

# 天翼：加密手机，独此一家

2014年7月11日，中央电视台新闻频道（CCTV13）“新闻直播间”报道，苹果公司iOS系统会记录用户曾去过的地点，有泄露用户隐私的可能。即在苹果手机系统中，系统数据文件以明文形式，详细地记录了用户常去的地点及次数，堪称绝佳的跟踪器。

随之而来的是《新闻晨报》8月13日报道，因苹果手机频频曝出的信息安全漏洞，上海的不少机关公务员纷纷更换国产加密手机来规避信息泄露的风险。

在信息安全面前，大到国家，小到个人，都要保持高度警惕性。“保密无小事。”在手机功能越来越强大的今天，主流媒体报道的信息安全问题，值得每一个机不离手、享受智能手机带来便捷服务（如手机通话、手机购物、手机理财、手机上网等）的市民们高度重视，以避免不必要的经济损失。

而众说纷纭的加密手机，由于技术的限制，三大运营商中，目前只有中国电信的天翼手机才可以提供加密通信服务，因为该业务只能基于CDMA技术。

那么，天翼手机又具有加密手机的哪些特殊法宝呢？

## 手机卡可以被复制吗？

复制手机SIM卡可能吗？复制出的卡能实现跟踪窃听别人电话短信的功能吗？用复制出的卡能打出电话吗？本报记者按照网站上提供的方法，试验复制五部手机的SIM卡，结果有四部都成功了。记者在复制的过程中发现，除了电信的天翼手机卡不好复制外，其他的电话卡复制起来都相对容易多了。

在部队从事通讯行业15年的软件工程师寇先生告诉记者，KI是制卡的时候就以特殊工艺烧进SIM卡的一个参数值，由32个十六进制的字符组成，如D17F20239EEDBE1520F64A851F3C44\*\*。

“SIM卡扫描软件的原理是利用Comp128算法的冲撞漏洞来计算KI。”寇先生说，KI由KI0~KI7，8个子KI组成，每个子KI是双字节，子KI的所有组合是 $256 \times 256 = 65536$ 个。以每小时14000个计算， $65536/14000 = 4$ 小时40分钟左右可以跑完一个KI对。也就是说，理论上在5小时内就有可能破解KI值，复制一张新卡。最多40小时就可以跑完所有KI组合并复制一张电话卡。

那天翼的手机卡为什么无法复制呢？这是因为天翼手机采用的是CDMA技术。CDMA采用的是先进的伪随机码技术，用长达42位的伪随机码来标识区分用户，每次

通话都有4.4万亿种可能的排列，创造出万花筒般的码址变化，复制软件根本无法计算CDMA的编码，也就谈不上复制天翼手机卡的KI值了。这就好比如博彩，如果把GSM比作福彩3D，那CDMA就是双色球了！福彩3D中大奖的概率是千分之一，而双色球中大奖的概率是1772万分之一！

## 移动网络可以被破解吗？

艺术来源于生活，当科技不断进步，人们发现美国大片里出现的种种高科技桥段已经突破荧幕，出现在日常生活中。

“只需一部普通手机，加上开源软件，就能在GSM网络上秘密跟踪到手机用户地理位置”，近日，一位IT人士在微博中写道：“在试验中，无需电信服务商的额外帮助，实验人员就在10个街区的范围内跟踪到目标！”这不禁让人想起一些谍战片中的跟踪桥段，看不到对方，却不知道对方所处的经纬度，与谁联系，甚至联系的内容，这就是轰动一时的“GSM Hack”技术。

该技术是由德国研究人员卡尔斯滕诺在2009年12月27日于柏林举行的安全技术会议Chaos Communication Congress上所做的名为GSM: SRSly?的讲座上演示，他本人已破解了GSM技术的加密算法。换句话说，只要是有心人，就很容易破解GSM网络。

但迄今为止，尚无人宣称自己破解了CDMA网络。这是因为，CDMA网络采用的是扩频技术，即将原先要传输窄带信号扩展成一个宽带信号，扩展后的信号带宽比原有的窄带信号带宽要大100多倍，这样一来，信号的能量被分散到一个很宽的频带上，使信号淹没在一种很大噪声里，用户的信号被隐藏在不相干的信号之中，要想听到有用信号变得非常困难。

## “窃听风云”真实存在吗？

从外观上来看，加密手机和普通手机没什么区别。二者之间微妙的区别是，出厂时在声码器，也就是手机屏幕上的通话话筒后面增加了一个加/解密模块。每拨打一次电话，屏幕上除了绿色拨号键，还有一个红色的加密键，点击红色加密键就可进入加密通话模式。

这个加密键与中国电信集团内部信息中心连接，系统会对SIM卡号、手机号码、唯一的机身验证码予以核实，

只有三个信息均符合后，才会下发一个类似于验证码的“密钥”，随后进行主叫与被叫功能。换句话说，天翼手机是以网络端（SIM卡）、手机端双重加密形式，实现了机主通话的全程加密。

“如果普通通话过程中，说着说着，觉得通话内容比较敏感，也可以转入加密模式，大概1秒左右，就会转移过去。”整个验证操作过程历时仅需1至2秒，而且加密算法确保每次通话的加密密码都不一样，实现了“一话一密”。

## 手机丢失后信息会泄露吗？

如果加密手机不小心丢失，也不用担心手机里面保存的信息被泄露，机主可以立即与电信方面联系，工作人员会启动中国电信远程删除指令，只要该手机再次开机，里面所有的信息就会被自动删除。

“很多智能手机的内存信息在其后台或者‘云存储’端是可以看到的；但电信加密手机里面的内容，连电信本身也无法知道或者破解，只能提供删除指令。”中国电信工作人员强调。

以全球首款4G双卡双通手机酷派S6为例，其手机内部有防盗模块，当手机丢失后，拾机人换上新卡，一样可以输入密码后正常开机，但无法获取手机内原有的通讯记录及短信记录，仅能开启基本的通话功能。一旦拾机人拨通了电话，其通话信息会在第一时间反馈到机主的关联手机上，机主可启动远程删除指令，删除相关信息，并立马锁定拾机人，追讨手机。

## 恶意软件手机无法阻挡吗？

国产加密手机通常包含有主打“安全”的功能，即云时代的“云安全”功能整合数据保护、流量监控、病毒杀毒、系统优化、通信卫士和省电管理几大功能，提供深度系统防护的同时独具优势。

其中数据保护功能，可有效拦截含有木马程序的恶意软件，防止第三方软件窃取相关信息，为手机上网安全保驾护航。流量监控保护，随时盘点清算，进行流量统计，及时为流量大户控制上网模式。防窃听功能，可以有效防止在通话过程中被窃听，保证机主的通话安全。私密保护，隐藏重要手机信息，内容涵盖联系人、通话记录、短信息等众多私密信息。

小贴士：即日起，加密通信业务在中国电信各营业厅均可优惠办理，详询10000！



# 天翼，安全可靠



## 全网通 安全手机



华为 Ascend Mate 7

- 芯片级安全OS, 360°按压式指纹传感器
- 6英寸1080P屏幕, 7.9mm金属机身
- 智能超八核芯片, 4100mAh超大电池



酷派 铂顿

- 双系统, 一键毫秒级快速切换
- 硬隔离, 安全系统独立存储、运算
- 铂顿拥有最高商用级别加密芯片



华为 麦芒3

- 国家商密级认证, 全程加密
- 5.5英寸全贴合瀑布屏, 金属纳米工艺
- 智能省电技术, 超长待机

中国电信号段：189、181、180、153、133、177

www.189.cn

天翼客服 kefu.189.cn

中国电信 CHINA TELECOM

世界触手可及

