第三只耳是怎样偷听的

■专家解密五种窃听方式，对比看看你是否曾遭遇其中一种
■3G手机和CDMA手机凭什么比普通手机更安全
■装上“安全芯片”的手机就真的安全了吗

“无需母卡能复制手机SIM卡窃听任何人的通话。”“想知道妻子(老公)领导或生意伙伴的通话、短信内容吗？××最新科技，一切尽在您的掌握之中。”“……”不经意的哪天，你就会收到类似的短信。

而电影《窃听风云》中，吴彦祖的对话更让人惊悚：“现在每个人身上都有窃听器，我们的GSM阻截器只要输入目标的手机号，就可以截听到对方的通话，哪怕对方没有开机，只要电池没有拆掉一样能听到。”这些难道是真的？那些“第三只耳”是怎样偷听我们的呢？

在人多处打开手机蓝牙功能，信息极易失窃

在手机中安装微型窃听器，是最老土的贼耳

被“偷”指数：★★

每天随身携带的手机，一直都在出卖着我们吗？我们的私密通话又是怎样被“传播”出去的呢？带着一肚子的疑惑，记者昨天来到了东南大学信息安全研究中心。多年来，信息安全研究中心主任胡爱群教授一直致力于移动信息安全技术的研究，同时他也是江苏省信息办信息安全咨询专家。

胡教授告诉记者，“相对于传统的电话而言，手机窃听的技术含量更高。”因为固定电话在通话时传输的是模拟信号，并没有加密措施，如果窃取了这段信号，很容易还原成语音。手机信号发送到空中，传输的信号是加密的，想要破译还得费点心思。可即便如此，手机窃听还是肆无忌惮地发生着。例如，在手机中安装微型窃听器，就是一种最原始、最老土的窃听方式。

可是，我们打开手机后盖，手机里的零部件排得十分紧凑，哪里还有安装窃听器的空隙呢？胡教授解释说：“空间还是足够的，纽扣大小的窃听器都能安装进去。”比方说手机电池，完全可以做成只有原来一半大小，这样就有足够的空间了。不过，这种窃听方式，传输距离多半在几十米左右，也就是说，如果想要监听手机通话，必须在一定的范围内，再远就失效了。

专家支招：
不要让陌生人靠近你的手机

专家提醒，如果手机被安装微型窃听器，一般不太容易发现。因此建议大家在购买手机、维修手机时，最好到正规专业的店去，手机最好不要借给陌生人使用。还有，别人赠送的手机也要留个心眼，说不定那就是一部“改装”手机。另外，如同电影里的防窃听一样，如果你有非常机密的通话，也高度怀疑有人窃听，不妨学电影的情节制造噪音。因为，窃听器都一样，对噪声也很敏感。周围很嘈杂窃听效果就大受影响。

伪基站，半路“劫”走通话信号

被“偷”指数：★★★

热播的港片《窃听风云》中，其台词中说“我们的GSM阻截器只要输入目标的手机号，就可以截听到对方的通话”。影片中的“GSM阻截器”像电脑机箱一样，这个方方正正的家伙真的有那么大能耐吗？

GSM阻截器其实就是一个伪基站。相隔数万里的人们能够通过手机对话，靠的就是附近的基站。一方面，基站接收信号，另一方面又负责将信号传递出去，在通话者之间充当着“桥梁”的作用。而这个伪基站并不传输信号，只接收信号。

伪基站大小不一，规模小点的伪基站和电脑主机差不多，但是它却能接收到周围所有的通讯信号。虽然接收那么多信号，但这个阻截器可以聪明地辨别，找到打算窃听的那个手机。奥秘就在伪基站能在空中获取每部手机的IMSI号。IMSI号就像手机的“身份证号”，独一无二。伪基站获取这个号码后，这个手机上发出的所有信号都被拦截。

专家支招：关机状态基本安全

只要上网搜索一下，兜售“GSM阻截器”的信息就不断跳出来，卖家叫价并不高，三四百元一套。如何防止这样的窃听呢？“一般情况下，手机处于真正关机的状态就进入安全状态了。”胡爱群解释，如果再把电池拔了就更安全了，因为在没有通电的情况下，任何芯片都不会发挥作用，手机当然也不例外。当然，这也并非绝对的，如果你的手机被人“改装”过，里面多了一块充电电池，那很有可能仍被监控。为了防止窃听，还有一招——手机关机，放在密闭的金属盒中。

手机“黑客”，无孔不入抢钱不商量

被“偷”指数：★★★★★

电脑病毒让网民们苦不堪言，实际上，手机也有病毒！手机“卧底软件”早已不是传说，这个软件也叫手机间谍软件。一旦你的手机“中招”，你就毫无隐私可言了。

手机“黑客”比伪基站更可怕，它们几乎无孔不入。“全世界手机病毒种类估计有1000种左右。在我国，由于大家对手机的认识大多还停留在打打电话、拍拍照上，用来上网的人还不算多，所以中毒的现象相对少，而国外手机中毒现象时有发生。”

胡爱群说，刘奶奶的手机被“劫持”就是很明显的中毒现象。手机病毒就是一段程序，如果你用手机上网，就很容易中毒。中毒后的手机非常“疯狂”，它会造成手机关机的假象，让手机黑屏，键盘失效；中毒手机还可以自动开机，泄露手机所在环境内的一切信息。

中毒后，手机除了会自动开关机外，还会被用来自动给别人发短信，自动拨打电话，自动上网，甚至会破坏SIM卡芯片。有些不良商家，就利用手机病毒，把广告信息、垃圾短信通过中病毒的手机发给其他人。“他既做了广告，而且还不用花一分钱。最倒霉的还是中招的手机主人。”更有甚者，为了发泄情绪，会利用你的手机把骂人的话发给身边的人。

中毒的手机如果和电脑联网，就连电脑也会“感染”中毒；如果和固定电话联网，固定电话就会“出卖”你。

那么你的手机什么情况下会中招呢？胡爱群笑了：“中病毒的途径太多了！你是一个喜欢上网的人，病毒程序就通过电脑传到你的手机上；为了和好朋友共享一首歌曲，你开通了蓝牙或红外，而病毒就通过蓝牙(红外)入侵到了你手机上，出现手机不断初始化，其实，你的所有个人信息都被手机给卖了。彩信也同样不安全，病毒没准就种在彩信里。”

专家支招：不妨用用杀毒软件吧

中毒的手机，可以用杀毒软件攻克。只是，杀毒软件总是赶不上新病毒产生的速度。以目前的水平，一旦你手机中病毒了，那就向运营商申请手机安全增值服务，或者换个新手机也行。专家提醒那些喜欢用手机上网的人们，如果没什么要紧事，尽量不要用手机上网。“用手机上网时间越长，中毒风险越大。”还有，不要随意开蓝牙和红外，不要随意下载不明来源的软件。

SIM卡复制，悄悄偷走你的隐私

被“偷”指数：★★★

在网络上，“无需母卡就能复制手机SIM卡窃听任何人的通话”的群发短信又骤然找到了“顺风车”。不仅是通过群发短信方式发布这种消息，记者在网上也搜索到众多叫卖SIM卡复制器的帖子，价格从1000多元到3000多元都有。

胡教授说，在有母卡的情况下，复制SIM卡是件很容易的事情，“类似于我们拷贝其他文件，只要有了机器设备，谁都能做到。”比如，前文提到的吴桐，他的SIM卡，就有可能被别人复制了。而那位小郭，他的手机信号之所以被泄露，有可能是他朋友的SIM卡被人复制了，而那张卡里，正好存有小郭的号码。还有小林看到的那个广告，如果对方真能够做到用一个小芯片窃取手机机密的话，可能也是利用SIM卡复制技术。

不过，在没有母卡的情况下，复制SIM卡的难度其实相当大。胡教授告诉记者：“知道SIM卡的加解密方法、国际身份认证识别码等数据，必须利用高科技进入运营商系统，这可能性极小。网上叫卖的这些无需母卡即可复制，应该是骗人的。”当然，胡教授说，也不排除有些人会非法利用高科技进入运营商系统，所以手机用户一定要看好自己的SIM卡。

专家支招：遗失SIM卡后尽早挂失

专家提醒，一般情况下，防止SIM卡被复制，手机用户只要保管好自己的手机SIM卡以及密码，不法分子就不可能凭空克隆手机卡。用户一旦丢失SIM卡，应该立刻去挂失。

人多之处开蓝牙，差不多等于当众裸体

被“偷”指数：★★★

蓝牙让人们享受到了信息共享的惊喜和愉悦，但是，就在你感受到这份快乐的同时，也潜伏着危机。

据说，“蓝牙”原是一位在10世纪统一丹麦的国王，他将当时的瑞典、芬兰与丹麦统一起来。用他的名字来命名这种新的技术标准，含有将四分五裂的局面统一起来的意思。

蓝牙是一种短距的无线通讯技术，电子装置彼此可以通过蓝牙连接起来，省去了传统的电线。通过芯片上的无线接收器，配有蓝牙技术的电子产品能够在十米左右的距离内彼此相通。

在国外，流行用手机交换电子名片，通过蓝牙发送，但是没准电子名片里就带有病毒，一点开立刻中招。最悲惨的是，你无意间开通了蓝牙，手机里的秘密完全泄露了，你都还不知情。

比如，前面讲到的鲍峰，后来经过朋友提醒，他意识到可能是自己手机的蓝牙功能被无意中打开了。鲍峰找到蓝牙功能，发现果然是开着的。

专家支招：别在人多处开蓝牙

由于无线可以穿墙，一旦你蓝牙开了，就是“隔墙有耳”。如何才能安全？胡爱群说，蓝牙传播的范围相对有限，人多的地方、混杂的地方不要开蓝牙，这样你就进入了相对的安全地带。当然，如果你根本不用蓝牙，你的世界就真清净了很多。还有，可以经常检查一下你的手机蓝牙功能是否开启，在不用时，应及时关闭。

»相关链接

3G手机凭啥更安全

目前市场上，虽然3G手机已经横空出世，但使用者还是没有2G(也称GSM手机)和2.5G(CDMA手机即属于2.5G)的多。而在东南大学的课题中，有的教授已经着手研究4G通信技术。有一种说法是，2.5G手机相对安全。真是这样吗？

专家说，手机信号的传输，其实就像谍战片里演的那样，通过无线传输，然而，现在已经有专门的解码软件诞生。而CDMA手机，在空中传输的过程中进行了加密，而且和GSM的加密方式不同，不容易被截获。

“为了减少功耗，使得待机时间长，CDMA手机加密编码程序相对简单；而3G手机解决了集成电路的问题，在减少功耗的同时，又在密码上更加复杂，更为安全。”胡爱群说，3G手机在信息安全上更加可靠一些，目前非专业人员还破解不了。

不过，“空中”安全并不代表手机就安全了，手机病毒实在太厉害了，遇上了手机黑客，也只能惨叫一声。

未来流行 手机带个“安全芯片”

难道手机的安全问题真的解决不了？面对形形色色的窃听大法，记者不由感叹。

“要维护手机安全，厂商在开发手机时就可以安装一个特殊的芯片。”胡爱群教授告诉记者，他就在研制这样的芯片，目前方案设计部分已经完成，需要经过严格的验证后再制成芯片。这是一个国家863科研项目——移动终端安全防护系统研究。

芯片并不大，但是有了它手机就真的安全了。在开机或者关机的时候，小芯片就开始“工作”，它将会检测手机系统的完整性有没有被破坏，一旦发现异常，就会发出警报提示。当然，如果发现突然增多了一个软件或病毒，它也会发出警示信息，并且帮你清除手机里的病毒。

不过，要使得这个芯片真正发挥作用，还需要手机运营商的大力支持。胡爱群介绍，普通的手机用户很难辨别到底该对警报提示作出何种反应，该点击“是”还是“否”，这就需要运营商的配合。对一些不合法的软件，需要由运营商帮助拦截，构建一个安全服务体系。

本版主笔
快报记者 胡玉梅 谢静娴

网上叫卖的一种手机窃听器