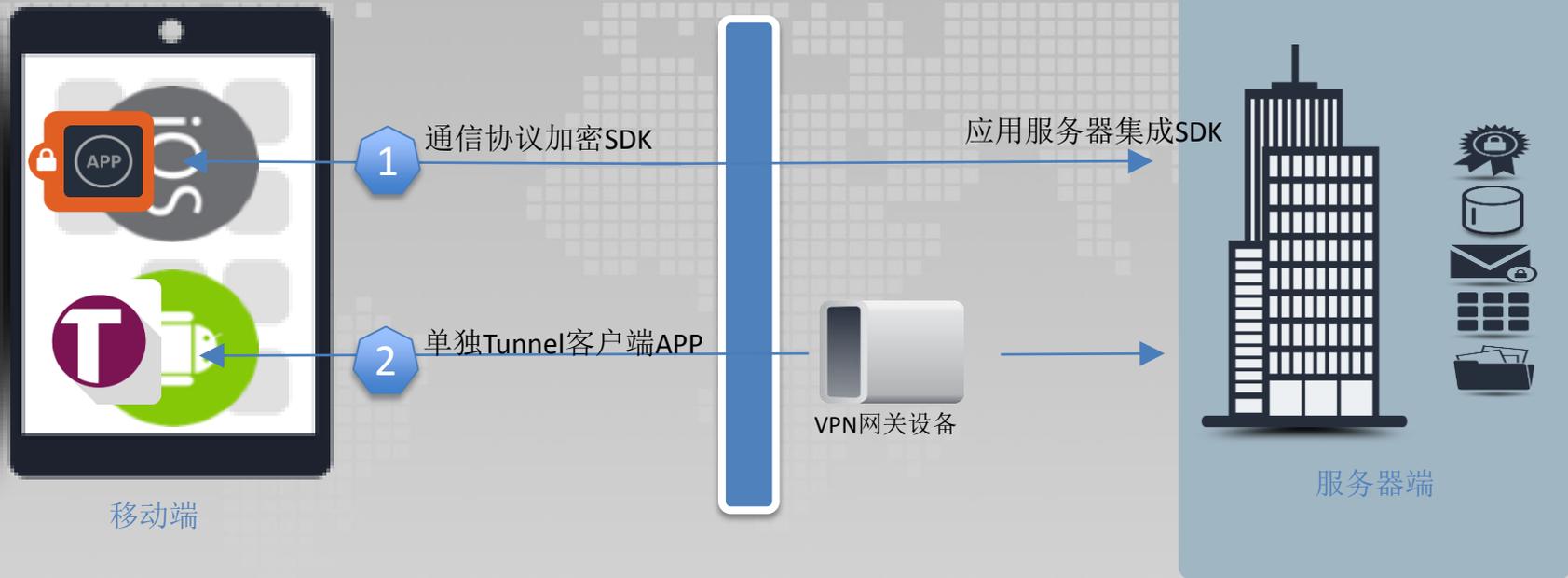
界面劫持感知  
IDA Pro工具调试感知  
内存中readmaps安全感知  
ptrace感知  
动态调试感知  
zjdroid攻击感知  
签名破坏/篡改感知  
应用完整性攻击感知



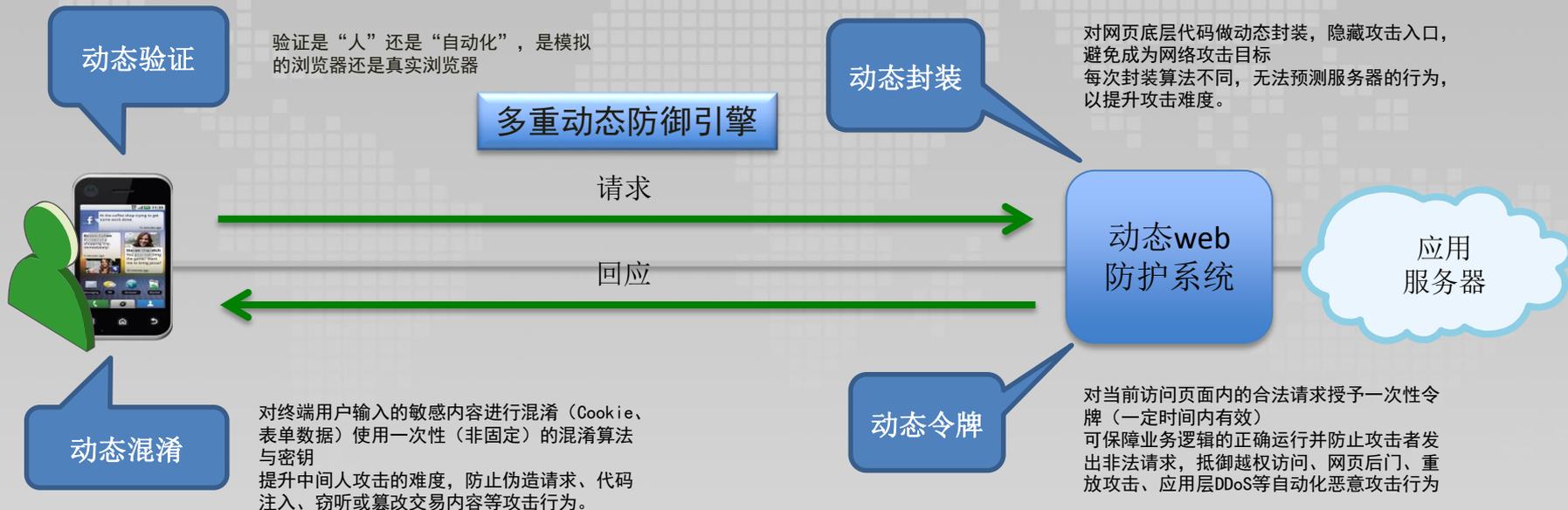
设备型号  
root权限  
系统版本



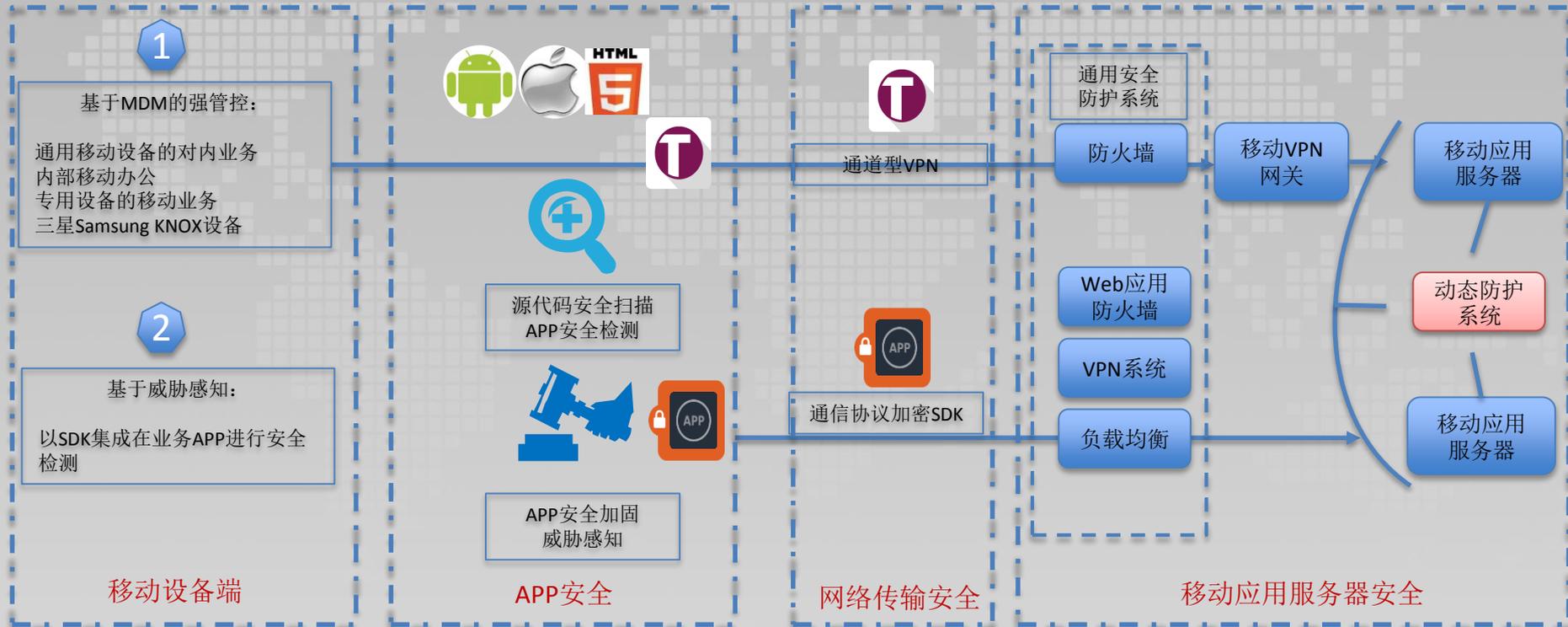
# 移动应用网络传输安全防护技术



# 针对移动应用服务器业务层风险的防护



# 移动业务系统整体安全防护技术体系

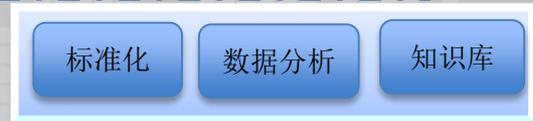


# 移动应用安全监控管理中心MSOC

页面展现层  
功能服务层  
功能支持层



## 移动应用安全监控管理中心+MSOC



## 移动应用安全监控管理中心+MSOC



数据应用层

数据分析层

数据采集层

数据来源层

