手机加速计等于窃听器？

手机语音数据“零授权”或成巨大安全隐患

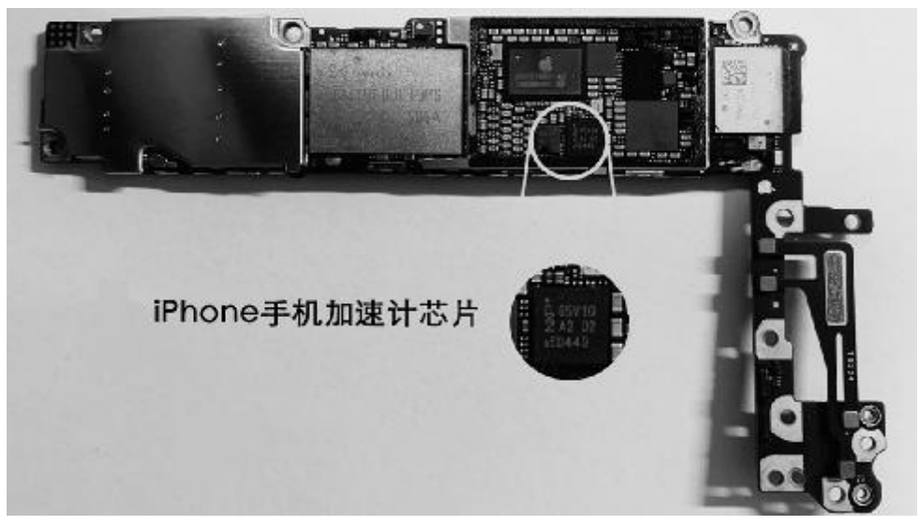
■本报记者 卜叶

“是否允许该App共享您的位置信息？”
“是否允许该App访问您的通讯录？”
“是否允许该App使用您的麦克风？”
……

面对当前智能手机中App“过度收集”“系统越权”两大问题，“是否允许”越来越多地出现在用户使用App的时候。只有经过用户允许，App才能收集手机麦克风、照相机、位置等敏感信息。这是否意味着手机的安全漏洞被堵死了呢？

在2月23日召开的国际四大信息安全会议之一的网络与分布式系统安全会议（NDSS）上，浙江大学网络空间安全学院院长任奎团队带来一个令人不安的声音。研究团队在会上发表论文称，他们发现了一个新攻击路径——手机加速度传感器（加速计）的侧信道攻击。其可怕之处在于，这一攻击方式不仅隐蔽而且“合法”。

“当前，诸多手机系统对加速计这种传感器没有任何系统权限的授权要求，认为它们不会泄露用户的隐私及相关信息，这为手机App在不触及隐私条款与非法权限的前提下，‘合法’收集用户的语音信息、获取敏感数据提供了渠道。”任奎告诉《中国科学报》。



加速计或成窃听灰色地带

当前，与智能手机隐私安全相关的研究纷纷将重点集中于App“过度收集”“系统越权”两大方向。

软件之外的硬件是否万无一失呢？对此，任奎团队注意到近年来快速发展的传感器技术。越来越多不同用途的传感器植入手机中，不仅让手机功能越来越强大，反应也更加灵敏。传感器设备准确地采集用户的多维度数据，但这样的数据是否会被半路劫持呢？

为此，任奎团队联合加拿大麦吉尔大学及多伦多大学的研究团队展开研究，并发现了一种新型的基于内置加速计与深度学习算法的智能手机语音窃听攻击。该研究表明，当前智能手机App可在用户不知情、无需系统授权的情况下，利用手机内置加速计采集手机扬声器所发出声音的震动信号，进而使用深度学习算法进行语音识别与重构，实现对手机扬声器所播放内容的窃听。

该论文共同作者、加拿大麦吉尔大学博士后巴钟杰介绍，这种攻击技术使得每个智能手机的加速计可以像麦克风一样采集用户手机发出的声音信号，从而实现对用户的语音通话、语音消息、语音备忘录等敏感信息的窃听。与传统的手机窃听手段相比，这种攻击最可怕的地方在于它不依赖于任何的系统漏洞，也不需要获取任何系统权限。

还原实验验证加速计风险

加速计是一种用于探测手机本身的移动的传感器。由于手机中的扬声器和加速计距离十分接近且都安装在同一块主板上，扬声器在播放声音时所产生的震动可以显著影响手机中加速计的读数。

为什么此前忽略了这一“巨大”的手机安全漏洞呢？任奎介绍，在手机操作系统中，加速计被认定为是低敏感传感器，任何手机App均可以在用户不知情的情况下在后台“合法”收集加速计数据。但随着传感器技术的精进，这种低敏感传感器的敏感程度远超预期。

该论文共同作者、浙江大学计算机科学与技术学院博士生导师秦湛表示，结合深度学习算法，加速计收集到的手机发声所引起的震动信号，可以还原为声音信号。为了验证这一猜想，研究人员进行了大量基于实际使用场景的实验。最终，研究人员实现了语音识别与语音还原，发现了3种有效的窃听攻击。

第一种攻击是语音密码识别。通过这种技术，攻击者可以识别出智能手机播放过的用户语音中所包含的所有数字和字母信息。例如，用户A通过语音消息给用户B发送了一段银行卡密码。当用户B播放这段音频时，一个采集运动数据的App可以在后台采集对应的加速计数据，进而通过分析加速计数据识别出语音信息中包含的密码。

“在安静环境中，我们的模型可以准确识别出语音信息中86%的数字。即使是在嘈杂的环境中，比如有人说话的实验室或播放音乐的酒吧，模型也可以达到80%以上的识别率。”秦湛说。

第二种攻击是语音敏感词识别。攻击者可以通过这种技术定位并识别用户语音通话中的敏感信息，包括省份、城市、信用卡、身份证等。例如，用户A打电话告知B自己的家庭住址等敏感信息，这时，第三方App可以通过后台采集加速计数据，识别出用户语音中包含的信息，进而确定用户的住址。实验发现，在这类针对敏感词的检索攻击中，模型可以准确定位超过88%的敏感词汇。

第三种攻击是语音还原。这种技术可以通过学习加速计数据与音频数据之间的映射和关联，将加速计采集到的震动信号还原为原始的音频信号。也就是说，用户拨打电话或接收语音信息时，攻击者可以直接通过加速计数据还原出手机所播放的语音信息，进而通过人工来识别敏感信息。

秦湛介绍，由于加速计采样率的限制，目前这种攻击的语音重构模型仅能重构1500赫兹以下的音频数据，但重构出的音频已经包含了成人语音所有的元音信息，可以被人工轻易识别出来。

急需重新定义传感器安全

“尽管目前的技术还无法100%准确还原语音信息，但不可否认的是，一旦这些技术被黑客或不法分子掌握，对国家安全和个人隐私的威胁和损失都是不可估量的。”任奎提示，我们需要仔细研究和理解各类传感器的功能以及它们在安全领域的安全隐患。

如何解除加速计带来的安全威胁？该论文共同作者、浙江大学网络空间安全学院博士生张心语介绍，一种方案是提高调用加速计的系统权限安全等级，将调用手机加速计读数的安全权限提升到手机麦克风的级别，但这种解决方案将会严重影响到所有需调用加速计的App运行，导致大规模的系统更新与App软件升级；另一种方案是通过修改硬件设计，使用物理隔离的方法，让加速计难以采集到扬声器声音的震动信号，从而彻底防御这一类的侧信道攻击。

不过，这两种解决方案实施起来的经济与社会成本都较高，短期内难以完全杜绝这类窃听攻击的发生。

而上述解决方案也并非一劳永逸，任奎认为，随着技术的进一步发展，以加速计为代表的各类传感器的采样率和精度还将进一步提高，攻击也会变得更加多样。

“为了防止加速计等硬件设备被滥用，我们希望更多人能关注手机硬件，特别是传感器安全，及时为手机安全‘上锁’。接下来，研究团队还将继续对手机的硬件以及软件两方面同时进行安全研究和排查。”任奎说。

抗疫消毒有利器

“随着企业陆续复工，人流量加大，进一步加强疫情防控成为各行各业面临的新挑战。近日，高校科研工作者自主研发出多款高科技产品，助力疫情防控。

战“疫”机器人整装待发

自动消毒、自动发药、自动量体温……近日，湖南大学机器人国家工程实验室加快科技攻关，研发了面向病患的双臂协作辅助诊疗机器人、智能消毒与巡检机器人、配药检测机器人等。

智能消毒与巡检机器人能够自动无死角喷洒次氯酸消毒液进行消毒，同时还可以自主巡逻；双臂协作辅助诊疗机器人具备语音交互、智能诊断、远程遥控等功能，可帮助前线医务人员在不接触病患的前提下完成测温、看护等。

中国工程院院士、机器人国家工程实验室主任王耀南表示，团队研发的系列机器人投入使用后不仅可缓解医护人员紧缺问题，还可减少医护人员的工作时间和劳动强度，显著降低交叉感染的概率。

空气净化消毒设备驰援武汉

疫情当前，空气净化消毒是很重要的一个环节。元宵节前后，哈尔滨工程大学联合旗下企业哈尔滨工程大学船舶装备科技有限公司捐赠一批杀菌消毒率99.6%以上的空气净化消毒设备驰援武汉。

由哈船科技出品的FG-BG-100型空气净化消毒设备，可通过高压脉冲放电的形式将气体激活，产生大量离子氧，在高能离子的瞬时高能量作用下，在极短的时间内氧化其他有害分子，同时破坏微生物的外围构造或细胞壁，从而实现快速杀菌消毒。

消毒机器人走上街头

履带自走式风送高射程喷雾机，之前一直用于农业农药喷洒。考虑到疫情防控的现实需要，苏州大学机器人与微系统研究中心团队的成员们加班加点，对设备进行改造，调整喷雾系统，使其更适合消毒药液的喷洒。

“我们目前实验了84消毒液的喷洒，通过喷洒消毒液，降低病毒通过气溶胶传播的可能性。”苏州大学机器人与微系统研究中心副教授耿长兴说。

该消毒机器人采用微机控制，工作人员可远距离无线遥控操作，确保人员安全；小度机器人自带喷雾装置，喷雾系统采用压流和风力的二次雾化，采用特殊风道设计，水平喷幅可达30米，雾滴附着率高，药液利用率高。

目前，该机器人已被投入到苏州市相城区开展消杀作业。

“人造龙卷风”实现快速杀毒

近日，厦门大学特聘教授尹应武团队正利用“人造小龙卷风”技术及装备系统，研制防疫相关技术、装备及产品。

这项通过流体压力推动喷头高速旋转的技术装置，可将水柱立即雾化，喷出旋转气雾流体，形如“龙卷风”，可以提高消杀、除尘、降温灭火的效果，通过对现有洒水车、消防车、液体罐车、手持式喷雾器等进行简单改造就可以使用。

“我们原来是开发过程强化和高效节能技术的科研团队，此次疫情的出现，让我们想到把高效雾化的核心技术和装备用在防疫工作上。”尹应武说，上述成果可形成“咖啡+伴侣”的组合效果，“咖啡”是指原来的装备系统，“伴侣”是指应用对象或防疫药品，原来是清水或溶入肥料、除菌、除虫剂的水溶液，现在可换成水稀释防疫药品的消毒液。

目前，该团队正在进行效果全面评价，未来可应用于各种突发疫情的防控。 （温才妃整理）

学术经纬


包云岗


于剑


高新波

伯克利科研模式的启发

■包云岗

近来，第五代精简指令集架构（RISC-V）在全球受到越来越多的关注。2019年10月，《经济学人》刊出了*Your own RISC*一文，判断“像RISC-V这样的开源硬件也许会在未来十年实现类似开源软件式的扩张”。RISC-V的发明者与推动者——加州大学伯克利分校在计算机体系结构领域的引领地位，令绝大多数大学和研究机构难以企及。

然而3年前，依托于中国科学院计算技术研究所（以下简称计算所）的计算机体系结构国家重点实验室（以下简称国重）开展的一项论文发表统计工作，却让我们对伯克利的论文发表情况产生了困惑，甚至一度怀疑统计数据是否出了问题。

当时，国重统计了2006~2015年十年间全球所有研究机构在计算机体系结构领域四大国际顶级会议（ASPLOS、HPCA、ISCA、MICRO）上发表论文的数量，结果显示：得州大学奥斯汀分校、威斯康星大学曼迪逊分校和密歇根大学位列前三；计算所共发表了19篇，位列世界第25名、亚洲第一。但是，我们惊讶地发现加州大学伯克利分校竟排在计算所之后，10年间只发表了18篇论文，而2010年启动的RISC-V项目正好处于这十年间。

这表明该校在计算机体系结构领域的学术声誉和产业影响并不是通过论文数量产生的。伯克利有自己的学术评价标准，并不追求论文数量，那他们追求的是什么呢？

带着这些困惑，国重开始探究伯克利的科研模式，发现另一个令人吃惊的数据——虽然那10年间伯克利只发表了18篇论文，但伯克利在2011~2015年的5年里围绕RISC-V进行了12次流片。这种处理器级别的流片次数和频率远远超出了全世界所有其他大学。5年12次流片必然需要大量的工程投入，以至于很多美国大学的教授对此并不认可，他们甚至认为大量工程会扼杀创新思想的产生。

但事实确实如此吗？

回顾伯克利的科研历程，可以发现他们在过去几十年研制了大量的原型系统，如1950年代CALDIC系统、1960年代Project Genie系统、1970年代BSD Unix操作系统与INGRES数据库系统、1980年代RISC处理器、1990年代RAID存储系统与NOW机群系统……这不仅推动了技术进步甚至颠覆产业，也培养了一代代杰出人才。

如果用一句话来总结伯克利的科研模式，那就是热衷于研制真正能改变现状的原型系统，哪怕需要大量工程投入，中国工程院院士、国重主任孙凝晖称之为“科研重工业模式”。

最近，中国工程院院士李国杰指出，国内陷入了某些科研模式上的思维定势。如何打破？加州大学伯克利分校给了我们一些启发：科研模式也是多元化的，“科研轻工业模式”发表大量高水平论文能产生影响力，而“科研重工业模式”做出高水平原型系统，可能产生更大的影响力。但是“科研重工业模式”也是一种“Hard模式”，论文少、见效慢、风险高，即使在全世界范围内愿意选择这种模式的学者也很少。不过在美国，至少还有加州大学伯克利分校在践行。而在中国，随着论文数量不断攀高，是时候通过科研机制上的创新，鼓励一部分人去试一试“科研重工业模式”、去试一试“Hard模式”了。

（作者系中科院计算所研究员，本文转载自《中国计算机学会通讯》2020年第1期）

科研存在轻工业模式吗？

■于剑 高新波

简单说来，科研“轻工业模式”是指发表大量高水平论文，科研“重工业模式”是指做出高水平原型系统。诚然，高水平原型系统由于难度高、工作量巨大，“不可能”有很多。

高水平的论文难道有很多吗？这可能取决于对高水平论文的定义。如果高水平论文是指发表在顶级会议、顶级期刊上的文章，那么包云岗的意见也许是正确的。因为近年来，顶级期刊、顶级会议越来越多，论文的录用也越来越慷慨，甚至在同一个会议上，同时发表9~10篇文章的高手也是大有人在。

如果真的把顶会、顶刊论文等同于高水平论文，对于整个社会来说，则是极大的误导。在某种程度上，甚至可以说是本末倒置、是非不分了。

严格意义上说，只有包含一流学术成果的论文才是高水平论文。这样的“高水平论文”与“高水平的原型系统”相比，对工作量和时间的要求一点也不低。这样的高水平论文，从孕育到完成，常常以八年、十年为时间单位，这还是鸿运当头的时候。

非常遗憾的是，除了极少数一流学术成果能即时判定外，大多数一流成果的判定需要较长的时间，其时间跨度经常以十年，甚至百年为单位。

顶会顶刊存在的合理性与必要性

改革开放初期，国内很多领域的研究还达不到顶会顶刊的水平，更不要说更高水准了。因此，以顶会顶刊论文为评判批准，对于当时国内的研究，无疑具有极大的促进作用。

顶会顶刊的论文，大多是热点问题的扩展修正或热点方法的延伸改进，大多体现的是热点问题与时髦方法，虽然会有极少例外。这类论文特别适合学生和年轻老师练手——既有一定难度和品位，又不至于无处下手，可以比较容易地做到“前有车后有辙”。时间可控，结果可期，可以做批量化的研究，既能显示研究水平，又不至于露怯。

一般来说，顶会顶刊的论文，水平还是相当不错的，它们也是很多未来研究的起点。对于学生和年轻研究人员，是否能发表顶会顶刊论文，确实是一项衡量科研能力的客观标尺。对于他们来说，如果只有一流工作才算成果，那实在是太苛刻了，可能全世界也没有几个人适合做科研了。目前来看，用顶会顶刊论文来评估学生和年轻研究人员，是一个相对具有操作性的合理指标。

一流成果与学术自信

同时，我们也应该注意到，经过40多年的改革开放，国内很多方向的研究水平已经达到了顶会顶刊的水准。国家对于研究人员的期望，已经不再是跟踪模仿，而是原始创新。因此，对于研究人员特别是正高级职称研究人员而言，不宜再以“顶会顶刊模式”作为自己追求的“大目标”了，而只能作为训练学生的“小目标”。正高级职称研究人员不应当再满足于跟踪模仿、改进修正的“从1到N”的研究，而是要追求原始创新、颠覆既有的“从0到1”的研究。

即便没能彻底解决问题，能提出原创问题或猜想也很好。做公开的难题、做有用的研究、做自己的问题，这是一个学者成熟自信的表现。可以解决难题促进科学进步，可以攻克难关推动技术革新，也可以勇闯“无人区”开辟新天地。这样的勇气、这样的定力、这样的自信、这样的气魄、这样的志向，仅仅依靠顶会顶刊论文很难实现。

为此，我们需要改革科研评估体制，特别是改革科研人员评估体制。国外终身教授体制的一个目的，就是希望能有一批人不以短期目标为主，能够追求长远目标，比如以一流成果为目标。总体看来，国外的终身教授体制大致是成功的。如果没有这样的体制保护，科研仅以发表顶会顶刊论文为目标，顶会顶刊模式必然流行。未来，期待中国也能有类似国际上终身教授一样的制度。

（作者分别系北京交通大学教授、西安电子科技大学教授，本文转载自《中国计算机学会通讯》2020年第2期）

速递

2020世界机器人大赛启动筹备工作

本报讯 记者2月24日从世界机器人大赛组委会了解到，目前组委会通过云办公的形式已重新启动大赛的各项筹备工作，并于近日召开了“2020世界机器人大赛—共融机器人挑战赛和BCI脑控机器人大赛”第二次专家会议。会议讨论并确定了相关比赛任务考察方向、竞赛内容、赛项难度、部分任务细节等，并围绕智能机器人技术在疫情防控、复工复产等方面的研发与应用展开探讨。

据悉，BCI脑控机器人大赛比赛内容延续技能赛、技术赛、创新展区优秀成果展示三部分，同时计划在2020年竞赛中增加优秀论文评选等内容。共融机器人挑战赛将设置双臂协作机器人组和特种机器人组两个组别。其中，特种机器人组竞赛中拟加入相关消毒、测温等考察任务，探索并推动相关机器人关键技术在重大传染病防控中的应用。 （卜叶）

政企云办公软件“光圈儿”在线发布

本报讯 2月25日，中科院旗下信息科技企业中科曙光联合北京北信源软件股份有限公司，共同在线发布了一款面向政企用户的安全可信协同办公系统“光圈儿”，并宣布该产品在疫情结束之前将免费以SaaS云服务的方式供用户使用。

新冠肺炎疫情暴发以来，远程协同办公需求剧增。与此同时，大量核心信息通过网络传输，给政府部门及各类对安全保密性要求较高的企事业单位带来了较大的安全隐患。中科曙光云计算集团总裁助理徐辉明介绍说，基于此，“光圈儿”协同办公系统专为对数据敏感、信息安全性要求较高的政企用户打造，主打安全、高效实用、灵活扩展三大优势。

中科曙光云计算集团总裁助理张晓辉还介绍说，“光圈儿”能够提供安全私有云Saas服务，基于曙光城市云中心或者企业私有云部署，可以有效保证敏感数据的高私密性。此外，该软件在支持Android、iOS、Windows和MacOS多种客户端环境基础上，服务端还可适配多种国产化软硬件环境，实现多平台兼容。 （赵广立）