警惕黑客新招——耳机瞬变麦克风

郝耀鸿 王立金 朱学军 顾 茜 / 广州市国资委

前段时间，朋友圈被一则消息刷屏，以色列本·古里安大学的研究人员开发出了一款名为“SPEAKE（a）R” 的软件，该软件的特别之处在于，能够控制目前在我们电脑中使用最为广泛的一款声卡——瑞昱（Realtek）声卡，结果令人瞠目：将没有话筒功能的普通耳机，变成一个麦克风，你以为在听音乐，其实你在被录音！那么，到底耳机如何变成一个窃听者，这其中的机理是什么，我们又应该如何防范呢？

★声波与电流★

声音是人类最原始，也是最直接的通信载体，即使进入信息网络时代，智能手机、网络电话、多媒体应用等，也无非是让声音传播变得更远、音质变得更好而已，本质上声音的传播依靠的就是电流。我们知道，声音在外太空（真空）是听不到的，而且在空气中的传播距离有限，这主要是由于空气虽然稀薄，看似透明，但空气中存在着许多粉尘、颗粒、水蒸气等杂质，这些物质一定程度上会吸收、反射、散射声音，就为空气的传播带来“阻力”，因此声音传输一定距离后就衰减没了。那该怎么解决呢？人类能够不断进步得益于我们“善假于物”，虽然声音本身传播距离有限，但可以依托传播远、速度快的“物质”——电流。

★话筒和耳机★

明白了声音和电的关系后，我们来看一看到底麦克风和耳机是怎样工作的，为便于大家理解，我们以电话为例。

声音到电流

首先，人们通过话筒，将声波（即人的声带振动引起的空气波动），转换成电流的波动，如图1所示。

就话筒实现机理而言，最重要的就是“声变电”的转化，而实现该功能的就是一组装置：振膜、线圈和磁铁。振膜顾名思义，就是对声音很敏感，当声音传播过来时，振膜就随之振动，并导致附着其上的线圈也跟着振动，而线圈缠绕的磁铁是固定的，也就是说，声波的振动

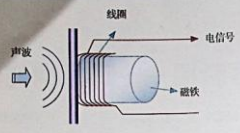

图1 动圈式话筒结构组成

最终带来磁铁和线圈之间的相对运动，带来线圈内部磁通量的变化。讲到这里，大家是不是觉得很熟悉，这不就是我们中学所学的“法拉第电磁感应定律”吗？变化的磁场产生变化的电场——电流出现了。而且这个电流是反映声波变化的，也就是说，这时电路中产生的电流携带了声音信息。

高速、长距离传输

声波直接转化成的电流，并不能完成长距离传输。这主要是因为该电流信号属于“基带”信号，频率低、损耗大。这个不难理解，拿木棍搅动水面，搅动的地方就是振源，如果我们越用力，搅动的频率越快，产生的水波纹传输的距离就越远，电流亦是如此。为了将电信号传播更远，一般采用“调制”的方式，就类似于人们外出，如果从广州到北京两千多公里的路途，纯粹靠两条腿走，那恐怕得几个月，为了加快速度，我们考虑坐高铁（人承载于火车），那时间就缩短到八九个小时；如果坐飞机（人承载于飞机），那就更短了，不到三个小时就到了。载波调制就是这个道理，既然高频信号传输的距离更远，那么就通过调制，把基带电信号（低频）承载到载波（高频），加上中继放大等措施，就实现高速、长距离的信息传输。

电流到声音

传输再远，用才是目的。信号经过长距离输送，到达目的地后，首先要解调，把低频信号过滤出来，这就类似于到站后我们下飞机、下火车。那么，电信号如何变成人们能听到的声音呢，关键就在于“电变声”，结构如图2所示。根据电磁感应定律，接收到的电流信号，会通过线圈产生一个变化的磁场，这个磁场会与磁铁的磁场产生相互作用，进而引起与线圈相连的振膜，振膜就类似于耳朵的骨膜，它的振动带动周边空气的振动——声音便产生了，我们也就听到了对方的说话，由于声音从产生到接受，中间经过“声到电”“电到声”的多次转化，同时

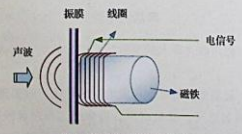

图2 动圈式耳机结构组成

在传输中信号也受到了各种各样的噪声影响，这也就解释了为什么电话里的声音与“本尊”有所不同。

＊耳机变话筒＊

通过上述讲解，相信大家都清楚了，其实细看图1、图2，听筒（耳机）结构组成与话筒（麦克风）几乎相同，硬件组成、原理实现都如出一辙，只是功能相逆罢了。可以想象，如果黑客通过病毒程序，远程控制我们电脑、手机中的声卡（Sound Card），耳机本来是单向电流输出的，比如我们听音乐，手机中的mp3音频通过振动发生装置，变成耳朵能听到的声波，但黑客夺取声卡的控制权后，会悄悄地把手机的“输出通道”改成“输入通道”，也就是说，耳机可以进行数据采集了，在我们享受音乐曼妙的同时，耳机也在偷偷收集外界的声波，窃密就这么发生了。其实这种情况不是个例外，以色列本·古里安大学的研究指出，不仅在全球使用最广泛的瑞昱声卡存在这个问题，事实上，绝大部分嵌入式声卡在某种程度上都存在这个漏洞。

＊防范措施＊

强化保密意识

无论窃密技术多先进，良好的保密意识和工作习惯永远是安全保密的“防火墙”。保持好的习惯，要经常性地学习和了解网络和通信常识，掌握其工作机理。尤其是在处理涉密资料、组织涉密活动时，要做足功课，充分考虑每一个可能的泄密环节，确保保密工作的万无一失。

加强设备检测

严格按照相关保密规定，对涉密场所、重要场地的信息设备，尤其是进口器材和产品，必须进行信息技术安全检测，在采购关键核心设备时，尽量选择国产品牌，以防不法分子在信息产品中植入病毒程序、预留后门。

严格会议制度

涉密会议必须要在符合保密规范的场所进行，未经批准，不能私自将录音、录像设备带入会场，手机、笔记本电脑应放置在会场外的保密柜中，尤其是电视电话会议更要注意会场和传输链路的安全性。

涉密办公网络严禁接入互联网

只要有连接外界的通道，被黑客入侵就是一件大概率事件。计算机就是一台硬件、软件的综合集成体，文字、图片、音频、视频，只要能想到的应用，电脑都能完成。哪怕是在涉密场所放一台能连入互联网的电脑，都有可能藏了一个窃密者。因此，应严格物理隔离，确保涉密场所的安全。M