RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

移动互联网之

开放平台安全

李铁岩

爱迪德公司

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

专题会议主题：移动与网络计算

专题会议分类：中等

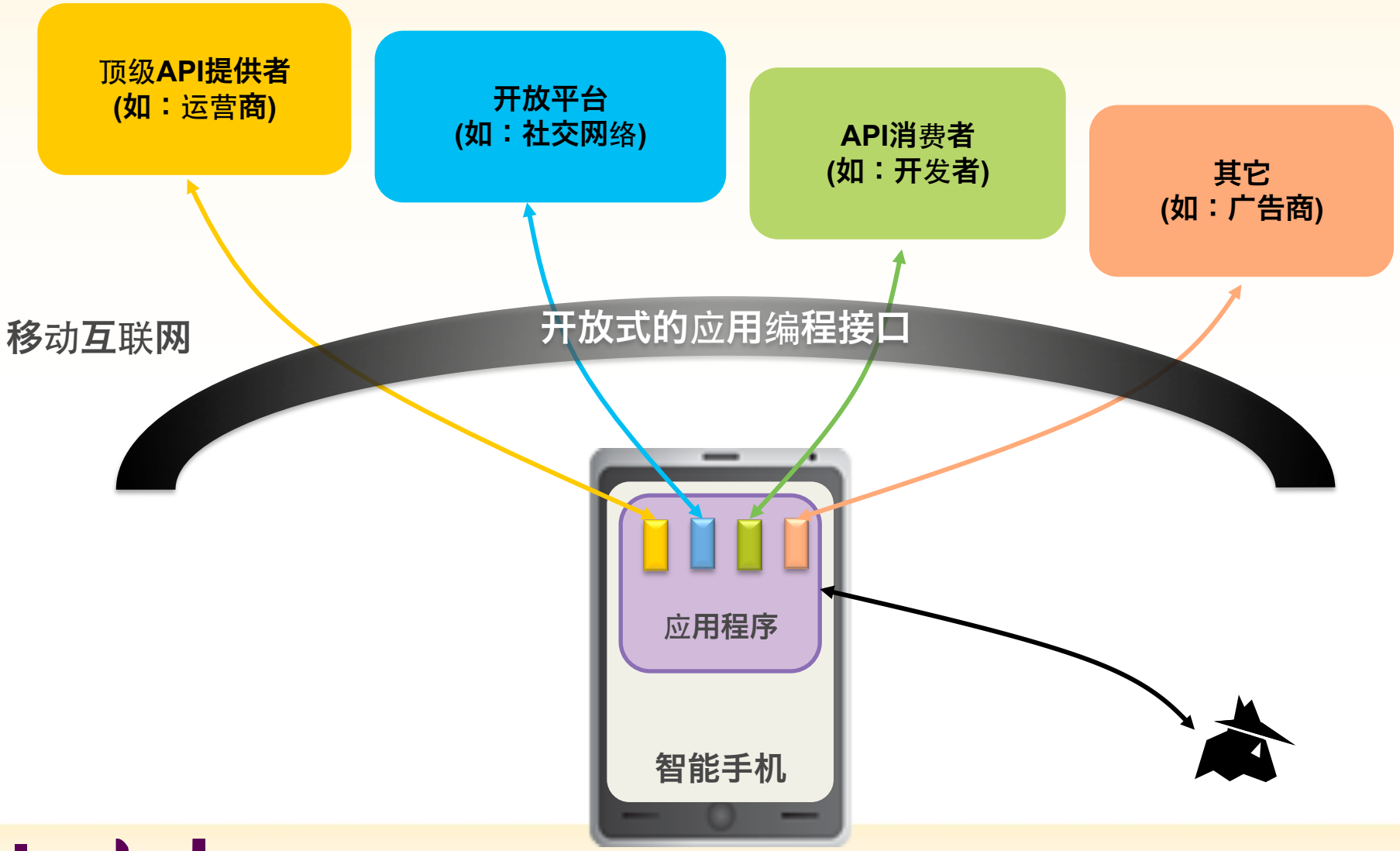
概要

- 开放平台风险与应对
- 移动应用保护
- 安卓平台安全
- 动态及全生命周期的安全

Alice

移动开放平台

开放平台生态系统


顶级API提供者
(如：运营商)
开放平台
(如：社交网络)
API消费者
(如：开发者)
其它
(如：广告商)
移动互联网
开放式的应用编程接口
应用程序
智能手机

选择开放

围墙花园 ⟷ 开放系统

- Apple 管控其平台的安全性
- Apple 限制开放其平台上的系统级服务
- Apple 认证及审核所有在其平台上发布的应用
- Apple 关注其平台生态系统的健康状况

优点
- 较好的安全性 (不包括越狱)
- 很好的用户体验

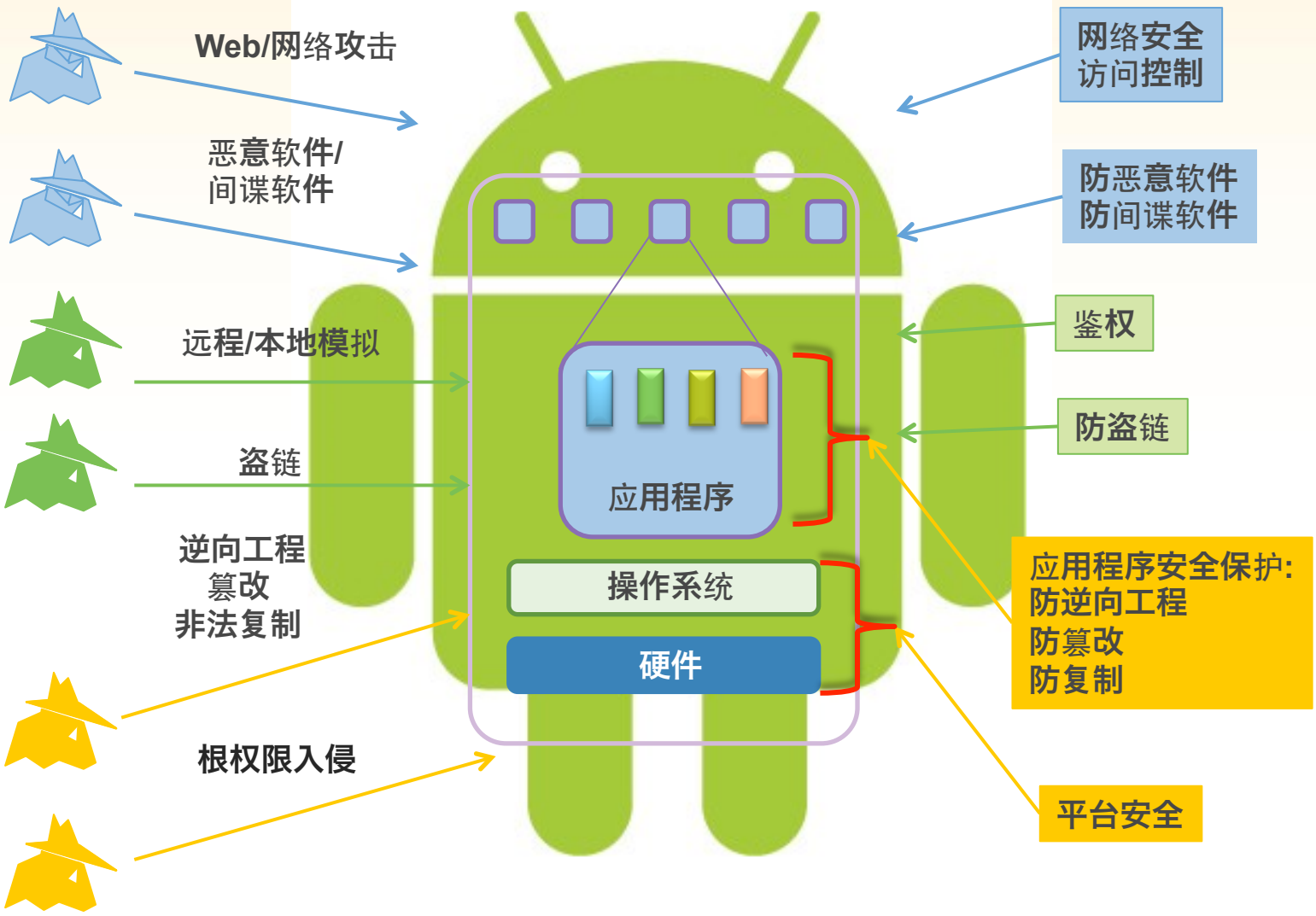
缺点
- 封闭性的生态系统
- 较贵的设备

- 开源
- 应用可调用操作系统底层的服务
- 许多第三方市场无认证及审核过程
- 依赖用户自行判断安全性
- 较复杂的生态系统

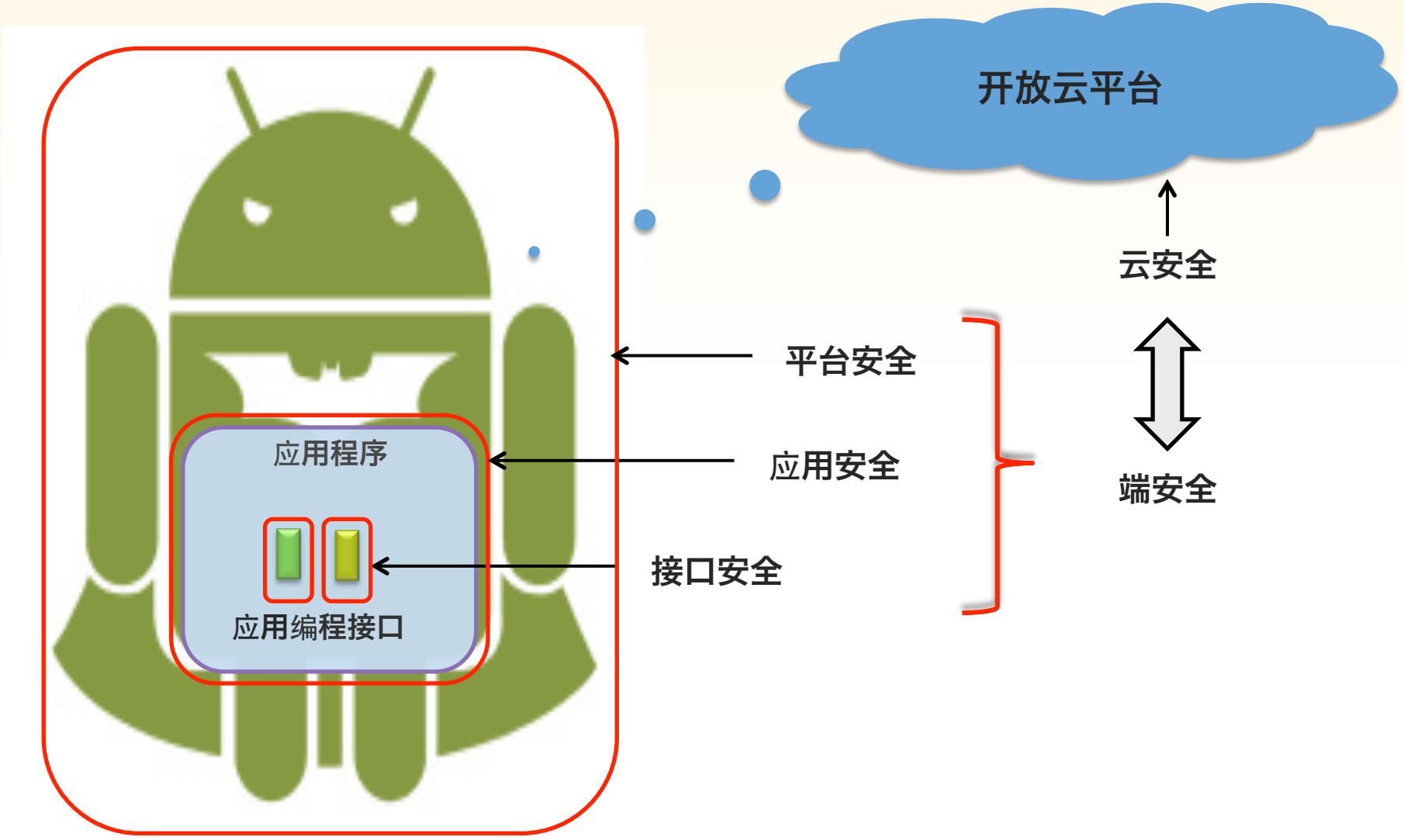
优点
- 开放式的生态系统
- 较便宜的设备

缺点
- 安全性差
- 碎片化，运维代价较高

风险及应对

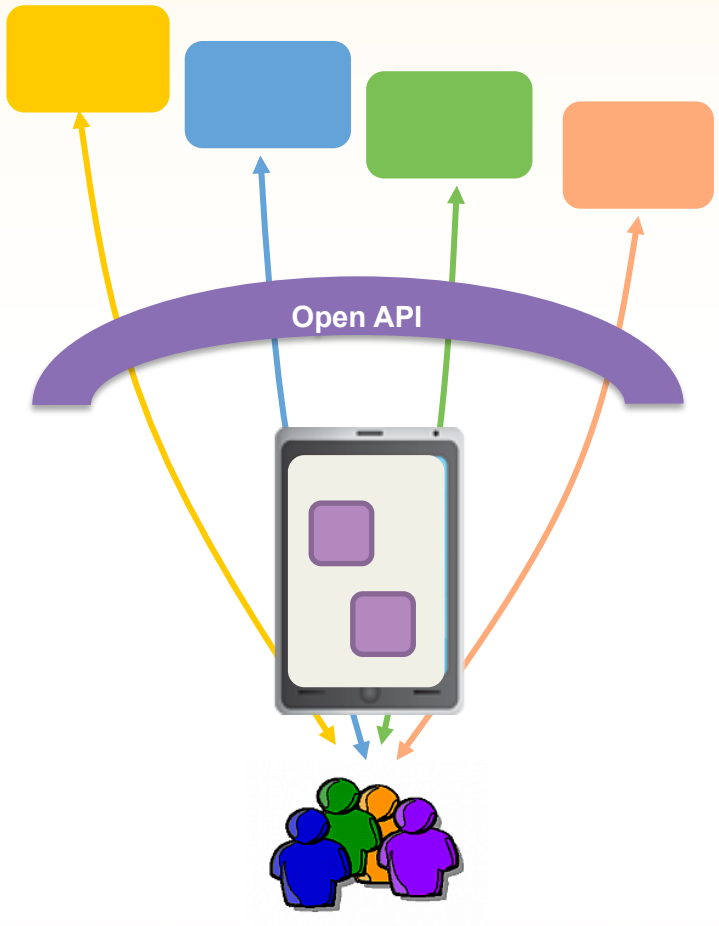

Web/网络攻击
恶意软件/
间谍软件
远程/本地模拟
盗链
逆向工程
篡改
非法复制
根权限入侵
网络安全
访问控制
防恶意软件
防间谍软件
鉴权
防盗链
应用程序安全保护:
防逆向工程
防篡改
防复制
平台安全
应用程序
操作系统
硬件

层层防护

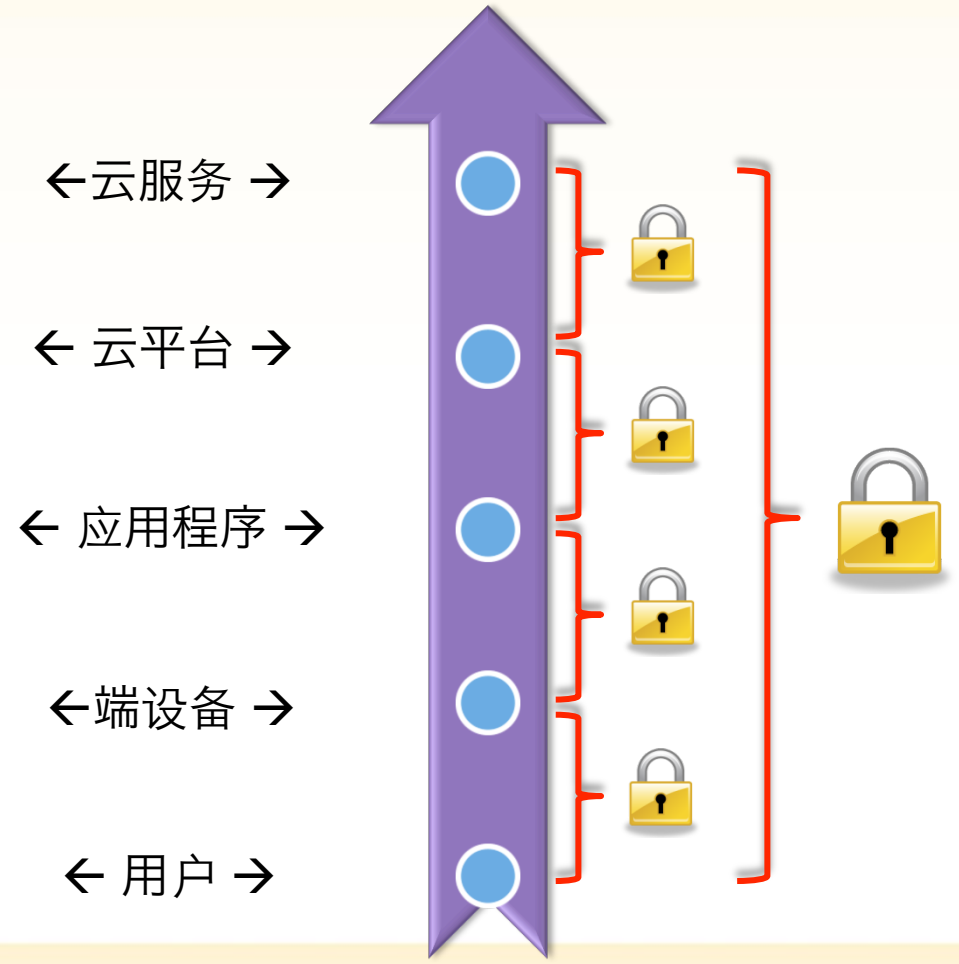


更简单、更贴近用户要求、更具有针对性的安全

移动互联网



垂直安全性



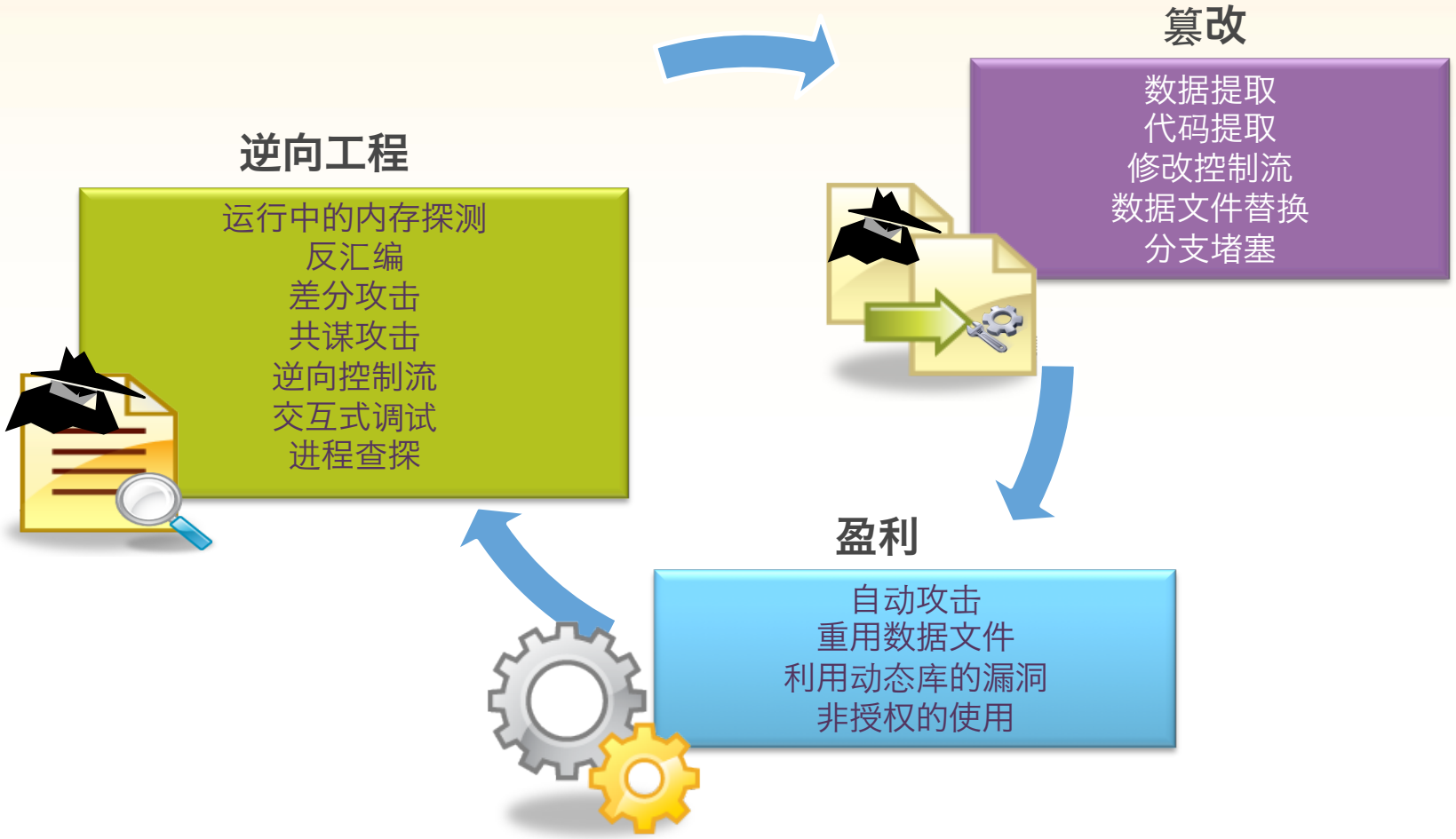
移动应用保护

为何保护应用？

- 移动应用面临邪恶的一对
  - 盗版: 破坏应用开发者的知识产权.
    - 最近的一份研究报告指出100% 的付费安卓应用被破解。
  - 病毒: 应用中嵌入恶意代码，窃取用户隐私等.
    - 另一份学术报告指出约86% 的恶意软件隐藏在重新包装的合法应用中。

- 通过对应用程序的安全保护，防止未经授权的使用，从而实现对业务模式的保护。未经授权的使用包括如下：
  - 逆向工程（如：导致知识产权的流失）
  - 篡改（如：游戏作弊、注入恶意软件）
  - 非法复制（如：拷贝已支付的资产）

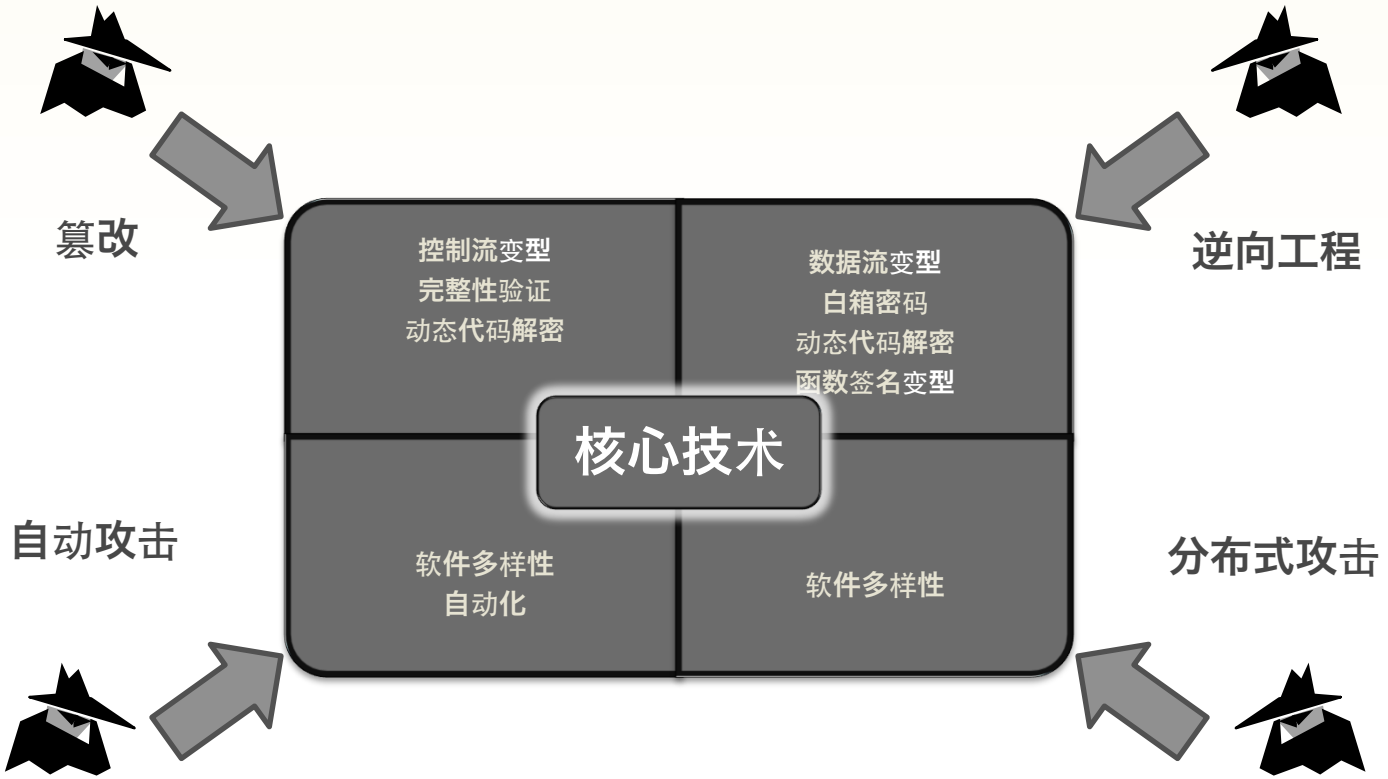
软件面临的攻击



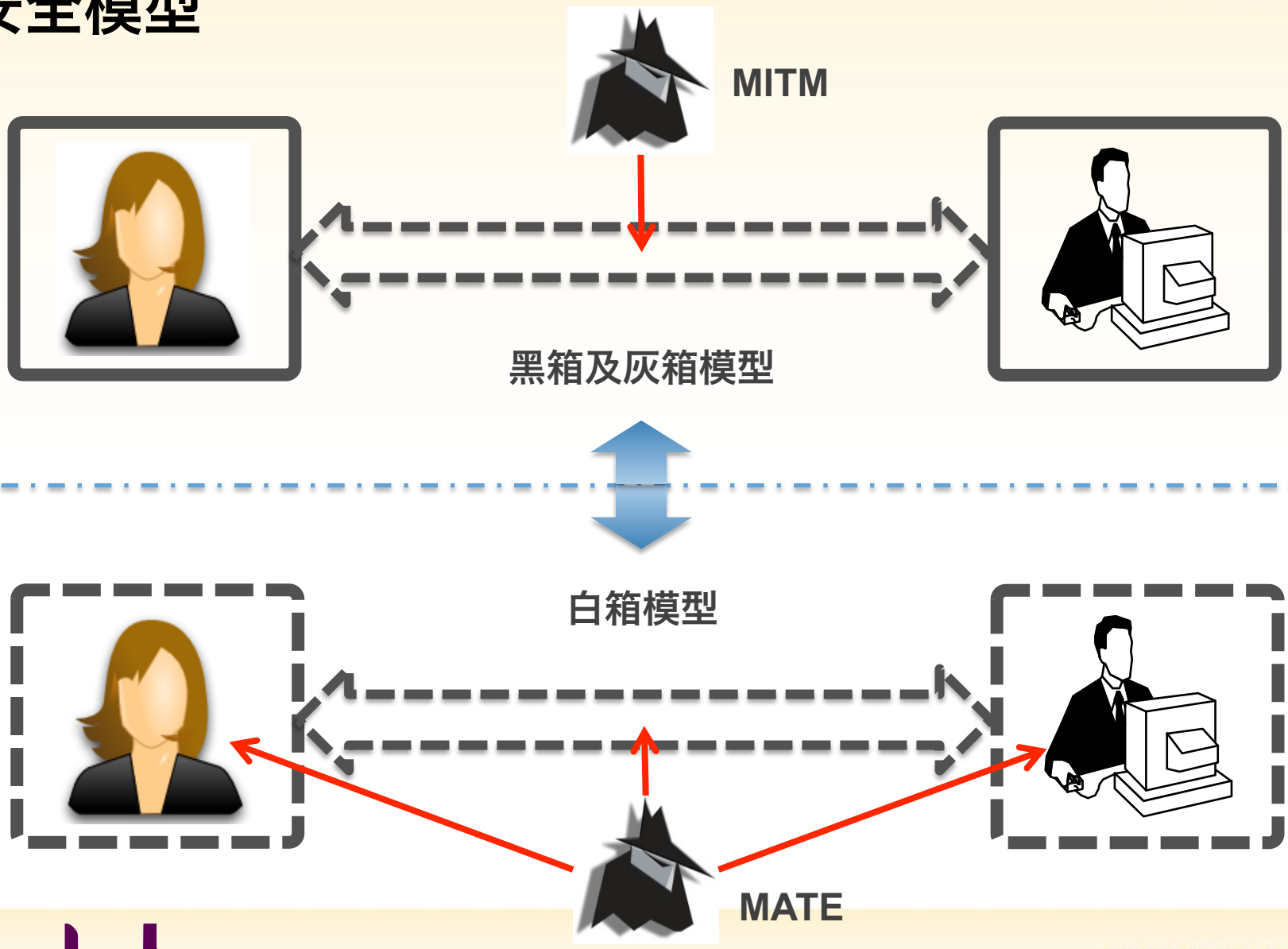
不同的攻击需要不同的保护机制

软件保护

- 软件保护技术(包括源代码级和二进制代码级的保护)， 防止逆向工程,篡改， 自动及分布式攻击



安全模型

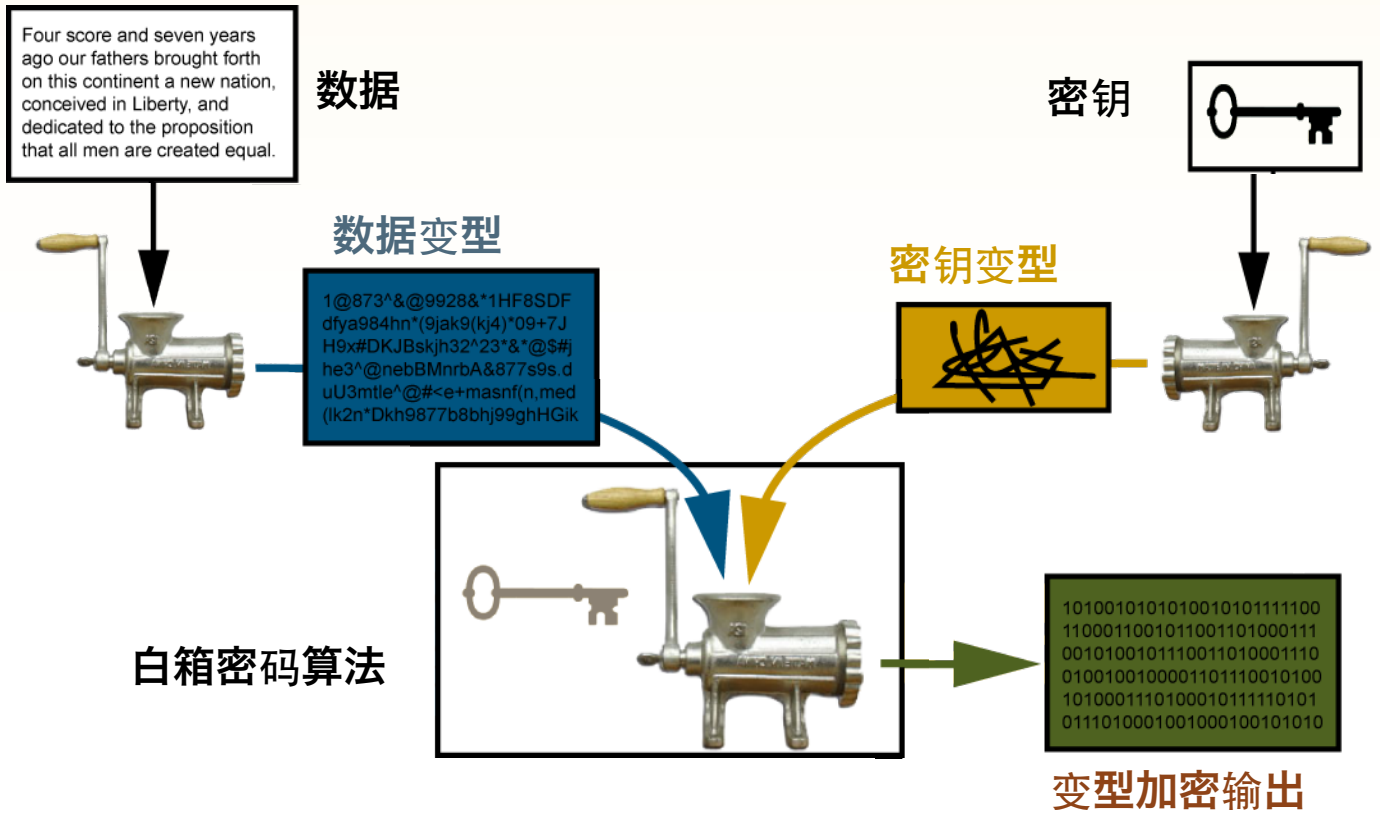


安全模型

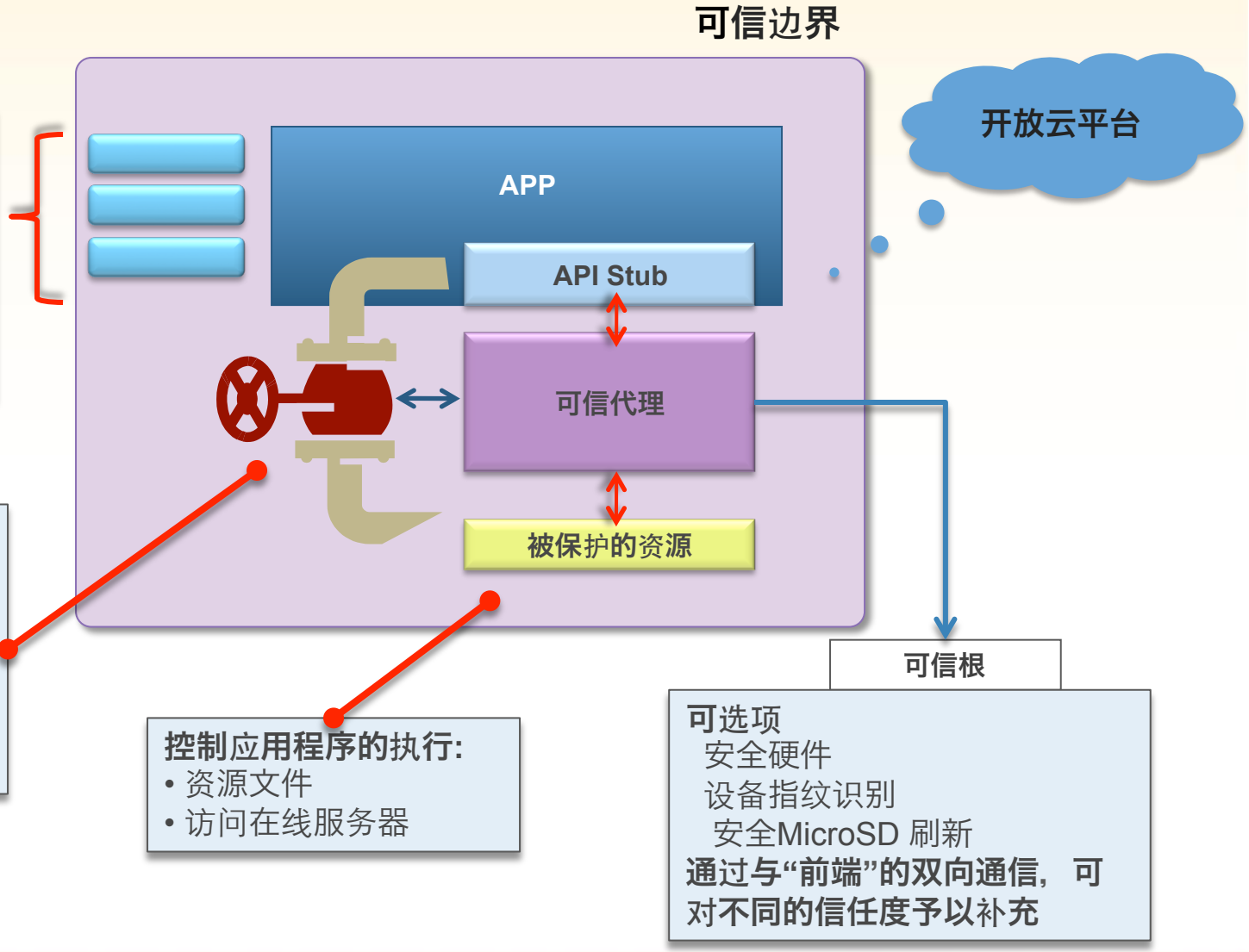

最难
白箱
分析调试工具
模拟攻击
其他攻击工具
灰箱
时间分析
旁路攻击
错误注入
黑箱
输入、输出
最易
资产保护难度
最弱
攻击有效性
最强

白箱密码

白箱密码确保输入数据，密钥及输出数据在任何时刻都是安全的！



可信代理



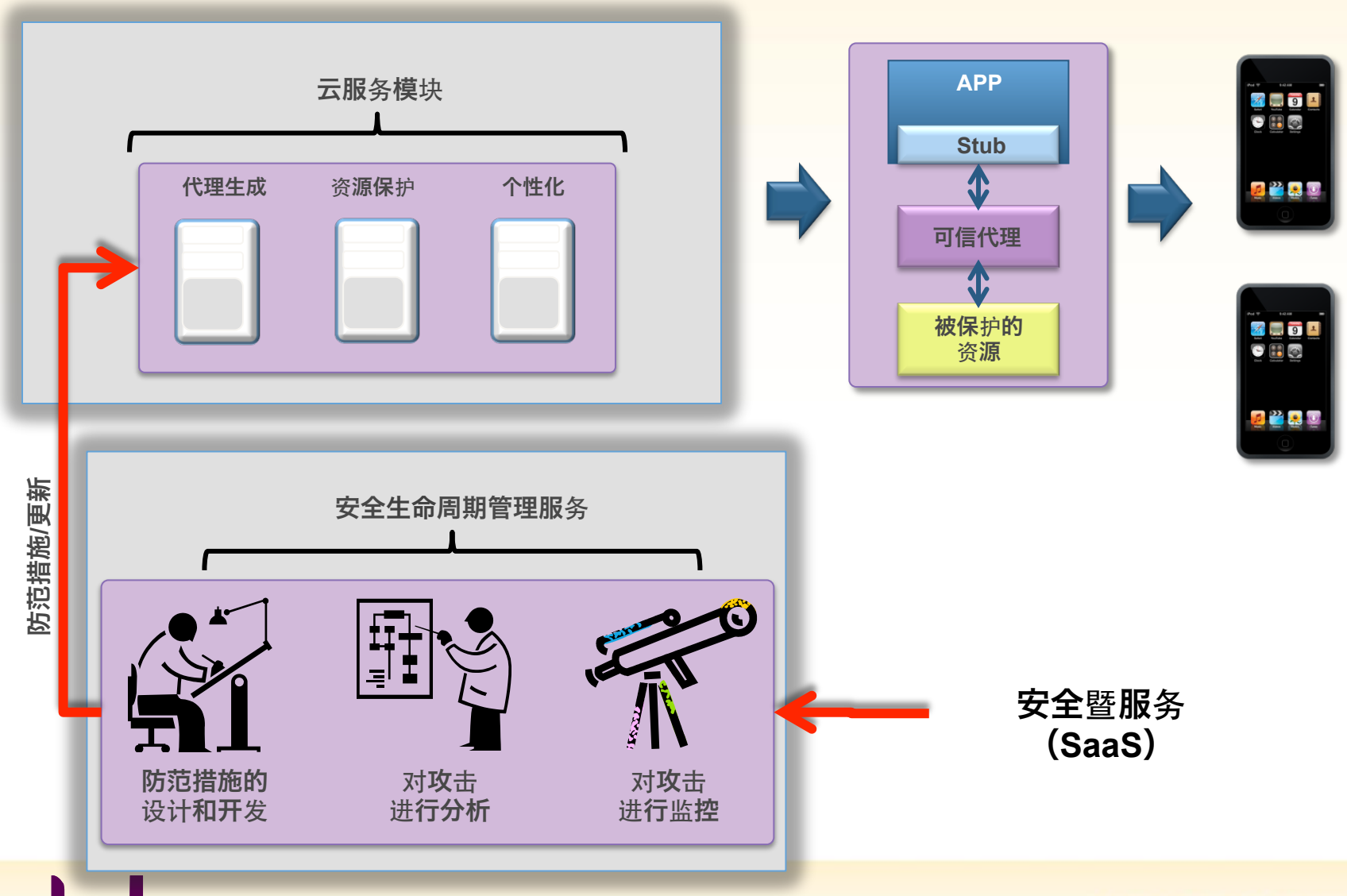
平台组件：
- 程序启动器
- 数字证书
- 引导装载程序
- 硬件锚
- 驱动
- 固件

开启/关闭决定：
- 平台完整性
- 节点锁定 /用户锁定数据
- 应用完整性
- 资源完整性
- 调试检查

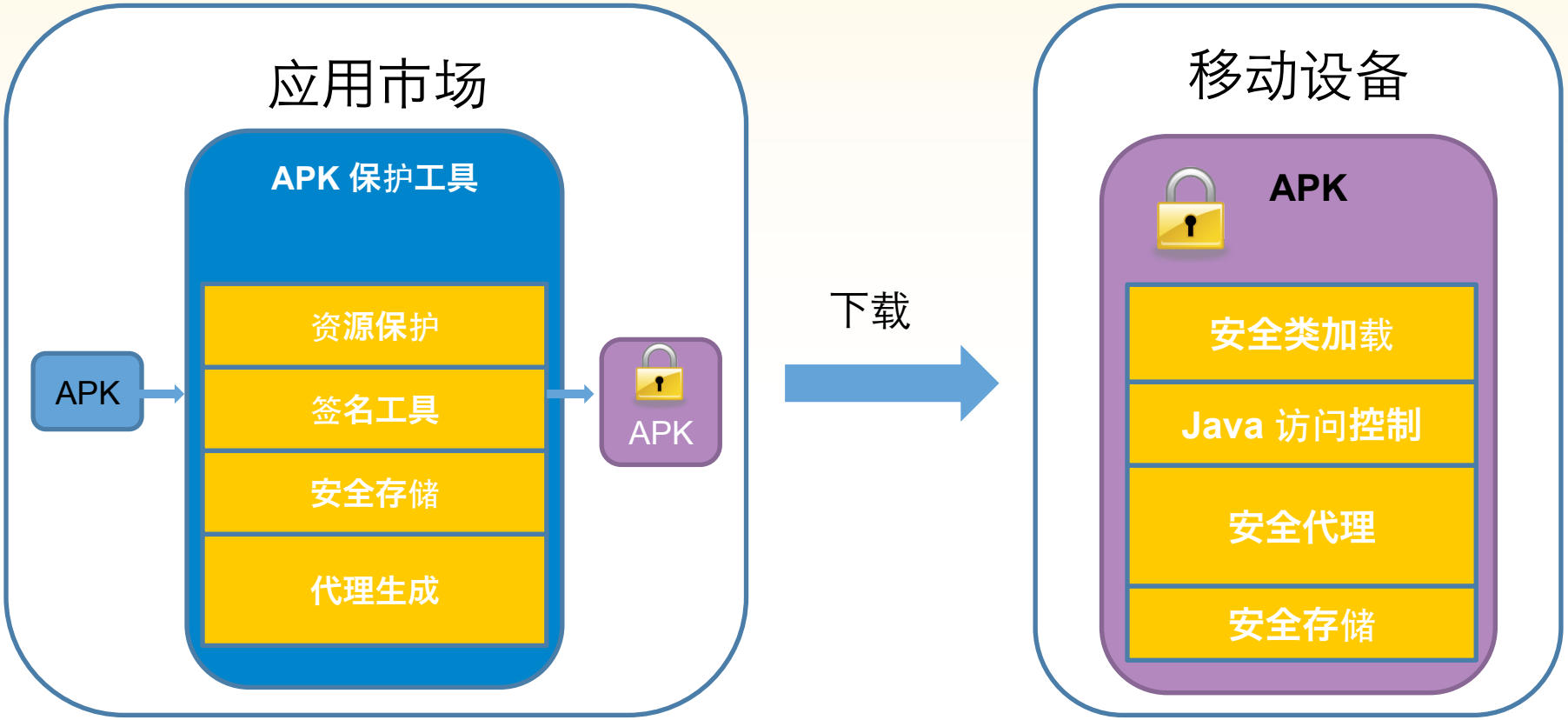
控制应用程序的执行:
- 资源文件
- 访问在线服务器

可选项
安全硬件
设备指纹识别
安全MicroSD 刷新
通过与"前端"的双向通信，可对不同的信任度予以补充

应用安全架构


云服务模块
代理生成
资源保护
个性化
APP
Stub
可信代理
被保护的资源
防范措施/更新
安全生命周期管理服务
防范措施的设计和开发
对攻击进行分析
对攻击进行监控
安全暨服务(SaaS)

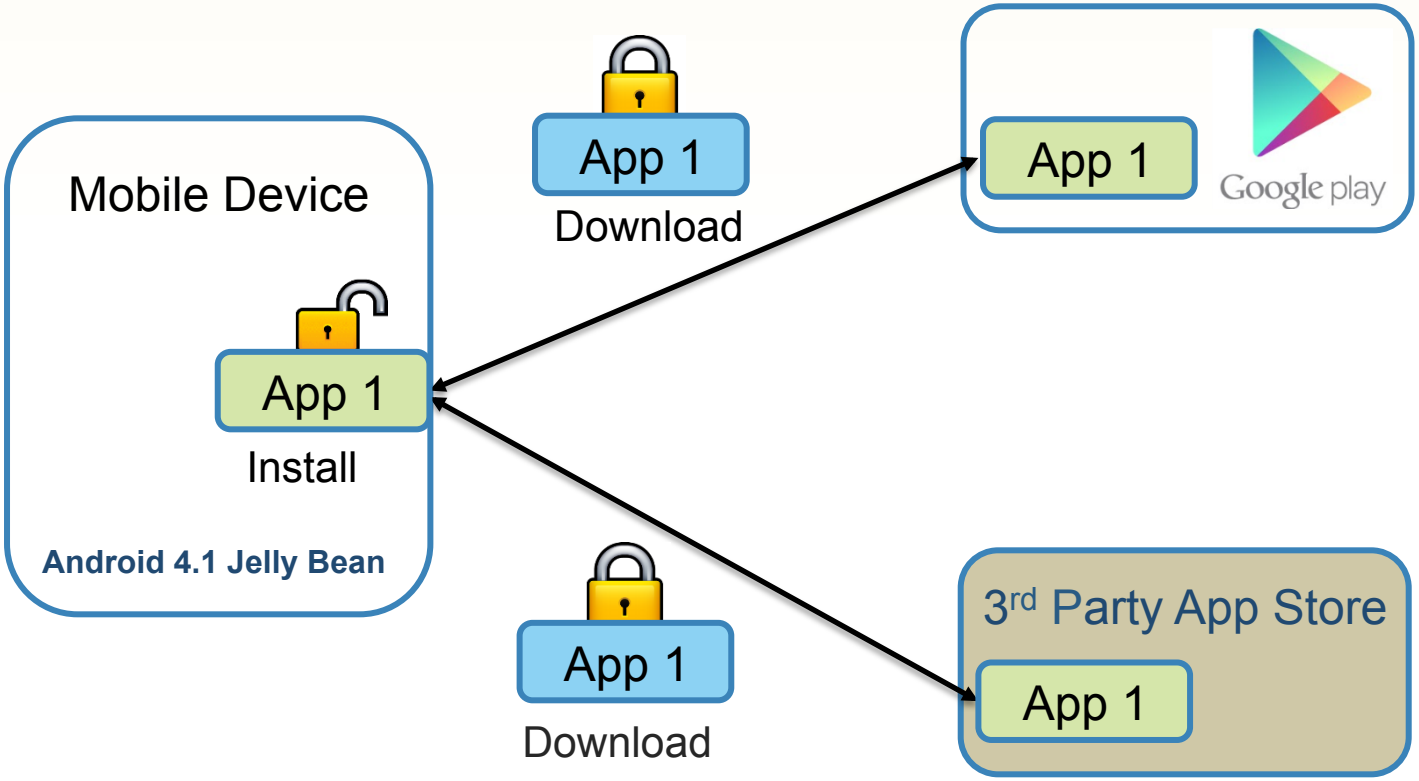
运行中的应用保护



- Google Play 的 **应用加密**措施（Jelly Bean， Android 4.1) 不能提供**下载安装后的应用保护**!

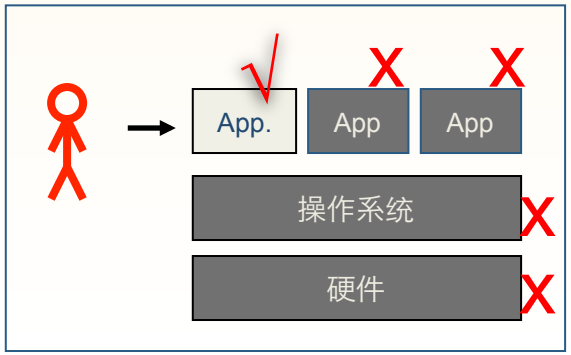
安卓4.1应用加密

- Google Play
  - Android 4.1, a.k.a., Jelly Bean, supports App Encryption feature.
  - 应用只在下载过程中加密， 安装即解密。



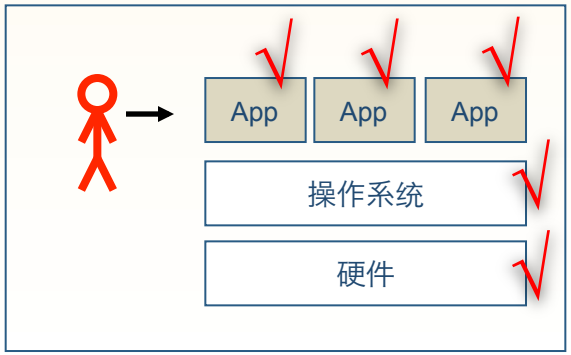
应用安全过渡到平台安全

应用安全



- 应用程序被依次保护
- 被保护的应用程序都是可信的
- 没有被保护的应用不可信
- 整个平台不可信

平台安全



- 另外一个可供选择的方法是创建一个“可信平台”，(通常情况下是采用可信的应用程序)
- **“平台安全”可间接确保应用程序的安全性。**

安卓平台安全

安全挑战

恶意软件

- 用户级病毒
- 高级威胁
  - 内核级病毒
  - 木马
  - 间谍软件
- 感染应用

不明软件

- 滥用隐私的应用
- 广告
- 通信应用
- 劫持的应用
- 攻击分析工具
- 审查的应用

正常应用

由下列渠道安装:

- 运营商
- 正规的安卓市场
- 第三方应用市场
- 其他渠道

可信应用

- 安全应用
- 支付及电商应用
- 企业应用，如邮件等

安全挑战;
- 检测，预防恶意或不明软件
- 保护系统及合法应用的安全

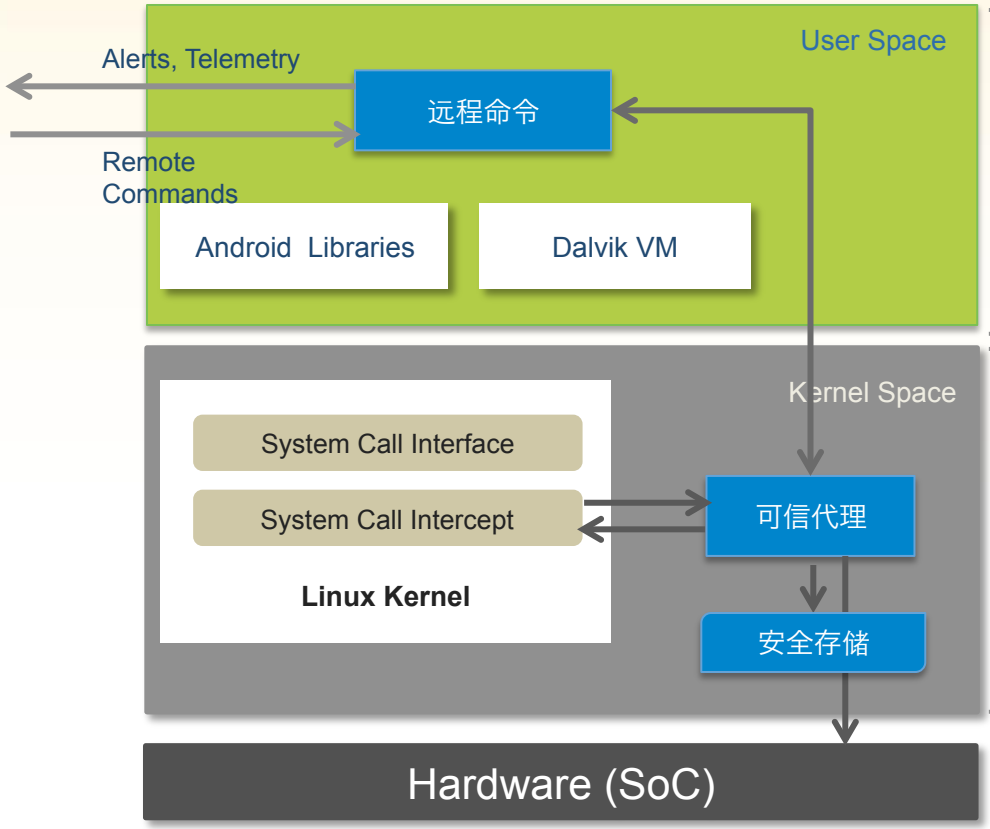
安全挑战;
- 防止可信应用和企业应用受感染
- 防止应用盗版和劫持
- 保护安全应用机制

irdeto

安全方案

- 谷歌保镖 “Bouncer”
  - *Once an application is uploaded, the service immediately starts **analyzing it for known malware, spyware and trojans**. It also looks for **behaviors** that indicate an application might be misbehaving, and compares it against previously analyzed apps to detect possible red flags. We actually **run every application** on Google’s cloud infrastructure and **simulate how it will run on an Android device** to look for hidden, malicious behavior.*
- 分析－Jon Oberheide and Charlie Miller, on SummerCon’12.
  - Bouncer使用 Linux + Cloud + Simulation (QEMU)
  - 它可发现初级的病毒，不能发现复杂的病毒
- 其他安全方案:
  - 云应用审查工具: RiskRanker, jointly by NCSU and NQ Mobile.
  - 云病毒查杀, 及移动安全解决方案.
  - 学术领域专注于安卓系统本身较弱的权限机制.

设备模块



标准安卓系统中间件

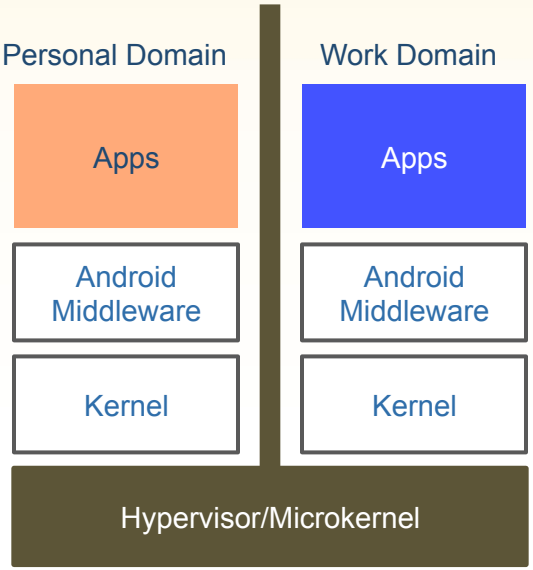
可信代理:

- 可加载内核模块
- 对内核各组件的强制访问控制
- 内核完整性校验
- 防范内核级病毒侵入
- 应用及权限校验
- 安全存储病毒库，策略，及分析数据

安全性：

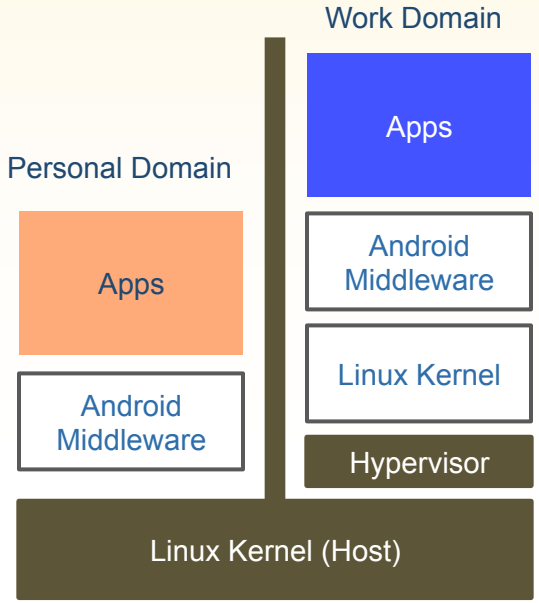
- 可信代理可防反编译及防篡改
- 所有通讯在安全通道上
- 建立在较小的可信基上
- 与硬件绑定

域隔离方案



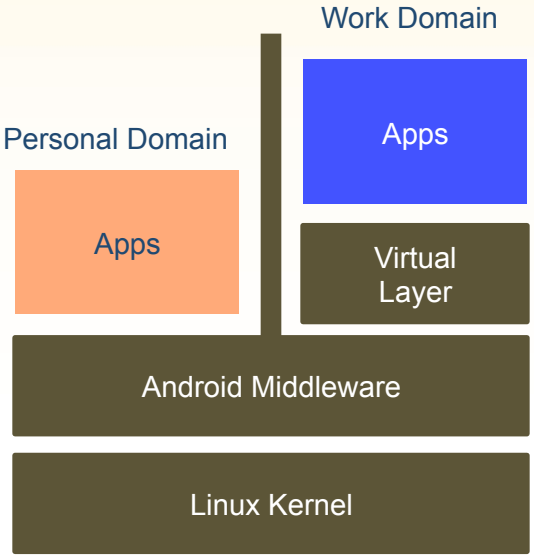
Type 1 Hypervisor

- 现今的ARM指令集还未支持
- OEM厂家集成是一个问题
- e.g. Redbend



Type 2 Hypervisor

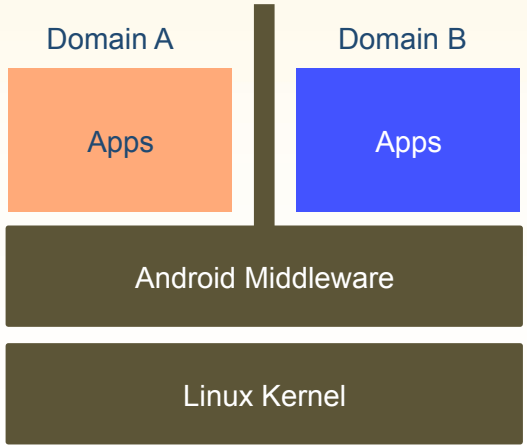
- 不能防内核级的病毒入侵
- 对OEM厂家的集成需求较少, 不需预装
- e.g. VMware Mobile Horizons

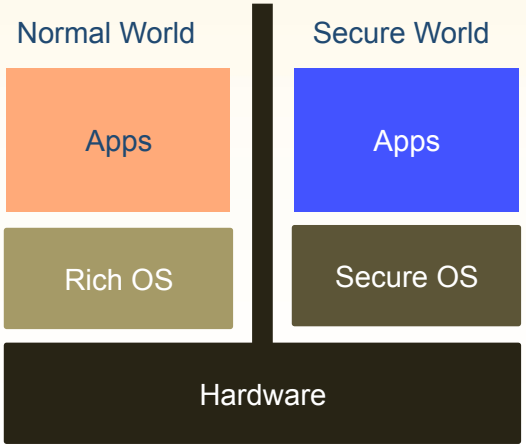


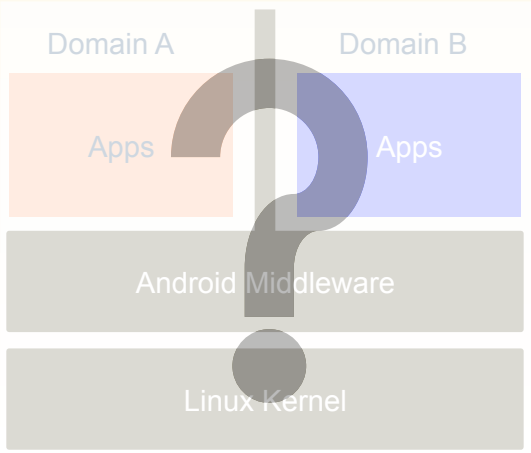
OS- Level VM

- 不能防用户和内核级的病毒入侵
- 性能影响较大
- 应用须加载到虚拟机中
- 应用间通讯在虚拟机中处理
- e.g. Enterproid Divide

域隔离方案







TrustDroid

- 对安卓中间件做修改
- 用Tomoyo Linux内核
- 不能防内核级的病毒入侵
- 较少的 CPU/内存/电池的消耗
- 是研究工作，不是产品
- 依赖于较大的可信基

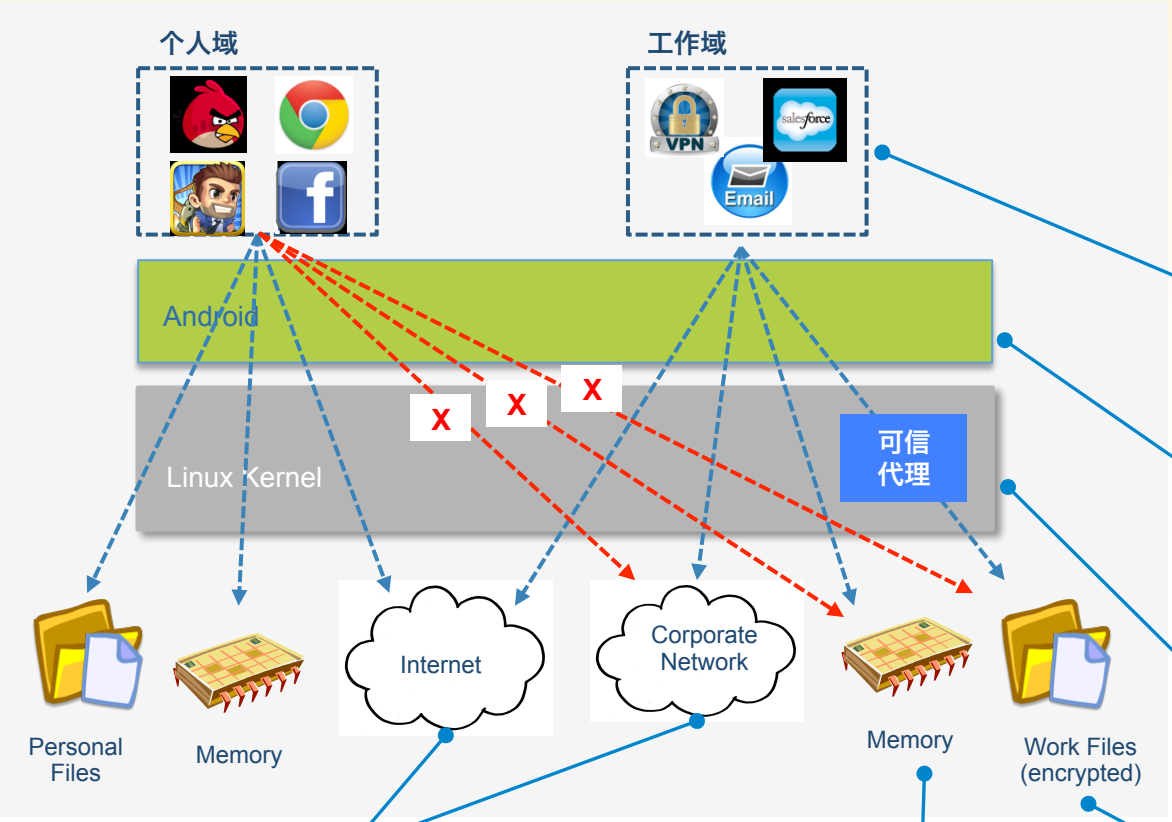
TrustZone

- 依赖硬件安全
- 较高的安全性
- 对一般应用提供安全调用接口
- 需要产业链的整合，如芯片商，手机商等
- e.g. ARM TrustZone, TEE

理想的方案?

- 不依赖硬件
- 不复制软件栈
- 防内核级病毒
- 易集成部署
- 较小的可信基
- 较高的性能
- 较小的负载
- 无缝的域隔离

域隔离安全分析



工作域中白名单上的应用允许执行。而这些应用都需要公司*IT*准许。

进程间的通讯被阻止。

域隔离防止个人域中的内核级病毒感染到工作域。这可通过内核中强制访问控制实现。

工作域中的文件加密存放

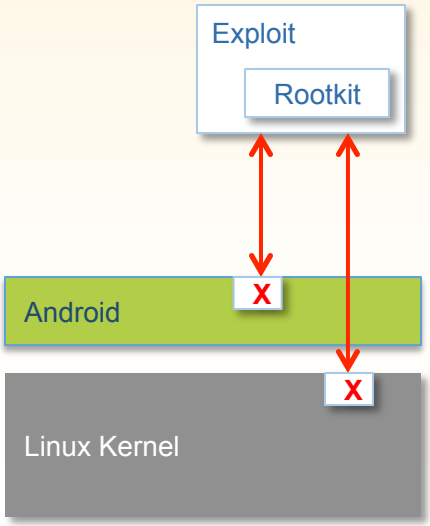
工作域中的应用允许访问公司的私有网络。而访问公共的*Internet*则需受控。

工作域中的内存也是隔离的，可以防侦听及各种内存攻击。

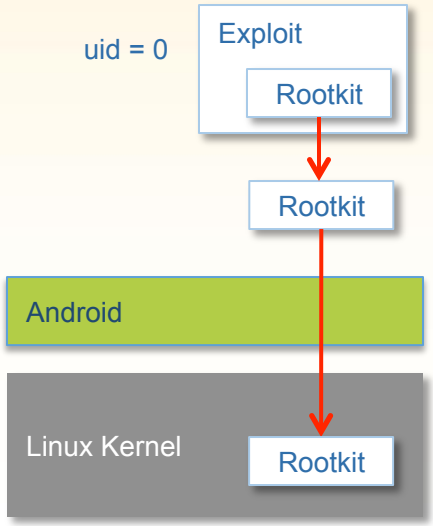
内核级病毒和根权限入侵

- 安卓系统中较易利用内核漏洞提权
  - 最近发表的一篇论文, *“Dissecting Android Malware: Characterization and Evolution,“ (Oakland 2012),* 发现 37% 安卓病毒样本携带内核级的病毒，超过90% 的病毒包含受控僵尸。
  - 内核级病毒之危害还在于其一旦装入，很难被发现，并且将常驻内核之中。
  - 安卓操作系统的底层构筑在Linux内核上，一旦进程获取内核权限，也就拥有整个系统，因为内核中并无强制安全控制。
- 完整的安卓平台安全方案除了应该解决用户级的安全问题，如域隔离，也必须应对内核级病毒和根权限入侵。

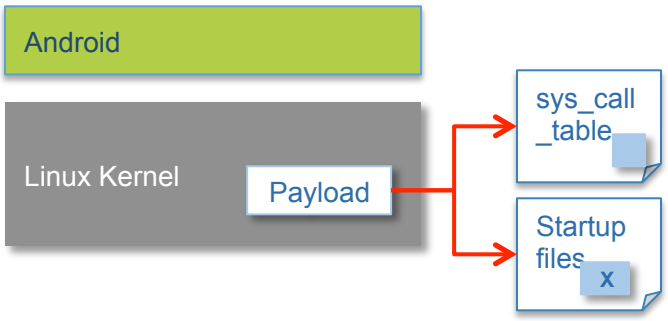
内核入侵过程



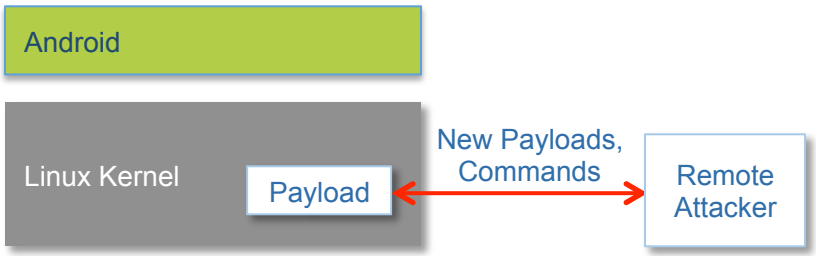
1. 获**取root权限** – 利用系统内核漏洞



2. **注入病毒代**码– 利用 LKM or /dev/kmem加载病毒体



3. 贮**存/隐藏** -- 修改sys_call_table and startup files 以使病毒长期贮存及隐藏在内核.



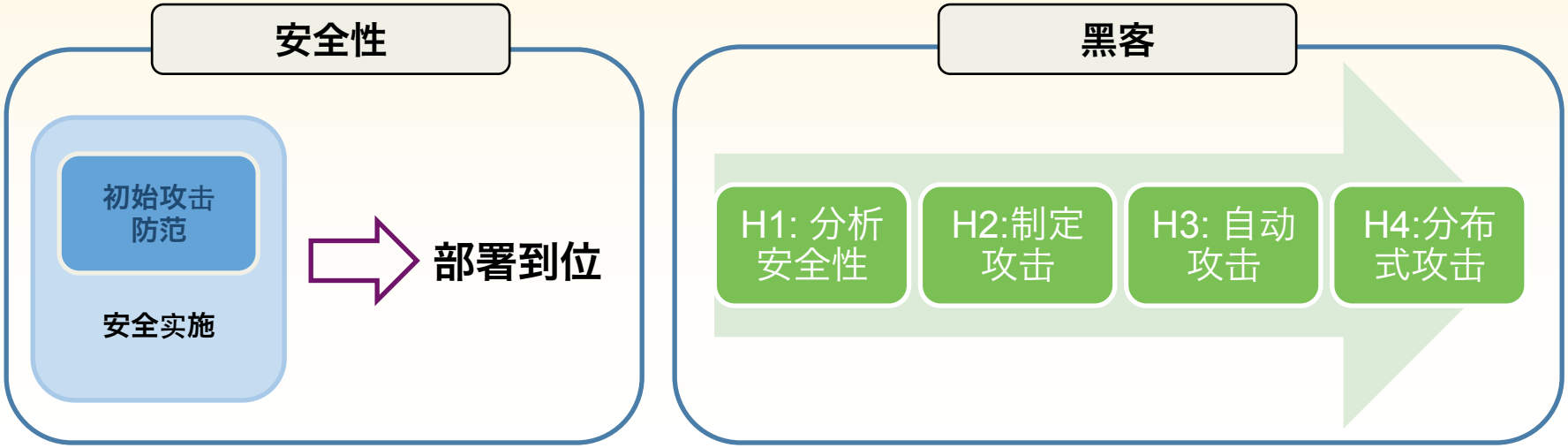
4. **攻击** – 已经存在的病毒可以发动任何攻击，如安装新软件，泄露隐私，甚至毁坏设备。

内核入侵防范

	防御机制	可防范：
已知攻击	病毒签名值	• 针对于已知病毒及签名值
0day 攻击	阻止加载未签名的可加载内核模块（LKM）	• 试图通过LKM加载到内核中的病毒。
	阻止对 /dev/kmem的访问	• 试图修改内核中/dev/kmem驱动器的病毒。
	内核完整性校验	• 试图修改硬盘中或内存中内核代码的病毒。
	保护SYS_CALL_TABLE	• 试图篡改系统调用表，劫持系统调用的病毒。
	攻击行为	• 分析病毒攻击的行为模式，有预见性的分析潜在病毒。

动态及全生命周期的安全

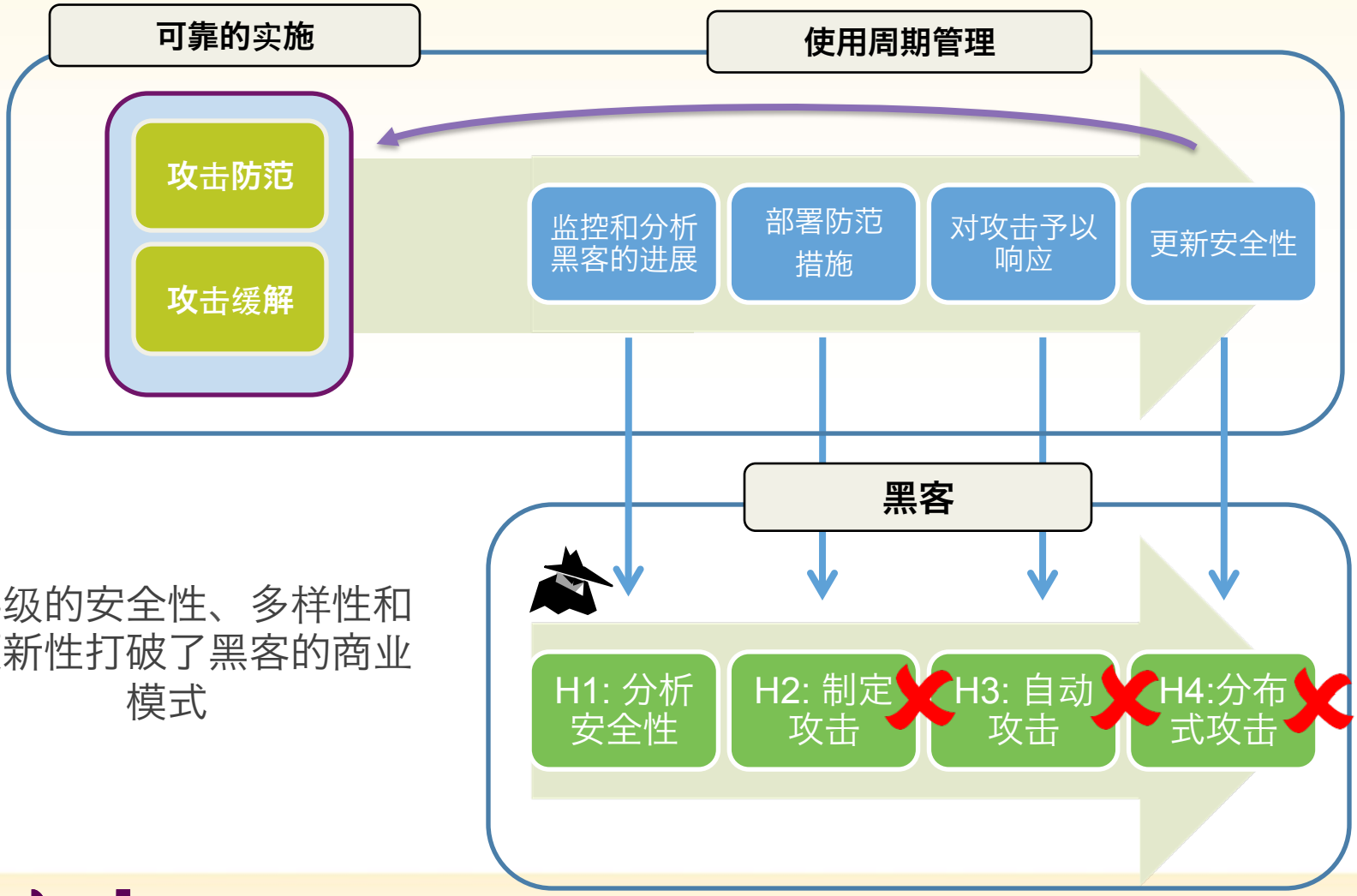
静态安全



- 只注重于对初始攻击的防范
- 其结果是：将被破解
  - 市场上所有的静态安全性解决方案– 即使是最强的 – 都被破解了(参见右表)

device	y	security	hacked	for	effect
PS2	1999	?	?	piracy	-
dbox2	2000	signed kernel	3 months	Linux	pay TV decoding
GameCube	2001	encrypted boot	12 months	Homebrew	piracy
Xbox	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
iPod	2001	checksum	<12 months	Linux	-
DS	2004	signed/encrypted executables	6 months	Homebrew	piracy
PSP	2004	signed bootup/executables	2 months	Homebrew	piracy
Xbox 360	2005	encrypted/signed bootup,encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
PS3	2006	encrypted/signed bootup,encrypted/signed executables, hypervisor, eFuses, isolated SPU	4 years	Homebrew Piracy	piracy
Wii	2006	encrypted bootup	1 month	Linux	piracy
AppleTV	2007	signed bootloader	2 weeks	Linux	Front Row piracy
iPhone	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy

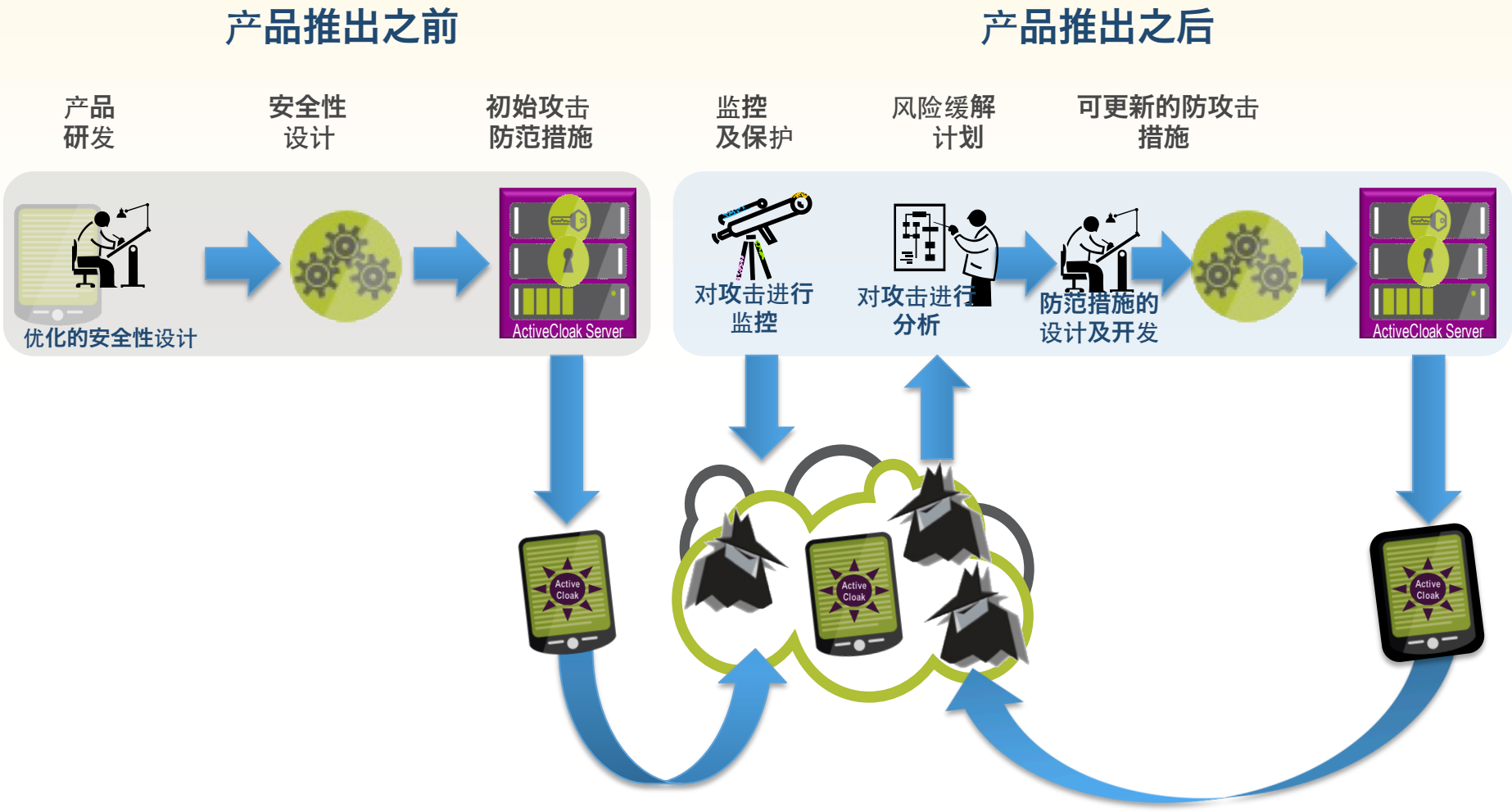
动态安全性



多层级的安全性、多样性和可更新性打破了黑客的商业模式

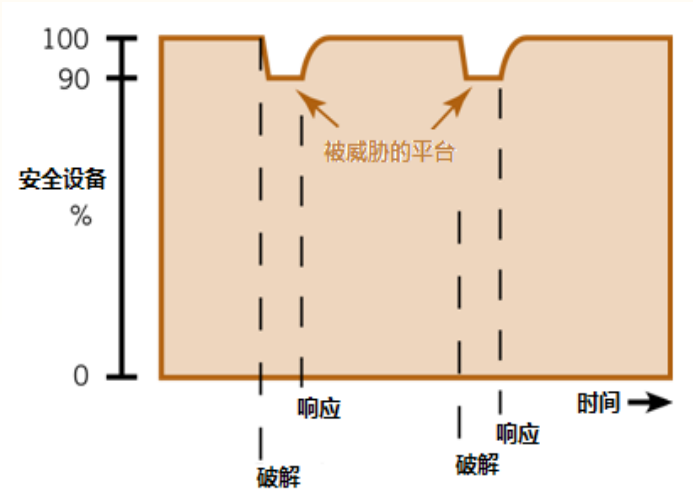
安全生命周期

RSA CONFERENCE CHINA 2012



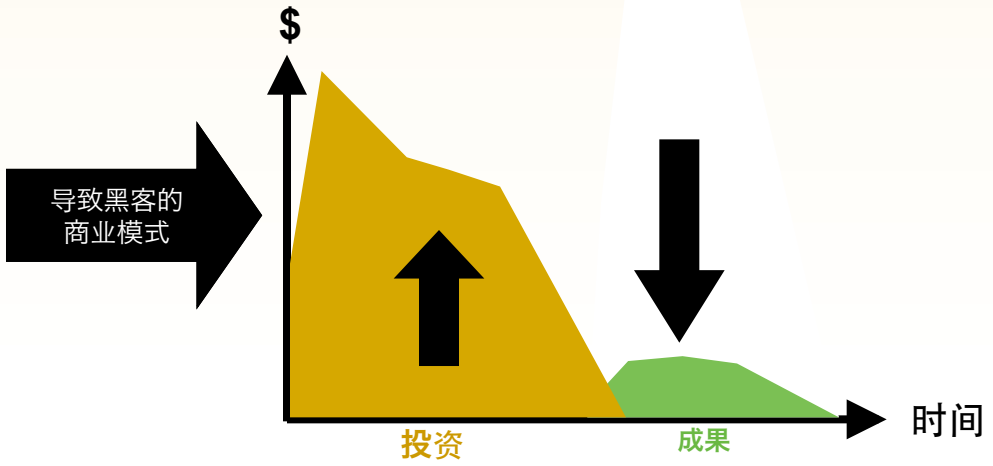
缓解攻击及系统修复

- 快速攻击响应能力
- 缩短攻击持续时间



防篡改
提高攻击成本

多样化的产品
缩小攻击范围



软件多样性的好处

使攻击范围被控制到最小– 预防自动攻击

当受到攻击时，提供快速修复的能力

使业务对于黑客而言不具有吸引力

结语 -开放共赢，安全第一!

1, 开放性 vs. 安全性

移动互联网需要开放式平台

新的恶意软件将肆虐

创新的安全是必要的

2, 安全保护

从应用保护到平台安全

动态的、多层级的、全生命周期的安全

更简单、更贴近客户需求、更具针对性

谢谢

li.tieyan@irdeto.com

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012