手机随时可能变成窃听器？解密“第三只耳”如何偷听

电影《窃听风云》中，吴彦祖的一句台词让人不寒而栗：“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。”这是真的吗？那些“第三只耳”是如何偷听的？看看专家对五种窃听方式的解密吧。

最老土
手机里装微型窃听器

被“偷”指数：★★

东南大学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，他也是江苏省信息办信息安全咨询专家。

胡教授告诉记者，“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，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。如果怀疑有人窃听，不妨学电影的情节制造噪音。因为所有窃听器都对噪声很敏感，嘈杂环境中窃听效果就大受影响。

最霸道
伪基站半路“劫”信号

被“偷”指数：★★★

相比之下，“GSM阻截器”的技术含量就更高了。手机通信靠的是附近的基站，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。GSM阻截器其实就是一个伪基站，它不传输信号，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

如何防止“GSM阻截器”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。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。

最狠毒
手机“黑客”抢钱没商量

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，全世界手机病毒种类估计有1000种左右。手机中毒后，不仅会自动开关机，还会自动发短信、自动拨打电话、自动上网，甚至会破坏SIM卡芯片。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。

“中病毒的途径太多了！”胡教授说，“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<<<
不妨用杀毒软件

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。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。

最迷糊
SIM卡复制偷走你的隐私

被“偷”指数：★★★

在网络上，有很多叫卖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。”前文提到的吴桐，他的SIM卡就可能被别人复制了。

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。

网上叫卖的一种手机窃听器。

最隐秘
人多开蓝牙几乎是当众裸体

被“偷”指数：★★★

蓝牙是一种短距离无线通讯技术，通过蓝牙，电子装置不用数据线就能彼此连接。通过芯片上的无线接收器，配有蓝牙技术的电子产品能在十米左右的距离内彼此相通。

在国外，流行用手机蓝牙功能交换电子名片，但是没准电子名片里就带有病毒，一点开立刻中毒。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。

专家支招<<<
别在人多处开蓝牙

由于无线可以穿墙，一旦你的蓝牙开了，就是“隔墙有耳”。胡爱群说，人多混杂的地方不要开蓝牙，这样你就进入了相对安全地带。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。（本版据《现代快报》）

他跟老婆的聊天短信　为啥别人一清二楚

前段时间，吴桐（化名）换了部时尚的新款手机，是客户请他办事时送的，还顺带送了一个号码，是个靓号。

但很快，一些令吴桐不解的怪事出现了。刚刚和业务单位通了电话，约好了见面详谈。到了对方公司才发现，已经有人早一步到了那里抢占先机；自己和老婆谈的私事，第二天在QQ上竟有人拿来打趣。

“你小子，不会是手机被人窃听了吧，别干坏事噢！”说者无心听者有意。吴桐悄悄拆开手机，可没发现什么异常，也没有多出什么窃听器模样的东西。

莫非这部白得的手机被人做了什么手脚？吴桐开始怀疑那个送他手机的客户。

一天，吴桐没打招呼就闯进了这个客户的单位。门开着，一部陌生的手机通过USB连接着电脑，屏幕上显示着一排排短信内容，竟是吴桐和老婆的短信聊天记录！吴桐当场就傻了。

□相关链接

未来手机流行带个“安全芯片”

难道手机的安全问题真的解决不了？

“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，这个芯片要真正发挥作用，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，需要运营商帮助拦截，构建一个安全服务体系。