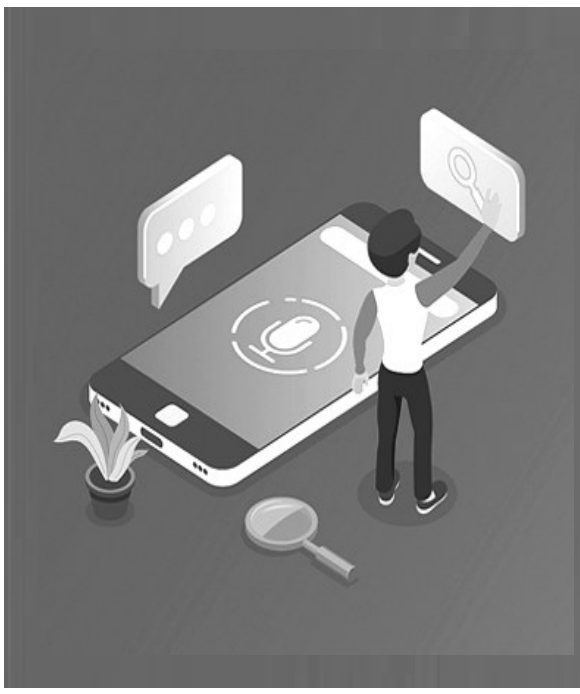
超声波攻击下，语音助手可能被“策反”！



随着人工智能和自然语言处理技术的发展，声音已经成为人机交互的重要方式。语音助手可以在很多场景下为人类提供便捷的服务，比如当你双手提着东西，不方便拿手机，可以唤醒“Siri”帮忙拨打电话；睡觉前，你躺在床上就可以通过智能家居语音助手关闭卧室的灯光而不用自己起身……然而，近期有学者发现，这些语音助手在提高我们生活便捷度的同时，也可能会在不经意间成为“泄密者”。

日前，在美国加州召开的国际信息安全界顶级会议“网络与分布式系统安全会议”上，美国密歇根州立大学严奇犇教授带领的SEIT实验室联合圣路易斯华盛顿大学、内布拉斯加林肯大学以及中国科学院的学者，披露了一种名为“SurfingAttack”的超声波攻击方式，攻击者可以通过放置手机的桌子或者其他固体接触物来传输携带指令信息的超声波，从而实现操控语音助手的效果。

“SurfingAttack”如何实施攻击？会带来哪些风险？用户以及技术厂商应该如何加强防护？《科技日报》记者就此采访了有关专家。

利用“隐身”的超声波发起进攻

在模拟的攻击场景中，智能手机被放置于普通桌子上，只见研究人员在桌子另一侧的电脑上输入代码后，没过多久便唤醒了手机的语音助手，并成功地通过语音助手让手机执行指令信息，例如使用前置摄像头拍摄等。

“SurfingAttack”之所以能够实施攻击，是基于什么原理？

“频率高于20KHz的声波，我们称为超声波，蝙蝠在飞行过程中就是使用超声波来进行障碍物定位的；频率低于20Hz的称为次声波，大象就是利用次声波进行相互交流。人耳听觉的频率范围在20Hz—20KHz之间，因此，无论是蝙蝠还是大象发出的声音，我们都是听不到的。”360安全研究院专家郝经利介绍说，而手机等智能设备中的麦克风，大部分使用驻极体麦克风和MEMS（微机电系统）麦克风，频率在10Hz—40KHz范围内的声波一般都能获得响应。

“正是基于这两个原因，‘SurfingAttack’利用人耳识别不了的超声波，向手机等智能设备的麦克风发送激活语音系统指令，接收到激活指令后，声控系统就会被激活，而这个过程我们的耳朵是听不到的。”郝经利解释说。

“SurfingAttack”虽然刚刚被揭示出来，但这已不是研究人员第一次发现这种通过外部信号注入而发起的攻击。据福建师范大学数学与信息学院黄欣沂教授介绍，2017年浙江大学研究团队首次实现了“海豚音攻击”，能够对智能语音设备悄无声息地进行控制。2018年的信息安全领域国际顶级学术会议IEEE S&P召开时，研究人员就演示了如何利用超声波对硬盘造成物理损坏，甚至可以让电脑死机。

“‘海豚音攻击’主要利用了声波在空气中的传播，遇到雨、雾、灰尘等视线障碍后，声波传播的性能就会下降；而‘SurfingAttack’主要利用声波在固体中的传播特性，通过固体介质启动攻击，不受视线障碍的影响。”黄欣沂说。

同时，“SurfingAttack”还实现了30英尺（约9.14米）的“远距离攻击”，而此前，人们发现的超声波攻击距离约为5英尺（约1.52米）。黄欣沂说，与传统的超声波攻击相比，“SurfingAttack”实施攻击过程可能会更加隐蔽。

语音助手易成为攻击对象

据了解，目前研究人员总共测试了17款带有语音助手的智能设备，其中13台设备携带了安卓系统的数字助手，另外4台设备携带的是苹果系统的Siri。

“研究人员测试发现，包括小米、三星、华为和苹果等主流手机品牌的15款不同型号的手机，在3种桌面上均受到来自该种攻击的影响，某两款来自三星Galaxy系列和华为Mate系列的手机则‘相安无事’。”北京邮电大学信息安全中心副主任辛阳表示，研究人员使用了不同材质（例如金属、玻璃、木材）的桌面分别来进行测试，发现这种攻击在所有这些材质的桌面上都可以发生。

郝经利进一步补充说，目前除了带有语音助手的手机，还有一些智能硬件设备例如智能音箱等，同样会受到超声波攻击的威胁。但是由于智能音箱的功能所限，不具备较强的攻击目的性，所以相比智能手机来说风险性较小。

那么，语音助手被“攻破”，会带来哪些风险？“该技术一旦攻击成功，便会获得相应的系统权限，利用‘SurfingAttack’，攻击者可以在用户不知情的情况下，窃取含有银行转账验证码的短信等数据，完成支付、转账等一系列操作，对用户的财产安全造成威胁。”黄欣沂说。

郝经利指出，当前语音助手所拥有的拨打电话权限也是一个很显著的攻击目标，攻击者可通过让语音助手拨打特定的电话，泄露被攻击者的电话号码等个人信息，或在用户毫无感知的情况下，利用用户的手机和合成声音进行虚假欺诈呼叫，即俗称的电信诈骗。

“SurfingAttack”的狡猾攻击方式，是否意味着如果你的手机放在桌子上，而且刚好没有锁定，黑客就能通过这种方式，悄无声息地获取你设备中的敏感数据呢？

科技日报记者了解到，事实上，发动“SurfingAttack”还需要包括超声波发射器、压电式转换器、隐藏式麦克风等硬件和软件的协同，这也使得发动攻击具备了一定的成本和技术门槛。

柔软的“铠甲”或可防御

“针对这类攻击方式，目前没有较理想的修补方案，但用户可以在日常生活中谨慎一些。”辛阳建议，较好的预防方式是用完手机之后随手锁屏，降低语音助手在锁屏状态下的权限。同时，用户在使用手机时，应尽量减少手机与桌子的接触面积，还可以在桌子上垫上一层柔软的编织物，或者使用较厚的手机壳等。

对于厂商，郝经利建议，可以通过系统升级等策略，将能够激活语音助手麦克风的声音频率做一个过滤，降低对超声波和次声波的感知，这样可以有效杜绝和防范此类攻击的发生。同时，手机厂家在选用麦克风硬件的时候，可以关注麦克风整个声波感应频率范围，选用一些仅针对人类能识别的音频范围的麦克风。

“对于普通用户来讲，不必过于恐慌，此类攻击的局限性非常大，预计未来不太可能会造成较大的威胁。”郝经利表示，当前各种智能设备的诞生在给我们提供了便利的同时，可能会带来安全隐患，在公众场合，我们应该保护好自己的智能设备，防止被不法分子攻击和利用。

与此同时，辛阳也指出，为了避免个人信息安全遭受不法侵害，除了需要提升个人的信息安全意识之外，还需要政府和行业采取相应规范措施，从整体上提升国家的信息安全水平。

“物联网技术的发展已经将人与人、人与物、物与物紧密地联系在一起。恶意攻击不仅仅局限于使用传统的技术，周围环境中的声音、震动等都可能被用来实施攻击。”黄欣沂表示，这些新变化也对做好网络空间安全防护提出了新的挑战。

（据《科技日报》）

◎科技短波

●据中国载人航天工程办公室消息，近日，中国空间站天和核心舱、天舟二号货运飞船、空间应用系统核心舱任务分别顺利通过载人航天工程主管部门组织的出厂评审，标志着空间站建造即将转入任务实施阶段。

●宇宙年龄究竟几何？这一问题一直让科学家们争论不休。近日，美国科学家对宇宙中最古老的光进行了重新观测，得到的观测结果，再加上一些宇宙几何学方面的计算，他们给出了宇宙的最新年龄：137.7亿岁，误差不超过4000万岁。

●日前，采用西南交通大学原创技术的世界首条高温超导高速磁浮工程化样车及试验线在四川成都正式启用。这标志着我国高温超导高速磁浮工程化研究实现从无到有的突破，具备了工程化试验示范条件。

●近日，数字医疗健康科技企业丁香园宣布推出专业级医疗数据开放平台，该平台为可全面覆盖药品、疾病、医院、科室、诊疗、医学资讯等多场景应用的开放式数据平台。

●中国首个海底数据舱近日在珠海高栏港揭幕，标志着中国大数据中心走进海洋时代。“海底数据中心项目”是将服务器等互联网设施安装在带有先进冷却功能的海底密闭的压力容器中，用海底复合缆供电、并将数据回传至互联网。

●近日，科技部火炬中心发布国家级科技企业孵化器2019年度评价结果，共有1173家国家级科技企业孵化器参与，最终235家国家级孵化器被评为优秀（A类），其中我区包头稀土高新技术产业开发区科技创业服务中心荣获优秀（A类）。

（据新华社报道）