语音助手存漏洞 可远程操控手机

浙大实验发现利用超声波能直接下单购物
涉及苹果、三星、联想等多个品牌

设想一个场景:你正在与同事讨论问题,放在一旁的手机却在暗中“忙活”,比如打开购物网站下单、拨打电话、打开文档和照片逐个查看。

这样的场景并非“黑科技”,而是切实发生在浙江大学智能系统安全实验室内。近日,浙江大学电气工程学院徐文渊教授团队经过上千次实验后证实,利用智能手机普遍应用的语音助手,通过麦克风收集使用者语音,并将之加载至人耳无法听见的超声波上,可以实现对智能手机的远程操控。

9月13日,徐文渊接受新京报独家专访时称,语音助手所存在的漏洞,广泛出现在包括苹果、三星、华为、谷歌、亚马逊等品牌中。目前,团队已将相关数据发送至厂商,并收到积极回应。

徐文渊教授和她的研究团队发现语音助手存在安全漏洞。

Manuf.	Model	OS/Ver.	SR System	Attacks	
				Recog.	Activ.
Apple	iPhone 4s	iOS 9.3.5	Siri	√	√
Apple	iPhone 5s	iOS 10.0.2	Siri	√	√
Apple	iPhone SE	iOS 10.3.1	Siri	√	√
			Chrome	√	N/A
Apple	iPhone SE †	iOS 10.3.2	Siri	√	√
Apple	iPhone 6s •	iOS 10.2.1	Siri	√	√
Apple	iPhone 6 Plus •	iOS 10.3.1	Siri	×	√
Apple	iPhone 7 Plus •	iOS 10.3.1	Siri	√	√
Apple	watch	watchOS 3.1	Siri	√	√
Apple	iPad mini 4	iOS 10.2.1	Siri	√	√
Apple	MacBook	macOS Sierra	Siri	√	N/A
LG	Nexus 5X	Android 7.1.1	Google Now	√	√
Asus	Nexus 7	Android 6.0.1	Google Now	√	√
Samsung	Galaxy S6 edge	Android 6.0.1	S Voice	√	√
Huawei	Honor 7	Android 6.0	HiVoice	√	√
Lenovo	ThinkPad T440p	Windows 10	Cortana	√	√

研究结果显示苹果、三星、华为、联想等品牌的多个语音助手可被远程操控。

多个品牌语音助手存在漏洞

浙江大学电气工程学院的实验室内,导师徐文渊正在与同事商量周一出差的细节。不远处,研究生张国明等通过一种超声波发射装置,对徐文渊的手机进行远程控制,并操控语音购物助手,自如地在亚马逊网站上下单了一箱牛奶,以及一些零食,完成了付费。整个交易过程中,张国明所使用的,一直是导师徐文渊的账号。

这是徐文渊团队正在进行的一项实验:通过人耳无法听见的超声波,实现对智能手机的远程操控。在另一项实验中,团队成员利用超声波启动了车载语音助手,开启了天窗。

近年来,语音助手占领几乎全部智能设备。用户只需动口,便能操控电子设备。然而,浙江大学电气工程学院徐文渊教授团队研究发现,利用手机麦克风的硬件漏洞,可实现让语音助手接收并执行超声波指令。

新京报记者从浙江大学获悉,徐文渊教授团队在实验中,成功攻击了谷歌、亚马逊、微软、苹果、三星、华为等品牌的多个语音助手产品,均无一幸免。

已向相关厂家提出“补漏”建议

语音助手的工作原理,就是通过麦克风收录人类语音,通过语音识别系统加以识别,把语音转化为文本,系统依文本执行指令。麦克风作为一种基本的电子器件,将声音信号转换为电信号。“这是模拟信号转换为数字信息的第一道门。”

徐文渊团队研究发现,当把普通语音转换成超声波的形式之后,麦克风依然能够接收,并继续转化为语音系统能够识别的语音信号。“当我们把人类语音搭载到超声波这样的高频率时,人耳就听不到了。但是,由于硬件漏洞,它仍然能够被这些麦克风录取,随后又被解调成人类语音的频率,从而能被语音识别系统识别。”

按照徐文渊的说法,目前语音助手产品所使用的麦克风,集中由几家主要供应商生产,因此一个漏洞会出现在几乎所有产品上。团队发现,即便是采用声纹保护的语音助手,攻击者仍然可以用语音合成的方法模拟声纹,并进行破解。

团队成员冀晓宇介绍,实验室将这种攻击形式命名为“海豚攻击”,“因为海豚的叫声是一种超声波。”

新京报记者了解到,这一研究的相关论文已被网络安全领域四大顶级学术会议之一的ACM CCS接收,并引起全球范围内的关注。“事实上,我们一直与业界有沟通”,徐文渊解释,在研究结果正式发表之前,他们已经把研究结果递交给苹果、华为等厂商,并提出“补漏”建议。

■ 对话

实验负责人、浙江大学电气工程学院教授徐文渊

“手机麦克风能听到人耳听不到的声音”

实验的负责人,浙江大学电气工程学院教授徐文渊在接受新京报记者独家专访时称,在进行上千次实验,发现语音助手存在安全漏洞后,自己仍然不会对这一技术产生疑虑。

徐文渊强调,安全本身是一个不断改进加固的过程,“不会因为有安全隐私顾虑,就不往前发展”。

“一直关注物联网安全领域”

记者:为什么会关注手机语音助手安全漏洞这一领域?

徐文渊:我们实验室的名称叫浙江大学电气工程学院智能系统安全实验室,本身一直在关注物联网安全领域,对一些移动设备推出的新功能比较敏感,加上对于这一方面,具备一定的背景知识,所以会关注这一领域。

记者:利用漏洞“黑”进手机的操作方式,是怎么提出来的?

徐文渊:团队在开会的时候,会进行一些头脑风暴,这个操作方式就是这样出现的。有人提出这一设想后,大家知道根据相关的原理,这件事可以做成,于是就按照实验步骤进入实施阶段了。

记者:实验的对象是什么?

徐文渊:用于实验的设备,是市面上常见的智能手机,并对其麦克风发送超声波指令。一共进行了上千次实验,涉及的品牌包括苹果、三星、华为、谷歌、亚马逊等。

“不补救,漏洞的应用场景会更多”

记者:验证出来的安全漏洞,主要是哪方面?

徐文渊:我们找到的是硬件上的漏洞,麦克风存在的问题。比如,手机麦克风可以听到超声波频段,但是人耳听不到,利用这种漏洞,可以实现对手机的远程操控。

记者:这样的漏洞,对社会生活会产生怎样的影响?

徐文渊:目前能做的是,可以直接下单购物。一些用户为了方便,把账号绑定进行语音下单。未来语音助手的应用场景会越来越多,这也意味着,如果不及时补救,这种漏洞的应用场景会更多。

记者:怎么去应用本次实验的结果?

徐文渊:实验的本意,是想让各大厂商重视这个漏洞。我们将实验数据发送给涉及的厂家,目前都有回复,还挺积极的,甚至有一些不在产品列表上的厂家,也主动来了解。

做语音识别的团队,应该此前都关注过这个问题,但是做到这样程度的还没有。我们是第一个公开发表实验结果的团队。

“安全和便利有时候是矛盾的”

记者:有人说,技术的发展必然会导致隐私的泄露?

徐文渊:做了上千次实验后,我并不会对语音识别技术产生这种疑虑。语音助手一定会发展,人机交互的方式也会发展,安全本身是一个不断改进加固的过程,新事物刚出来时,一定会有没人注意到的安全问题,但是经过修复后,设备会越来越安全。

记者:面对潜在安全漏洞,对消费者有什么建议?

徐文渊:对消费者建议是,有些问题是两秒钟就可以解决的。手机里如果开启了语音解锁功能,就把它关了。对于公司来说,我们也提供了一些技术上的建议。

安全和便利有时候是矛盾的,技术让生活越来越便利,必然带来副作用,比如数据泄露。但是人类不会因为有安全隐私顾虑,就不往前发展。互联网会有各种危险,人类也在选择。

记者:未来关于这项研究,还有什么期许?

徐文渊:想要改善设备的安全性,希望有厂商可以采用完善的解决方案。关于这方面的研究,我们也会持续下去。 (王煜)