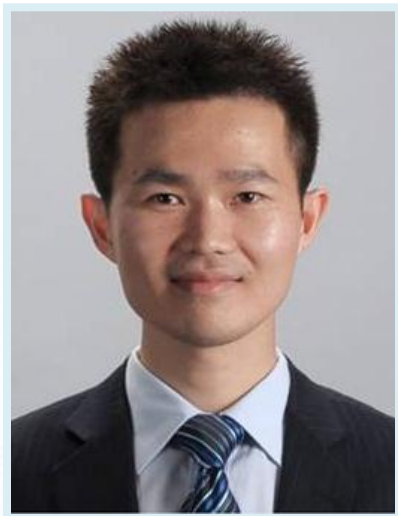




智能终端安全与取证

演讲：徐志强

个人简介



徐志强 美亚柏科技术专家委员会(MTEC)
首席技术专家

主要研究方向：计算机取证、手机取证及信息加解密技术。

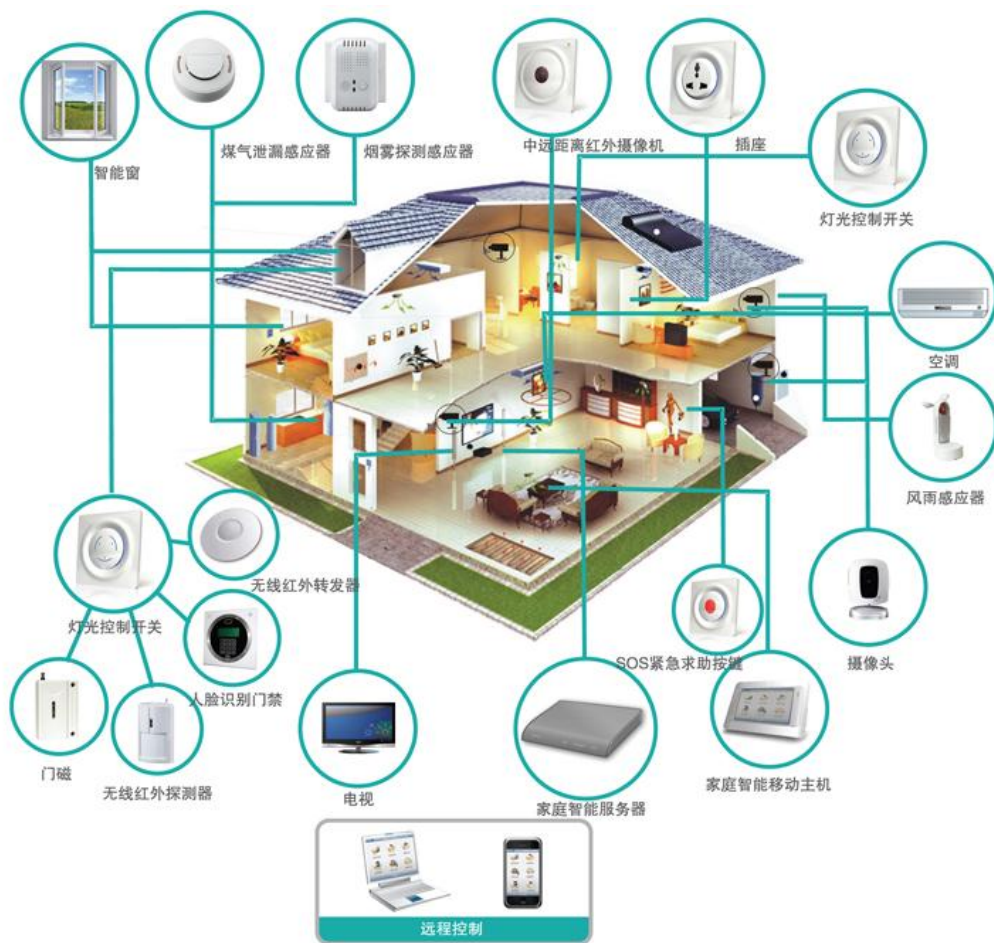
- ◆ 福建省公共网络信息安全协会专家组专家
- ◆ 中国政法大学法务会计研究中心特聘研究员
- ◆ 江西警察学院计算机犯罪中心特聘研究员
- ◆ 中华全国律师协会信息网络与高新技术专委会特邀委员
- ◆ 南昌大学工程硕士专业学位兼职研究生导师
- ◆ 中国计算机学会(CCF)高级会员
- ◆ 高科技犯罪调查协会(HTCIA)亚太分会会员
- ◆ ISC² Certified Cyber Forensics Professional (CCFP)
- ◆ EnCase Certified Examiner (EnCE)

内容

- 1.智能终端发展
- 2. Android系统与取证
- 3. iOS系统与取证
- 4. 系统安全机制新变化及挑战
- 5. 小结

1.智能终端发展

- 智能手机
- 平板电脑
- 可穿戴智能设备
- 物联网终端
- 体感设备
- 智能路由器等



2. Android 系统安全现状

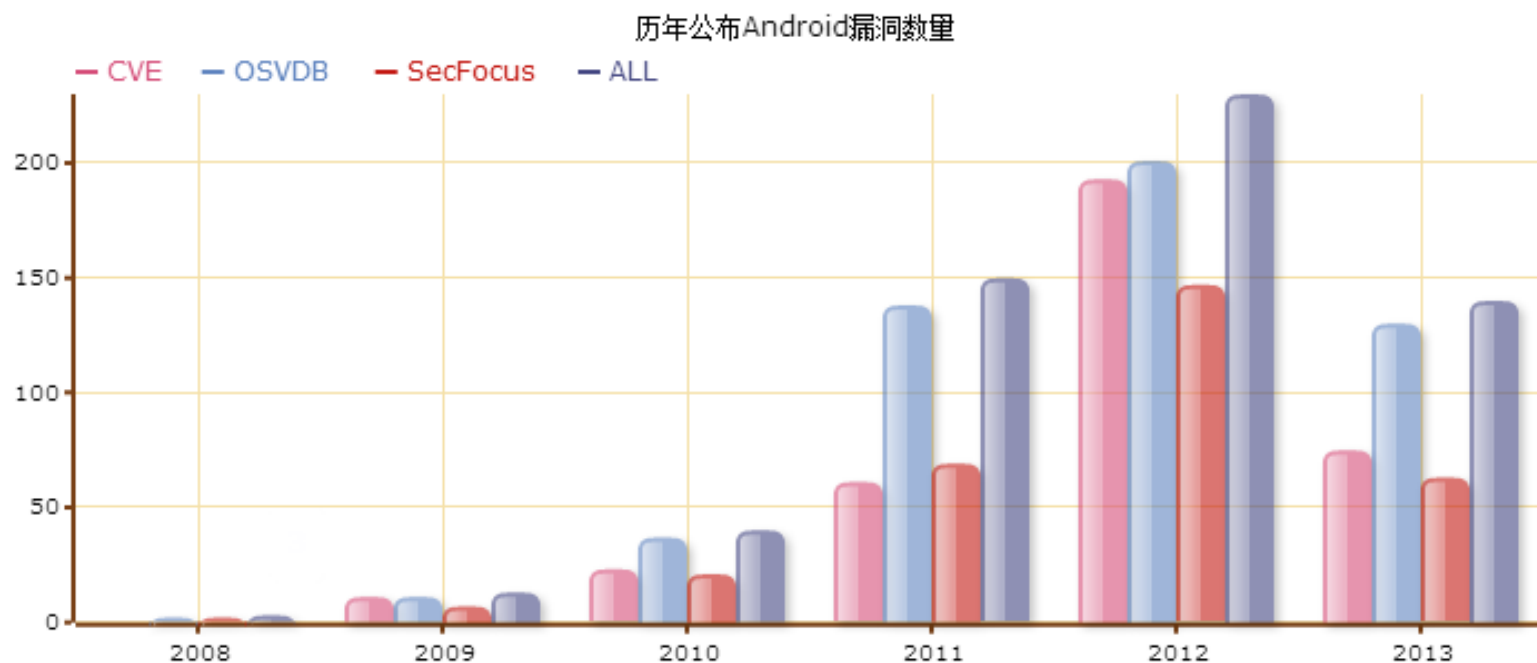
Android漏洞信息库 (374项)

374条漏洞信息; 171条到OVAL定义的映射; 277条到CWE定义的映射

58条原生漏洞; 13条框架层漏洞; 14条内核层漏洞

18条Native层漏洞; 151条应用层漏洞; 13条原生应用层漏洞

138条第三方应用漏洞; 167条第三方组件漏洞; 11条第三方系统漏洞



2. Android 系统安全现状

- Android因为平台开放拥有最多用户群体，也因为平台开放，恶意代码，广告植入等APP泛滥，存在安全隐患。



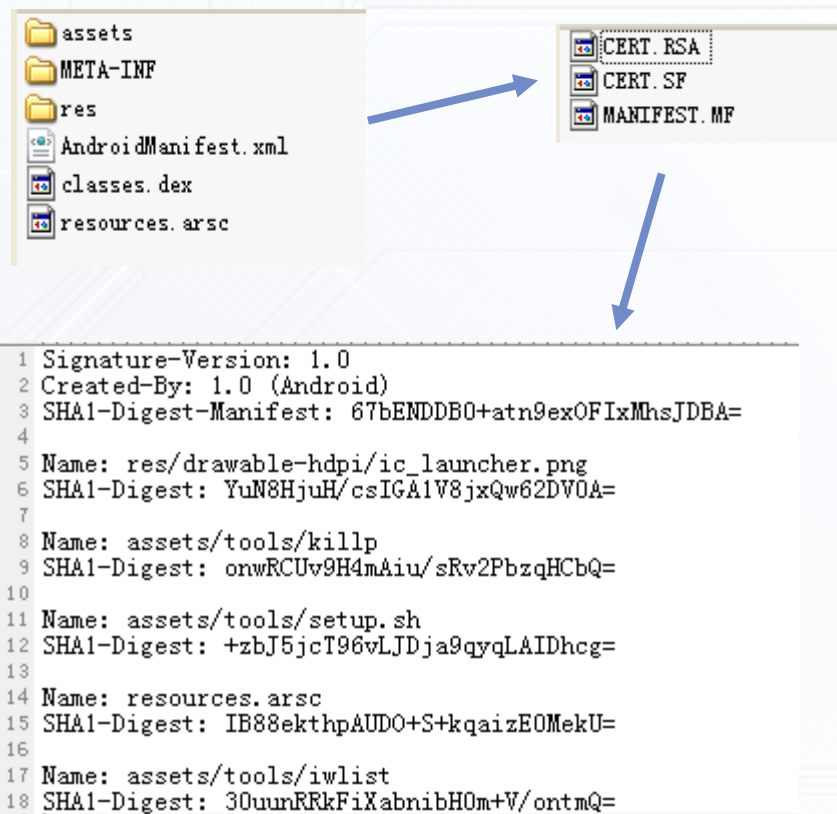
2. Android系统安全与取证

- 系统安全漏洞
- 安全保护机制(屏幕锁及PIN保护)
- 数据存储安全



2.1 签名漏洞

- 覆盖的手机范围广
 - Android 系统1.6-4.2版本, Galaxy S4之前的手机, 9亿部、99%的手机都存在此漏洞
- 隐蔽性高
 - 可以不改变签名而注入恶意代码
- 难以统一修复
 - 框架层漏洞, 厂商不一



2.1 签名漏洞

```
root@oyblxmu:/mnt/hofs/Shared/ld# gdistfile1 sh weibo_575.apk
I: Baksmaling.
I: Loading res
^[aI: Loaded.
I: Decoding An
I: Loading res
I: Loaded.
I: Regular man
I: Decoding fi
I: Decoding va
I: Done.
I: Copying ass
Modify files,
```

已下载	全部	SD 卡中	正在运行
			1 个进程和 1 个服务 22:52:02
			6.6MB 10:05:22
			22MB 10:39
			8.2MB 10:05:21
			29MB 06:24
			3.6MB 22:53:34
			12MB 22:53:32

**WeiboService** 10:05:43
已由应用程序启动。

此服务由其应用程序启动。停止服务可能会导致应用程序失败。

停止 马上报修

**evilService** 9:40:13
已由应用程序启动。

此服务由其应用程序启动。停止服务可能会导致应用程序失败。

停止 马上报修

**SinaAppMarket** 10:53
已由应用程序启动。

此服务由其应用程序启动。停止服务可能会导致应用程序失败。

停止 马上报修

2.2 XSS漏洞

- Cross Site Scripting 跨站脚本漏洞，Android原生浏览器Webkit存在XSS漏洞

Android系统版本4.0以下手机，成功率40%左右



2.2 XSS漏洞

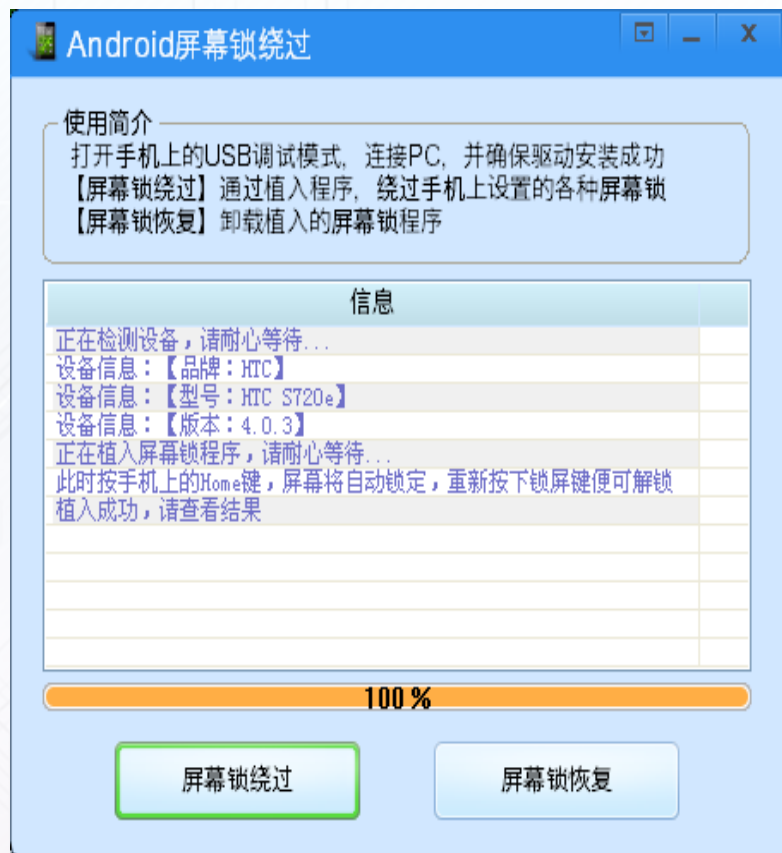
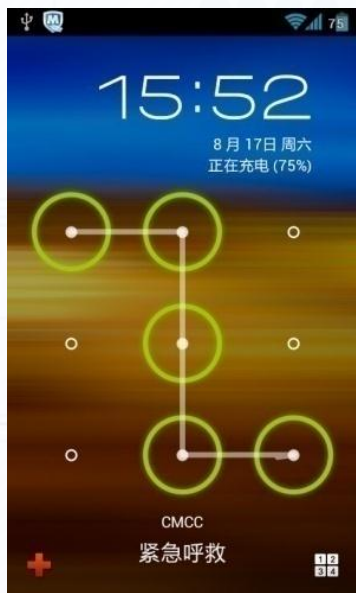
The screenshot shows a mobile phone interface with a list of saved passwords. A red callout box points to the '登录密码信息' (Login Password Information) section. The list contains one entry:

序号	访问地址	用户名	密码	导入时间
1	httpsmart.mail.163.com	safetest	hello123	2013-06-06 17:18:58

The interface also shows a sidebar with categories like 'XT301(2.1-update1)', '自带浏览器', '历史记录(12)', 'cookies(13)', '登录密码(1)', '新浪微博', '腾讯微博', and 'HTC Sensation Z710e(2.3.3)'.

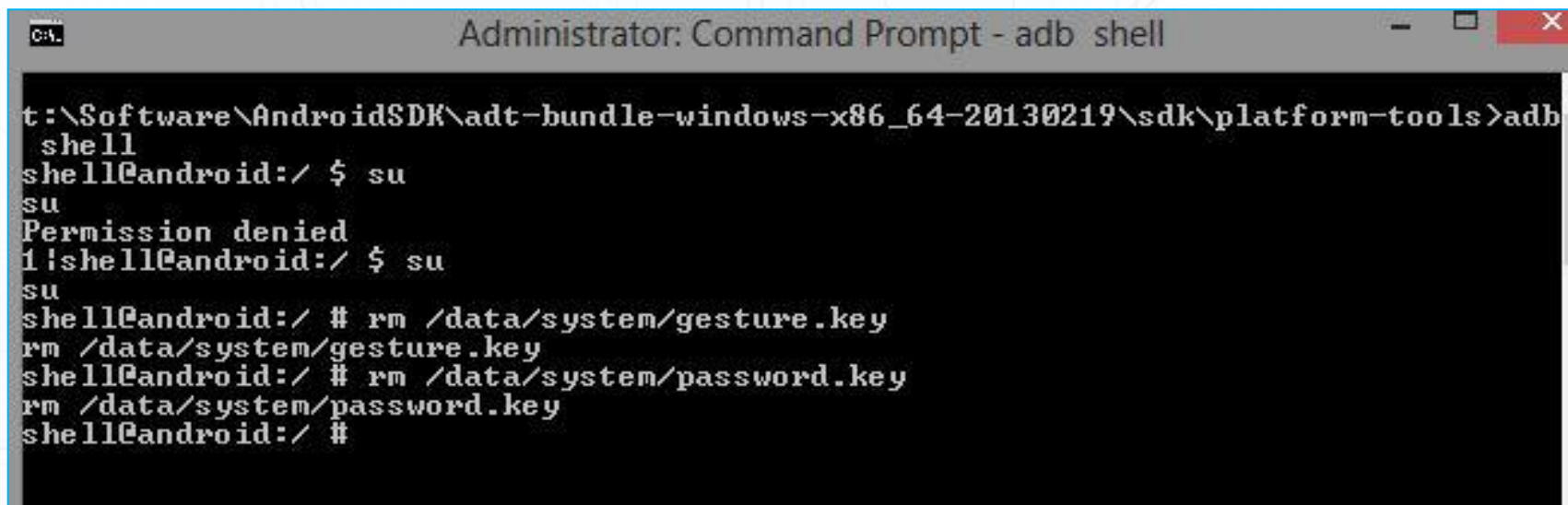
2.3 图形锁/密码绕过

- 手机取证工具可直接绕过图案锁/密码 (开启调试模式)



2.3 图形锁/密码绕过

- 开启USB调试模式情况下，Android的安全保护形同虚设，可直接通过adb命令绕过。



```
Administrator: Command Prompt - adb shell

t:\Software\AndroidSDK\adt-bundle-windows-x86_64-20130219\sdk\platform-tools>adb
shell
shell@android:/ $ su
su
Permission denied
1!shell@android:/ $ su
su
shell@android:/ # rm /data/system/gesture.key
rm /data/system/gesture.key
shell@android:/ # rm /data/system/password.key
rm /data/system/password.key
shell@android:/ #
```

2.4 图形锁/密码破解

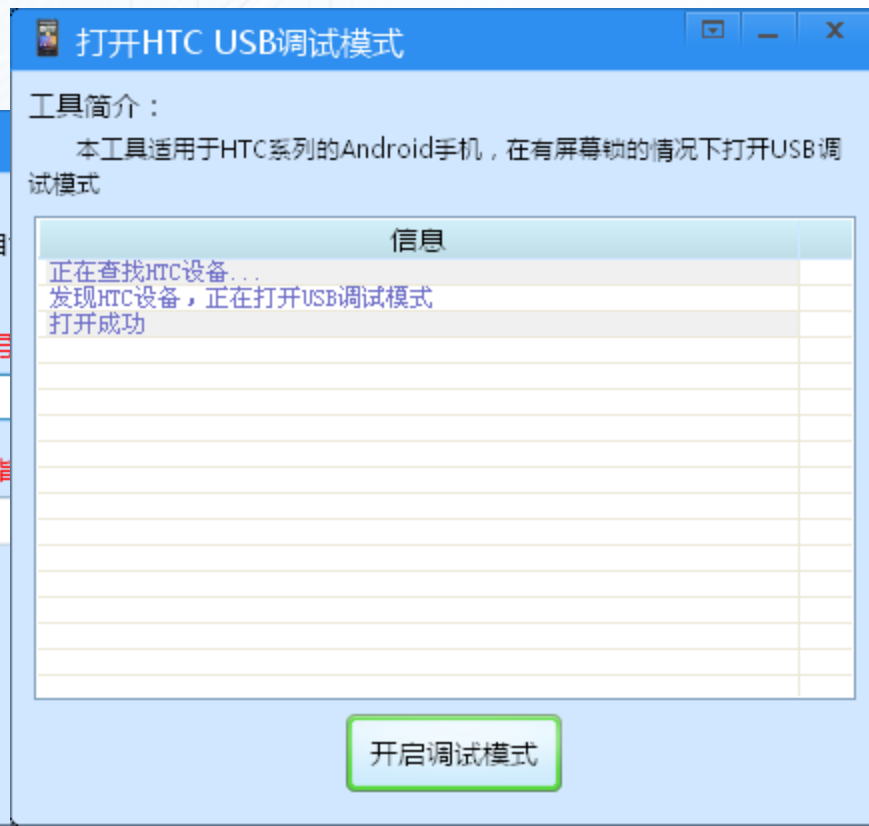
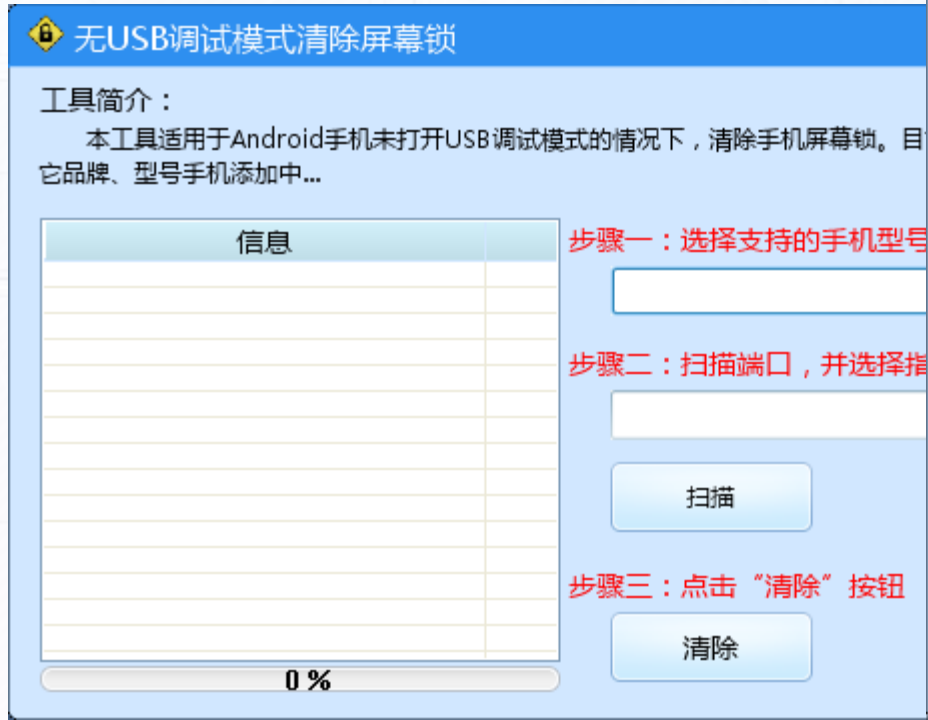
○ 屏幕锁/开机密码破解

- ✓ **九宫图屏幕锁破解**
- ✓ **1.5-4.2版本**
- ✓ **需已打开USB调试模式**
- ✓ **需已经root**
- ✓ **可直接载入密钥文件破解密码**
- ✓ **加密算法：图形转数字，然后SHA-1散列，查表法5秒内完成破解**



2.5 清除屏幕锁(未开机调试模式)

- Android手机未开启调试模式、锁屏情况下，可绕过屏幕锁或密码
 - 三星 (**60%**)
 - HTC (**70%**)
 - 小米 (**MIUI 5.0**以上)
 - 阿里云手机



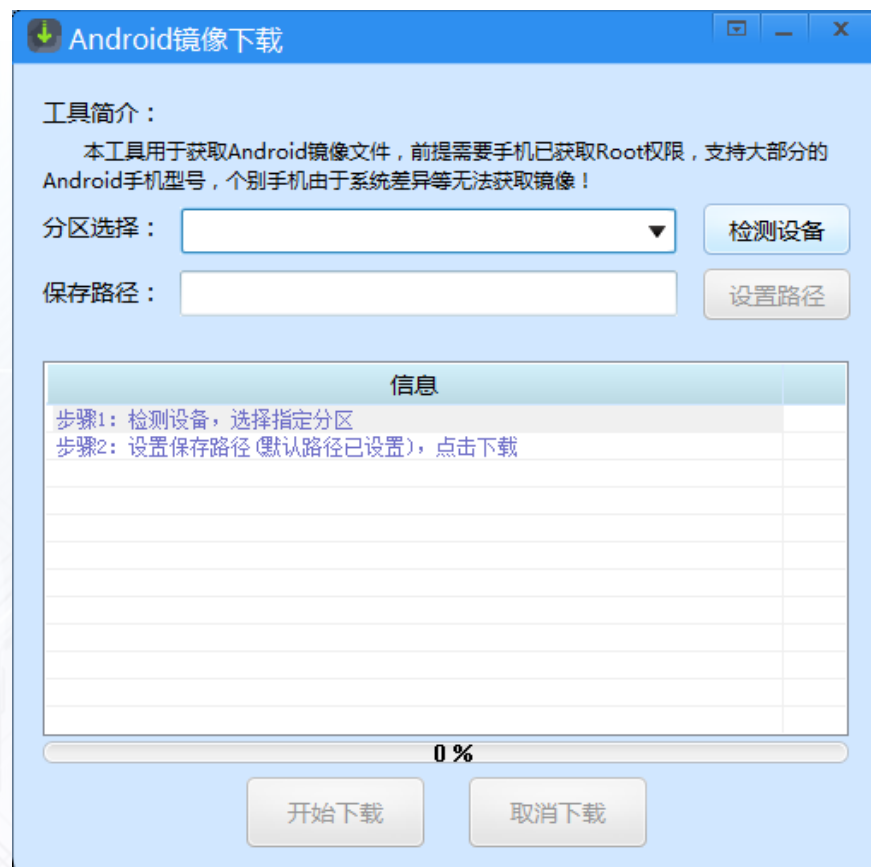
2.5 清除屏幕锁(未开启调试模式)

- MTK 芯片系列手机, **无需开机**, 可使用专门的镜像终端进行镜像取证



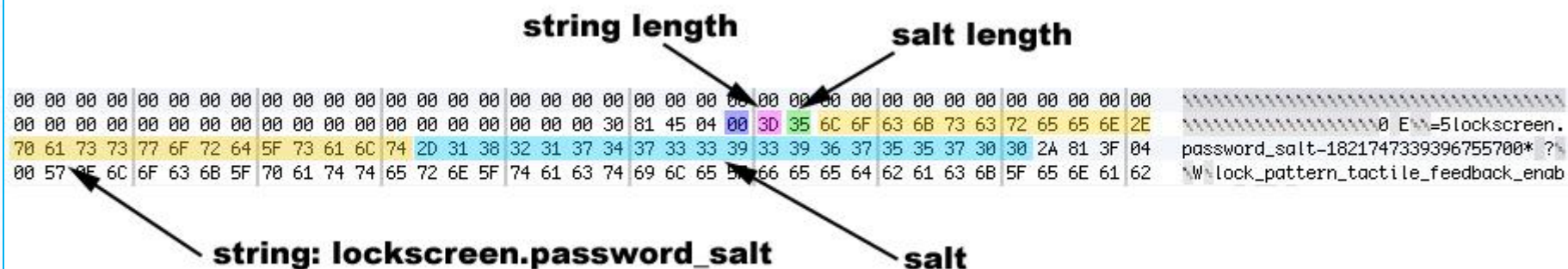
2.6 Android手机内存镜像获取

- Android手机在root后，可在线获取镜像，**不依赖SD卡**，直接镜像到本地。
- 可在线恢复手机中特定文件类型（文件签名）
- 可恢复手机内存中的已删除文件。



2.7 JTAG获取手机密码

- 借助JTAG技术dump手机内存再分析密码
- ORT Box
- Riff Box
- Medusa Box



2.8 手电筒轻松破解图形锁

- Android用户大部分采用图形锁来保护手机，长时间使用在屏幕上会留下痕迹。



3. iOS系统安全现状

- iOS系统较为封闭，第三方应用APP均需经过严格审核才能上线，在未越狱状态下，系统相对安全。
- iOS越狱后，与Android存在类似的平台安全性隐患，系统安全等级下降。
- iOS也存在一定数量的系统安全漏洞。



3. iOS系统安全与取证

- 安全漏洞
- 数据存储安全
- iOS 8安全机制变化

3.1 iOS系统安全漏洞

- iOS同样存在一些系统安全漏洞，2013年7月美国乔治亚州理工学院的华裔科学家比利·刘和博士生张永进展示了他们研发的一款假的iPhone充电器，名为“Mactans”（黑寡妇蜘蛛）。



3.2 iOS开机密码

- 开机密码(PASSCODE)容易被破解
 - iPhone4
 - iPhone 3GS
 - iPad1
 - iPod Touch3
 - iPod Touch4



3.2.1 iOS开机密码

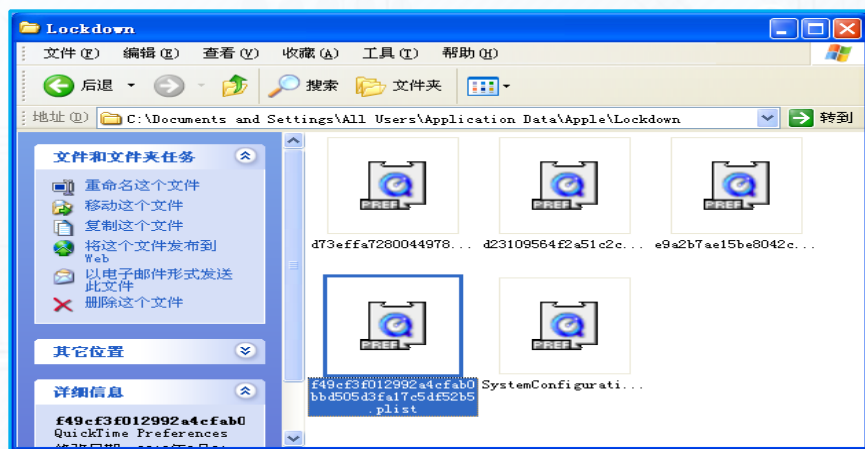
○ DFU技术的应用

- 破解开机密码
- 获取物理内存镜像



3.2.2 iOS的开机密码

- iOS设备连接PC后，成功同步后，在PC上留下一个同步密钥；借助该密钥可绕过开机密码进行手机数据提取和分析。



3.2.3 Touch ID指纹识别

- 苹果公司将指纹识别技术第一次应用在iPhone 5S手机上，将引发新一轮的智能手机的身份验证革命。提供手机安全性的同时也简化了身份验证繁琐的输入用户名和密码的操作过程。
- 据国外的最新测试，iPhone6的TouchID仍然可以绕过。



3.2.4 iPhone FileRelay漏洞

- iPhone未越狱，采用iTunes隐藏服务接口file_relay，读取iPhone除通话记录外的所有数据。
- iOS8已经关闭该服务。



3.2.5 iPhone数据存储

- iPhone4S/iPhone5/5c/5s/iPhone6/iPhone6 Plus及后续的产品都支持通过Passcode保护硬件加密密钥，对手机芯片中存储的数据进行加密。
- 即使未来可借助DFU或采用芯片编程工具获取手机内存数据，如无法获得密钥，加密数据仍然将无法读取。

3.2.6 iTunes备份数据

- iOS设备均可通过iTunes同步软件备份iPhone、iPAD及iPod Touch等终端的数据，并支持对数据进行加密保护。

Win 7/Win 8

Users/(username)
Computer/Mobile

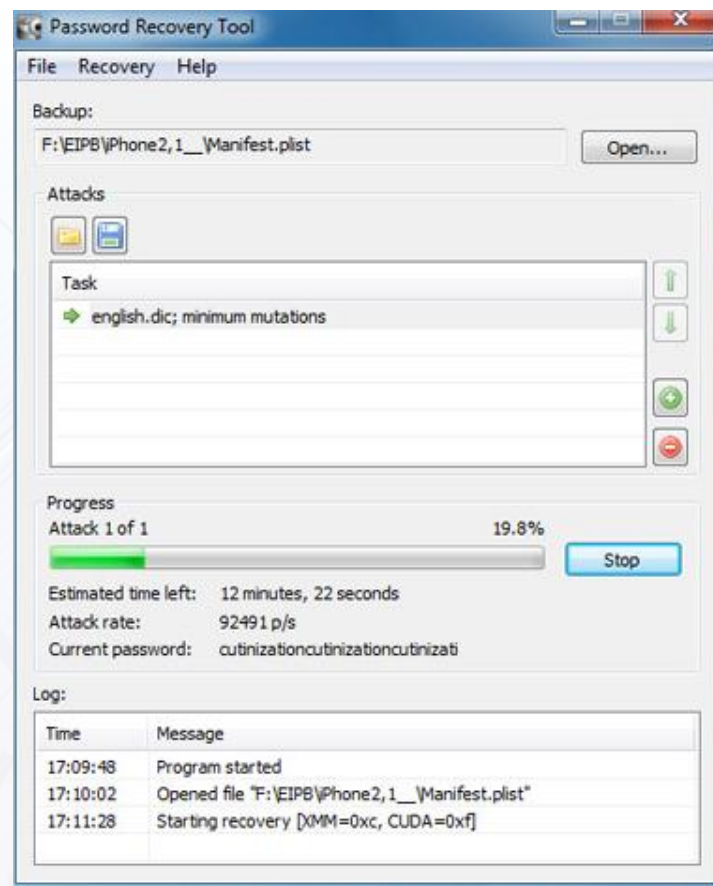
Mac OSX

~/Library/Application



3.2.6 iTunes加密备份的破解

- iTunes加密备份可通过某些解密工具破解原始密码或直接绕过。
 - ⑩ Passware Kit Forensic
 - ⑩ Elcomsoft Phone Password Breaker



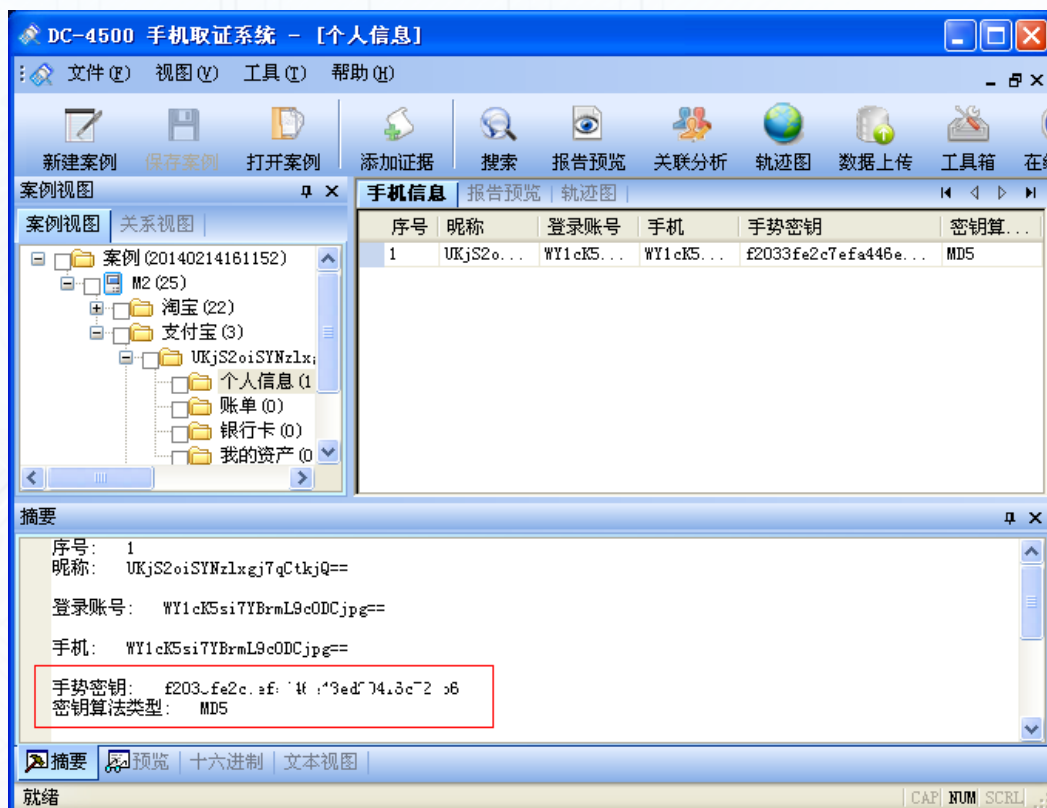
3.3 手机芯片中的数据安全

- 智能手机及山寨手机中存储芯片中的数据通过一些特有的编程器来提取手机内存镜像，并通过工具解析其文件系统，可恢复出完整文件系统及各种已删除数据。



3.4 应用程序密码安全

- 智能手机中的各类应用程序由于经常使用，大多数用户保存了登录帐号及密码，然而用户密码安全也值得关注。



4. 系统安全机制新变化及挑战

- 美国“棱镜门”斯诺登曝光美国NSA滥用权力获取数据，该事件让数据的安全及个人隐私保护得到关注。



4.1 Android系统安全机制新变化及挑战

- 2014年10月即将发布正式版的谷歌Android L系统，该系统默认将开启数据加密功能。实际上从2011年安卓系统(Android 3.0)中就已经有数据加密功能了，但是它隐藏的很深，并且有着吓人的提醒，因此很少有人会真正开启过它。



4.2 iOS系统安全机制新变化及挑战

- 面对公众对数据安全存储的关注（特别是涉及个人隐私数据），苹果公司2014年9月发布最新的iOS 8系统，该系统在数据安全保护（个人隐私）做了较大改变，以期得到用户的认可。



常去地点

○ iOS 8对原来曝光的涉及个人隐私数据采取加密

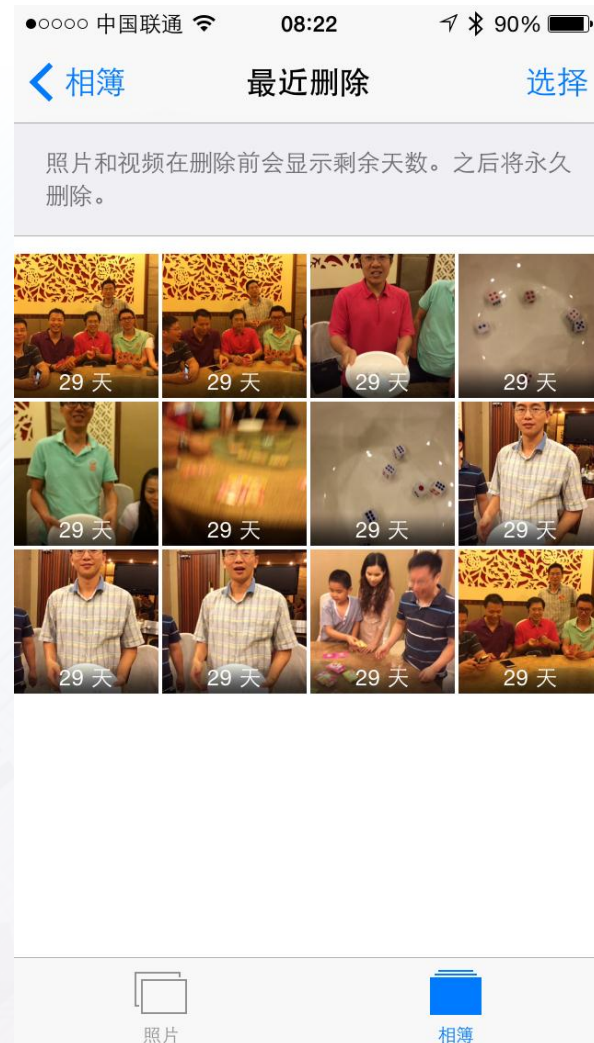


家庭	>
自 2014年8月4日 以来记录到 37 次访问	
厦门市	>
自 2014年8月4日 以来记录到 31 次访问	
厦门市	>
自 2014年8月9日 以来记录到 3 次访问	
后埭溪路	>
自 2014年8月16日 以来记录到 3 次访问	
江华里	>
自 2014年8月17日 以来记录到 3 次访问	



删除图片

- iOS 8 增加删除图片回收站功能
- 默认保存30天
- 使用不当易造成隐私泄露



随机MAC地址

- iOS 8加入了MAC地址的随机变换功能，使得你的手机在未接入Wi-Fi的时候MAC地址出现变化，导致无线局域网无法追踪你的手机，相对于以往的永久性标识来说，随机标识更加隐蔽安全性也更强。

MAC Address



In iOS 8, Wi-Fi scanning behavior has changed to use random, locally administrated MAC addresses

- Probe requests (management frame sub-type 0x4)
- Probe responses (management frame sub-type 0x5)

The MAC address used for Wi-Fi scans may not always be the device's real (universal) address

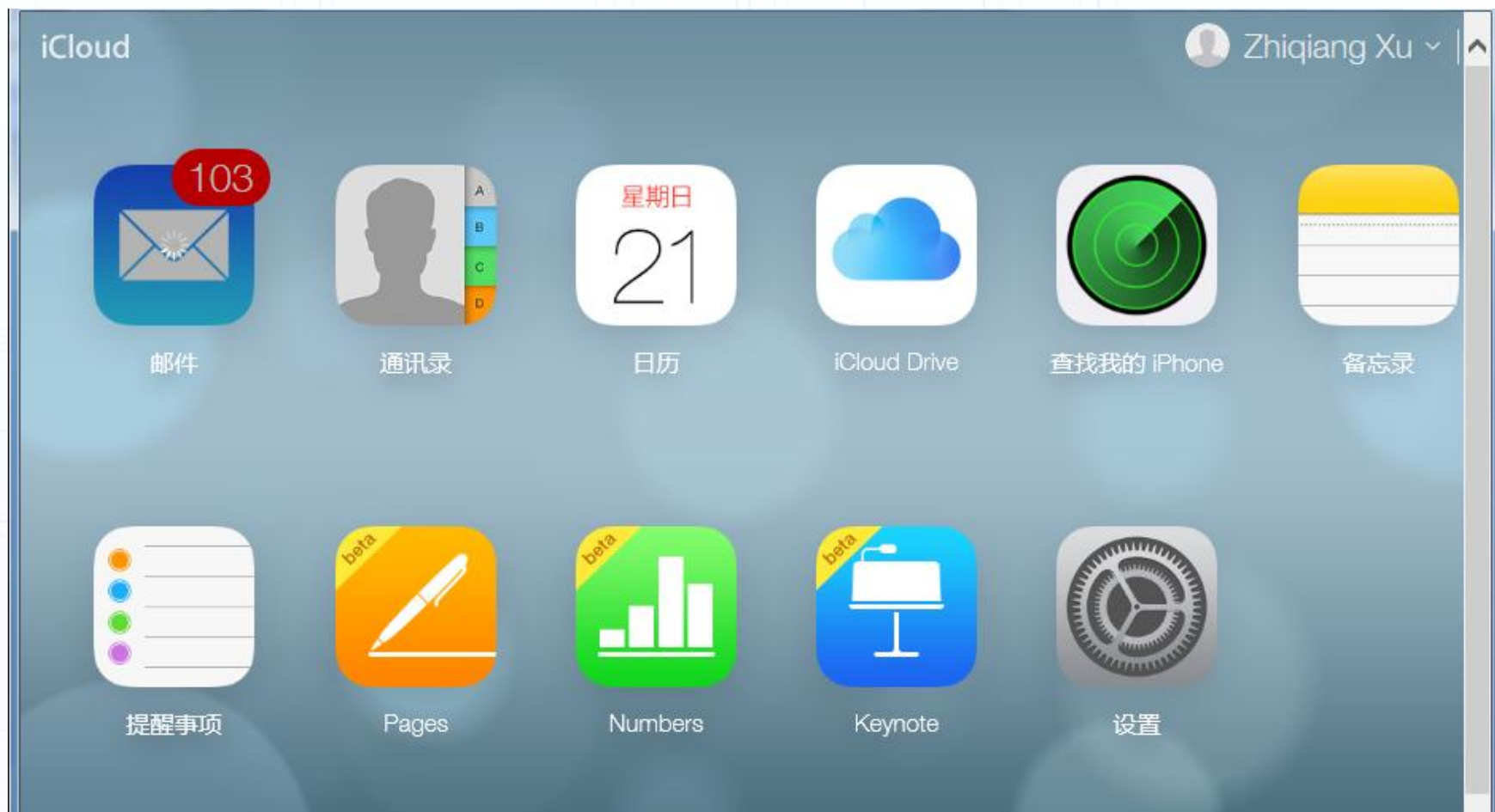
两步验证 (Two-step Verification)

- 两步式验证是 Apple ID 的一种附加安全功能，旨在防止任何人访问或使用您的帐户，即便其知道您的密码。
- 两步式验证要求您在执行以下任意操作之前，使用您的其中一部设备验证您的身份：
 - 登录“[我的 Apple ID](#)”以管理您的帐户
 - 在新设备上登录 iCloud 或 访问 [icloud.com](#) 站点
 - 通过新设备在 iTunes、App Store 或 iBooks Store 中购物
 - 获取 Apple 提供的与 Apple ID 相关的支持



iCloud两步验证

- 两步验证可提升iCloud的安全性，减少个人隐私数据的泄漏。



数据安全保护

- iCloud 通过以下方式确保数据安全：通过互联网发送数据时对数据进行加密、在服务器上保存数据时以加密的格式存储。
- iCloud 使用至少 128 位 AES 加密 - 安全级别可与大型金融机构相媲美 - 并且从不向第三方提供加密密钥。



iCloud 安全性

数据	加密		备注
	传输 中	服务器 服务器	
日历	是	是	至少 128 位的 AES 加密
通讯录	是	是	
书签	是	是	
提醒事项	是	是	
照片	是	是	
文稿云服务	是	是	
备份	是	是	
查找我的 iPhone	是	是	
查找我的朋友	是	是	

iCloud 安全性

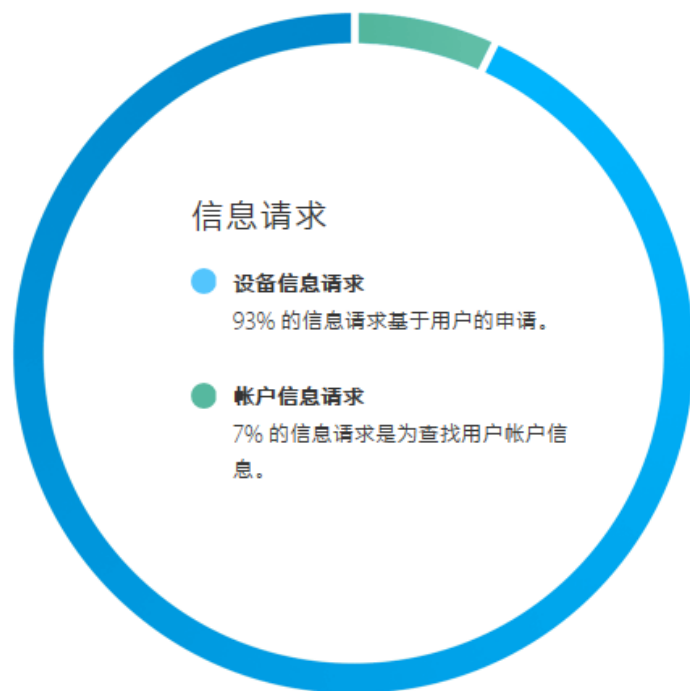
iCloud 钥匙串	是	是	使用 256 位的 AES 加密来存储和传输密码和信用卡信息。并且还使用椭圆曲线非对称加密和密钥加密。
iCloud.com	可以	不适用	iCloud.com 上的所有会话均使用 SSL 加密。如此表所示，通过 iCloud.com 访问的任何数据均在服务器上加密。
回到我的 Mac	可以	不适用	回到我的 Mac 不会在 iCloud 上存储数据。从其他电脑获得的数据在传输中使用 SSL 加密。
iTunes 云服务	可以	不适用	由于已购或匹配的音乐文件不包含任何个人信息，因而未在服务器上加密。
邮件与备忘录	是	否	设备和 iCloud 邮件与备忘录之间的所有通信都使用 SSL 加密。与标准行业惯例一致，iCloud 不会加密 IMAP 邮件服务器上存储的数据。所有 Apple 电子邮件客户端均支持可选的 S/MIME 加密。

隐私政策

- 在我们收到的来自执法机构的信息请求里，最常见的形式表现为“**设备信息请求**”或“**帐户信息请求**”。
- 苹果法务部门会认真审核每项请求，确保请求符合有效的法律流程。所有内容请求都必须持有调查函。
- <http://www.apple.com/cn/privacy/government-information-requests/>



隐私政策



[阅读 Apple 的透明度报告 >](#)

设备信息请求

Apple 收到的来自执法机构的绝大多数请求，都与用户请求协助查找被盗设备有关。如果用户怀疑自己的设备被盗，我们鼓励用户去联系相应的执法机构。

帐户信息请求

Apple 在回应帐户信息请求时，通常会涉及提供某位用户的 iTunes 或 iCloud 帐户信息。只有一小部分执法请求会索取电子邮件、照片，及其他存放在用户 iCloud 或 iTunes 帐户中的内容。

不足
0.00385%

的用户数据因政府信息请求而披露

小结

- 了解智能手机系统中的安全机制，并正确使用。
 - 启用系统的数据加密 (如Android L)
 - 启用系统安全保护机制 (如iCloud钥匙串)
 - 启用手机备份数据加密
 - 启用云服务帐号增强身份验证 (如两步验证)
 - 启用应用程序的第二重保护机制

小结

- 了解涉及个人隐私数据的开关，慎重使用。
 - 常去地点
 - 位置服务(GPS)
 - 无线网络及蓝牙功能
 - App信息分享功能
 - 彻底清除已删除文件(如iOS8 最新删除照片)

小结

- 要养成良好的安全意识
 - 不随意对手机系统进行越狱、Root
 - 不随意安装未知来源的第三方应用（推荐通过安全商店Apple Store、Google Play下载）
 - 不随意通过手机发送敏感信息
 - 不轻信已认识的联络人发送的文件及URL
 - 输入密码时注意周边是否有人偷窥

THANK YOU

新浪微博：计算机取证研究

微信：digitalforensics

QQ: 7850350