新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报 2019年8月21日 星期三

视觉中国

别乱开蓝牙 当心你的隐私

本报记者 **谢开飞**

蓝牙耳机、蓝牙手环、车载蓝牙……蓝牙技术自问世以来，不仅解决了许多数据传输方面的难题，同时也开启了无线生活的大门，得到各类智能设备的青睐。但这项技术为我们生活带来便利的同时，也带来一些安全隐患。

据外媒报道，来自波士顿大学的研究人员于日前发现，在Fitbit智能手环等蓝牙设备上，蓝牙通信协议中存在的漏洞，其会导致敏感的个人信息被窃取，允许第三方追踪设备所在位置。这些数据很可能被“有心人”拿去使用，考虑到如今蓝牙产品的普及率之高，专家建议用户要在这方面提高警惕。

那么，这个漏洞是什么？目前蓝牙设备还存在着哪些安全隐患？作为消费者以及技术厂商应该如何防范相关的技术风险？科技日报记者就此采访了有关专家。

“商标”信息导致设备被跟踪

那么，波士顿大学研究者们发现的漏洞究竟是什么？

“这一漏洞与蓝牙设备建立通信连接的方式有关。”福建省网络安全与密码技术重点实验室副主任、福建师范大学教授黄欣沂解释道，蓝牙设备与目标终端设备建立通信连接，需要一个“配对—连接—传输数据”的过程。在此过程中，蓝牙状态改变、搜索设备、绑定设备等信号，都是通过广播接收到的，攻击者可在无线网络中“监听”到蓝牙设备的广播信息。若能确定在一定范围内仅有一名用户，那攻击者在该范围内搜索到的蓝牙信号、蓝牙地址，就只会是该用户的，从而建立起蓝牙设备和用户之间的一一对应关系。

“一些蓝牙设备内的蓝牙地址具有唯一性，一旦这个地址与用户相关联，他的行动就可以被记录，用户隐私也就难以得到保障了。”黄欣沂说，那么即使该用户不在原来的地点使用蓝牙设备，只要其设备的蓝牙地址被“盯”上，攻击者仍能知道哪些蓝牙数据是属于该用户的。

“在大部分设备上，蓝牙地址都会被定期重新随机设置，以切断设备和用户之间的对应关系。”360安全研究院独角兽安全团队专家秦明闯说，据波士顿大学的研究人员公布的最新研究成果显示，在蓝牙通信标准中最新找到的漏洞正存在于蓝牙的身份识别功能中。该漏洞不需要攻击者主动发数据包，只要“监听”蓝牙的广播信道就能“跟踪”某个设备。

为何蓝牙设备地址被随机改变后，攻击者仍可以找到原用户？“一些厂商为了能‘认识’自家设备，在随机化的蓝牙地址、广播信息中，编入了一些与设备有关的信息，好比产品商标，导致设备还是可以被追踪到。”秦明闯说。

360安全研究院独角兽安全团队专家殷文旭举例解释说，如Windows 10系统广播的蓝牙数据包中，部分数据在每台设备上不同，且会出现周期性变化。与随机化的蓝牙地址类似，其初衷也是防止被“有心人”跟踪，但这部分数据变化的周期和蓝牙地址变化的周期不同步，攻击者可通过周密的分析和解读，将二者关联起来，实现对设备的持续追踪。

根据波士顿大学研究者们的测试结果，他们发现的漏洞出现在Windows 10系统、iOS系统、macOS系统等软件系统以及Apple Watch、Fitbit智能手环等拥有蓝牙功能的设备上，因为这些设备都会定期发送含有自定义数据的信息，以便和其他设备进行互动。

可穿戴蓝牙设备隐藏更多风险

据统计，目前全球有数十亿台智能设备采用了蓝牙技术。尽管Wi-Fi可替代蓝牙满足用户的无线传输需求，但在无线耳机、扬声器等设备上，通常会同时配备蓝牙和Wi-Fi功能。

“无线扬声器、车载信息娱乐系统，这类带有蓝牙功能的设备通常只涉及点对点的单线传输，几乎不涉及其他设备，因而比较少泄露隐私。例如，无线耳机通常只连接用户自己的手机或其他个人设备，不会连接他人的设备。”黄欣沂说，但与体育和健康有关的、备有蓝牙功能的智能可穿戴设备，如智能手环、智能眼镜、智能运动鞋等，则会通过手机软件将用户的心率、睡眠、体脂等个人信息上传至服务器中，也就是非个人用户设备中，这就会存在较大的隐私泄露风险。

据福建宜准信息科技有限公司技术总监蔡云鹏介绍，因为可穿戴设备要启动蓝牙功能，就需要广播地址和名称，在广播过程中，攻击者就可通过“监听”间接定位到具体终端佩戴者的位置，也就能获取用户位置信息。另外，攻击者还可通过标准协议，获取部分设备实时采集到的健康体征信息，这部分数据一般都未经过加密处理，很容易就被“有心人”利用。同时，手机端的来电或应用消息一般都会推送到带有蓝牙功能的可穿戴设备上，当该设备被监控后，用户手机上的消息也可能随之被泄露。

黄欣沂举例说道，目前市面上大多数智能手环都采用直接工作配对模式，即用户主动发起连接却看不到配对过程，且设备通常对蓝牙指令的来源不经认证。在这种情况下，攻击者只要将一段含有特殊格式的数据传至蓝牙设备，就能对手环随意“发号施令”，如控制LED颜色变化、开启实时步数监控功能等等。

我国尚未出台专门的安全标准

据测算，预计到2022年，支持蓝牙功能的设备数量将从现在的42亿提升至52亿，相关的安全问题将会变得日益严峻。

不过，波士顿大学的研究者们也表示，Windows 10系统和iOS系统用户只需把蓝牙关掉再重新打开一次便可新设一个蓝牙地址。“在厂商们对此漏洞进行修复前，这个‘笨’办法对于注重个人隐私安全的用户来说，也许是最有效的了。”蔡云鹏说。

2018年6月11日，全国信息安全标准化技术委员会秘书处就国家标准《信息安全技术蓝牙安全指南》发出了征求意见稿，目前该文件处于报批阶段。“当前我国尚未出台专门的安全标准，我建议应尽快完善与蓝牙设备相关的安全标准，如对某些设备加入强制蓝牙地址随机化功能，规定盗用、滥用蓝牙数据将受到严厉惩处，让攻击者不敢利用技术漏洞做违法的事。”黄欣沂说。

在技术方面，蔡云鹏建议企业和生产厂商应对蓝牙系统在配对和连接环节加强保护措施：在配对时，增加验证配对密钥环节；在连接时，要使用相互身份验证方式来保证连接安全。在保护云端数据安全方面，厂商应尽量选择高安全性的服务商，及时备份用户信息、加密传输重要文件、使用加密云服务、认真对待密码，加强生产环境数据安全审计；硬件上可采用高安全性的蓝牙系统芯片和模块，尽量降低技术漏洞给用户带来的影响。

“消费者在选择产品时，应尽量选择正规大厂家生产的产品，不要一味追求低价，这样在安全性方面会更有保障。此外，在使用产品时，用户在不使用的情况下，应尽量关闭蓝牙功能，还要及时更新系统软件版本，堵住漏洞。”蔡云鹏建议，用户应尽量减少蓝牙配对次数，并选择在安全的地方进行配对，不要让其他人看到配对口令。同时，用户在使用手机时，尽量不去连接、配对不可信的设备，只与熟悉的设备进行配对。

殷文旭表示，前不久Windows 10技术团队已修复了波士顿大学研究者发现的漏洞，用户只要进行软件更新就可完成修复。但对于手环这类更新比较慢的物联网设备，漏洞或将存在一段时间，建议其他生产厂商及时跟进并修复该漏洞，发布系统更新，同时检查其余产品中也是否存在类似漏洞。

一“官宣”系统就崩溃？微博宕机或为营销策略

第二看台

本报记者 **陆成宽**

近日，新浪微博的服务器又经受了一次考验。日前，演员文章和马伊琍在微博宣布离婚，随即微博流量短时间内出现暴增。早前，在鹿晗、冯绍峰等明星“官宣”喜讯时，微博曾出现过服务器宕机事件，因此也有人担心此次离婚消息发布是否会再次引发宕机事件。

那么，究竟什么是宕机？引发宕机的原因又是什么？就上述问题，科技日报记者采访了相关专家。

预防宕机不存在太大技术问题

实际上，宕机是IT行业术语，宕为英文down的音译。所谓宕机，是指网络空间的信息系统无法提供正常服务，出现卡顿甚至“停摆”现象，用户的直接体验就是系统长时间无响应，比如无法正常访问、搜索无响应、无法发帖等。

“造成系统宕机的因素有很多，比如机房供电故障、服务器硬件崩溃、系统处理能力不足、遭受网络攻击等。”北京理工大学网络攻防对抗技术研究所所长闫怀志告诉科技日报记者。

突发热点事件引发的微博服务器宕机事件，通常是由于瞬间访问量暴增，导致后台服务器不堪重负，只好“一宕了之”。资料显示，微博系统服务器的访问量上限被设计为预估平时流量的峰值，相关服务资源均依此配置。一旦突发事件导致访问量超出此峰值，系统将无法承受，宕机也就在所难免。

“单就技术层面来说，预防微博服务器宕机不存在太大问题，只要扩充容量即可。而微博服务器宕机事件频发，原因主要有两方面。”闫怀志解释道，一是微博服务器部署规模及其处理能力受限。很多公共服务平台的平时流量基本稳定，基于成本考虑，在保持适度冗余处理能力的前提下，微博运营商不会主动去租用或配置大量超出日常数据处理需求的计算和存储资源。服务器扩容多了，如果没有流量支撑，就会造成资源闲置及成本增加。另一方面，微博流量具有瞬间峰值高、持续时间短的特征，在热点事件出现时表现得更明显。微博热点流量较难预测，使得微博运营商在扩容问题上陷入两难境地：扩容多了易亏，扩容不足易挂。

平台可预测峰值流量加以应对

在闫怀志看来，热点流量虽较难以预测，但不等于不可预测。只要能预估出流量峰值范围，就可通过定时扩容和提供弹性计算存储资源来从容应对。很多平台在这方面都有过应对流量突增的成功案例，比如应对“双十一”时的峰值流量。明星离婚等网络突发事件，虽不受微博运营商控制，但微博运营商应该可通过舆情监控等手段感知即将到来的流量大潮，通过启动应急预案（比如临时租用“备勤”服务器）来应对。

“此外，微博宕机不能排除的另一个可能，这或许是某些微博运营商的营销或推广策略。”闫怀志说，因为微博宕机本身也是个突发热点，客观上会提升微博关注度。更有甚者，某些明星经纪公司在“娱乐至上、流量为王”的观念驱使下，联合微博运营商人为制造这些宕机事件来吸引公众眼球、提升明星知名度，也不是没有可能。毕竟，微博已经历了多次的宕机，理应具备相当的应对经验。再出现新的宕机事件，到底是运营商无能为力还是有意不为，有时还真要打个问号。

边缘计算、人工智能都能帮上忙

“依靠现有前沿技术，有可能避免或缓解宕机问题。”闫怀志解释道，主要的手段就是构建弹性伸缩业务系统，辅以人工智能预测和业务持续性监控，来保障峰值服务正常运行。比如，通过人工智能技术来预测网络突发流量，利用云计算弹性计算资源平台来实现快速扩容甚至实时扩容，以应对高峰流量。

据报道，商用云服务提供商目前可在宕机后数秒内探测到服务不可连接，然后在90秒内实现扩容，恢复运行中断业务。这种按需部署的服务器配置方式，既可显著降低网络平台服务器宕机的风险，又能很好地利用存储计算资源，实现双赢。

此外，闫怀志指出，还可采用“降级”运行策略，即将服务器的业务拆分为若干相对独立的业务，各业务之间共享数据库。一旦服务器出现过载，可启动降级策略来“丢卒保车”，至少保证核心业务能正常运行。比如，若微博热搜榜崩溃，可维持评论、转发等核心功能的正常运行。

“另一种有效的应对方式是利用边缘计算技术。”闫怀志说，通过在网络边缘实现数据分布式本地处理，可显著降低访问数据的汇聚和传输总量，这不仅能缩短用户响应时间、提升用户体验，还能大幅降低中心节点的数据传输和处理压力，也是一条应对宕机的新路径。

行业观察

数据垄断的伪命题和真问题

曲 创

“数据垄断”这4个字最近很常见，大意是指处于反垄断风口浪尖上的那些互联网大公司，垄断了用户的数据，据说这样会导致很严重的后果。最近，脸书、亚马逊等巨头都因涉嫌“数据垄断”，被监管机构调查，有的甚至还被开巨额罚单。

从“数据垄断”这4个字本身我们能解读出两层意思：首先，数据是很有用的东西，要不人家垄断它干嘛？其次，数据是能被垄断起来的，这里的垄断意为独占，数据被某些公司独占了，别人用不到。

“数据垄断”是否真是如此呢？我们一个一个来看。

数据有什么用

其实单纯的数据本身什么用也没有。“40”只是个数字，单从表面我们获取不到任何信息。

“40岁”，这是个年龄；“40元”，这可能是一个价格；“40度”，如果指的是体温，此人在发烧；如果指的是一杯水的温度，水就有点烫。

数据本身什么信息也不包含，必须和其他产品、服务、活动结合起来才能提供有用的信息。当我们把大量的数据集中在一起，奇妙的事情就发生了。

比如，每天上下班时，我们会打开地图APP看看交通拥堵情况，那些红色、黄色、绿色的线条能让我们避开拥堵路段，快点回家。这是基于成千上万车辆的位置、速度等数据计算出来的结果。这便是数据的第一个作用：揭示出个体信息无法体现的整体规律。

数据的第二个作用我们也天天见：匹配供需，提高既有市场交易效率。搜索引擎、电商平台、外卖平台，做的其实都是这个事。交易双方的数据越多，匹配的效率就越高。不过这只是理论上的结论，匹配效率最高的状态不见得就是平台利润最大化的状态。对于平台而言，匹配效率显然没有利润那么重要。

很快，掌握了大量数据的科技平台不满足于仅匹配现有的信息，他们还要基于用户的个体信息提供“个性化服务”，这就是数据的第三种作用。

亚马逊在这一点上做得比较好，它的“预先发货”系统体现得最为明显。亚马逊通过用户之前的消费数据，推断出用户未来几天会买什么东西，然后安排发货。在用户下单的那一刻，包裹就可能已在路上了。至于“个性化定价”“个性化推荐”之类的服务，和亚马逊的“预先发货”相比，只能算小儿科级的应用。

数据的以上3种作用还都是辅助性的，下面这个才是数据的“杀手级应用”：基于数据推出全新产品和服务。

苹果智能手表上有个很冷门的功能“跌倒报警”：如果你意外跌倒，会提示你是否需要报警，简单确认后会拨通事先设置好的急救电话。该功能可判断出你是自己趴下的，还是意外跌倒的，这依据的是智能手表上十几个传感器的数据计算结果。这就是数据创新的价值：关键时刻能救命。

按照生产要素的使用情况，我们可区分两种生产方式：劳动密集型和资本技术密集型，现在有必要加上第三种了：数据密集型。

图片来源于网络

数据能被垄断吗

基于上述分析，我们可以得出结论，数据确实是很有用的东西，那它是否能被垄断呢？

数据大致可被分成两类，第一类是像城市里的道路分布、某个区域内有多少幢楼、某个路口一天有多少人来车往这样的数据，它可被称为“公共领域的数据”。这类数据谁都可以获得，无法被垄断。第二类是公司自己在生产经营过程中产生的数据，例如平台每天的成交数量、一家餐馆每天卖出多少份菜、平均每桌的消费金额等。这类数据本来就是公司自己的，也就无所谓垄断与否。

所以，“数据垄断”本身是道不成立的伪命题。

更重要的是，从无用的数据到有用的信息之间，需要经过数据的收集、处理、存储、分析过程，这是一个不折不扣的生产过程。数据的生产有3个特性：数据量越大，平均成本越低；数据种类越多，平均成本越低；采用的数据种类越多，收益越大。

因此，对于数据密集型行业而言，提升数据集中度可提升数据生产效率。企业竞争会在数据的总量、类型、处理分析能力、应用开发等层面展开，数据的集中将是行业发展的必然趋势。

大家忧心忡忡的“数据垄断”多数情况下指的是“基于数据的垄断”，并不是对数据本身的垄断。就在今年8月，欧盟正式对亚马逊发起了反垄断调查，核心问题正是数据。亚马逊身兼二职，既有自营业务，也有第三方业务。在亚马逊上开店的第三方商家数据显然要对亚马逊开放，欧盟发现亚马逊很可能利用这些第三方商家的数据，对他们实施了不正当竞争行为。

此案刚开始调查，让我们拭目以待，其结果很可能对国内的电商行业具有很强的借鉴意义。

数据本身是无法被垄断的，但在一个数字化和大数据时代，数据却可能成为垄断和不正当竞争行为的“帮凶”，使得这些违法行为更加隐蔽，对市场竞争和消费者权益的损害也就越大，这才是需要我们关注的。

（作者系山东大学经济学院教授）