“小黑盒”轻易开锁、陌生人指纹和照片也可开锁、信息泄露……

智能门锁“太智能”面临市场考验

□信息时报记者 王颖婷

“小黑盒”一靠近就能自动开锁、未录入的陌生指纹及照片也能顺利开锁、开锁用的感应卡片放在包里就能被复制…… 这些曾经出现在特工电影中的情节，目前也出现在了智能门锁中。近期，市场监管总局在全国范围内，进行了一次智能门锁的风险监测，并对监测发现的风险发布了安全消费警示。自2001年国内第一把智能锁面世以来，截至2018年6月，智能锁品牌已经扩展到1500个以上，直逼传统机械制锁行业。门锁作为家庭中的第一道防线，智能锁的安全性显得至关重要。到底智能锁是方便了用户还是方便了不法分子?多名业内人士提出了智能锁企业需更改重启机制、增大指纹识别像素点、升级加密技术等对策。中国智慧人居产业促进会秘书长陈军称，目前大部分企业都意识到了诸多风险，摸索找到了相关的解决方法，并取得了初步成效。因智能锁属于新行业缺乏经验可参考，所以还需时间和市场来检验。

据央视新闻《每周质量报告》(以下简称“报告”)1月6日报道，此次监测从线上线下采集了38个品牌、40款型号的智能门锁产品，涉及的标称产地有广东、浙江、福建等7个省市。监测了识别方式安全、信息安全、电子安全和功能安全的17个项目。通过广州的国家通用电子元器件及产品质量监督检验中心(以下称检验中心)的实验发现，被采集的40批次样品中，存在“小黑盒”干扰开锁、指纹识别缺精准、人脸识别被照片开启、卡片开锁易复制、远程控制信息易泄露的五大方面风险。该检测结果一经发出，引起消费者的强烈反响，对于智能锁的安全性众说纷纭。记者对此采访了多名业内人士，对智能锁的风险原因进行剖析并为广大用户提出了使用建议。

风险1：“小黑盒”干扰下自动开锁

根据报告，检验中心在40批次中发现，6个批次能被特斯拉线圈打开，占比达到了15%。现行行业标准GA374-2001《电子防盗锁》规定，电子防盗锁在正常工作情况下，要能够抵御住50V/m的电磁场干扰。而检测中心发现，“小黑盒” 已经达到1000V/m，超过行业标准20倍。即使智能锁已经达到行业标准，也有被“小黑盒”干扰的风险。

前段时间，关于用“小黑盒”开锁的视频风靡网络。记者在网上看到，视频中将“小黑盒”靠近智能锁，部分锁便会自动打开。据了解，“小黑盒”名为特斯拉线圈，可以在短时间中发出强电磁脉冲，被誉为“人工闪电”。“小黑盒”在靠近智能锁时，通过强磁场来干扰门锁的电子元器件，使其死机重启，而部分智能锁在重启后会自动开启。

针对“小黑盒”干扰自动开锁的风险，记者采访了欧瑞博智能家居技术人员王小姐，她表示：“特斯拉线圈之所以能打开智能锁，原因主要有两个，一是因为智能锁的重启机制，有的门锁在受到干扰时，重启机制会先开锁然后再锁住，所以在开锁阶段，便能打开门锁；二是门锁的控制方式存在缺陷，容易受干扰而被开锁”，谈及如何避免此问题，他告诉记者：“欧瑞博采取了三种方法，一是优化智能锁重启机制，重启后跳过开锁阶段，直接锁住；二是采用更复杂的信号进行控制，可有效避免干扰导致的误触发；三是优化电子元器件，从根本上提高抗干扰性”。

安朗杰中国区总经理朱道明还提出了另一个方法，旗下西勒奇智能锁还通过运用整块金属背板来抵御“小黑盒”的干扰，他说：“整块金属板达到一定厚度能屏蔽电磁波，可以极大概率抵抗干扰”。

专家提醒：消费者尽量购买正规厂家生产的智能锁。

风险2：陌生指纹能开锁

此次检测中，部分智能锁在识别区域贴上胶带后，可以用陌生指纹开锁。检验中心人员表示，40个批次样品共有36个批次具备指纹开锁功能，10个批次样品存在高风险。而存在高风险的智能锁普遍不能识别非指纹图像，即如果锁上有异物(如头发丝、金属丝、胶带)、裂纹干扰并成功开锁后，门锁将会记住异物和裂纹的图像，作为下一次开锁的识别部分。

记者在淘宝上浏览智能锁产品看到，指纹识别开锁已经成为智能锁主流开锁方式之一。对于指纹开锁的安全性，朱道明在接受采访时告诉记者，其实用户使用指纹开锁时，每次手指的按压力度、角度等有所不同，如果想保持高识别率，一是使用大尺寸感应区域的指纹模块，但是成本高昂；二是在录入指纹时同个手指多次录入，就像苹果手机iphone的指纹录入一样，缺点是时间长、体验感差；三是调整指纹模块软件，增大指纹识别时可通过的差异比例，此方案便宜又快捷，部分智能锁厂家都采用此方法，但出现了陌生指纹也能开锁的问题”，他介绍称，有些厂家通过设计算法软件来检测到假指纹部分，在保持便利的同时保持了安全。

中国智慧人居产业促进会秘书长陈军透露，以前智能锁市场上的指纹识别模块大部分是176*176像素点，而现在部门企业为了降低成本，而采用160*160像素点的识别模块。他说：“指纹识别多数是通过比对特征点的方式开锁，在缩小像素点后，只需要符合10来个特征点就能开锁，安全性随之降低。”目前，消费者在购买智能锁时需注意指纹识别模块的配置，并在使用时注意保持模块的清洁度。

专家提醒：消费者需选择配备大面积、高像素指纹识别模块的智能锁，并在使用时定期清洁识别模块，能提升指纹识别功能的安全性。

风险3：人脸识别被照片开启

据了解，在监测智能锁中普及度不高的人脸识别系统中，也发现了“高风险”。据央视新闻公布的检验中心监测数据，40批次中仅有4批次样品具备人脸识别功能，不符合率达100%。检验中心人员称，4批次智能锁无法分别真实人脸与照片，录入用户多角度的照片，就可以开启智能锁。

据悉，人脸识别并不是一个新技术，已在手机、银行、酒店、公共场所运用得非常广泛，那么为什么放在智能门锁上就出现问题呢?就此，朱道明表示，在智能锁领域，目前人脸识别还属于“新兴事物”，现在出现的风险，一定程度上是因为企业为了节省成本使用2D识别技术、不使用3D识别技术造成的。

一位不愿具名的业内人士告诉记者，他认为智能锁开通人脸识别显得有些 “鸡肋”：“人脸识别和指纹识别区别并不大。人脸识别还会加快电池使用速度，其耗电量是指纹识别的上百倍。而在智能锁这种要求低功耗的应用场景中，用户需要对门锁频繁更换电池或者充电，体验感会大打折扣，还需考虑增加的使用和维护成本”，他说，如果是具有生物识别能力的人脸识别，通常会使用红外线或激光作光源，利用对特定器材来采集人脸，一般使用照片是无法验证通过的。但人脸识别技术的普及，需经历技术学习和供应链成熟的过程，时机尚未成熟，此技术安全应用到智能锁上还需要一定时间。

专家提醒：因为智能锁的人脸识别功能不够成熟，暂不建议消费者购买带人脸识别功能的智能锁。

(下转B10)

责编：刘伟 美编/本版制图：林燕芳