



# 移动互联网安全

## 第五章 智能终端操作系统安全基础

黄 玮



# 内容提要

- 智能终端概述
- iOS系统安全概述
- Android系统安全概述
- Android应用安全实验环境搭建



# 前言：为什么要研究智能终端安全



# 一组数据和现状（2014.5）

- 移动互联网已经成为最大的信息消费市场、最活跃的创新领域、最强的信息通信技术产业驱动力量
  - 2013 年全球移动业务收入达到 1.6 万亿美元, 相当于全球 GDP 的 2.28%
  - 全球智能手机出货量近 10 亿部, 达到 PC 的 3 倍
  - 移动互联网重构了互联网服务的模式与生态, 全球应用程序下载次数累计超过 5000 亿
  - 全球计算平台中移动操作系统的占比超过 50%
  - PC(Wintel) → 智能终端(Android&iOS+ARM)
  - 视频、微博等主要互联网平台来自移动计算平台(Android/iOS)的流量超过 50%



## 现状 (2017.1)

- 移动应用步入平稳发展阶段
  - 移动服务成为互联网服务主体
  - 全球移动互联网增长步入平稳期
    - 全球人口红利正快速消失，行业转入平稳发展新阶段
- 产业互联网发展全球提速
  - 万物互联时代全面开启
    - 从连接规模来看，全球联网设备数量保持高速增长，全面超越移动互联网设备数量
  - 工业互联网和车联网成两大热点



## 发展趋势 (1/2)

- 全球互联网正从“人人相联”向“**万物互联**”迈进
- 物联网推动互联网应用从消费领域向生产领域扩展，并逐步深入城市管理各环节
- 互联网逐步回归计算本源，进一步解放人脑的**人工智能**成为信息产业探索重心
- 互联网业务基础逻辑从“感知”，跃进至“理解与决策”，逐步具备自主“认知”能力
  - 便携式的**虚拟现实终端**有望成为继移动智能终端后，重构互联网业务生态的下一代计算平台



## 发展趋势 (2/2)

- 数据流动一方面促进了价值释放，另一方面不规范流动行为严重威胁了**数据主权**和隐私安全
- 关键基础设施面临严峻的网络安全威胁
- 新兴技术产业逐渐成为网络安全攻防的重点领域
  - 物联网终端与系统
  - 云端数据
  - 企业自带移动设备 (BYOD)
  - 智能家居、智能汽车等



# Android / 安卓

中国传媒大学



# Android生态圈——设备



ANDROID WEAR

PHONES

TABLETS



ANDROID TV

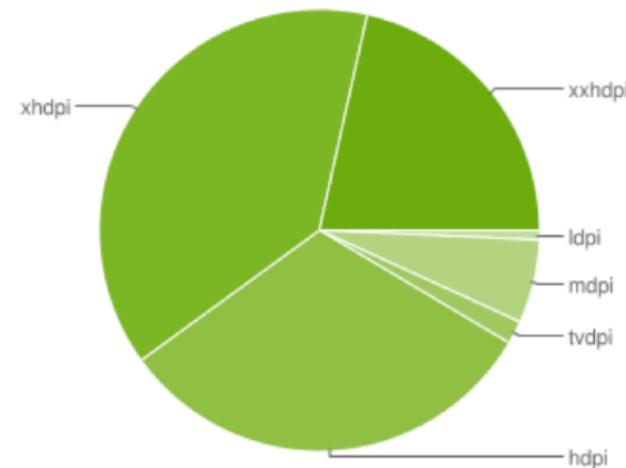
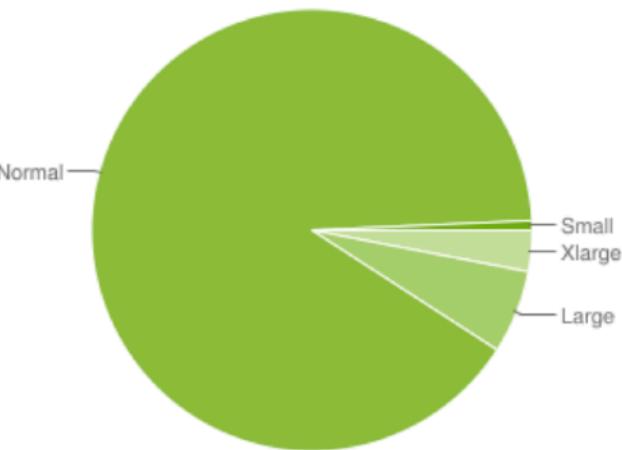


ANDROID AUTO



# Android生态圈——设备（全球） 2017.11

	ldpi	mdpi	tvdpi	hdpi	xhdpi	xxhdpi	Total
Small	0.6%						0.7%
Normal		1.4%	0.2%	30.5%	37.1%	21.0%	90.2%
Large	0.1%	2.7%	1.5%	0.5%	0.9%	0.4%	6.1%
Xlarge		2.0%		0.5%	0.5%		3.0%
<b>Total</b>	<b>0.7%</b>	<b>6.1%</b>	<b>1.7%</b>	<b>31.5%</b>	<b>38.5%</b>	<b>21.5%</b>	



以 7 天为周期收集的数据（截止于 2017 年 11 月 9 日）。

未显示任何分布份额不足 0.1% 的屏幕配置。



# Android 支持设备屏幕尺寸规范 (1/2)

## • 屏幕尺寸

### — 按屏幕对角测量的实际物理尺寸

- 为简便起见，Android 将所有实际屏幕尺寸分组为四种通用尺寸：小、正常、大和超大

## • 屏幕密度

### — 屏幕物理区域中的像素量；通常称为 dpi（每英寸 点数）。 例如，与“正常”或“高”密度屏幕相比，“低”密度屏幕在给定物理区域的像素较少。

- 为简便起见，Android 将所有屏幕密度分组为六种通用密度：低、中、高、超高、超超高和超超超高。



# Android支持设备屏幕尺寸规范 (2/2)

- 方向

—从用户视角看屏幕的方向，即横屏还是竖屏，分别表示屏幕的纵横比是宽还是高。请注意，不仅不同的设备默认以不同的方向操作，而且方向在运行时可随着用户旋转设备而改变

- 分辨率

—屏幕上物理像素的总数。添加对多种屏幕的支持时，应用不会直接使用分辨率；而只应关注通用尺寸和密度组指定的屏幕尺寸及密度。

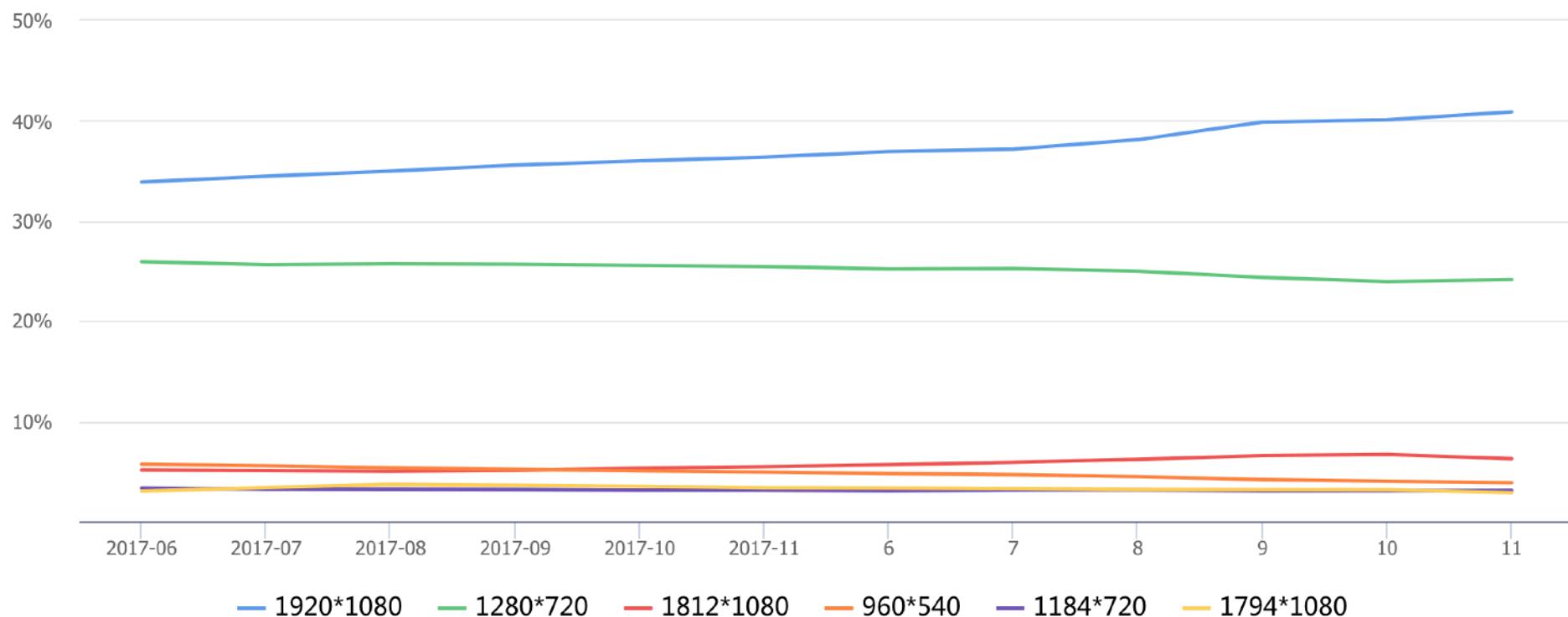
- 密度无关像素 (dp)

—在定义 UI 布局时应使用的虚拟像素单位，用于以密度无关方式表示布局维度或位置



# Android生态圈——设备（国内）

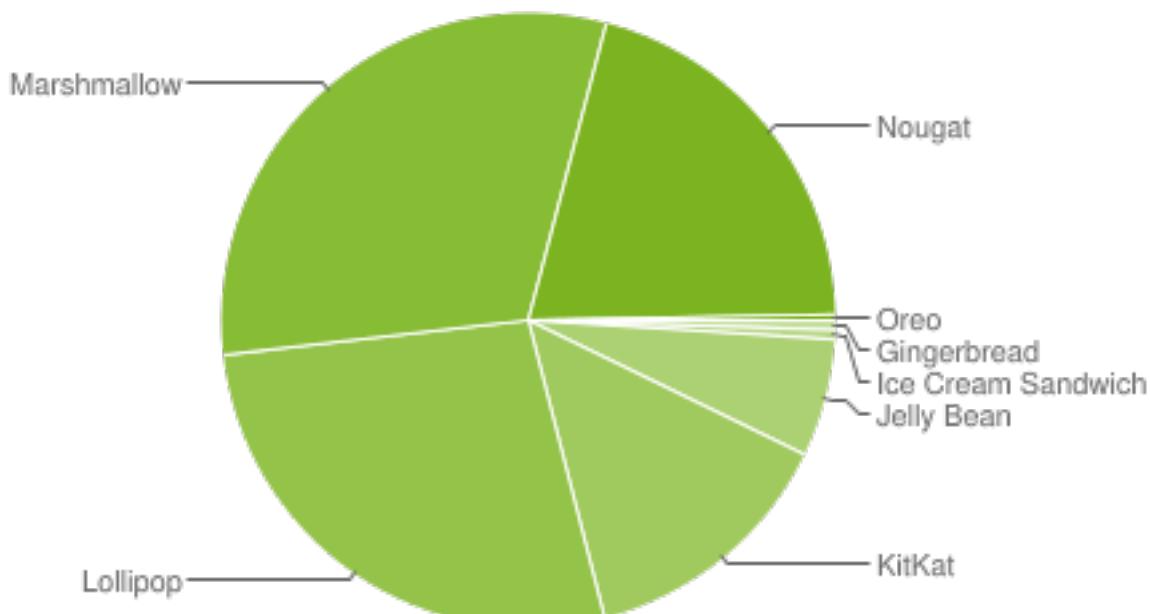
- Android设备分辨率趋势 展现统计设备的分辨率分布比例的趋势变化





# Android生态圈——系统（全球）2017.11

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.5%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.5%
4.1.x	Jelly Bean	16	2.2%
4.2.x		17	3.1%
4.3		18	0.9%
4.4	KitKat	19	13.8%
5.0	Lollipop	21	6.4%
5.1		22	20.8%
6.0	Marshmallow	23	30.9%
7.0	Nougat	24	17.6%
7.1		25	3.0%
8.0	Oreo	26	0.3%



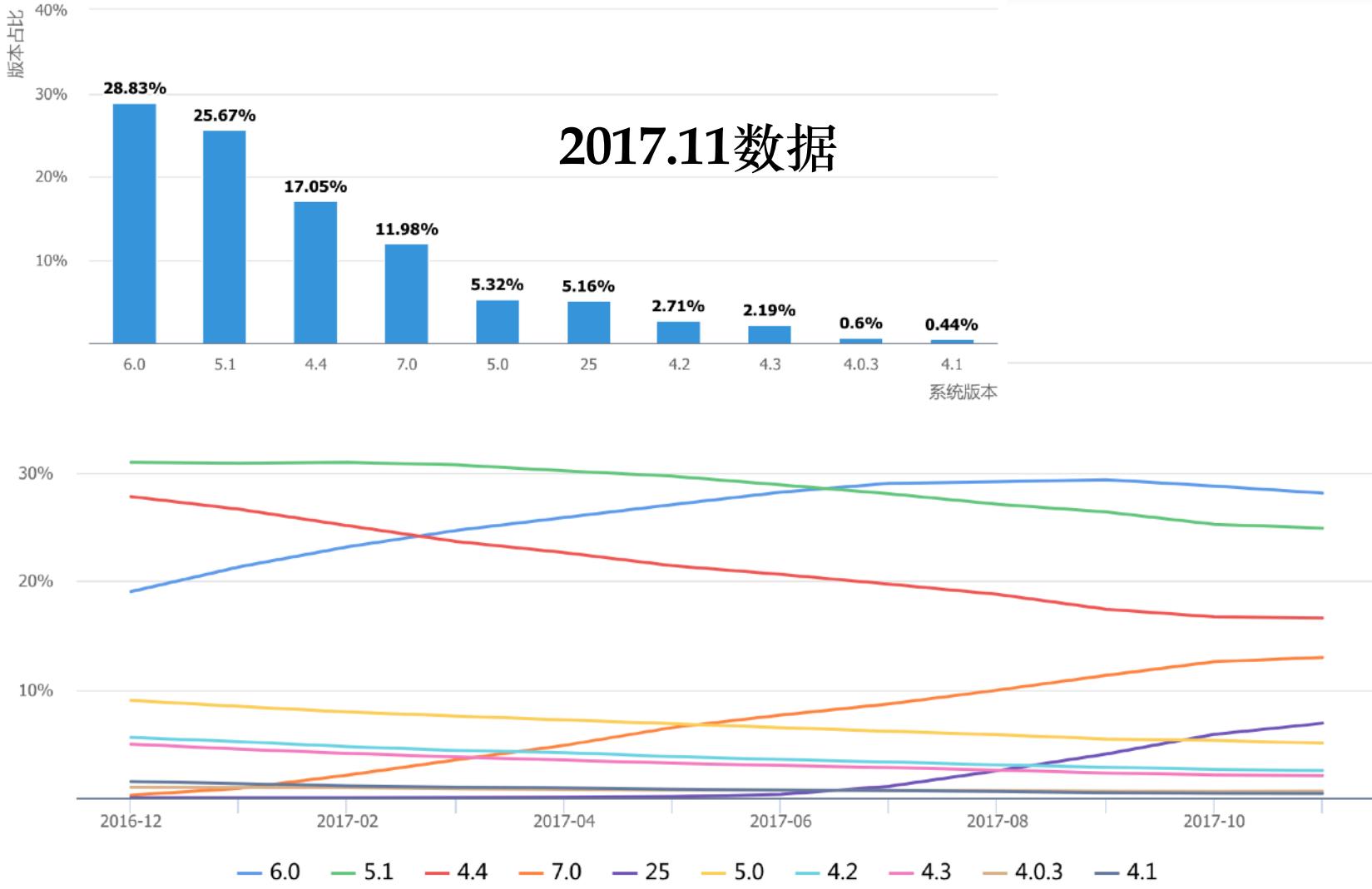
新版本系统更新部署到终端设备周期较长

以 7 天为周期收集的数据（截止于 2017 年 11 月 9 日）。

未显示任何分布份额不足 0.1% 的版本。



# Android生态圈——系统（国内）



中国传媒大学



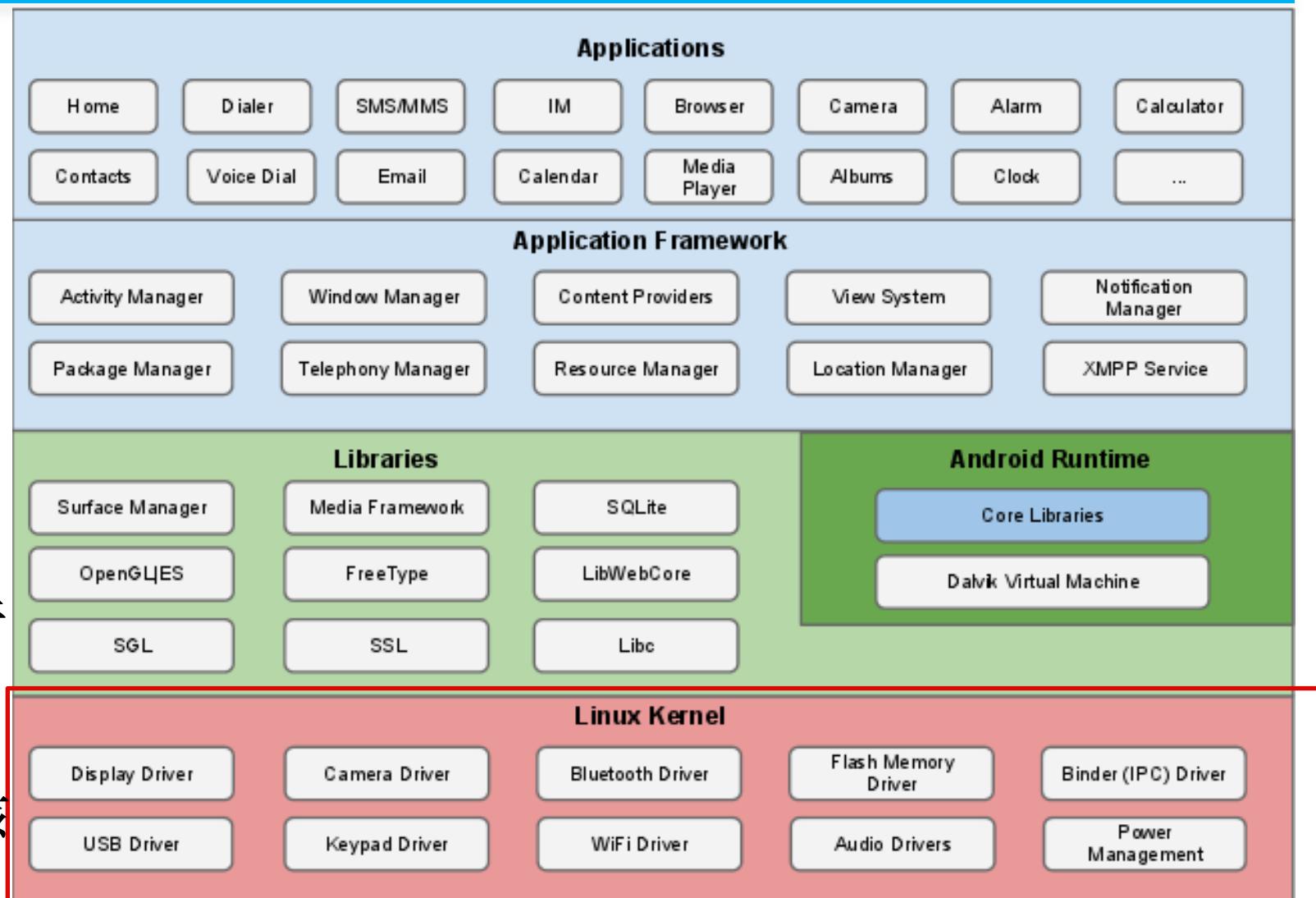
# Android版本号与API Level

版本号	版本代号	发布时间	API level	首发预搭载设备
1.0	N/A	September 23, 2008	1	N/A
1.1	N/A	February 9, 2009	2	N/A
1.5	Cupcake	April 27, 2009	3	N/A
1.6	Donut	September 15, 2009	4	N/A
2.0 – 2.1	Eclair	October 26, 2009	5-7	N/A
2.2 – 2.2.3	Froyo	May 20, 2010	8	Droid 2
2.3 – 2.3.7	Gingerbread	February 9, 2011	9-10	Nexus S
4.0 – 4.0.4	Ice Cream Sandwich	December 16, 2011	14-15	Galaxy Nexus
4.1 – 4.1.2	Jelly Bean	July 9, 2012	16	Nexus 7
4.2 – 4.2.2		November 13, 2012	17	Nexus 4, Nexus 10
4.3 – 4.3.1		July 24, 2013	18	Nexus 7 2013
4.4 – 4.4.4	KitKat	October 31, 2013	19	Nexus 5
5.0 – 5.0.2	Lollipop (棒棒糖)	November 3, 2014	21	Nexus 6
5.1 – 5.1.1		March 9, 2015	22	Android One
6.0 – 6.0.1	Marshmallow (棉花糖)	October 5, 2015	23	Nexus 5X, Nexus 6P
7.0-7.1	Nougat (牛轧糖)	August 22, 2016	24-25	LG V20



# Android生态圈——系统组成

第三方  
开源组件  
  
Linux内核

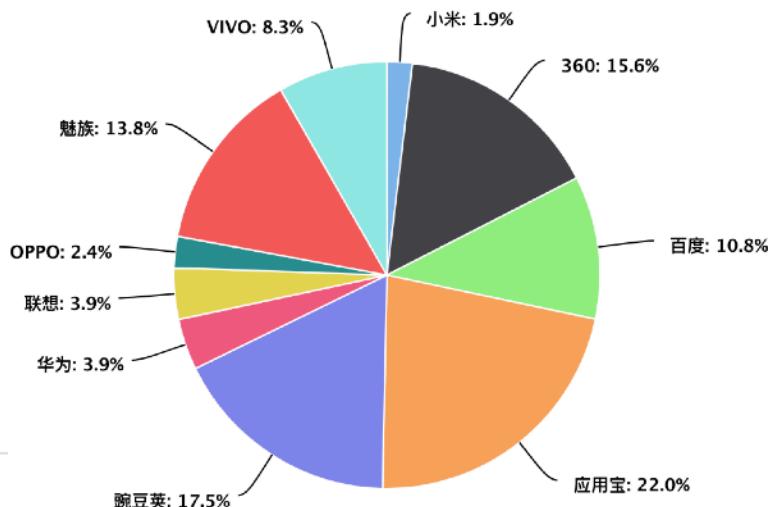


中国传媒大学



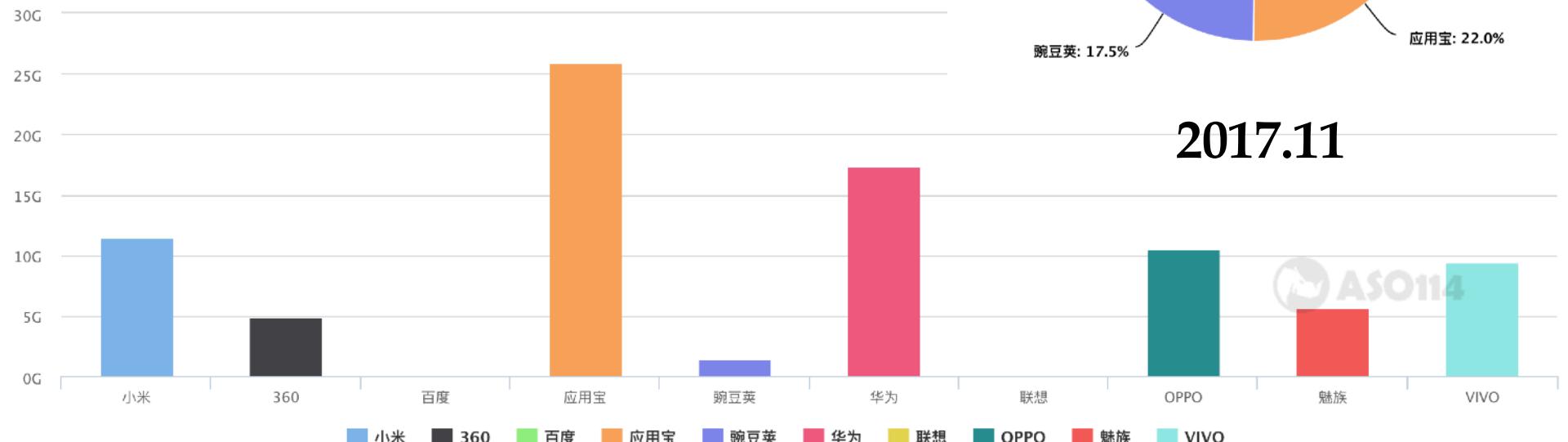
# Android生态圈——（应用分发）渠道

主流Android市场分发量统计



2017.11

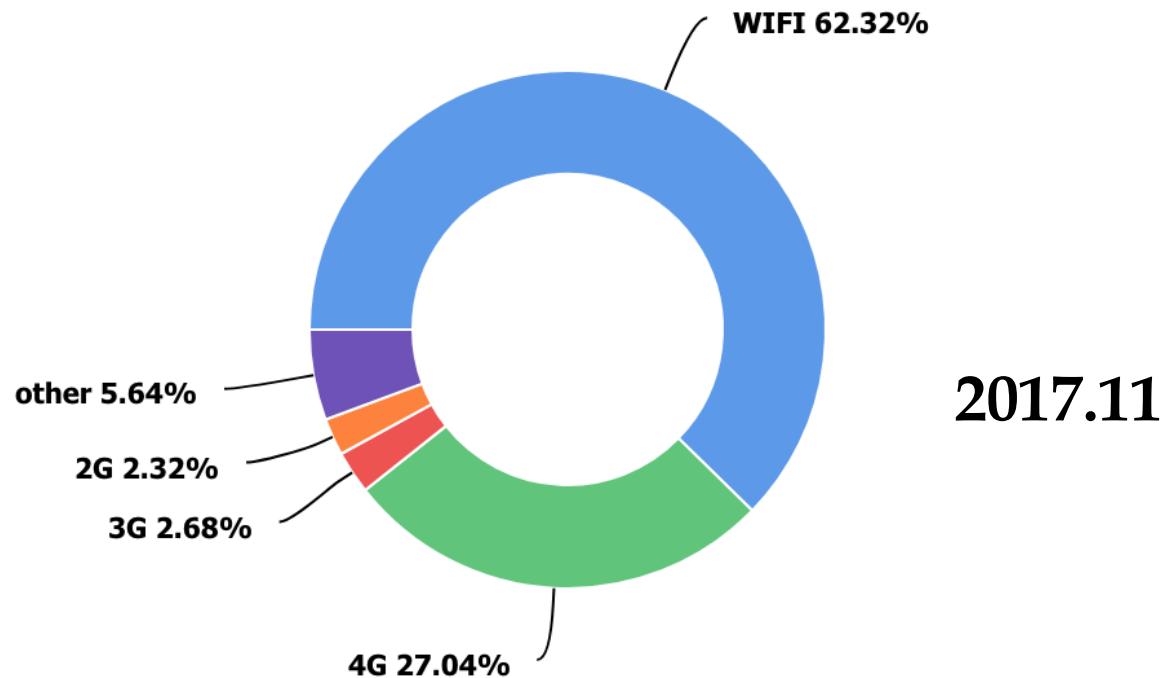
十大主流市场应用分发量趋势



中国传媒大学



# Android生态圈——联网方式（国内）



版本	占比
WiFi	62.32%
4G	27.04%
3G	2.68%
2G	2.32%
other	5.64%



# Android生态圈——厂商

- 设备
  - Google官方授权允许制造所有类型设备
- 系统
  - 基于开源授权协议标准自行修改和使用
- 分发渠道
  - Google官方未授权允许，也未禁止



# Android生态圈——总结

- Google主导的全面开放生态圈
- 以Android操作系统为核心的全面多行业发展
- 多样化的设备、系统与应用
- 开发者要面临碎片化应用运行平台
- 国内消费者只能使用定制化的安卓系统
  - 无法及时升级系统，安装系统级别的安全更新
  - 大多数设备厂商只知道每年推出多款新设备，却普遍忽视对已有设备上系统的持续更新维护



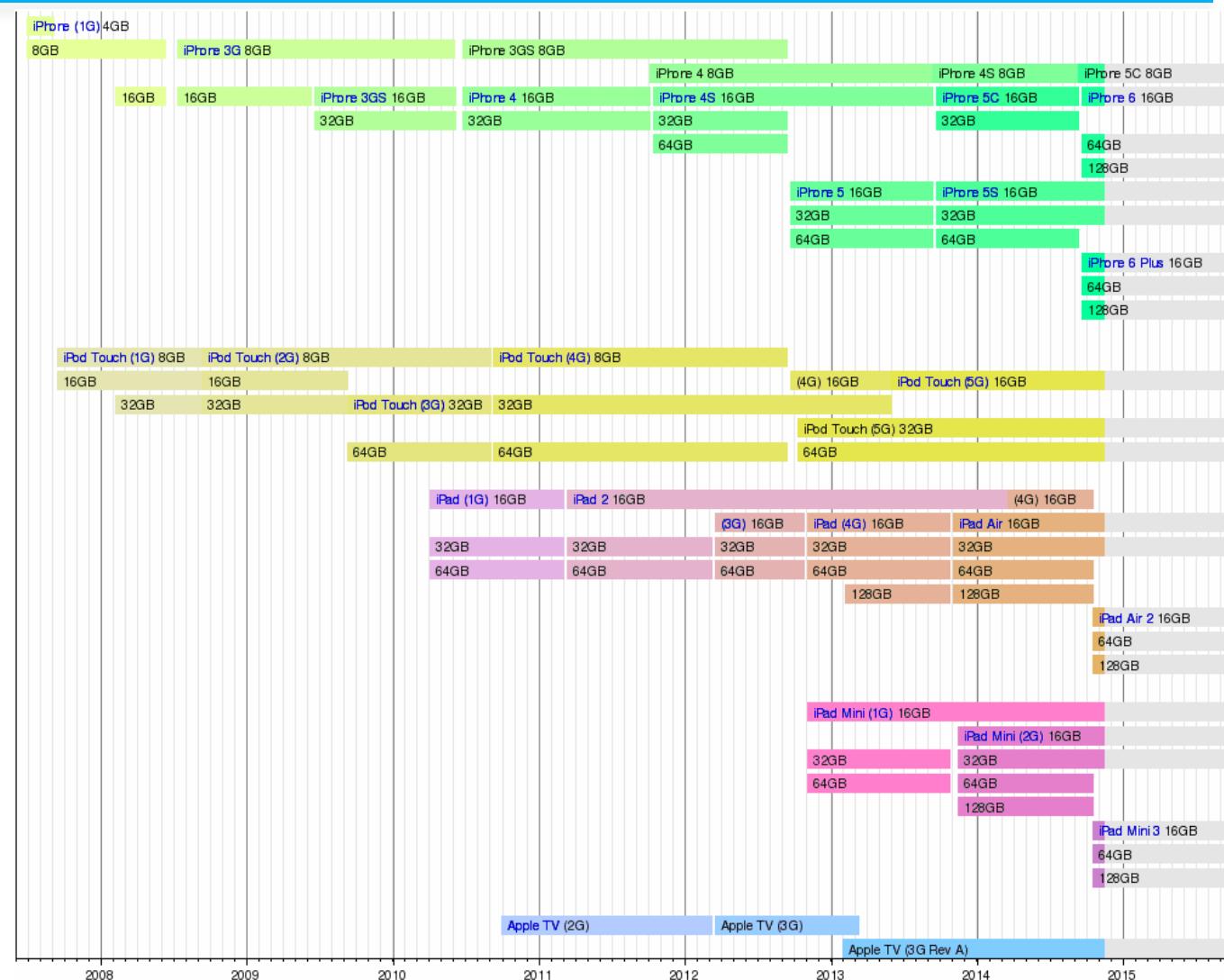
iOS

中國傳媒大學



# iOS生态圈——设备

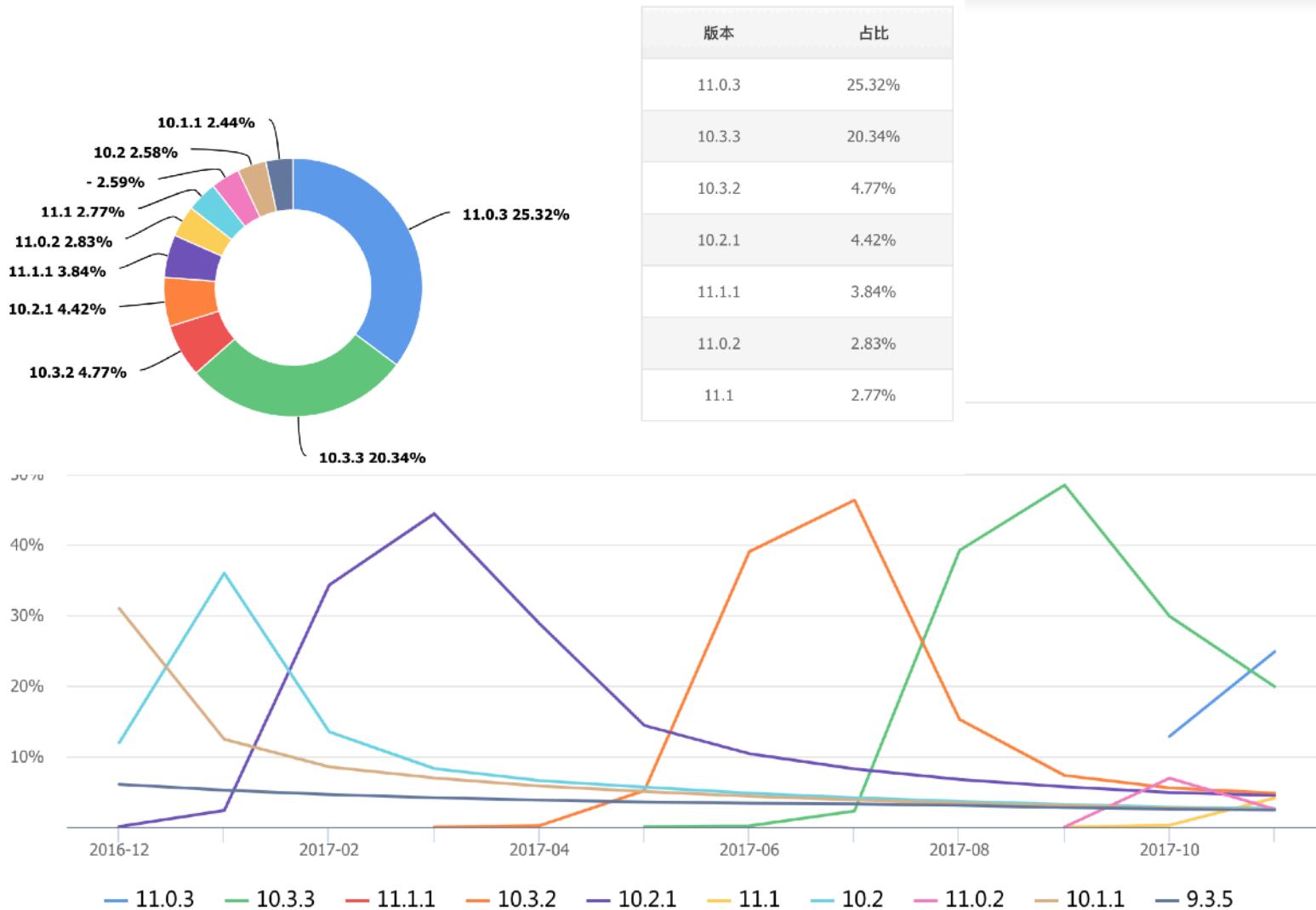
- iPhone
- iPod Touch
- iPad / iPad Pro
- Apple TV
- Apple Watch



中国传媒大学



# iOS生态圈——系统（国内）



中國傳媒大學



# iOS生态圈——系统（全球）

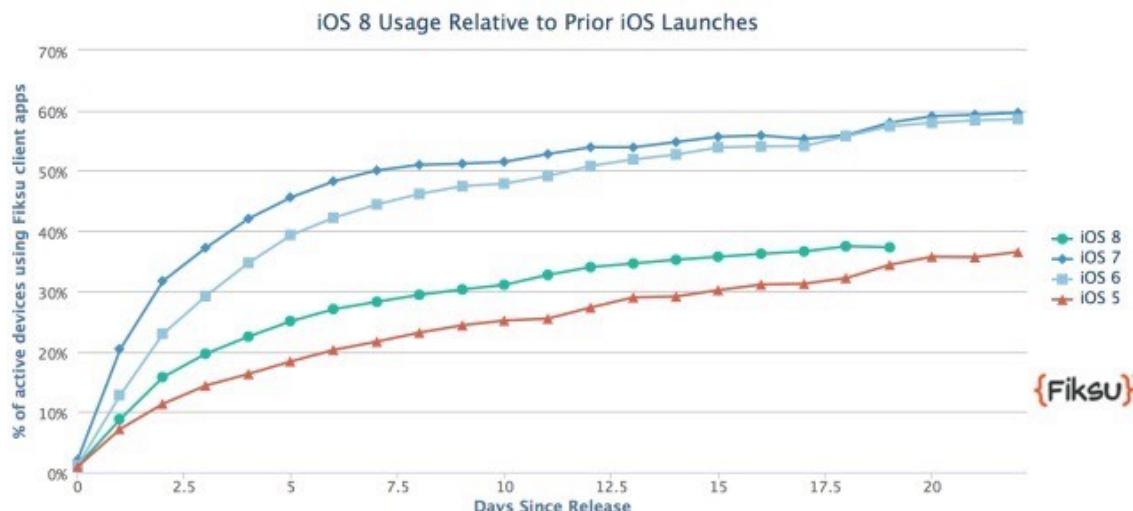
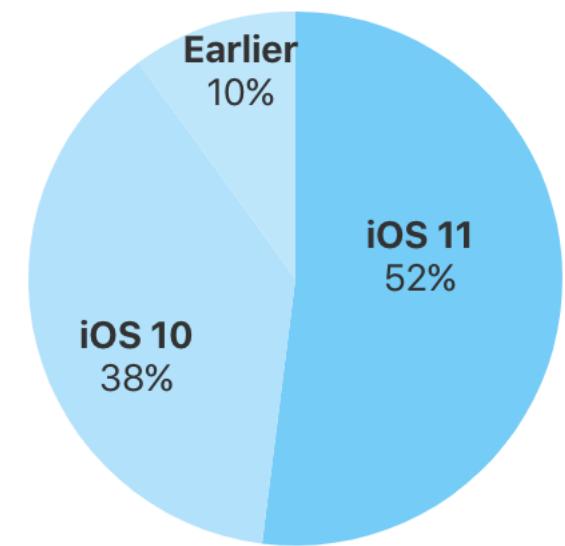
- **HomeKit**

—智能家居通信与开发框架

- **CarPlay**

—车载iOS系统

52% of devices are using iOS 11.



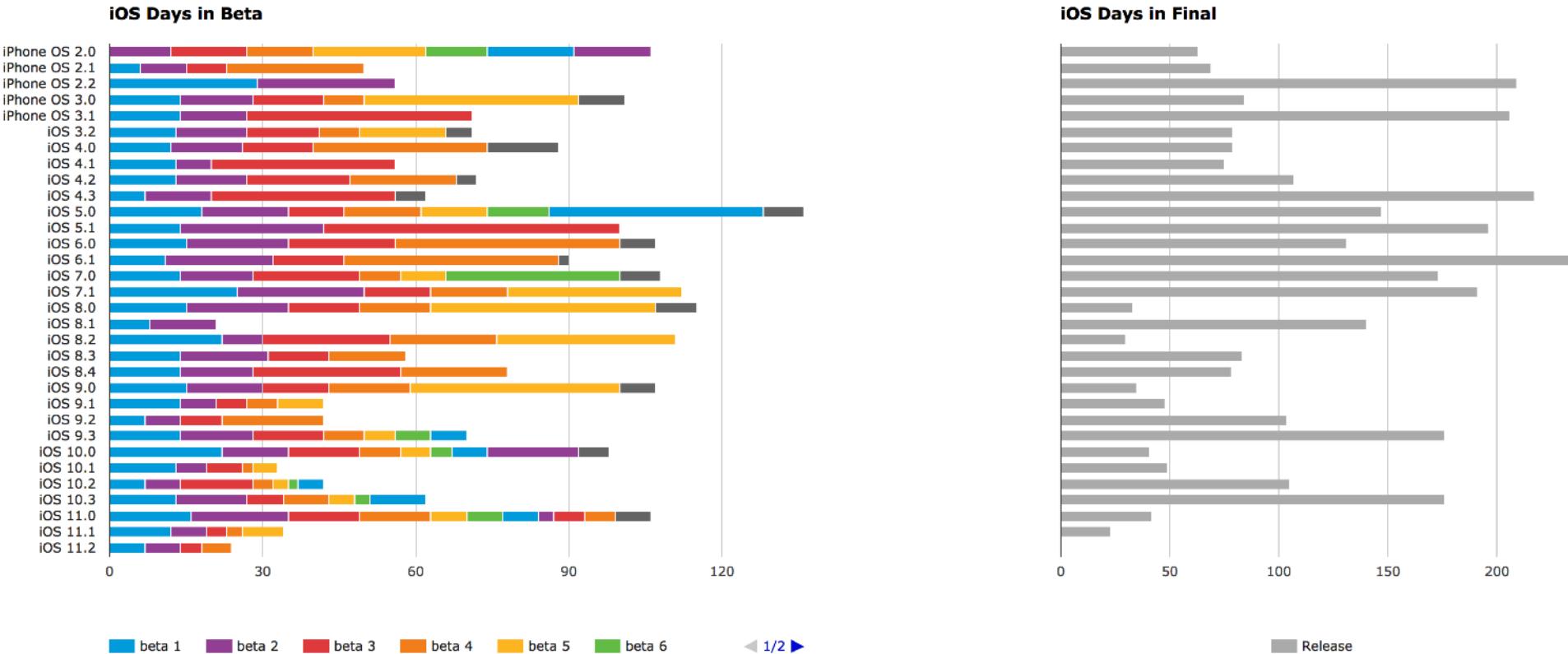
As measured by the App Store on November 6, 2017.

新版本系统被快速更新部署到终端设备

ref: <https://developer.apple.com/support/appstore/>



# iOS生态圈——系统（生命周期）



ref: <http://www.thinkybits.com/blog/iOS-versions/>

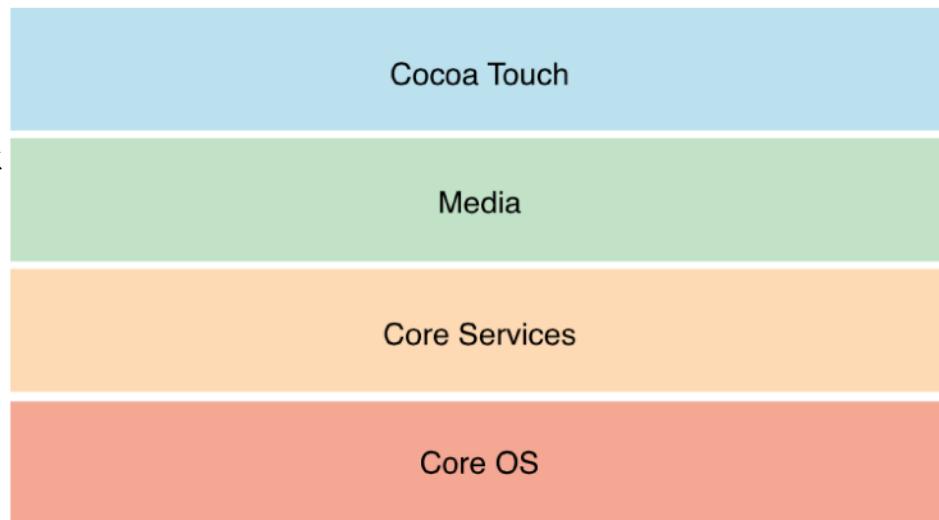


# iOS生态圈——系统组成与开源

- Core OS

- 基于FreeBSD和Mach所改写的 Darwin，是开源、符合POSIX标准的一个Unix核心
- 提供了整个iOS的一些基础功能
  - 例如：硬件驱动，内存管理，程序管理，线程管理（POSIX），文件系统，网络（BSD Socket），以及标准输入输出等等
  - 所有这些功能都会通过C语言的API来提供。

- Core OS层的驱动也提供了硬件和系统框架之间的接口。然而，由于安全的考虑，只有有限的系统框架类能访问内核和驱动





# iOS生态圈——厂商

- 设备
  - Apple官方授权允许汽车、智能家居领域厂商
- 系统
  - Apple官方唯一维护
- 分发渠道
  - Apple官方未授权允许任何第三方应用商店，仅允许企业级应用的自行分发和授权模式



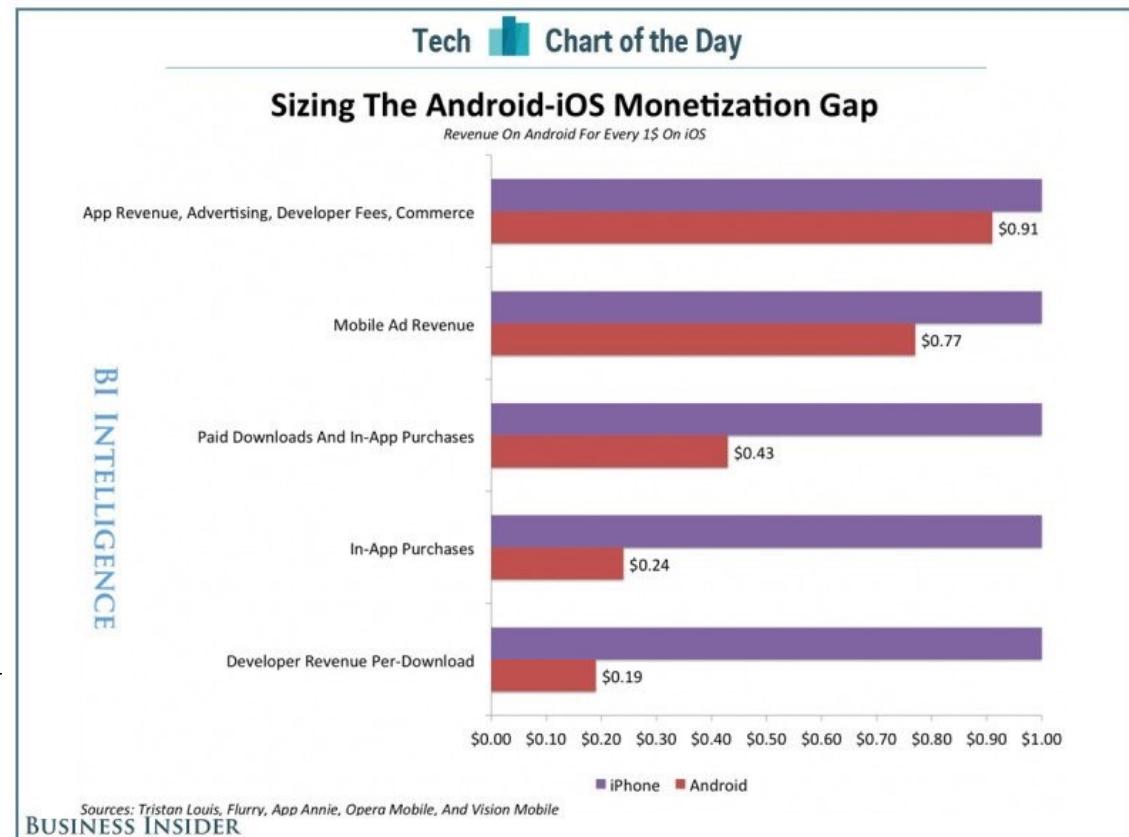
## iOS生态圈——（应用分发）渠道

- 下载市场（非法）：麦芽地（已被关闭）
- 应用商店：App Store
- 客户端（非法）：PP手机助手、同步推、91手机助手等



# iOS生态圈——总结

- Apple强势主导的有限开放生态圈
- 商业变现能力目前强于Android生态圈
- 应用多样性发展逐渐落后于Android生态圈
  - 电视、盒子、投影设备、智能家居等





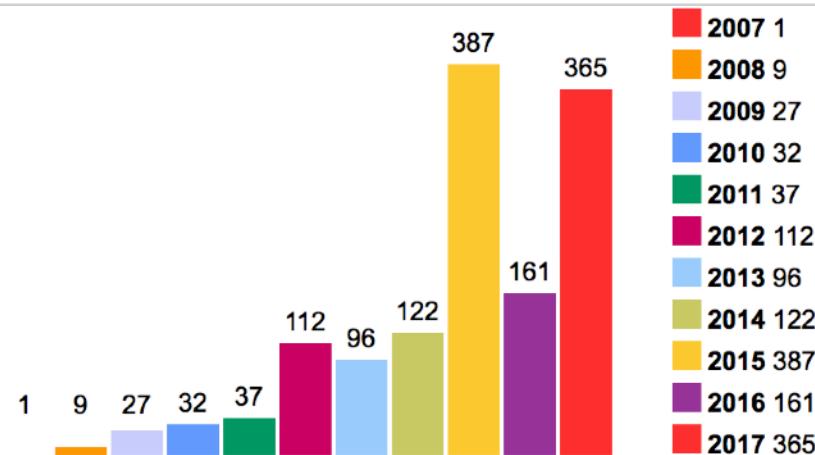
## 内容提要

- 智能终端概述
- iOS系统安全概述
- Android系统安全概述
- Android应用安全实验环境搭建

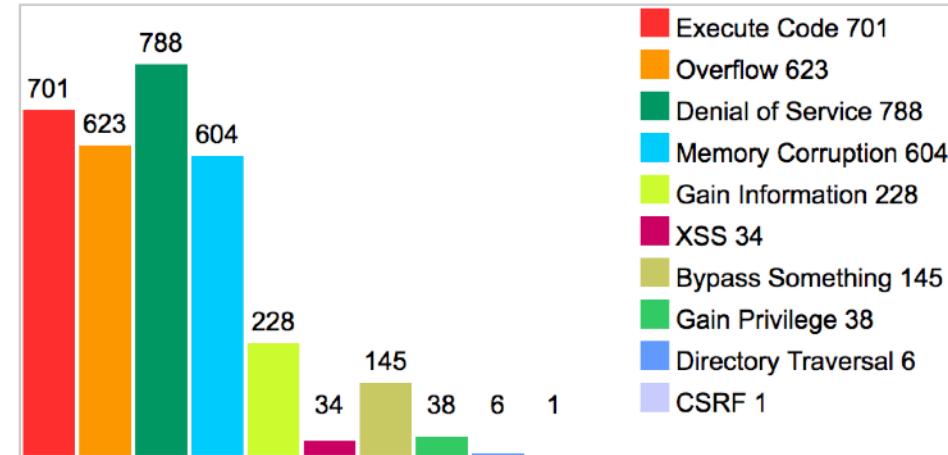


# iOS 系统相关漏洞统计数据

Vulnerabilities By Year



Vulnerabilities By Type

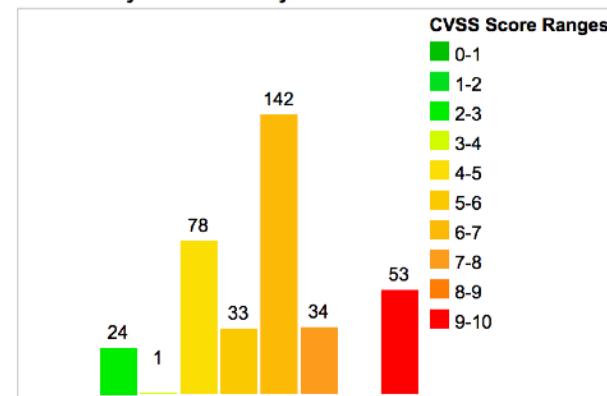


Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1		0.00
1-2		0.00
2-3	24	6.60
3-4	1	0.30
4-5	78	21.40
5-6	33	9.00
6-7	142	38.90
7-8	34	9.30
8-9		0.00
9-10	53	14.50
Total	365	

Weighted Average CVSS Score: 6.7

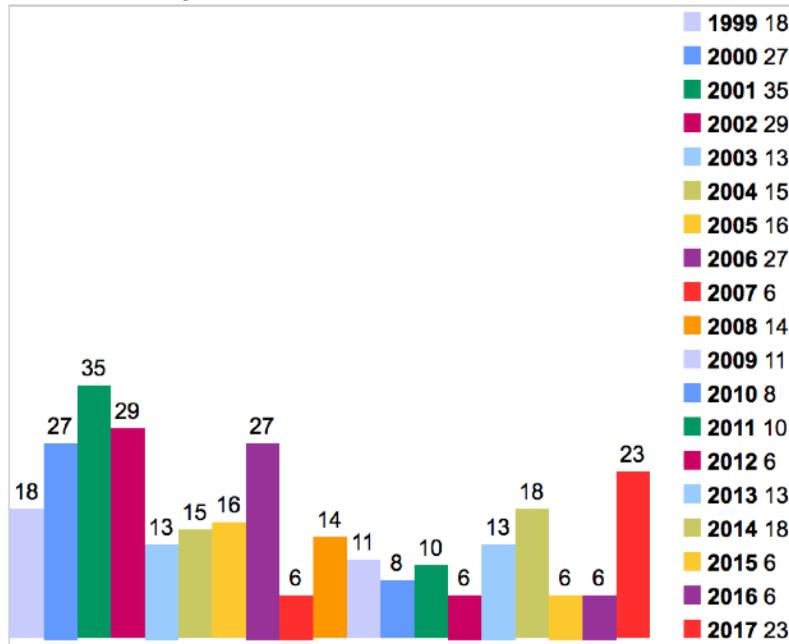
Vulnerability Distribution By CVSS Scores



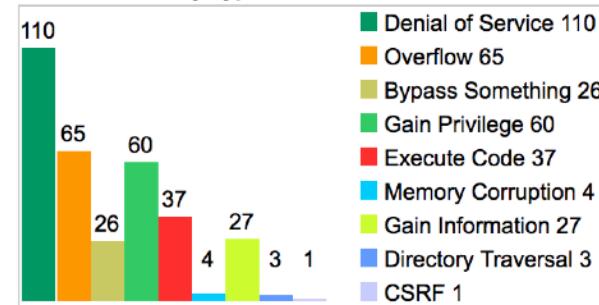


# FreeBSD系统相关漏洞统计数据

Vulnerabilities By Year



Vulnerabilities By Type

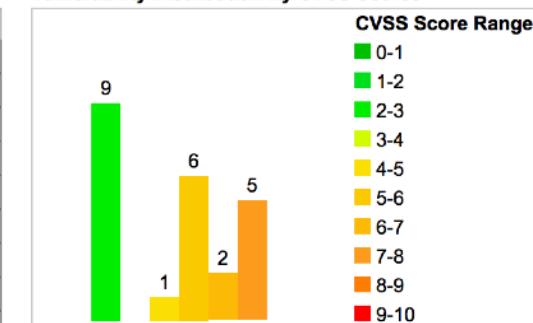


Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1		0.00
1-2		0.00
2-3	9	39.10
3-4		0.00
4-5	1	4.30
5-6	6	26.10
6-7	2	8.70
7-8	5	21.70
8-9		0.00
9-10		0.00
Total	23	

Weighted Average CVSS Score: 5.3

Vulnerability Distribution By CVSS Scores





# iOS系统安全特性发展变迁简史

- 禁止第三方程序访问所有通话历史 (iOS 4+)
- 禁止第三方程序拦截呼入和呼出的通话 (iOS 4+)
- 禁止第三方程序访问短信收件箱和后台静默发送短信 (iOS 5+)
- 第三方程序访问通讯录、日历、照片需要用户明确授权 (iOS 6+)



# iOS系统安全特性发展变迁简史

- GPS定位功能需要用户明确授权 (iOS 4+)
- 限制后台联网程序种类 (音乐、VoIP, iOS 4+), iOS 7开始放宽后台静默和联网程序的限制
- 限制后台静默运行程序 (音乐、GPS、VoIP、消息推送守护程序以及周边配件附属的程序, iOS 4+)
- 禁止系统全局的第三方输入法 (<iOS8)



# iOS系统安全特性发展变迁简史

- iPhone 5s (iOS 7) 引入 Touch ID
  - 指纹解锁
  - iOS 8+ 允许第三方程序使用 Touch ID 来进行身份认证
- 设备激活强制使用 Apple ID 并联网认证身份 (iOS 7+)
  - 防止设备被盗、恶意清空数据和设置等
- USB 首次连接时双向身份认证 (iOS 7+)
  - 杜绝通过 USB 植入恶意代码
- 电话号码黑名单 (iOS 7+)





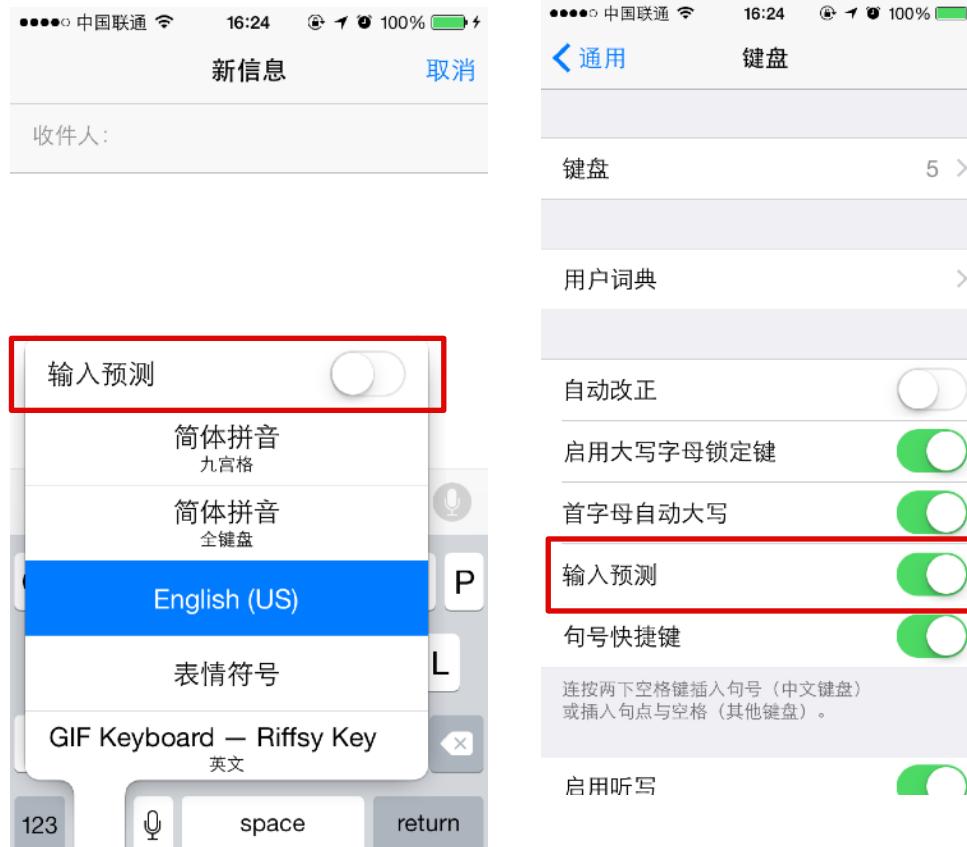
# iOS系统安全特性发展变迁简史

- App Store审核标准中新增对App读取设备MAC地址的禁令（2013.5开始）
- iOS 8 设备在扫描WiFi 时，系统会使用随机的MAC 地址来防止设备被跟踪，只有在连接成功后才会使用真正的那个



# iOS 8值得注意的一些默认隐私设置问题

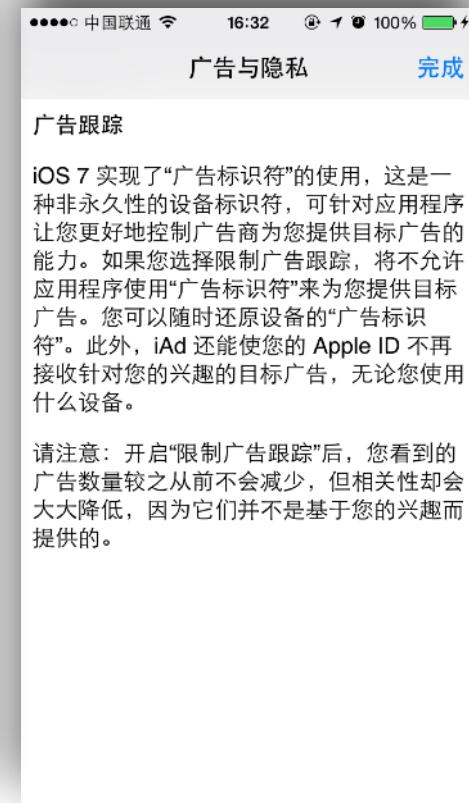
- 默认键盘设置会存储你输入的密码并在他人使用你的设备时（输入预测）泄露





# iOS 8值得注意的一些默认隐私设置问题

## • 广告与诊断数据自动发送

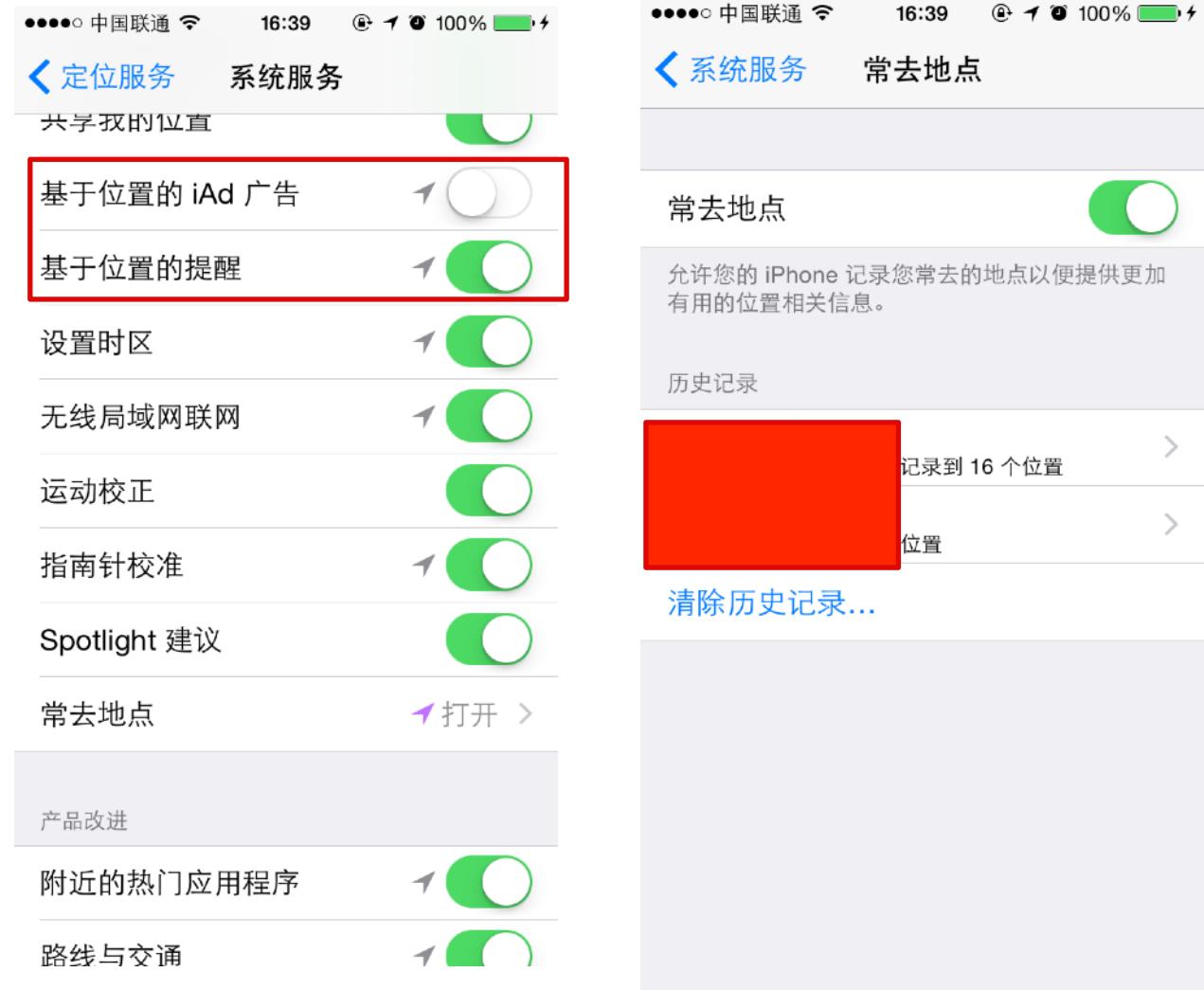




# iOS 8值得注意的一些默认隐私设置问题

基于位置的广告和应用内推荐

设置 -> 隐私 ->  
定位服务 ->  
系统服务 ->  
常去地点





# iOS 8值得注意的一些默认隐私设置问题

## • 看好你的Siri

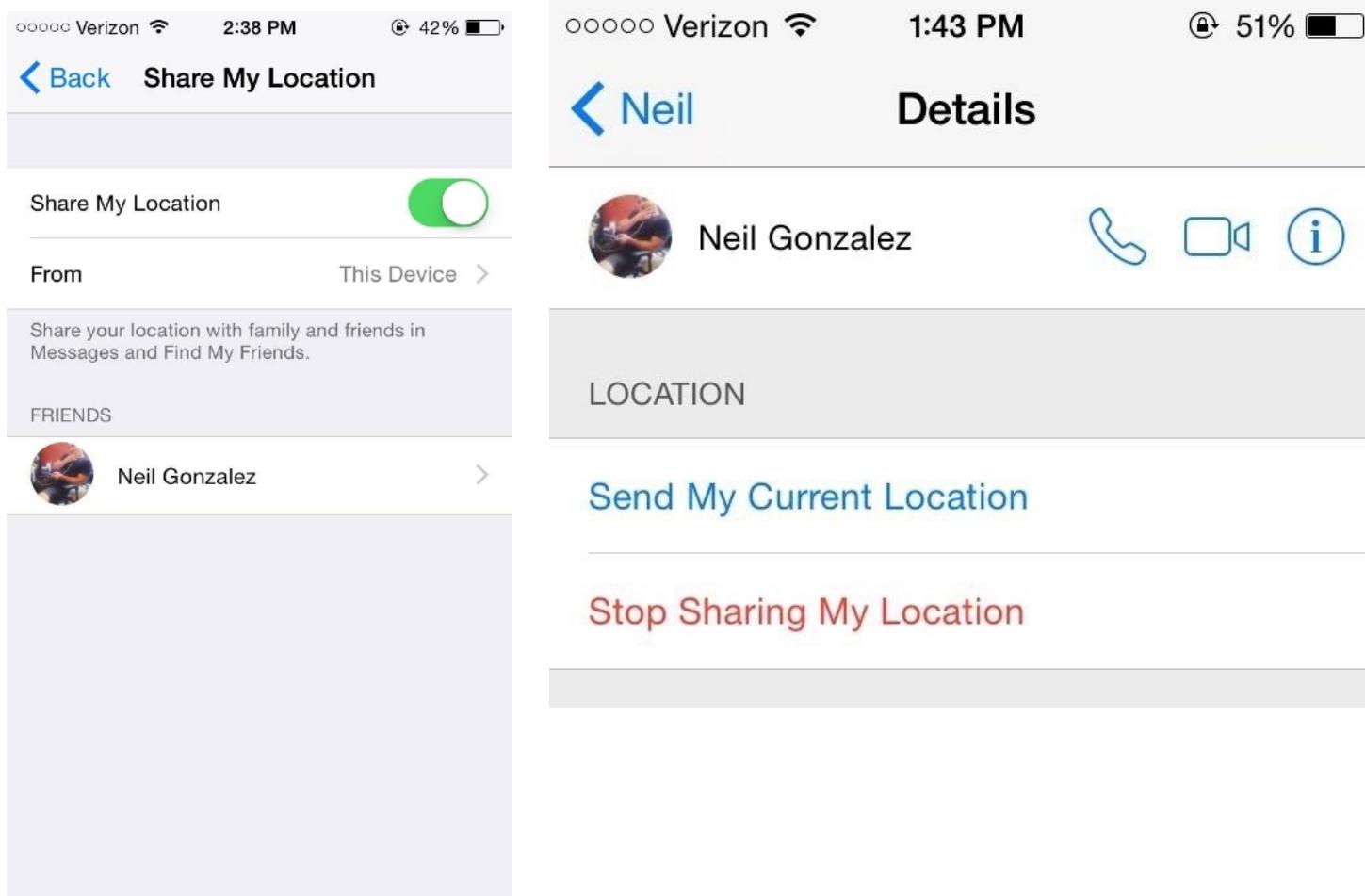


演示: 利用  
siri漏洞非授  
权访问你的  
通讯录和相  
册, 甚至  
是绕过你的解  
锁设置!



# iOS 8值得注意的一些默认隐私设置问题

- 发送我当前的位置 VS. 共享我的位置

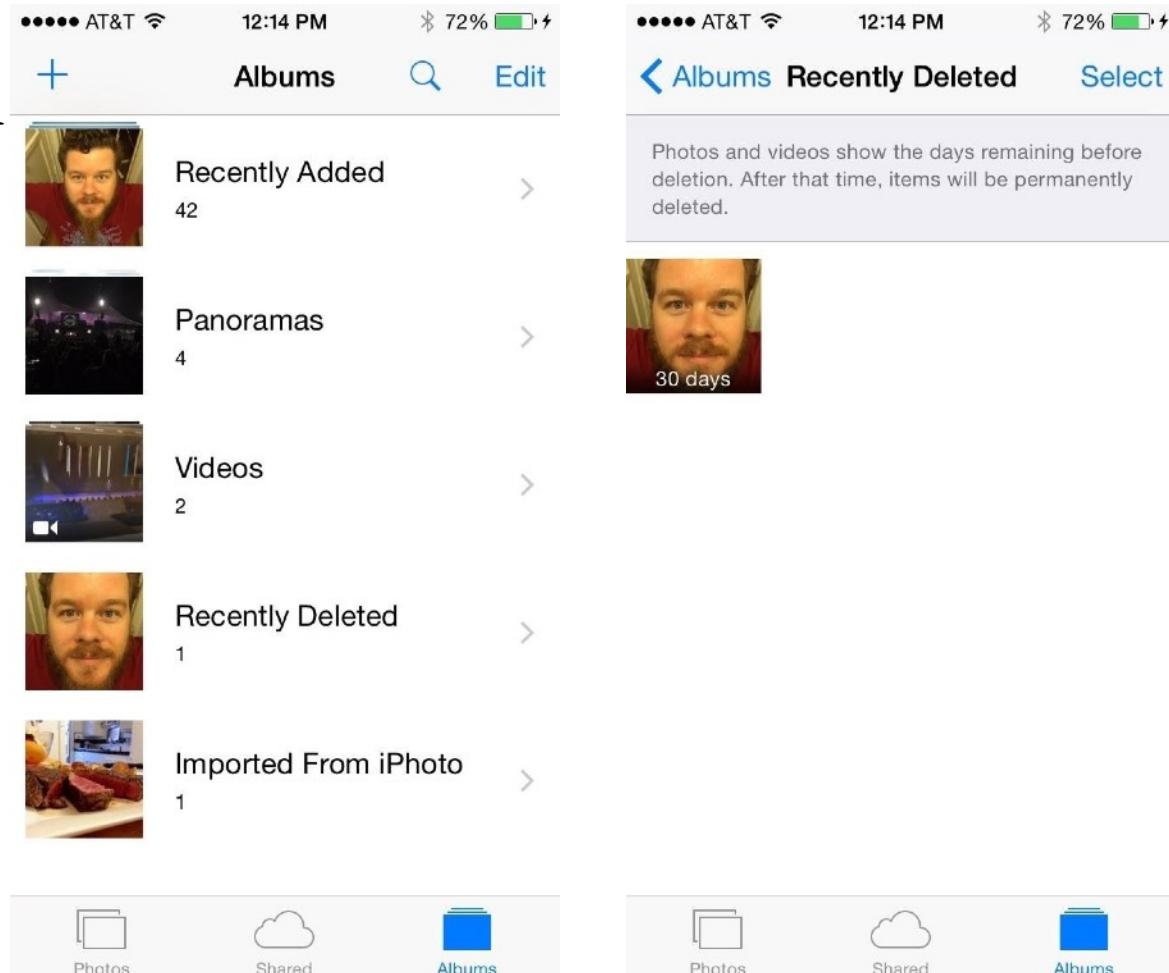




# iOS 8值得注意的一些默认隐私设置问题

## • 相片默认没有彻底删除

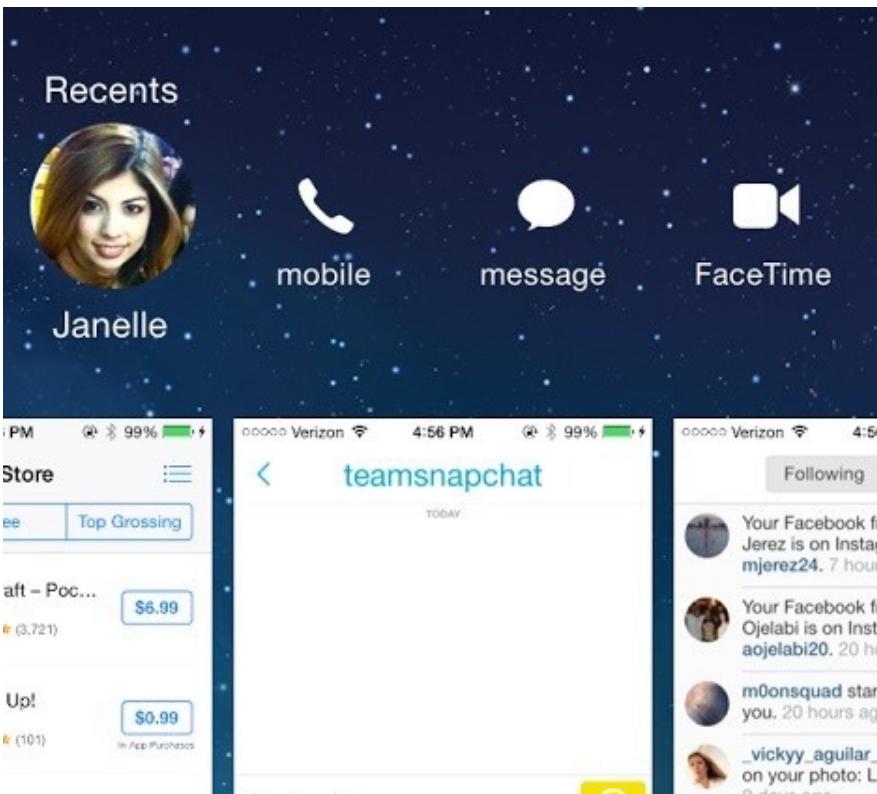
— 默认保存30天





# iOS 8值得注意的一些默认隐私设置问题

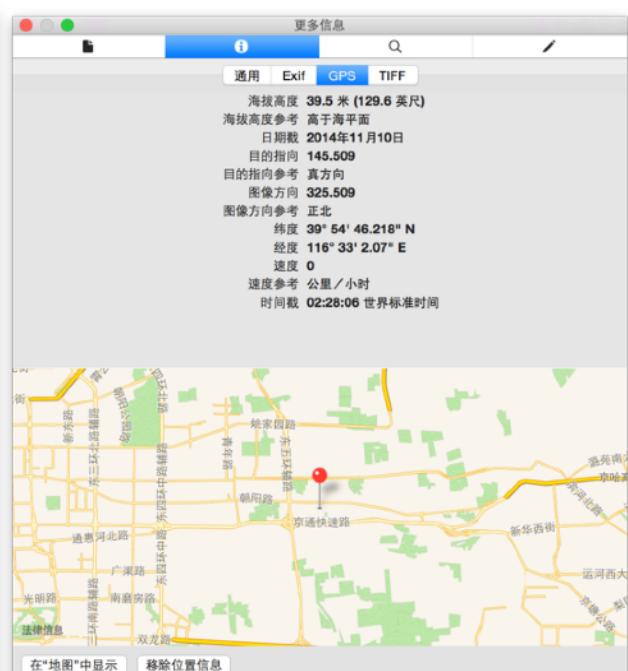
## • 删不掉的近期联系人





# iOS 8值得注意的一些默认隐私设置问题

## • 相机拍摄的照片包含GPS信息（不仅是iOS 8）





# iOS 日历中的垃圾邀请信息

- 广告商通过给你的 iCloud 账号发送日历邀请

—这种日历弹窗小广告，不显示来源，仅仅显示广告内容、发送人和一个时段。我们往往会下意识地点击「拒绝」，但没想到这个小动作就把自己的个人名字泄露了给对方。





# iOS日历中的垃圾邀请信息

- 保留iCloud日历同步功能的同时，防止垃圾邀请充斥日历

—1. 登陆iCloud

—2. 左下角齿轮-偏好设置-高级

— 邀请，选择发送电子邮件给XXX邮箱，保存

—3. 点击编辑，点击+ 完成

—4. 选择想删除的事件，在弹出框标题旁的颜色点上单击，选择新建的分类，保存

—5. 点击编辑，点击新建分类旁边的一，删除分类，确定

— 这样垃圾事件就被删除了，以后的事件邀请会发送到邮箱。然后垃圾邮件屏蔽即可





# iOS中的其他类型垃圾信息

- iCloud相册分享用于推广

- 只能禁用“iCloud照片分享”功能

- iMessage推广

- iMessage 是苹果设备自带的免费信息发送应用

- iMessage 通过Apple ID 来发现用户和发送信息





# iOS 11的新安全改进

- 位置信息访问控制更精细
  - iOS 10上的App开发者可以选择向用户隐藏“使用应用时访问位置信息”选项，iOS 11开始这个选项无法再被隐藏
- 照片库访问控制允许开发者申请只读访问授权
- 手机即使处于解锁状态通过数据线缆连接到一台陌生电脑时依然需要输入设备解锁口令才能信任这台电脑（原先只需要在解锁的手机上点击“允许”按钮）
- 强制已有的iCloud账户启用双因素认证来代替原先的“两步认证”



# iOS 11的一项争议功能设计

- 通过控制中心“关闭”Wi-Fi开关并不是真的关闭Wi-Fi功能，只是让当前设备从当前连接的任何网络断开
- 当 Wi-Fi 停用时，自动加入附近任何 Wi-Fi 网络的功能也会被停用，直到：
  - 您步行或驾车到新位置
  - 当地时间凌晨 5 点





# 脆弱的iOS锁屏绕过

CVE IDs list by Apple » Iphone Os : Security Vulnerabilities (Bypass)

- [iOS 9.2 CVE-2015-7080](#)
- [iOS 9 CVE-2015-5892](#)
- [iOS 9 CVE-2015-5861](#)
- [iOS 8.1.1 CVE-2014-4463](#)
- [iOS 8.1.1 CVE-2014-4451](#)
- [iOS 7.1.2 CVE-2014-1360](#)
- [iOS 7.1.2 CVE-2014-1353](#)
- [iOS 7.1.2 CVE-2014-1351](#)
- [iOS 6 CVE-2012-3736](#)
- [iOS 6 CVE-2012-3738](#)
- [iOS 6 CVE-2012-3739](#)
- [iOS 6 CVE-2012-3740](#)
- [iOS 5.1 CVE-2012-0644](#)
- [iOS 6.0.1 CVE-2012-3750](#)
- [iOS 6.1.3 CVE-2013-0980](#)
- [iOS 7.0.3 CVE-2013-5144](#)
- [iOS 7 CVE-2013-5147](#)
- [iOS 7.0.2 CVE-2013-5160](#)
- [iOS 7.0.2 CVE-2013-5161](#)
- [iOS 7.0.3 CVE-2013-5162](#)



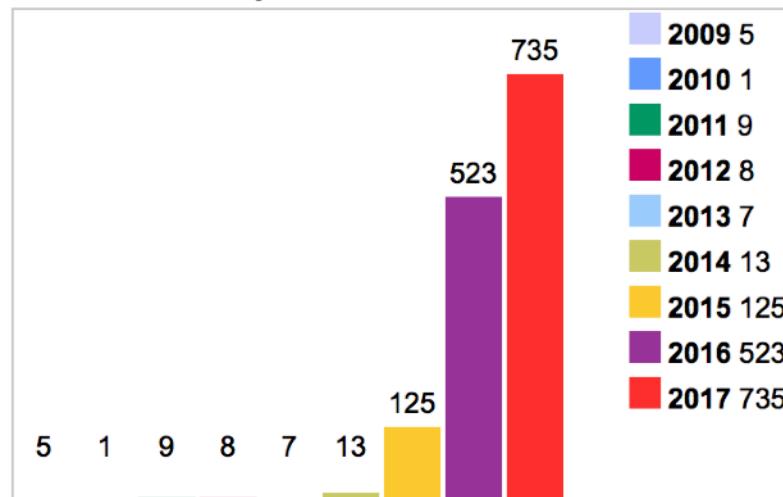
## 内容提要

- 智能终端概述
- iOS系统安全概述
- Android系统安全概述
- Android应用安全实验环境搭建

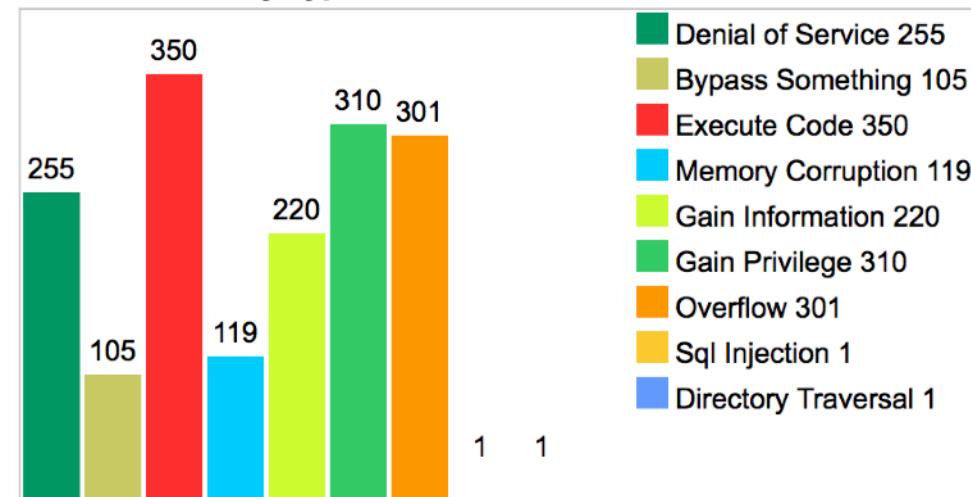


# Android系统相关漏洞统计数据

Vulnerabilities By Year



Vulnerabilities By Type

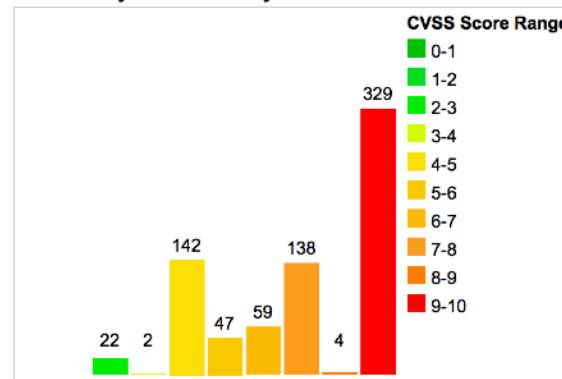


Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1		0.00
1-2		0.00
2-3	22	3.00
3-4	2	0.30
4-5	142	19.10
5-6	47	6.30
6-7	59	7.90
7-8	138	18.60
8-9	4	0.50
9-10	329	44.30
<b>Total</b>	<b>743</b>	

Weighted Average CVSS Score: 8

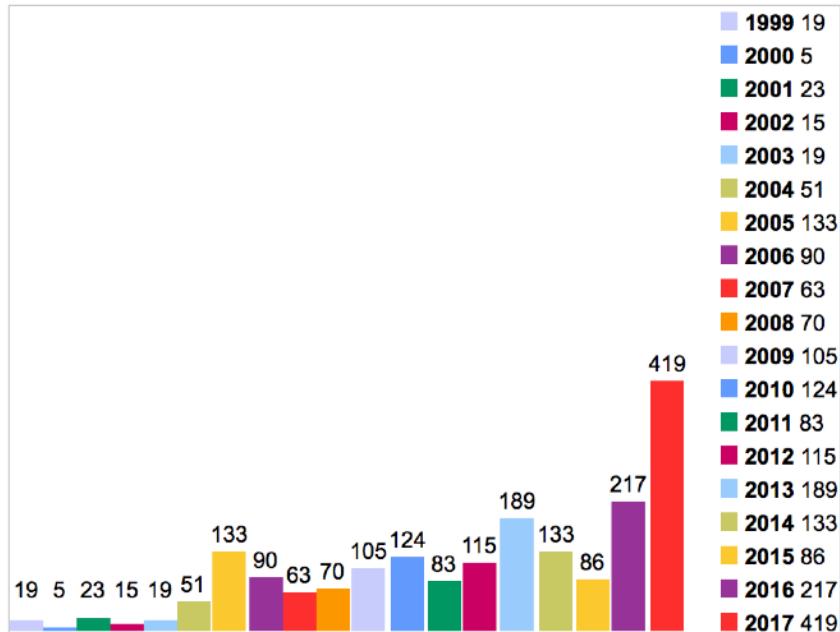
Vulnerability Distribution By CVSS Scores



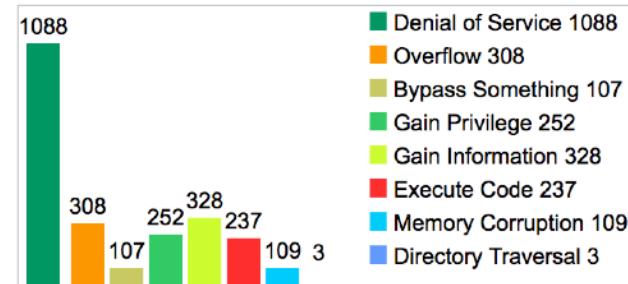


# Linux内核相关漏洞统计数据

Vulnerabilities By Year



Vulnerabilities By Type

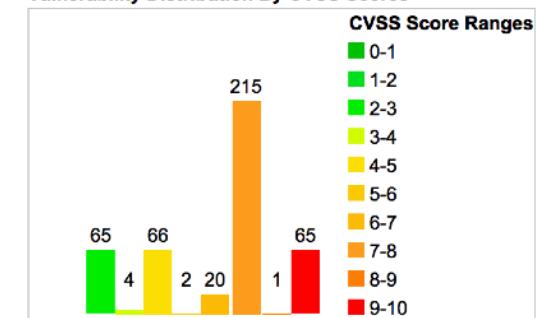


Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1		0.00
1-2		0.00
2-3		65
3-4		4
4-5		66
5-6		2
6-7		20
7-8		215
8-9		1
9-10		65
Total		438

Weighted Average CVSS Score: 7

Vulnerability Distribution By CVSS Scores





# Android系统安全特性发展变迁简史

- Cupcake 1.5
  - 基于ProPolice防止缓冲区溢出攻击，增强内存管理的安全性
- Froyo (冻酸奶) 2.2
  - 引入安卓设备管理API，支持企业级安全策略实现
- Gingerbread (姜饼) 2.3
  - 引入mmap\_min\_addr机制防御权限提升类攻击



# Android系统安全特性发展变迁简史

- Honeycomb 3.0
  - 文件系统加密
  - 用户口令存储使用更安全的加盐散列算法，对抗暴力破解和还原口令类攻击
- Ice Cream Sandwich 4.0
  - 实现地址空间随机化（ASLR），对抗内存破坏类攻击
  - 引入KeyChain机制，改进用户密钥存储和证书管理



# Android系统安全特性发展变迁简史

- Jelly Bean 4.2
  - APP使用短信发送权限需要得到用户的显式授权同意
  - 支持应用验证API，安全类APP可以基于此API对APK的下载、安装进行检查和拦截
  - 4.2.2版本引入了“安全USB调试”机制（真机ADB连接强制单向身份认证：手机认证PC机身份）
- KitKat 4.4
  - 禁止第三方APP获取电池使用量信息，避免恶意程序恶意消耗手机电量



# Android 系统安全特性发展变迁简史

## • Lollipop 5.0

- ART 运行时取代 Dalvik 成为平台默认设置
- 通知现在显示在用户的锁定屏幕上。用户可以选择保护敏感信息不被公开，此时系统会自动删减通知显示的文本
- 引入了对 64 位系统的支持，64 位支持也可改进用于加密的 OpenSSL 的性能
- WebView 默认情况下，系统会阻止混合内容和第三方 Cookie
- TLSv1.2 和 TLSv1.1 协议现已启用
- MD5、3DES、导出和静态密钥 ECDH 加密套件现已停用
- 首选使用前向保密性（Forward Secrecy）加密套件  
(ECDHE 和 DHE)



# Android系统安全特性发展变迁简史

## • Marshmallow 6.0

— 用户可直接在运行时管理应用权限

- 这种模式让用户能够更好地了解和控制权限，同时为应用开发者精简了安装和自动更新过程

— 用户可为所安装的各个应用分别授予或撤销权限

— 对于使用 WLAN API 和 Bluetooth API 的应用，Android 移除了对设备本地硬件标识符的编程访问权

- WifiInfo.getMacAddress() 方法和 BluetoothAdapter.getAddress() 方法现在会返回常量值 02:00:00:00:00:00
- 当运行 Android 6.0 (API 级别 23) 的设备发起后台 WLAN 或蓝牙扫描时，在外部设备看来，该操作的发起来源是一个随机化 MAC 地址



# Android 系统安全特性发展变迁简史

## • Nougat 7.0

- 移除了三项隐式广播，以帮助优化内存使用和电量消耗
- 为了提高私有文件的安全性，面向 Android 7.0 或更高版本的应用私有目录被限制访问 (0700)
- 一名为 Crypto 的 JCA 提供程序已弃用，因为它仅有的 SHA1PRNG 算法为弱加密。应用无法再使用 SHA1PRNG (不安全地) 派生密钥
- 对于面向 Android 7.0 的应用，Android 框架执行的 StrictMode API 政策禁止在您的应用外部公开 file:// URI



# Android系统安全特性发展变迁简史

## • Oreo 8.0

- 后台执行限制（默认情况下，这些限制仅适用于针对 O 的应用。不过，用户可以从 Settings 屏幕为任意应用启用这些限制，即使应用并不是以 O 为目标平台）
- 后台应用接收位置更新频率被降低
- 实现 HttpsURLConnection 时不会执行不安全的 TLS/SSL 协议版本回退，不再支持 SSLv3
- 使用安全计算 (SECCOMP) 过滤器来过滤所有应用。允许的系统调用列表仅限于通过 bionic 公开的系统调用
- 应用的 [WebView](#) 对象将在多进程模式下运行。网页内容在独立的进程中处理，此进程与包含应用的进程相隔离，以提高安全性。



# Android系统安全特性发展变迁简史

## • Oreo 8.0

- 在相同设备上运行但具有不同签署密钥的应用将不会再看到相同的 Android ID（即使对于同一用户来说，也是如此）
- 只要签署密钥相同（并且应用未在 OTA 之前安装到某个版本的 O），`ANDROID_ID` 的值在软件包卸载或重新安装时就不会发生变化
- 即使系统更新导致软件包签署密钥发生变化，`ANDROID_ID` 的值也不会变化
- 查询 `net.hostname` 系统属性返回的结果为空，系统属性 `net.dns1`、`net.dns2`、`net.dns3` 和 `net.dns4` 不再可用
- 如果应用请求 `READ_CONTACTS` 权限，查询联系人的使用情况数据得到的是近似值而不是精确值



# Android系统安全特性发展变迁简史

## • Oreo 8.0

- 更精细的最小化用户授权，没有用到特定权限时避免了隐式自动授权，确实用到“属于同一权限组并且在清单中注册的其他权限”时才会隐式自动授权
- 如果原生库包含任何可写且可执行的加载代码段，则不会再加载原生库
- Android 8.0 检查确保类加载器在加载新类时不会违反运行时假设条件



# 安卓 VS. Android 面临的威胁

- 安卓系统无法使用Google内置服务
  - 无法及时安装已知的系统安全漏洞补丁
  - 普遍默认启用了【允许安装来自未知来源的应用】
  - 第三方安卓应用市场数量大且良莠不齐，规模较大的第三方市场的APP上架审查机制不严格
    - 每天新增待审核APP数量巨大，人工审查存在疏漏，自动化审查存在技术局限性
  - 山寨机在出厂时、销售环节被『刷入』恶意代码



# Android VS. iOS 面临的威胁

威胁	iOS	Android
钓鱼及鱼叉式（定向）钓鱼 (邮件、网页、文件)	✓	✓
短信欺诈 (钓鱼)	✓	✓
应用欺诈 (钓鱼)	✓	✓
盗取上传通讯录	✓	✓
越狱、root、越狱伪装	✓	✓
SSL漏洞利用	✓	✓



# Android VS. iOS 面临的威胁

威胁	iOS	Android
恶意配置文件	✓	-
邮件附件未加密	✓	✓
勒索软件	✓	✓
备份（数据）劫持	✓	✓
系统（设备）碎片化	-	✓
非官方应用（恶意捆绑）	✓*	✓
通话和短信记录上传	-	✓



# 关于iOS上非官方应用风险与威胁

- 苹果的应用分发授权模式主要有2种
  - 个人应用
    - 必须且仅允许通过App Store审核通过后允许消费者下载安装使用
  - 企业级应用
    - 无需App Store审核，消费者可以直接下载安装使用
    - 如果企业作恶或者企业的分发证书被盗取滥用呢？

演示：假面攻击



# 关于恶意的iOS配置文件

- 攻击者利用配置文件绕过iOS的安全机制
  - 配置文件可以重新定义各种系统功能参数，如运营商、MDM（移动设备管理）和网络设置
  - 用户可能被诱骗下载这样的恶意配置文件，从而在不知情的情况下被导向攻击者控制的服务器，进一步被安装恶意软件，甚至被解密通信



# 恶意的iOS配置文件实例





# 系统安全与网络安全是密不可分的

- 系统与系统之间的通信过程时刻存在着监听、劫持等中间人攻击风险
  - Wi-Fi钓鱼
  - Wi-Fi口令破解
  - Wi-Fi中间人攻击
  - GSM监听
  - GSM伪基站
  - ...



## 奉劝iOS用户：谨慎越狱

- 越狱程序本身有可能已经被恶意捆绑后门和木马程序
  - 安装之后你的手机就成为黑客可以远程控制的对象了
    - 越狱应用本就可以无视iOS的沙盒机制、无限制访问原本受保护的资源和调用私有API



# 智能终端操作系统与桌面终端操作系统 安全问题与形势的区别与联系



# 层次化比较的方法

- 设备层面
- 系统层面
- 应用层面
- 产品生命周期层面



# 计算资源与能力

	PC (服务器、台式机、笔记本、工作站等)	智能终端 (手机、平板、智能家居等)
CPU	64位架构已成为主流	64位架构正在普及
耗电与续航能力	持续供电 (直流、交流电、UPS等)	有限容量电池
内存	可扩充能力强	可扩充能力较弱
存储	标配高，扩展性高	单机扩展能力差



# 联网条件

	PC (服务器、台式机、笔记本、工作站等)	智能终端 (手机、平板、智能家居等)
网络可用性	连续	不确定
网络移动性	弱	强
网络稳定性	高	一般
网络可控性	强	弱，随时可能接入不安全、不可控网络 (Wi-Fi、不安全蜂窝数据网络)



# 物理安全风险

	PC (服务器、台式机、笔记本、工作站等)	智能终端 (手机、平板、智能家居等)
被盗	低	高
损坏	低	高
非授权访问 (接触)	低	高



# 层次化比较的方法

- 设备层面
- 系统层面
- 应用层面
- 产品生命周期层面



# 系统功能特性

	PC (服务器、笔记本、工作站等)	智能终端 (手机、平板、智能家居等)
通讯录	电子邮件通讯录 (电话号码)	电话号码通讯录 (电子邮件、社交网络帐号等)
电话与通话记录	无	普遍
短信	无	普遍
定位	依赖Wi-Fi定位	普遍
传感器	非内置，可选	内置，且可通过外设扩充 (重力、光线、温度等)
拍照与摄像	使用率较低	普遍
多窗口	普遍	受限( <a href="#">Android 8.0 画中画模式</a> / <a href="#">iPad上的多任务处理</a> )
多任务	普遍	受限 (OS会根据计算资源消耗、耗电等动态强制结束进程)



# 访问控制

	PC (服务器、台式机、笔记本、工作站等)	智能终端 (手机、平板、智能家居等)
默认受限账户	部分	普遍
多用户	普遍	极少
应用沙盒	非默认配置	普遍



# 系统升级流程差异——PC

- 硬件设备制造商基于操作系统厂商提供的操作系统和SDK开发设备驱动程序
- 操作系统厂商提供系统升级时的相应版本SDK升级和前向兼容性支持
  - Microsoft 针对商务，开发人员和桌面操作系统产品提供最少 10 年的安全更新支持
- 应用软件对新版本操作系统的兼容性主要由操作系统厂商来保证

硬件升级换代周期：  
3~5年

兼容维护周期：  
5~10年+

系统应用层API  
兼容性周期长



# 系统升级流程差异——智能终端

	PC	iOS	Android	安卓	其他嵌入式OS
硬件升级换代更新周期	3~5年	1年	1年	6个月~1年	1年
操作系统维护周期	5~10年+	<1年	N/A	N/A	N/A
应用软件兼容性	少	中	中	难	难



# 系统层面的安全问题对比小结

- 如果把PC互联网时代比作二维网络空间，那么以智能终端为基础的移动互联网时代就是三维网络空间
  - 安全风险的来源、影响对象范围更加广阔和多样化
- 移动互联时代，操作系统和硬件的耦合性更高
  - 安全研究对象和问题的碎片化加剧
  - 硬件升级换代速度加快推动系统功能不断叠加，风险点随功能数量增加而呈无法控制的爆炸增长态势



# 层次化比较的方法

- 设备层面
- 系统层面
- 应用层面
- 产品生命周期层面



# 应用生命周期管理

	PC (服务器、台式机、笔记本、工作站等)	智能终端 (手机、平板、智能家居等)
下载	下载站、光盘、拷贝安装包	应用商店，在线获取
安装	可实现后台静默安装	普遍需要用户交互，静默安装难度高
使用	需要使用者具备一定的计算机使用经验与能力	普遍傻瓜化
卸载	顽固驻留型恶意代码和流氓软件实现技术成熟	普遍容易，恶意驻留难度高
自动更新	已普及	具体平台差异较大 (国内的安卓系统、智能家居设备内置系统)



## 应用层面的对比

- 软件加密与反破解技术的普及程度差异大
  - 互联网模式（免费使用）的应用加固服务和软件一方面降低了正规厂商的正规应用被破解和篡改的风险，同时被恶意代码用于对抗杀毒软件的查杀和安全专家的分析、研究；PC互联网时代的同类技术普遍采取收费模式，综合成本更高
- 移动端恶意应用的『变现』能力更强
  - 手机号码内的话费
  - 手机支付App
    - PC互联网时代基于短信验证码的双因素认证在手机上实际变成了『单因素』



# 层次化比较的方法

- 设备层面
- 系统层面
- 应用层面
- 产品生命周期层面



# 产品生命周期——PC时代的软件巨人

## • 微软

一对于企业、开发人员和桌面操作系统产品，在受支持的 Service Pack 级别提供 10 年的支持（至少 5 年主要支持和 5 年外延支持）

一对于消费类和多媒体产品，在受支持的 Service Pack 级别提供至少 5 年的主要支持

微软产品技术支持生命周期

	支持类型	主要支持阶段	外延支持阶段	自助式联机支持
更改产品设计和功能的请求	✓	X		
安全更新	✓	✓		
非安全更新	✓	★		
包括许可证、授权程序 <sup>2</sup> 或其他免费支持程序的免费支持 <sup>1</sup>	✓	X <sup>3</sup>		可以免费访问联机内容，如知识库文章、联机产品信息及联机支持网络广播
付费支持（包括按事件支付类的顶级支持和基础支持）	✓		✓	

\*请注意：Microsoft 的支持生命周期策略并非适用于所有产品。要查看适用产品的具体支持开始和结束日期，您可以搜索[支持生命周期产品数据库](#)。

1 参阅[电话支持和联机支持选项](#)。

2 例如，通过软件保障计划为服务器产品获取支持事件。

3 可能提供有限的免费支持（因产品而异）。

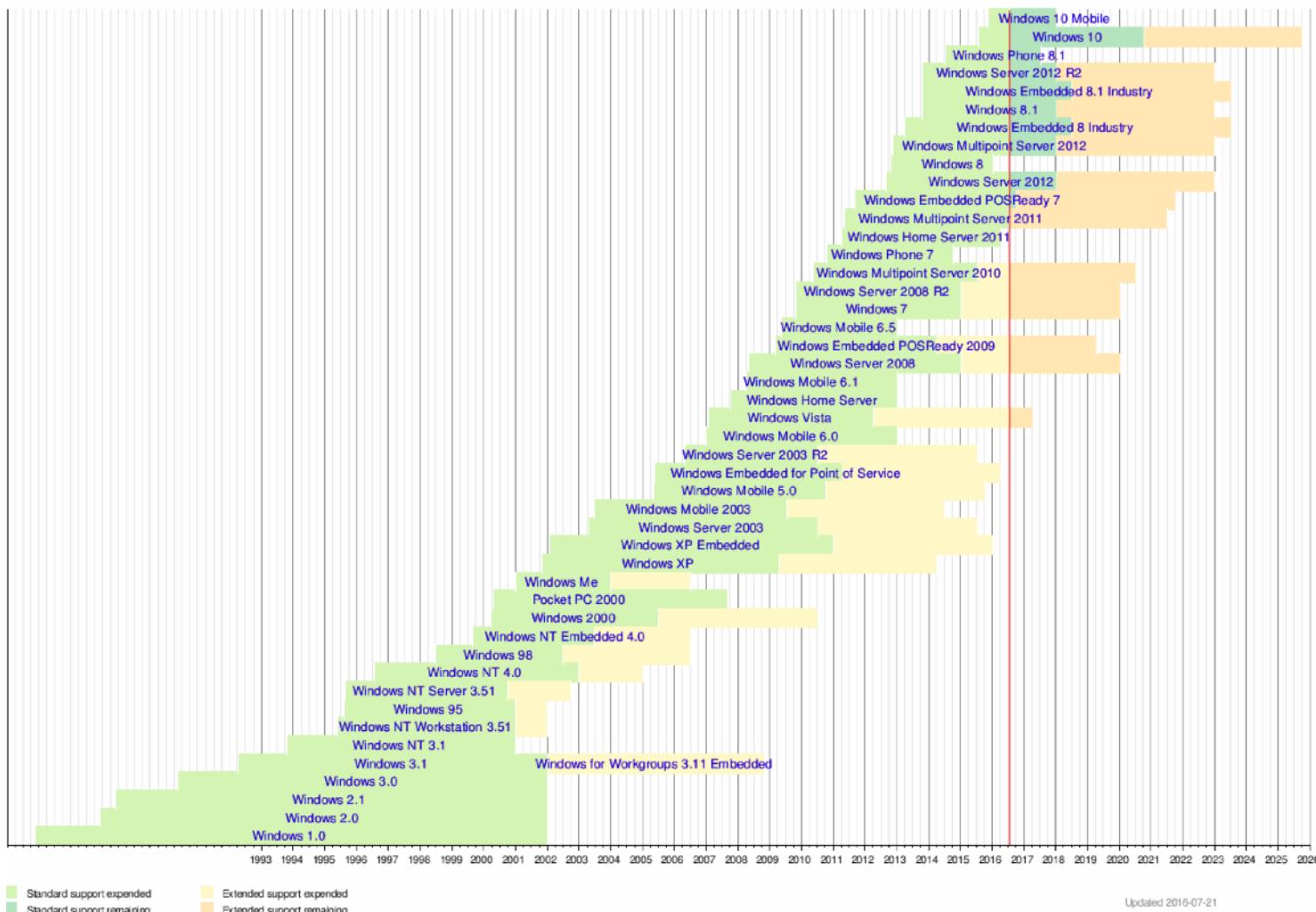
Windows 生命周期说明书 以下表格数据更新时间：2016年1月

客户端操作系统	最新更新或 Service Pack	主要结束支持日期	外延结束支持日期
Windows XP	Service Pack 3	2009 年 4 月 14 日	2014 年 4 月 8 日
Windows Vista	Service Pack 2	2012 年 4 月 10 日	2017 年 4 月 11 日
Windows 7*	Service Pack 1	2015 年 1 月 13 日	2020 年 1 月 14 日
Windows 8	Windows 8.1	2018 年 1 月 9 日	2023 年 1 月 10 日
Windows 10，已于 2015 年 7 月发布**	不适用	2020 年 10 月 13 日	2025 年 10 月 14 日



# 微软的Windows家族生命周期时间线历史

Timeline of Windows

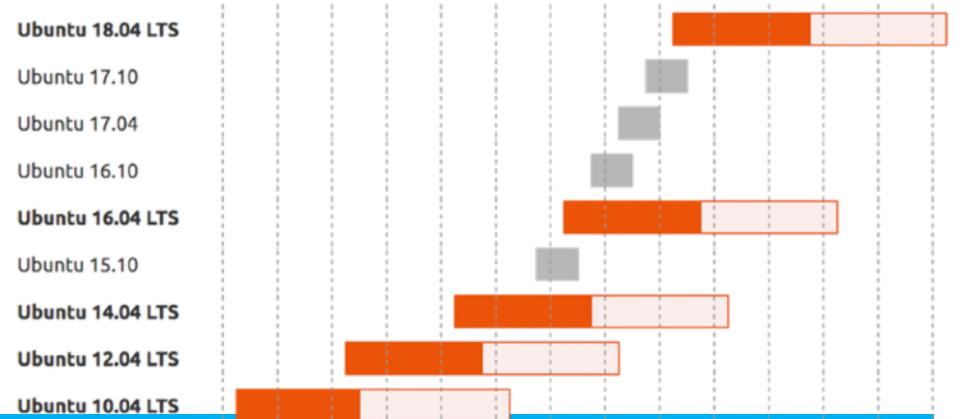




# 产品生命周期——开源社区之Linux

- Ubuntu

- LTS是长期支持（Long Term Support）的缩写
- 每六个月推出一个新的Ubuntu桌面和服务器的版本，因此能够获得至少18个月的免费桌面版和服务器版安全更新
- 一个新的LTS版本通常每两年发布一次，使用长期支持（LTS）版本的Ubuntu桌面版能够获得3年的支持，Ubuntu服务器版能够获得5年的支持。



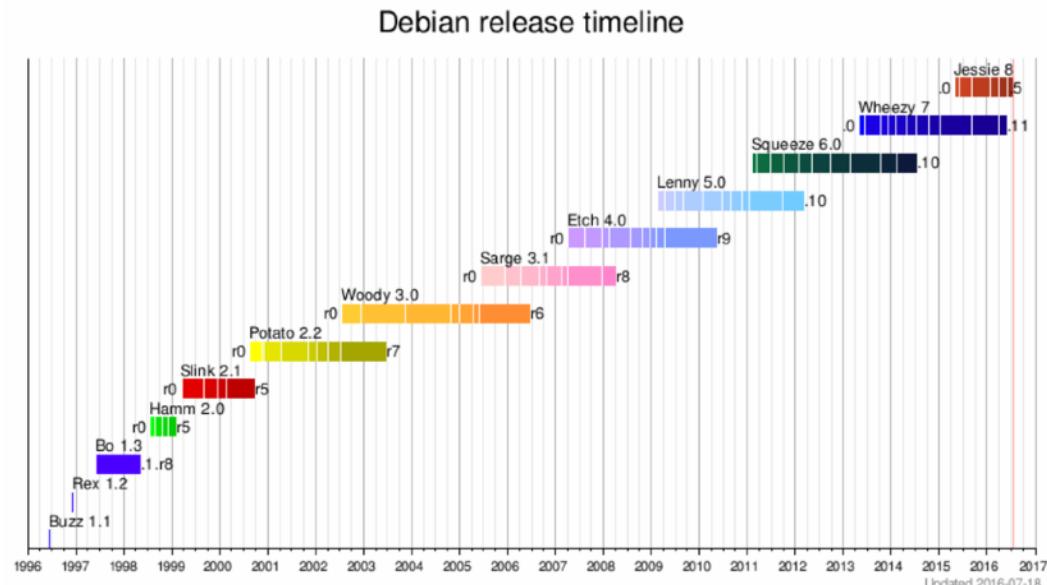


# 产品生命周期——开源社区之Linux

## • Debian

—Debian稳定版官方支持周期标准是3年

—LTS是一个由志愿者和公司组成的独立于Debian安全响应小组的团体负责在Debian稳定版官方支持周期结束之后继续提供到距离首个稳定版本发布之日起不少于5年的LTS承诺支持周期





# 产品生命周期——开源社区之Linux

## • Red Hat

—RHEL 5开始，10年标准支持和一个较长的扩展支持周期（RHEL 5是4年）

—安全更新仅限标准支持阶段

The Red Hat Enterprise Linux 5, 6, and 7 Life Cycle\*:



\* The life-cycle time spans and dates are subject to adjustment.

\*\*ELS offered on RHEL 5 only.

The Red Hat Enterprise Linux 4 life cycle\*:



\* The life-cycle time spans and dates are subject to adjustment.



# RedHat企业级Linux系统产品支持策略定义

Description	Production 1	Production 2	Production 3	Extended Life Phase <sup>7</sup>	Extended Life Cycle Support (ELS) Add-On <sup>8</sup>	Extended Update Support (EUS) Add-On <sup>8</sup>
Access to Previously Released Content through the Red Hat Customer Portal	Yes	Yes	Yes	Yes	Yes	Yes
Self-help through the Red Hat Customer Portal	Yes	Yes	Yes	Yes	Yes	Yes
Technical Support <sup>1</sup>	Unlimited	Unlimited	Unlimited	Limited <sup>9</sup>	Unlimited	Unlimited
Asynchronous Security Errata (RHSA) <sup>10 11</sup>	Yes	Yes	Yes	No	Yes <sup>8</sup>	Yes <sup>8</sup>
Asynchronous Bug Fix Errata (RHBA) <sup>2 11</sup>	Yes	Yes	Yes	No	Yes	Yes
Minor Releases	Yes	Yes	Yes	No	No	No
Refreshed Hardware Enablement <sup>3</sup>	Native	Limited <sup>4</sup> Native	Using Virtualization	Using Virtualization	Using Virtualization	Using Virtualization
Software Enhancements <sup>5</sup>	Yes <sup>6</sup>	No	No	No	No	No
Updated Installation Images	Yes	Yes	Yes	No	No	No



# Google Android

- Google NEXUS设备安全补丁更新周期 官方承诺
  - 可使用期间的3年的支持或者是Google Store最后销售该设备开始的18个月，两者取最长时间
- Android官方安全更新通告（数据/漏洞信息）来源
  - Android本身的漏洞修复代码会在官方漏洞通告发布的24-48小时之内整合到AOSP代码仓库
  - 上游Linux内核漏洞会在官方漏洞通告发布同时从Linux源代码仓库获得修复代码
  - 固件类漏洞直接从设备厂商获取修复解决方案



# 华为

## • 硬件产品



里程碑	全称	定义
GA	General Availability	指产品包可以大批量交付给华为客户的时间。
EOM	End of Marketing	产品停止接受新建和扩容订单。
LODSP	Last order date of spare parts	备件最后购买日。在备件最后购买日后，正常维护用备件可以通过购买服务产品获取。
EOS	End of service&support	华为公司停止此产品服务和支持。

## • 软件产品



里程碑	全称	定义
EOM	End of Marketing	华为公司停止接受软件版本的新建和扩容订单。
EOFS	End of full support	华为公司停止为软件版本开发新补丁。
EOS	End of service&support	华为公司停止对软件版本提供服务。

在产品和软件版本的生命周期关键里程碑点到来之前的至少6个月通过公司网站、邮件、电话等方式通知到华为用户

关于产品支持生命周期的公告信息：

2016年6月前可查看：<http://www1.huawei.com/cn/ProductsLifecycle/index.htm>  
2016年6月后可查看：<http://www.huawei.com/cn/products-lifecycle>

手机和手机系统  
并没有任何承诺支持

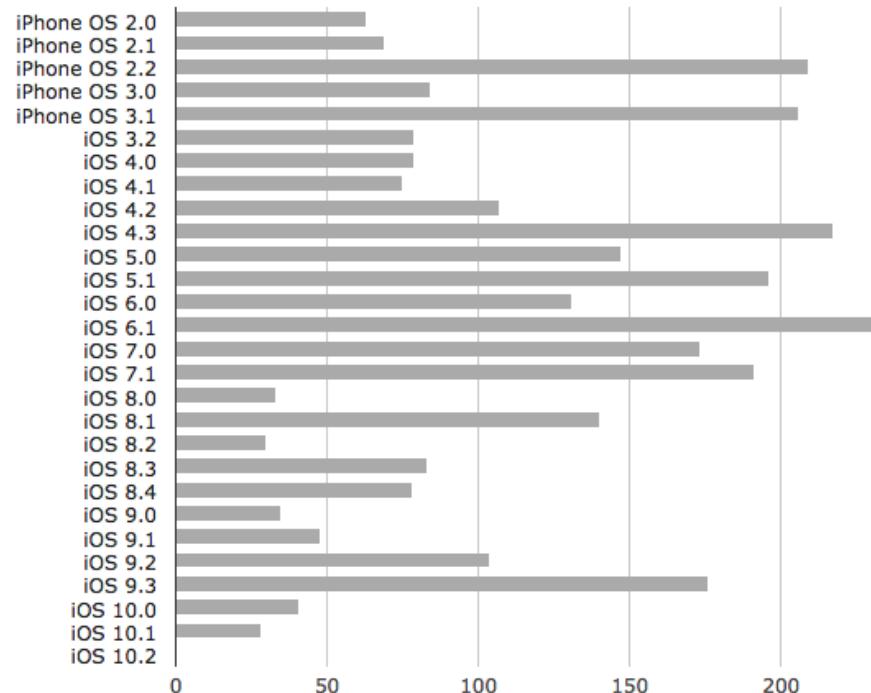


# Apple iOS/macOS

- 截止2016年11月21日，从未公开过旗下产品的安全通告策略和产品支持周期
- 硬件更新换代驱动软件更新
- 漏洞补丁？

— 报告一个，修复一个

— 没被曝光？等一堆打包到下次  
bug修复版本一起悄悄发布



<http://www.thinkybits.com/blog/iOS-versions/>



## 小结

- PC时代及其代表产品PC和服务器依然是企业级服务的主要支持对象，手机和手机系统目前的主要角色定位还是消费级产品
- 企业级产品比消费级产品有更长时间周期的（兼容性、**安全补丁**、功能补丁等）支持需求
- 消费级产品迭代更新周期要远小于企业级产品
- 企业级产品更强调服务承诺和稳定性，消费级产品追求创新和变化
- 手机软件（系统）和硬件的一体绑定性要强于PC、服务器



## 内容提要

- 智能终端概述
- iOS系统安全概述
- Android系统安全概述
- Android应用安全实验环境搭建



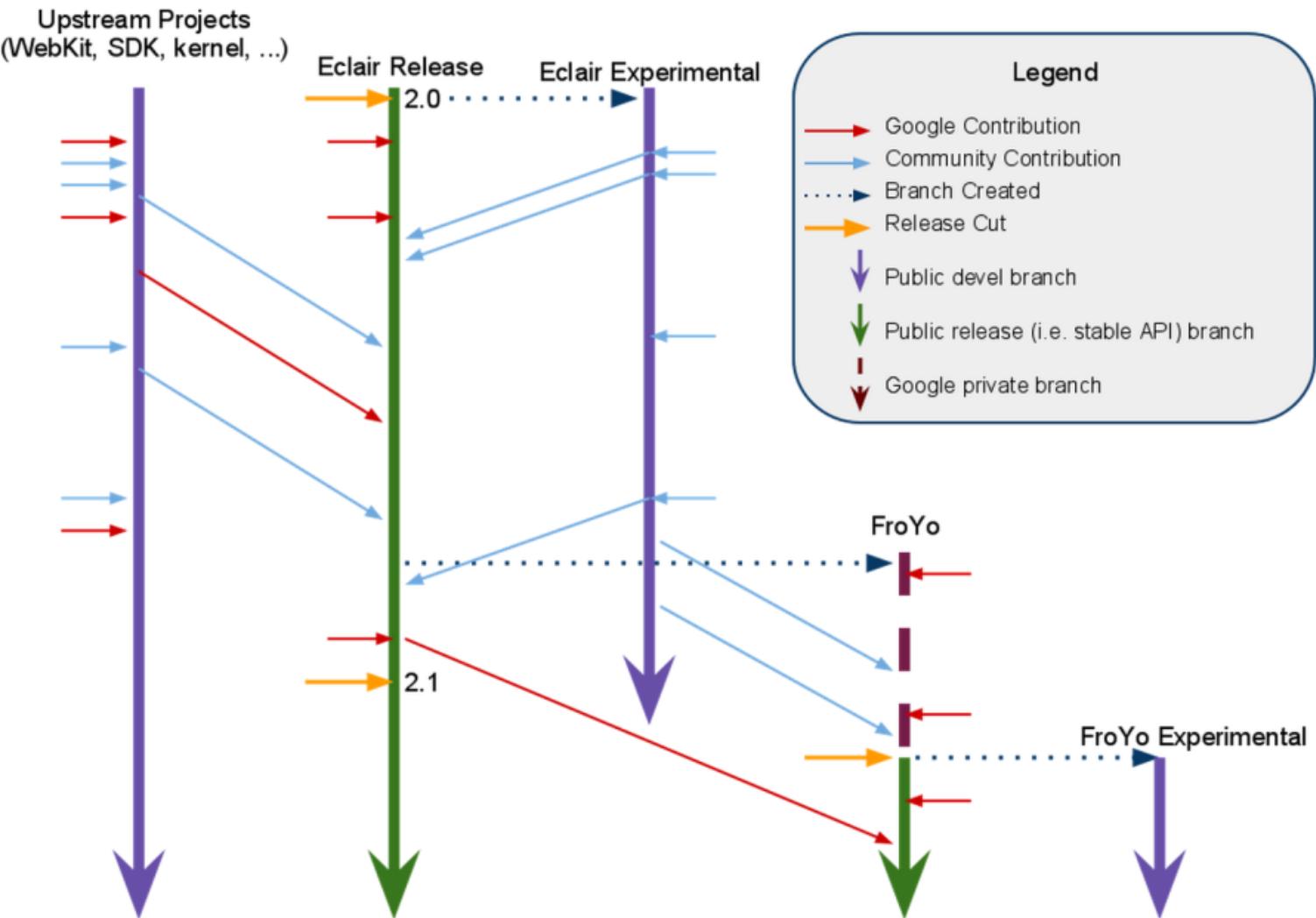
# Android（开源）项目基础

- Android是由Google所领导Open Handset Alliance组织发起并管理的一个开源软件项目
  - 项目首要目标是为电信运营商、OEM厂商和开发者提供一个开源的移动应用创新和应用平台
  - 任何组织和个人都可以使用Android项目源代码
    - 定制的设备和系统必须通过ACP (Android Compatibility Program) 测试（免费）才可以称之为Android兼容系统（产品）
  - 官方愿景和项目管理原则：Android是一个整体（产品），各个组件都是不可替代的。第三方厂商可以移植Android系统到自己的目标设备，但不应该实现一套自己的『新规范』



# Android (开源) 项目生命周期

- Android是一个全球协作开发项目
- Android项目的下一个发行版本由Google内部工程师进行私有化独立开发
- OEM厂商基于当前最新的稳定发布版本进行二次开发修bug等
- 上游开源项目代码会被定期合并到Google的私有开发分支版本代码库
- 平台API同时具备内部开发代号和对应Sdk版本号





# Android版本号与API Level

版本号	版本代号	发布时间	API level	首发预搭载设备
1.0	N/A	September 23, 2008	1	N/A
1.1	N/A	February 9, 2009	2	N/A
1.5	Cupcake	April 27, 2009	3	N/A
1.6	Donut	September 15, 2009	4	N/A
2.0 – 2.1	Eclair	October 26, 2009	5-7	N/A
2.2 – 2.2.3	Froyo	May 20, 2010	8	Droid 2
2.3 – 2.3.7	Gingerbread	February 9, 2011	9-10	Nexus S
4.0 – 4.0.4	Ice Cream Sandwich	December 16, 2011	14-15	Galaxy Nexus
4.1 – 4.1.2	Jelly Bean	July 9, 2012	16	Nexus 7
4.2 – 4.2.2		November 13, 2012	17	Nexus 4, Nexus 10
4.3 – 4.3.1		July 24, 2013	18	Nexus 7 2013
4.4 – 4.4.4	KitKat	October 31, 2013	19	Nexus 5
5.0 – 5.0.2	Lollipop (棒棒糖)	November 3, 2014	21	Nexus 6
5.1 – 5.1.1		March 9, 2015	22	Android One
6.0 – 6.0.1	Marshmallow (棉花糖)	October 5, 2015	23	Nexus 5X, Nexus 6P
7.0-7.1	Nougat (牛轧糖)	August 22, 2016	24-25	LG V20



# Android SDK

- 开发Android平台应用软件所需的工具软件套装
  - SDK Tools
    - 与具体Android平台版本无关的工具
  - platform tools
    - 与具体Android平台的新特性有关的工具



# SDK Tools

- Android SDK Manager
  - android sdk
- Android虚拟机管理器 (AVD Manager)
  - android avd
- 模拟器 (基于QEMU的Android硬件模拟器)
  - 可以在模拟器中安装Android不同版本系统，运行App
    - emulator
- Dalvik调试监视服务
  - ddms

```
→ sdk ls tools
NOTICE.txt          lib
android             lint
ant                 mksdcard
apps                monitor
ddms               monkeyrunner
draw9patch          proguard
emulator            screenshot2
emulator64-arm      source.properties
emulator64-mips     support
emulator64-x86      templates
hierarchyviewer     traceview
jobb                uiautomatorviewer
```



# Intel HAXM

- Intel Hardware Accelerated eXecution Manager
- 英特尔® 硬件加速执行管理器是一个硬件辅助的虚拟化引擎（hypervisor，虚拟机监视器），它使用英特尔® 虚拟化技术加速安卓应用在主机上的模拟
- 英特尔® 硬件加速执行管理器与英特尔提供的安卓 x86 模拟器映像及官方安卓SDK Manager（安卓软件开发套件）相结合，可在启用英特尔虚拟机的系统上更快地模拟安卓系统



## platform tools

- 每次安装新版本SDK时会更新，前向兼容
- 最常用的platform tools: Android Debug Bridge(adb)
  - 既可以管理模拟器中的Android实例也可以管理真机系统

```
→ sdk ls platform-tools
NOTICE.txt          fastboot
adb                 hprof-conv
api                source.properties
dmtracedump        sqlite3
etc1tool           systrace
```



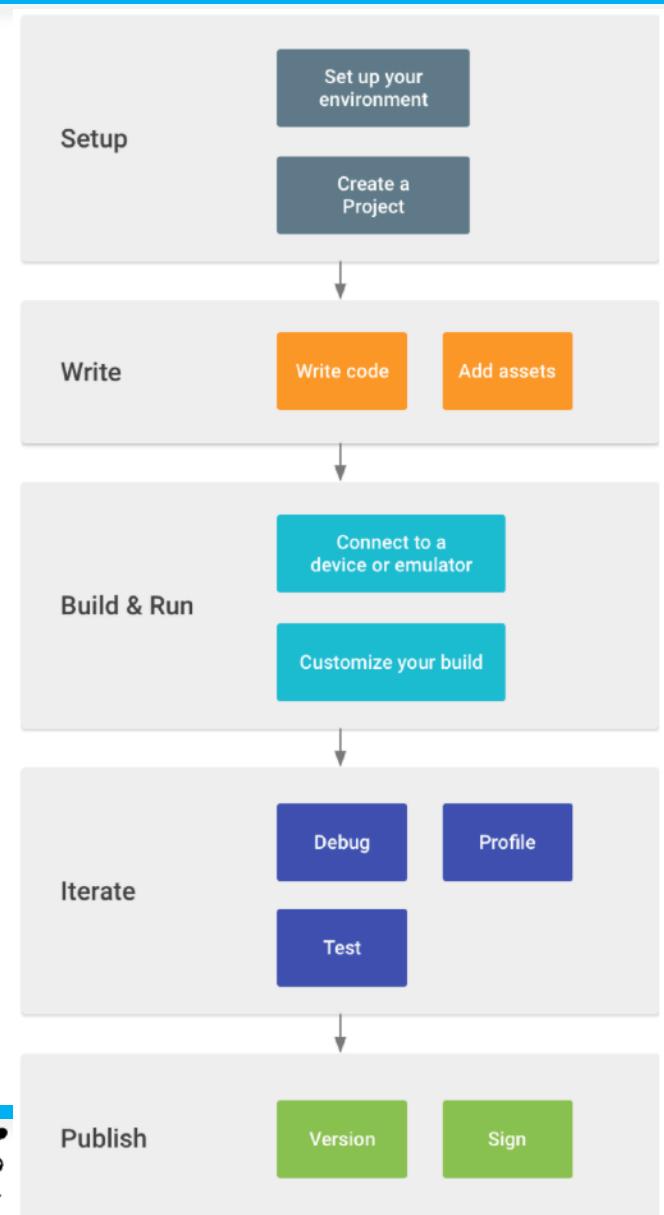
# 实验环境说明

- 操作系统无关
  - Windows平台进行真机调试需要额外安装必要的厂商专有USB设备驱动
- 所有必要软件都可以通过内网镜像源或FTP下载安装
  - 厂商专有USB设备驱动需要连接互联网下载



# 基于Android平台的系列实验规划

- Android实验环境搭建
- 安全分析类实验
  - 操作系统（访问控制）基础
  - 静态分析
- 动态分析与逆向实验
- 软件安全与取证相关实验





# 实验——Android实验环境搭建

- JDK开发环境搭建与配置
- Android Studio安装与配置
  - Android SDK Tools
  - Android Platform-tools
  - 某个版本的Android平台
  - 适用于Android模拟器的某个版本系统镜像
- 通过SDK Manager安装新软件包



# 实验——Android实验环境搭建

- AVD (Android Virtual Device) 管理与调试
  - 创建并配置AVD
  - adb连接与管理
    - 连接：USB模式与tcpip模式
- 真机管理与调试
  - 安装设备厂商的专用USB驱动（windows）
  - 开启设备的『开发者模式』



## 参考文献

- 工信部电信研究院2014年移动互联网白皮书  
(2014年5月)
- Android系统不同版本在不同时期的市场占有率
- Android Security Overview by Google Inc.
- Marble Labs Mobile Threat Report, June 2014
- 移动安全这五年