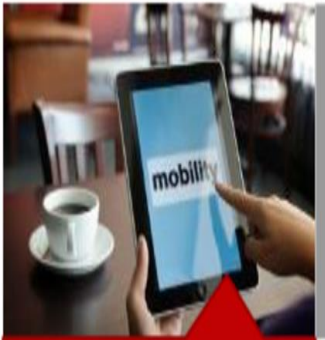
OWASP
Open Web Application Security Project

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

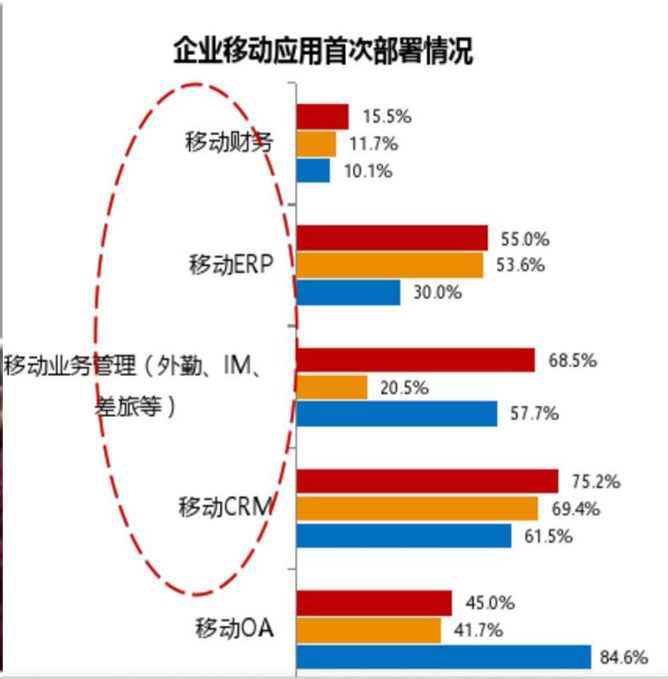


58.7%
已经或正在部署
移动办公

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

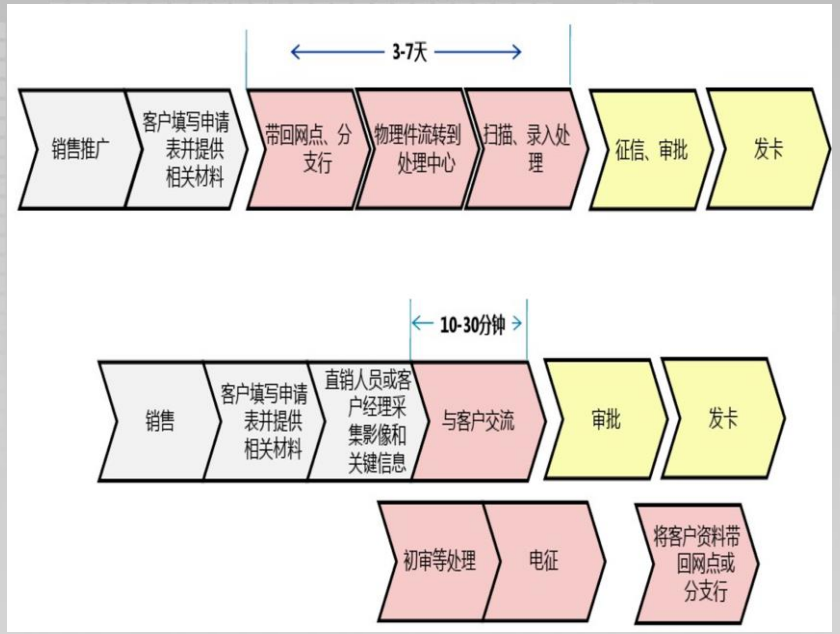
47.1%
CIO表示移动办公极
大推动业务的进展



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



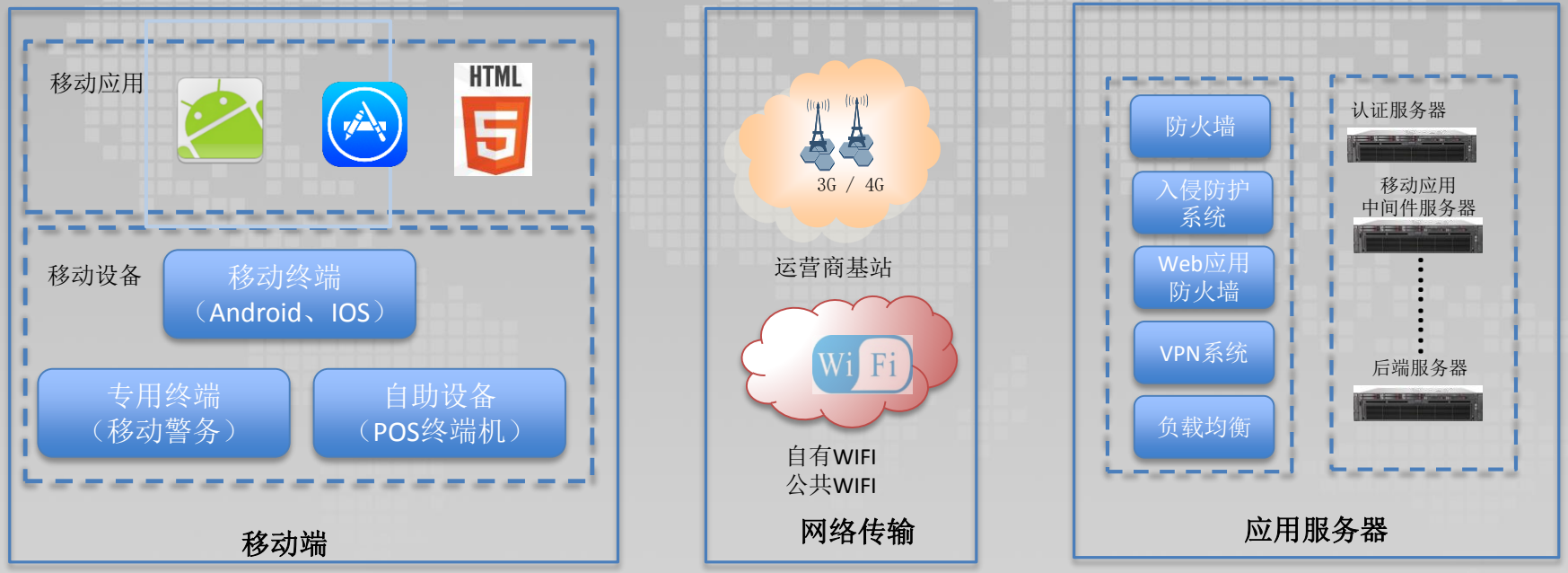
移动支付业务全球首位


终端设备
互联网
金融机构
应用提供商

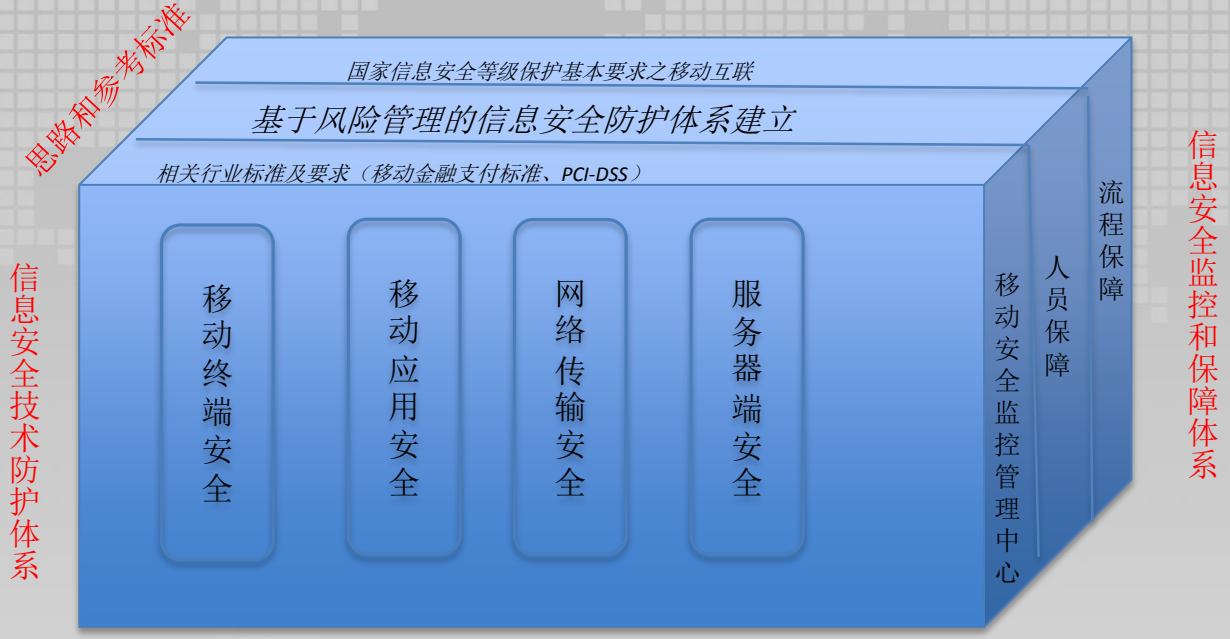

中国移动
16:57
账单
扫一扫
付款
卡券
收一眯
转账
红包
手机充值
余额宝
蚂蚁花呗
天猫超市
滴滴出行
淘票票
蚂蚁聚宝
淘宝
芝麻信用
外卖
科幻类青春大片


中国移动
17:02
徐源
扫一扫
付款码
拍立返
京东旺财
夺宝吧
全部应用
商城底价 再减10元
24
今日支出（元） 0.00
今日收入（元） 0.00
去记账
省钱攻略
拍立返 0元购
1元得充电塔扇
小蚁运动相机

移动信息化系统模型



构建多维立体防护体系的思路



风险分析-移动终端

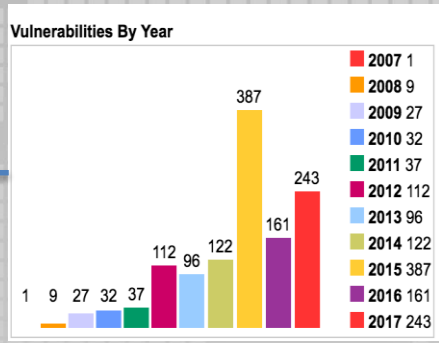
物理层：容易丢失、被盗

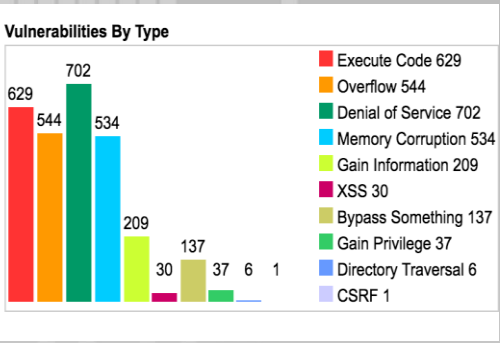
系统层：
1、Android系统漏洞非常严重
2、Android系统缺少补丁统一更新机制
3、iOS系统漏洞其实很多
4、缺少企业级的安全策略，比如锁屏、密码复杂度等

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

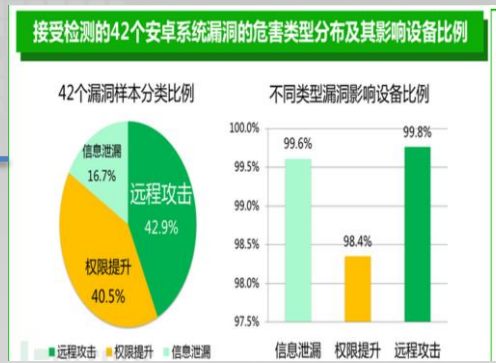
移动设备

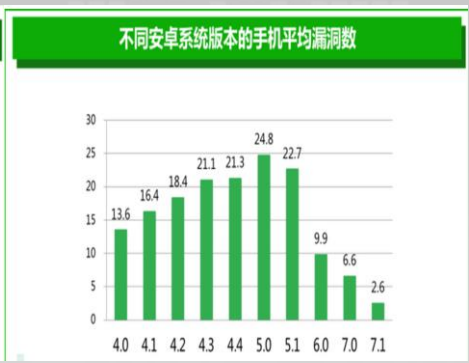
iPhone漏洞：CVE 统计数据





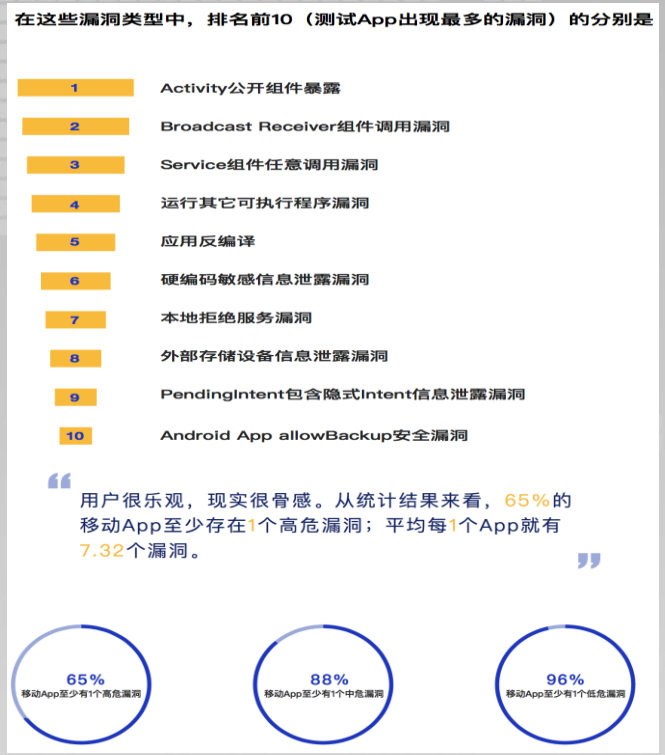
Android手机漏洞：国内机构统计数据





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



风险分析-网络传输

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

服务器端

服务器端没有对客户端的证书做认证

风险分析-服务器端

- 遭受恶意程序感染，数据不可用
- 遭受恶意攻击，导致数据泄露
- 数据缺少备份恢复机制
- 数据遭受未经授权访问导致泄露

- 各种恶意程序的感染
- 针对系统漏洞的恶意攻击
- 系统自身的高可用性
- 遭受拒绝服务攻击

- 服务器意味断电
- 服务器硬件出现故障
- 服务器遭受本地攻击

- 自动化的密码猜测和撞库
- 恶意抢购
- 批量盗刷和套现
- 网站恶意爬虫
- 批量建立虚假账号

A1:注入	A2:失效的身份认证和会话管理
A3:跨站脚本（CSS）	A4:失效的访问控制
A5:安全配置错误	A6:敏感信息泄露
A7:攻击检测与防护不足	A8:跨站请求伪造（CSRF）
A9:使用含有已知漏洞的组件	A10:未受有效保护的API

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sqllite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

基于APP的安全防护技术

源代码安全扫描
安全编码培训

APP安全检测
APP安全加固

安全压缩
增量/静默更新

盗版监测
APP崩溃监测

基于威胁感知的移动应用安全监控管理系统

开发 → 安全 → 优化 → 发布 → 运行

可以发现M1-10这10大方面的问题

源代码扫描
APP安全检测

重点解决M1-10方面的问题

APP安全加固
安全编码培训服务

源代码安全扫描（APP和服务器端）

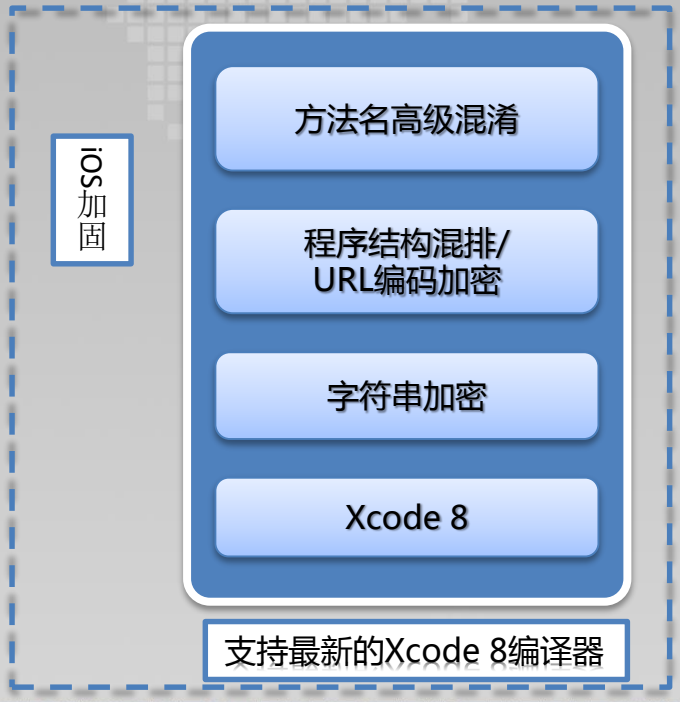
1、支持多种语言，支持字节码；
2、支持对接SVN、GIT等代码管理系统
3、支持单机版 / 群集版 / 云服务
4、支持自动任务

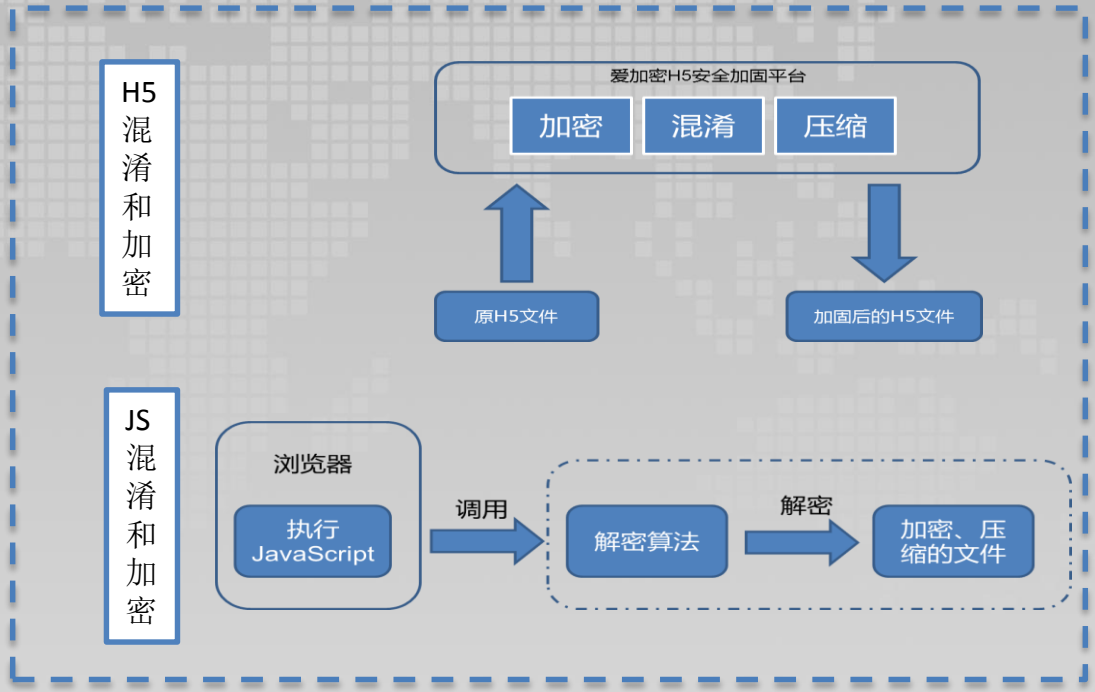
1、可以自定义引擎和规则库
2、代码扫描效率
3、支持漏洞库数量

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

iOS和H5安全加固





移动端威胁感知技术（设备+应用APP）

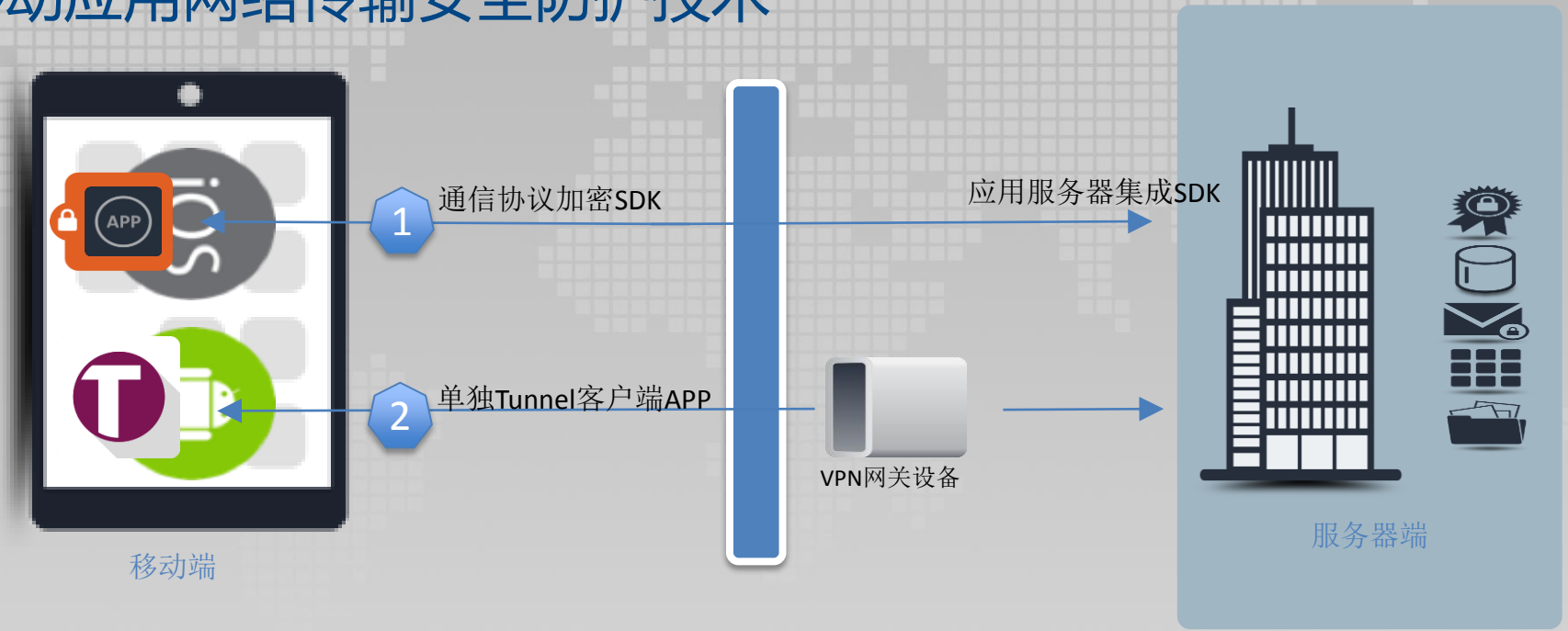
模拟器运行感知
终端Root/越狱感知
终端病毒APP感知
终端系统签名内核机制破坏感知
终端设备信息篡改感知
终端系统LIBC内核破坏感知

探针SDK

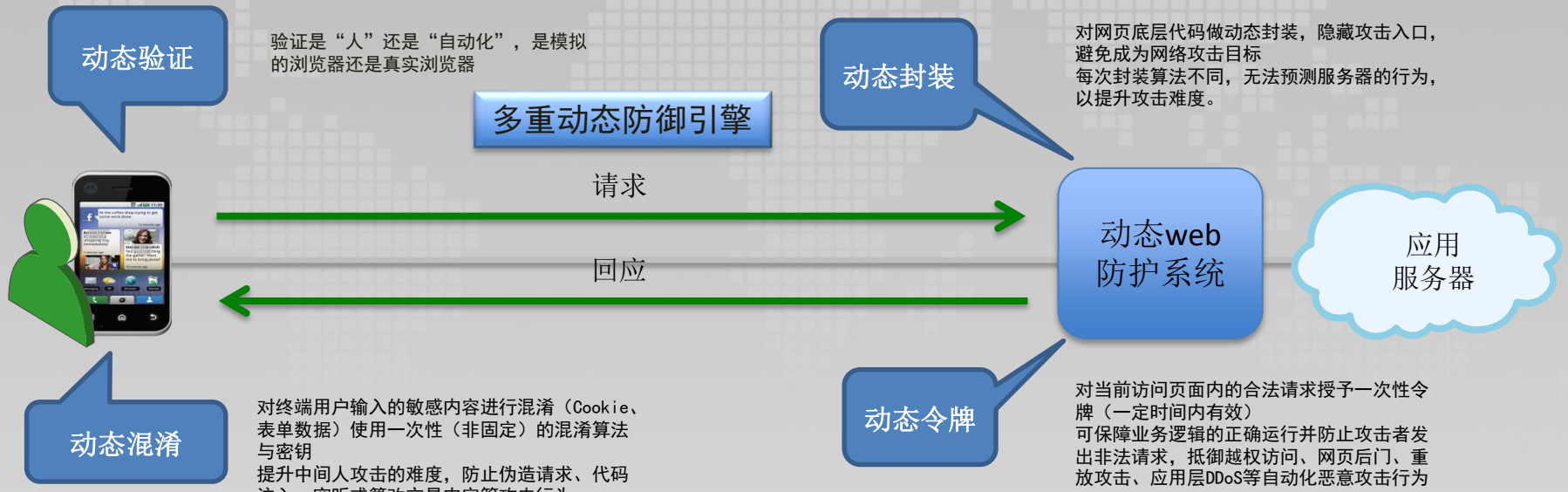
探针SDK

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

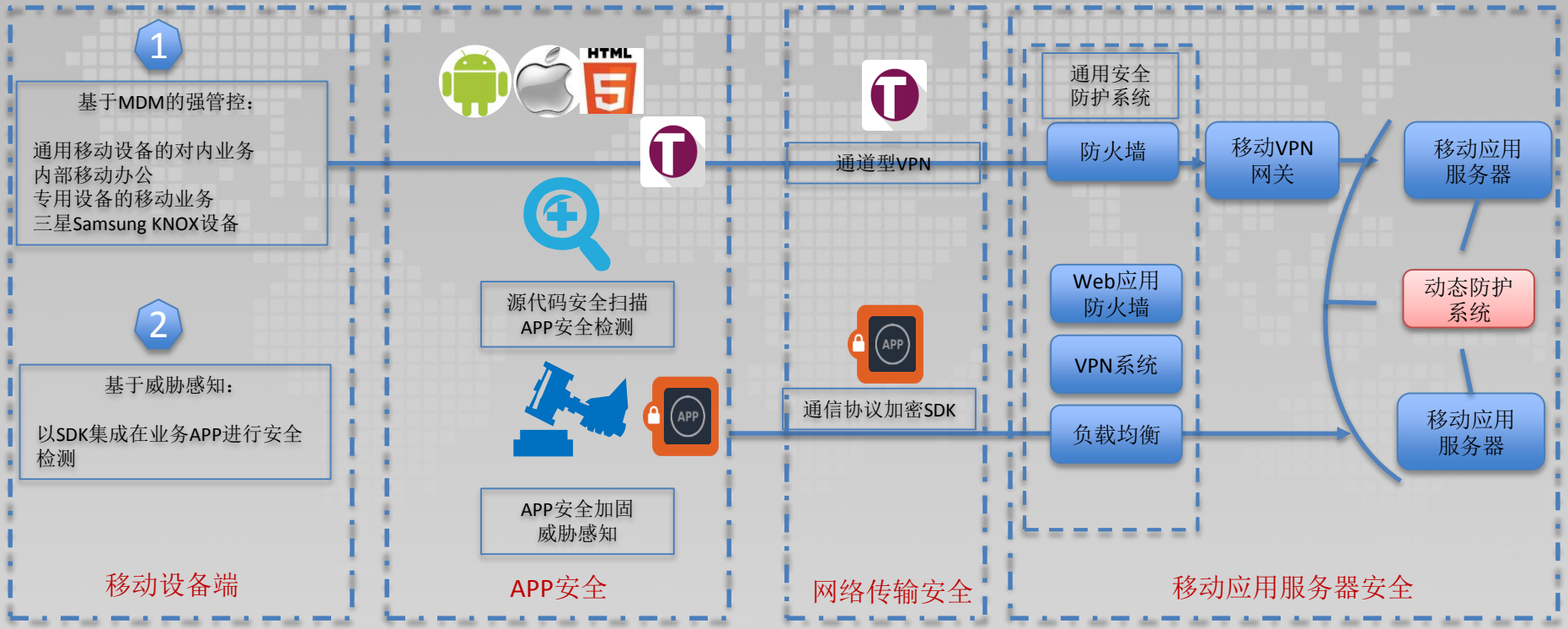
移动应用网络传输安全防护技术



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