ISC 2017

2017 中国互联网安全大会
China Internet Security Conference

移动智能设备持续性安全管理探讨

杨正军

中国信息通信研究院，泰尔终端实验室
信息安全部副主任

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

移动智能设备持续性安全管理探讨

·移动智能设备安全现状

·移动智能设备安全管理现状

·移动智能设备持续性安全管理探讨

ISC 2017 中国互联网安全大会

360互联网安全中心

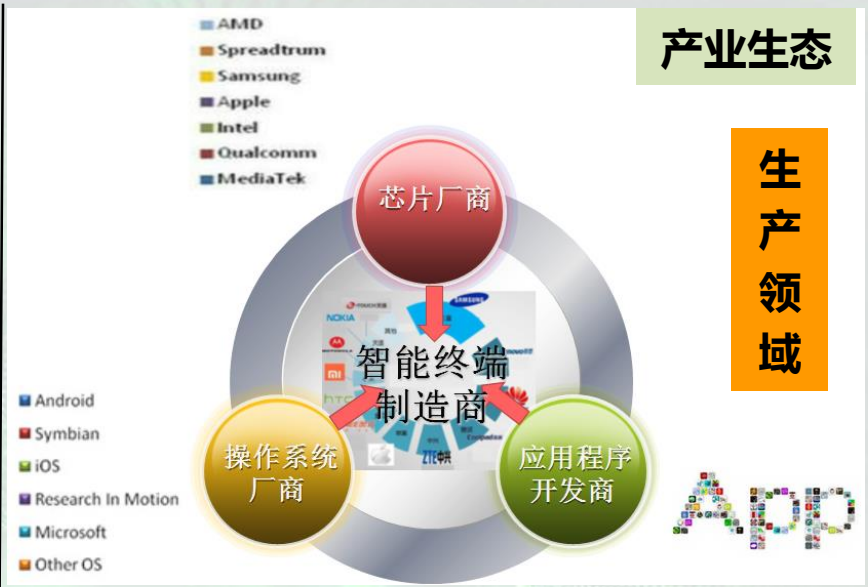
移动智能设备安全现状

安全生态、移动漏洞、勒索病毒、数据安全

移动智能设备安全生态

技术生态

产业生态



生产领域

移动智能设备安全现状

安全威胁日益严重，虽已在终端侧采用许多安全设计或检测防御手段，但由于攻击技术不断更新，安全抵御效果较为被动。

终端产业链是紧密结合在一起的一个整体的生态系统，一个环节受到威胁，会影响系统中的其它成员。

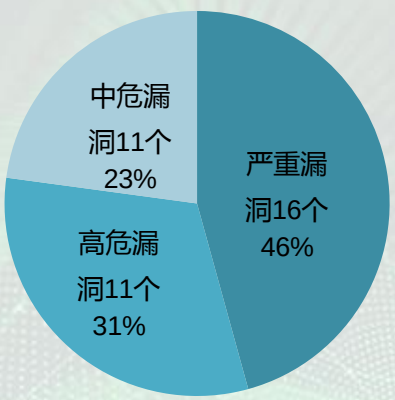
安全威胁可能出现在终端生态系统各个环节，如不对智能终端生态系统的进行整体安全管控，会影响整个终端生态系统的发展。

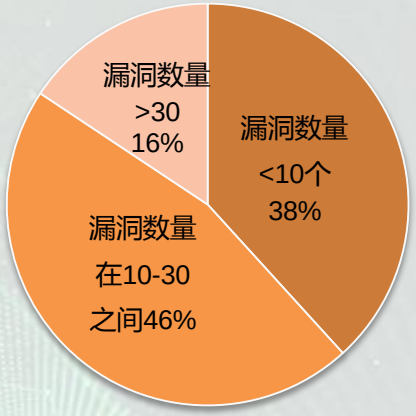
运营领域

移动设备漏洞频出，安全形势严峻

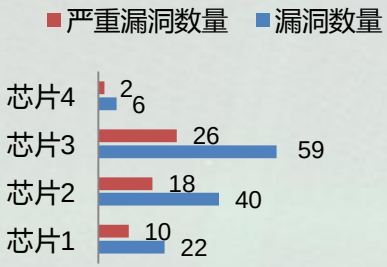
终端系统漏洞频出，形势不容乐观

- 泰尔终端实验室抽取2017年上市的108家厂商的217款移动智能设备，进行已知漏洞（选取262个）检测。
- 平均检测出漏洞数量为35个，其中严重漏洞16个，高危11个，中危漏洞8个。
- 终端中存在小于10个漏洞的终端为83款，占比38%；10-30个漏洞的终端为100款，占比46%；大于30个漏洞的终端为34款，占比16%。

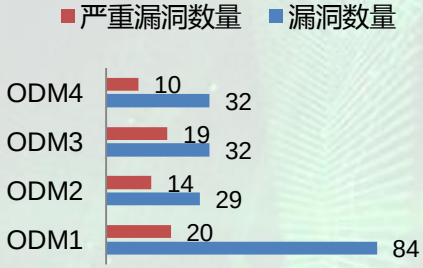




芯片厂商漏洞分布情况



ODM厂商漏洞分布情况

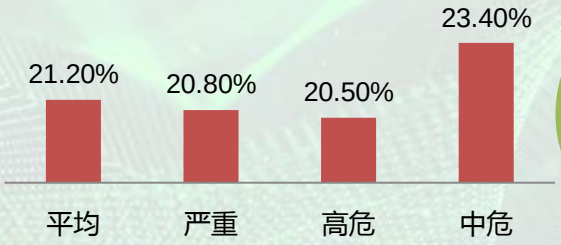


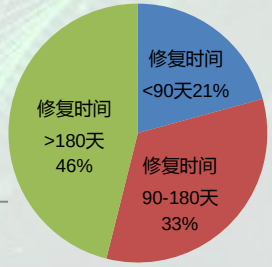
产业链条复杂，引入风险不断增加

- Google、芯片厂商、方案厂商、终端厂商、技术供应商（TEE、APP SDK等）均可能引入漏洞或安全风险。
- 方案商、芯片商修复不及时，很多设备维护周期较短。
- 消费者安全意识不足，百度安全实验室的报告显示近半数国内iOS设备依然停留在受高危漏洞影响的旧版系统，未升级的用户面临严峻的安全风险。

厂商修复能力不足，安全风险持续

- 总体漏洞未修复比例在21.2%，严重、高危、中危漏洞未修复比例分别在20.8%、20.5%、23.4%。
- 厂商打补丁不及时，平均延迟时间在165天，Top20厂商延迟时间稍短为148天，其他厂商为191天。

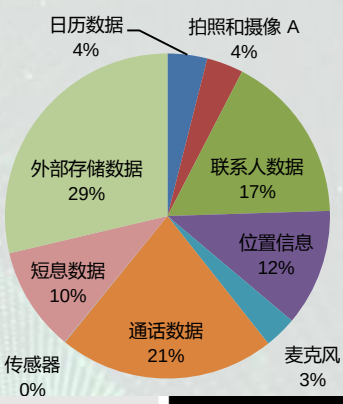




移动应用问题凸显，勒索病毒成趋势

预置应用权限滥用情况严重

- 泰尔终端实验室对7W多款预置应用进行评测，发现六成以上的预置应用申请了敏感权限如通话、联系人、位置和短信数据等，而多数权限在应用实际运行时并未使用。由于预置应用自身权限级别较高，权限滥用加大了应用脆弱性，若应用安全防护不足，有可能带来极大的安全隐患，增加终端攻击面。

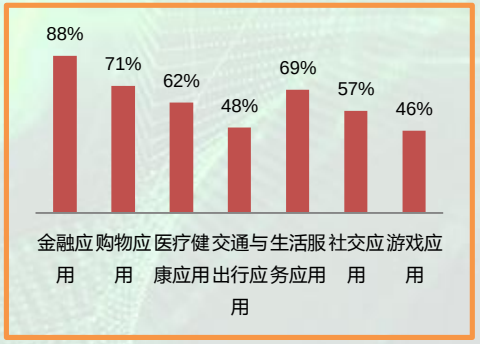


勒索病毒成移动安全新趋势

- 根据360烽火实验室的统计，2017 年1月-7月，共截获新增勒索软件416258个，平均每天新增1963个。“薄利多销”且制作成本低廉的点对点式直接性敲诈软件颇受制马人的青睐，语音解锁与二维码解锁成为新的表现形式。

金融客户端安全问题凸显，内存敏感数据泄露问题严重

- 泰尔终端实验室研究人员对303个移动应用的敏感信息保护进行了检测，发现其中96.2%移动应用存在内存敏感数据泄露风险。

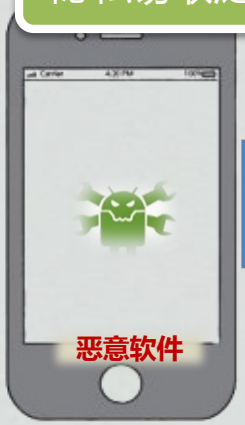


泛安全问题严重，侵犯用户权益情况

- 捆绑推广、难以卸载、关联启动、非法广告等泛安全问题泛滥。

移动数据被窃取、非授权获得情况加剧

隐私窃取泛滥



窃取隐私
非授权收集数据

通话记录、短信 通讯录、本机号码	● 个人信息遭贩卖 ● 垃圾短信、骚扰电话
身份证 账号信息	● 身份信息被贩卖 ● 账号丢失导致财产损失
位置信息、终端信息 应用列表信息	● 基于“LBS”的广告 ● 位置泄漏，安全存风险
音频、视频记录	● 商业机密、个人信息存隐患 ● 各类监听事件
其他	● 隐私问题越来越广泛 ● 其他可能问题令人困扰

数据、权限之争

- 终端厂商与互联网企业权限限度问题存在争议
- 终端厂商与应用厂商用户数据归属权问题存在争议

各执一词

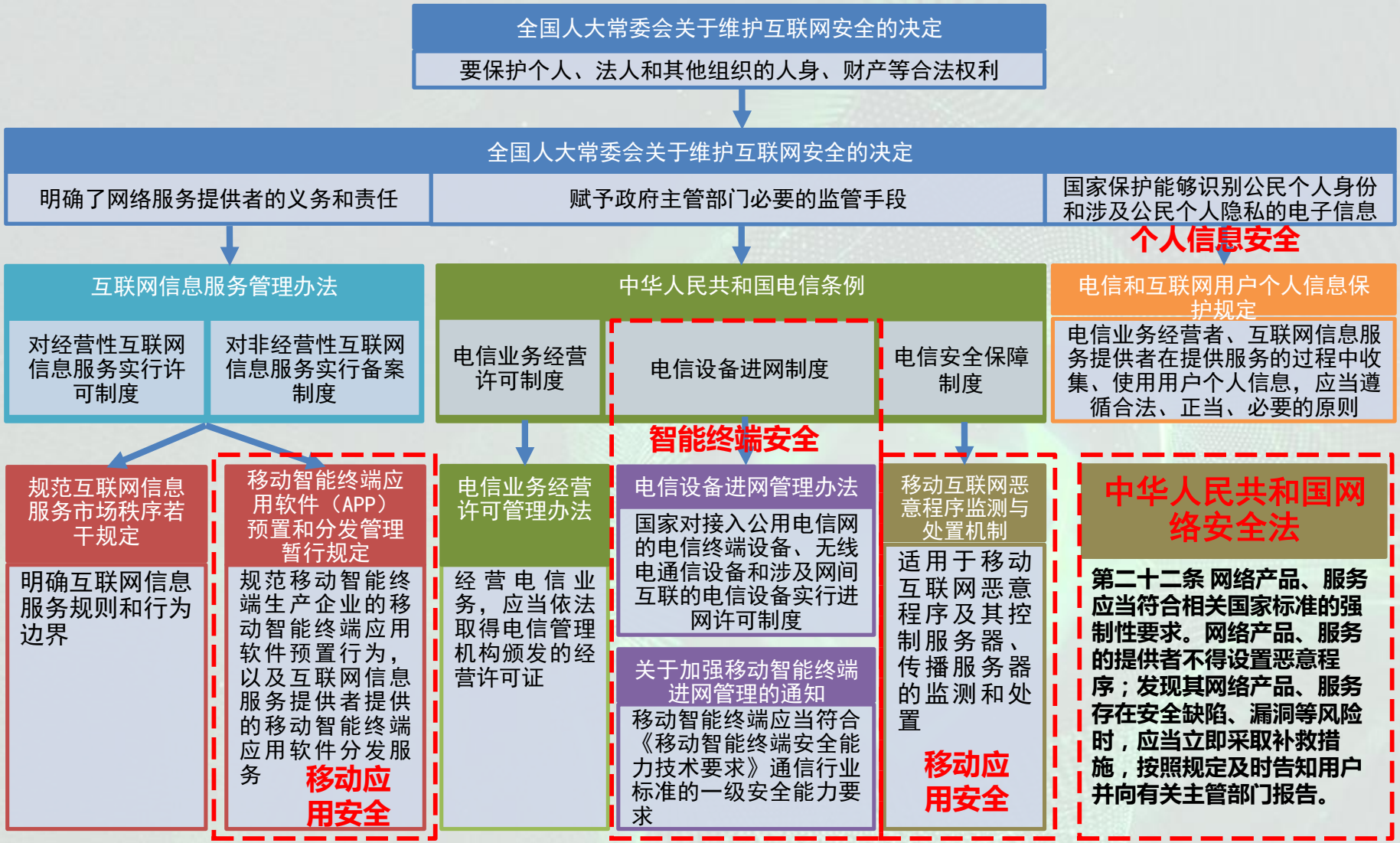
不正当竞争
阻止应用分发
阻止信息推送
禁止必要权限
禁止自启动

保护消费者权益
安全性
系统稳定性
功耗
兼容性

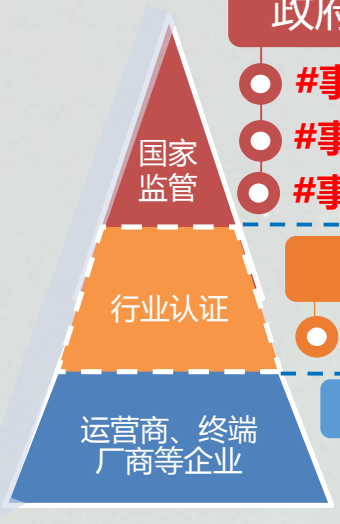
移动智能设备安全管理现状

多头管理，侧重于事前，缺少持续性监测手段

移动设备安全监管现状-相关法规



移动智能设备安全监管面临的挑战



政府监管，依托国家设备进网监管流程

- **#事前#进网审核**：依据电信设备进网管理制度在对终端设备进行安全检测
- **#事中#证后监督**：抽查上市终端是否与进网终端一致
- **#事后#变更备案**：上市后，终端系统、应用的安全更新需向工信部备案

行业规范

- TAF等行业协会推进智能终端及预置软件相关安全评估规范

企业自律

- 运营商：预置应用送测前把关、预装应用版本一致性检测、上市后进行定期抽测
- 终端厂商：经过内部标准测试、质量部门把关后，送测工信部备案、运营商入库等

目前针对移动终端及移动应用的安全监管主要放在事前的进网检测方面，针对移动终端设备事中事后监管主要通过证后监督检查、专项行动检查、服务质量通报、投诉举报等机制，终端持续性的、主动的监管方式方法有待完善，针对安全事件缺乏应急响应能力。

终端风险监控与安全预警主要依靠厂商自行维护，时效性和可靠性较难保证。

- 厂商能力参差不齐，对威胁和脆弱性感知较为被动，风险响应时效性较低。
- 缺乏规范和监管机制推动，依靠舆情影响和厂商自律，较难保障用户权益。

缺乏全面、权威的风险数据来源和安全风险预警响应机制。

- 漏洞信息和恶意应用监测平台众多，但缺乏支撑终端安全监测的全面、权威数据源。
- 缺乏数据有效关联分析机制，无法支持终端安全风险预警响应。

移动智能设备安全监管的新形势

- 网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
- 网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

- **健全网络安全保障体系：**
  - 全天候全方位感知网络安全态势。加强网络安全态势感知、监测预警和应急处置能力建设。建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。建立政府和企业网络安全信息共享机制，加强网络安全大数据挖掘分析，更好感知网络安全态势，做好风险防范工作。

- **总理连续三年在政府工作报告中提出要改变政府管理方式，推动简政放权、放管结合、优化服务改革，加强事中事后监管，坚持放管并重。**

建设针对移动终端漏洞、移动恶意应用持续性的、主动的监管能力

↓

建设针对移动终端及应用APP的监测预警和应急处置能力

↓

主管部门对移动终端的安全监管向事中、事后转变，提高监管的有效性和针对性

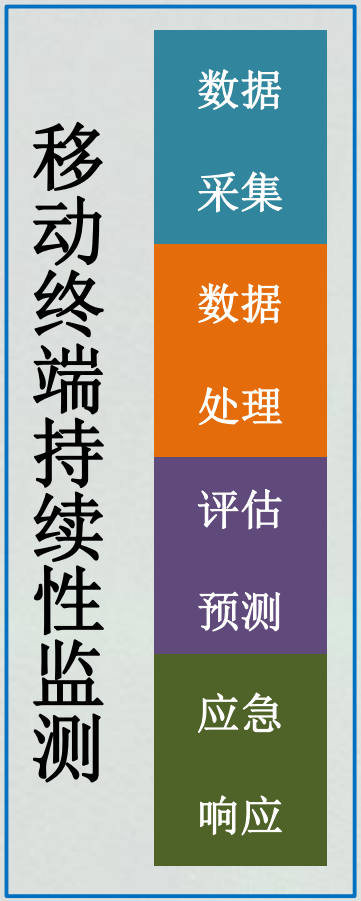
ISC 2017 中国互联网安全大会

360互联网安全中心

移动设备持续性安全管理探讨

数据采集、数据处理、预测评估、应急响应

持续性监测为移动设备安全监管提供新的思路



建立移动终端持续性和主动性监测能力

- 对于上市终端以及终端设备升级补丁插件后带来的智能终端设备受病毒感染或激活恶意行为进行感知监测，实现对检测后设备持续监测和管理，掌握智能终端设备运行环境安全，动态监测、响应、处置、改善移动终端设备安全状态。

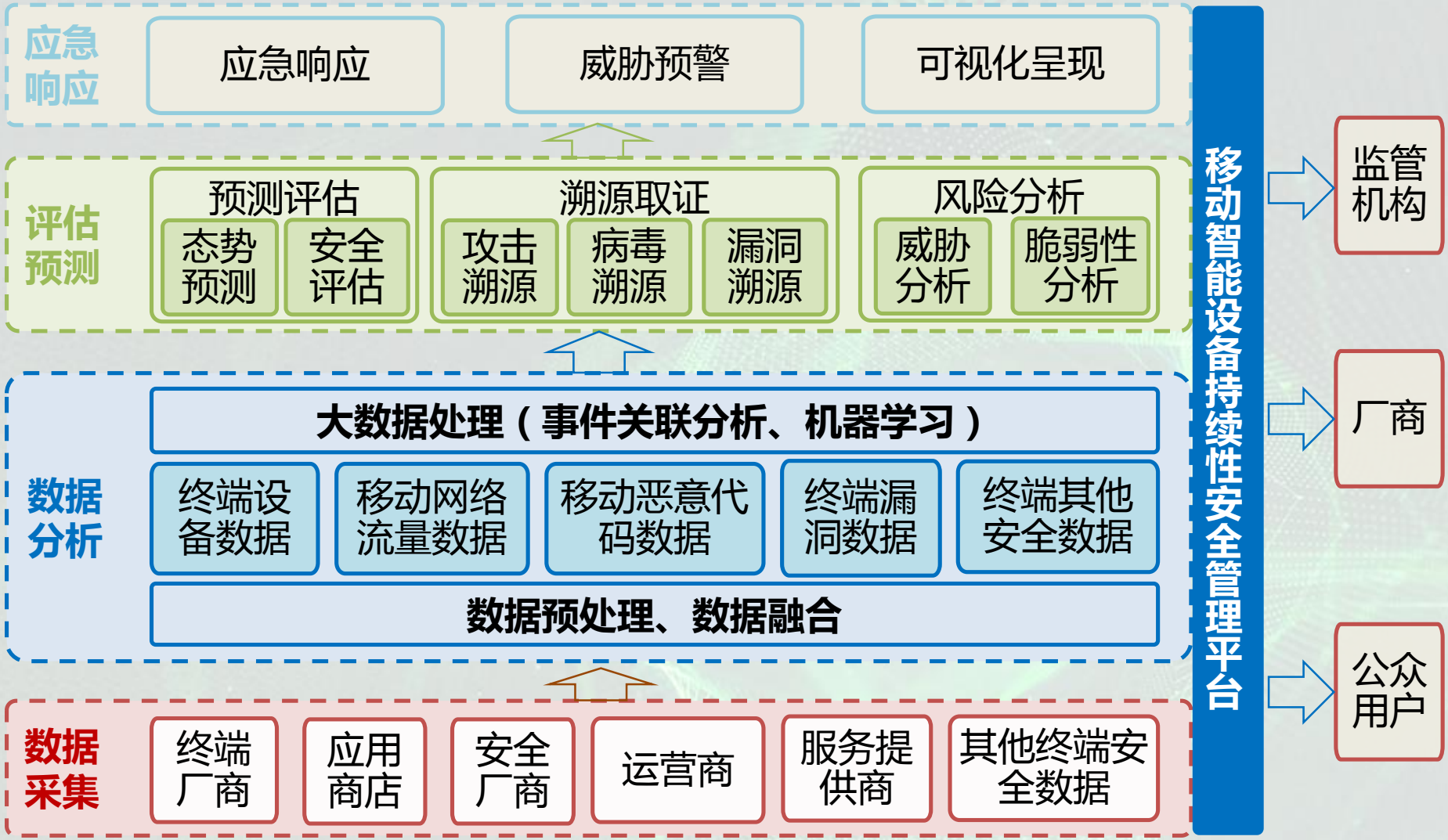
加强移动终端事中事后监管

- 利用移动智能终端安全持续性监测能力，结合运营商、设备制造商、安全公司等，将海量终端设备数据进行整合分析，解决移动终端事中事后监管的关键技术难题。

增强移动终端攻击溯源与应急处置能力

- 能够对恶意攻击、恶意应用、安全事件进行溯源取证，对恶意应用的发布者进行追踪。同时能够移动终端安全进行监测预警和应急处置，准确把握网络安全风险发生的规律、动向、趋势

移动智能设备持续性安全管理—关键技术架构



中国泰尔实验室—移动智能设备漏洞监控数据平台

ISC 2017 中国互联网安全大会 | 360互联网安全中心

CAICT 中国信息通信研究院

移动智能终端漏洞监控数据平台

漏洞监控数据总览

数据截止日期：2017年8月　累计监控：418款智能终端

2017年8月

检出漏洞数

17124

同比上升 102% (8477)

检出严重漏洞数

13736

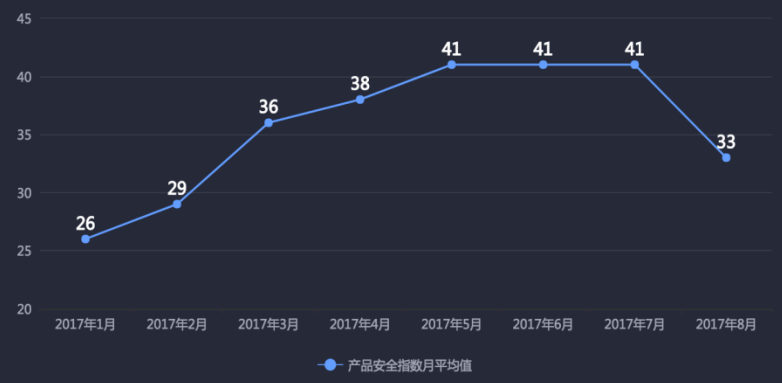
同比上升 105% (6692)

累计检测次数	累计检测漏洞	累计检出漏洞	平均漏洞修复延迟时间
813	13.0万	3.54万	311天

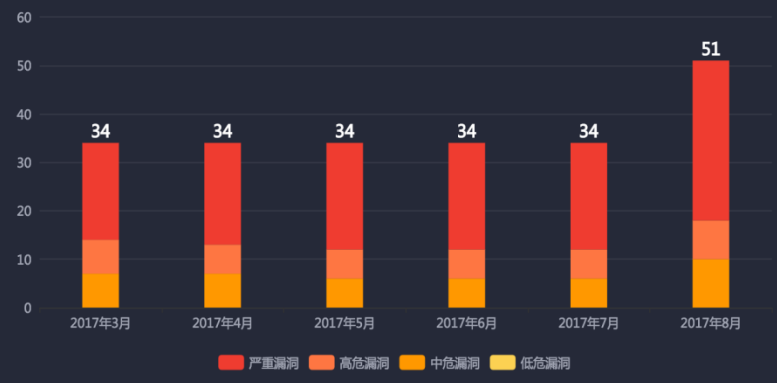
264 个漏洞

418 款智能终端

产品安全指数月平均变化趋势



未修复漏洞数月平均变化趋势



中国泰尔实验室—移动智能设备漏洞监控数据平台

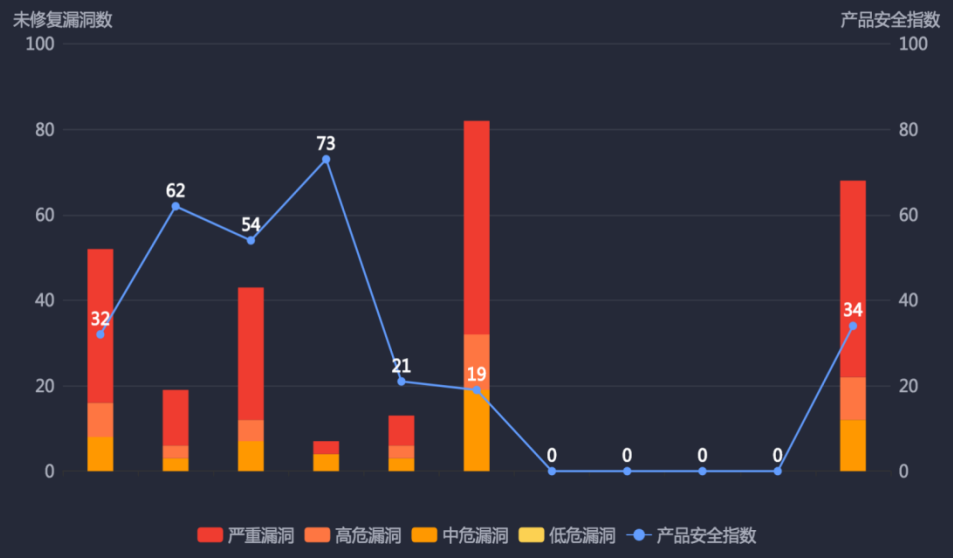
移动智能终端漏洞监控数据平台

产业链安全现状

数据截止日期：2017年8月　累计监控：418款智能终端

旗舰产品　中端产品　入门产品

旗舰产品按厂商统计



旗舰产品安全指数排行榜

排名	产品型号	安全指数	参考价格
1		96	3788
2		73	4498
3		71	5988
4		71	5688
5		65	3099
6		65	3099
7		64	3750
8		62	5088
9		58	3899
10		58	3199

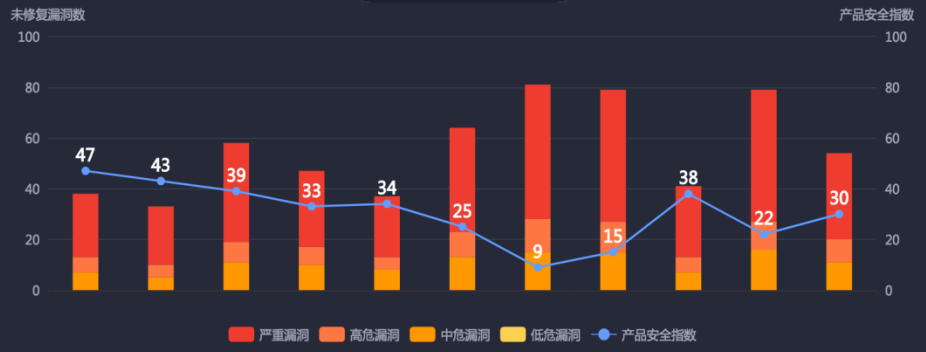
中国泰尔实验室—移动智能设备漏洞监控数据平台

移动智能终端漏洞监控数据平台

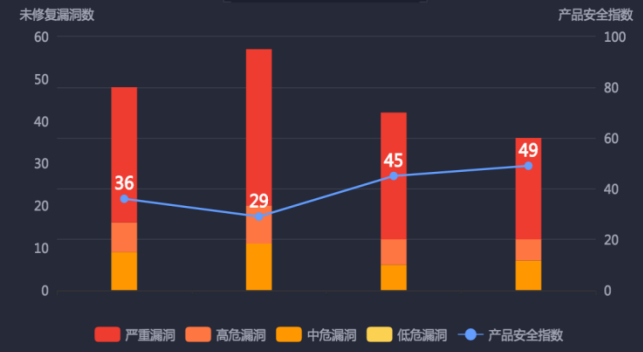
产业链安全现状

数据截止日期：2017年8月　累计监控：418款智能终端

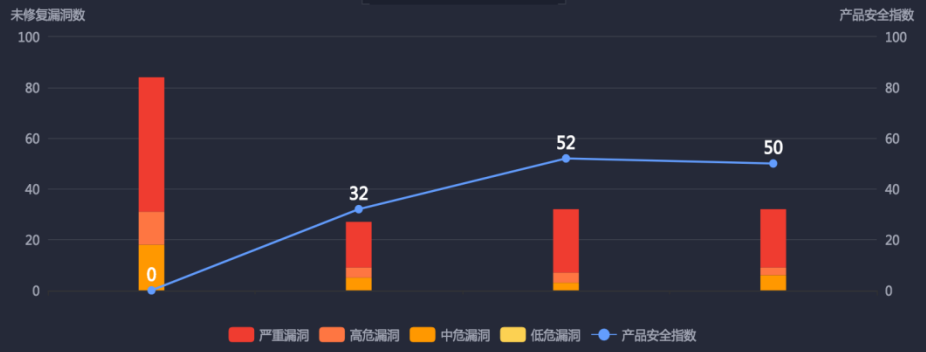
按OEM厂商统计



按芯片厂商统计



按ODM厂商统计



严重漏洞影响设备数量

1	CVE-2017-0386 270	6	CVE-2017-0418 219
2	CVE-2016-2182 269	7	CVE-2017-0416 219
3	CVE-2016-6704 251	8	CVE-2016-0827 216
4	CVE-2016-2476 222	9	CVE-2016-3880 210
5	CVE-2017-0417 219	10	CVE-2017-0540 204

中国泰尔实验室—移动智能设备漏洞监控数据平台

ISC 2017 中国互联网安全大会 | 360互联网安全中心

CAICT 中国信息通信研究院

移动智能终端漏洞监控数据平台

各OEM厂商全系列产品安全现状

数据截止日期：2017年8月　累计监控：418款智能终端

HUAWEI
SAMSUNG
oppo
vivo
小米
GIONEE
MEIZU
nubia 努比亚
smartisan
lenovo
其他品牌

全系列产品安全指数均值

47

高于行业平均 (30)

全系列未修复漏洞数均值

38

高于行业平均 (55)

序号	产品型号	未修复漏洞数	严重漏洞平均修复延迟时间	产品安全指数	产品安全指数全行业排名
1		1	0天	96	2
2		3	195天	78	5
3		4	468天	71	10
4		7	134天	71	10
5		8	180天	71	10
6		13	110天	65	16
7		8	403天	63	19
8		17	114天	62	22
9		15	166天	61	26
10		19	113天	61	26
11		17	192天	59	31
12		17	192天	59	31
13		21	138天	59	31
14		14	385天	58	34
15		26	140天	58	34

移动终端安全态势感知能力构建—实现难点探讨

1 产业方面：厂商安全数据私有，缺乏上下游联动推力和依托机制

- 目前移动终端安全防御（漏洞补丁等）基本依靠厂商自行维护，大家各管一摊，缺乏信息共享和沟通，单一的供应商或者企业无法对终端威胁全景有完整和实时的掌握。
- 现有涉及移动设备安全监测平台功能不够全面，只具备移动应用、安全漏洞等某一方面的监测、分析能力，缺乏全面的监测平台

2 技术方面：基于大数据分析的安全风险评估和预测是新的方向和技术难题

- 移动终端行为、数据复杂多变，目前威胁分析主要停留在微观时间和有限空间尺度，如何基于大数据分析对移动终端的运行规律和安全态势进行评估和预测是需要解决的新问题。
- 多数安全事件都会跨越和影响多个区域，在进行数据挖掘时，必须将不同来源的威胁信息进行关联分析，以便判断全局环境下的安全风险。

3 政策方面：缺乏持续性安全管理的风险监控技术、管理体系有待建立

- 移动智能设备持续性安全管理需要大量数据作为支撑，往往涉及个人隐私，为企业私有，在数据流通上限制较多。
- 不同机构间数据共享范围不明、方式不清。不同机构之间是互相交换还是单方面的数据获取？跨行业、跨区域机构数据合作如何实现？有待移动终端安全信息共享机制。
- 如何基于移动终端安全态势感知框架，建立安全监测的技术和管理体系，例如移动终端安全态势评估及预测的指标体系、移动终端事中事后监管策略、移动终端应急响应管理体系等都是有待解决的重要问题。

完善移动设备持续性安全管理策略的具体措施与建议

标准引导 **构建平台** **完善政策**

（一）推动建立移动智能设备持续性监测与安全管理标准体系，涉及移动设备数据采集、数据处理和数据分析，以及移动智能设备安全态势评估、预测、回溯和应急响应等方面，为移动智能设备持续性监测、安全态势感知平台建设提供指导，为国家移动终端监管部门与第三方测评机构的监管与测评提供参考依据。

（二）支持相关技术攻关和研发，引导和鼓励各方参与移动智能设备持续性监测和态势感知关键技术突破和创新。

（三）着力构建移动智能设备持续性监测平台，为厂商实施安全防御提供技术和数据支持；为政府监管部门掌握智能设备整体安全态势，制定安全策略提供权威参考；也有利于用户确认终端应用环境可能面临的威胁，及时采取防护措施。

（四）完善移动智能设备安全监管策略，加强事中事后监管，持续监测移动智能设备与应用软件安全态势，对安全事件及时作出应急响应。

谢　谢