专家称,一半物联网智能设备在“裸奔”,安全漏洞极易被攻击

扫地机器人分分钟变家庭偷窥者

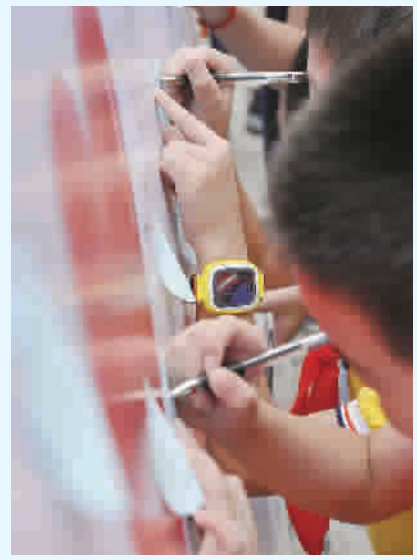
焦点

本报记者 程绩

“智能摄像头被曝导致大量用户隐私泄露。”昨天媒体的一则报道,揭开了物联网智能设备安全漏洞的冰山一角。

智能灯具、智能插座、智能手表、宠物婴儿监控器……当你购买这些智能家电的时候,或许不会想到,智能灯泡数据可能为小偷提供作案时间,智能摄像头正在现场直播你的生活场面,而智能冰箱也可作为垃圾邮件的发送端。

“大数据”时代,用户的网上行为数据往往在不知情的情况下被获取。专家提醒,目前市场上的物联网设备,至少一半都处于“裸奔”状态,存在安全漏洞极易被攻击。



▲▼► 儿童智能手表、家庭摄像头、扫地机器人等物联网智能设备很多存在安全隐患,一旦被攻击,很可能“出卖”你的隐私 图 CFP IC

智能儿童表
你的孩子可能被实时监控

临近暑假,上海市场上面对少儿的智能家电正热卖。昨天,记者来到市区某电子市场,发现近一半的柜台都把儿童智能手表放在最显眼的地方。商家的广告直击家长“痛点”:“儿童智能手表,孩子手上的贴身保镖”“担心孩子走失,那就给他戴款智能手表”。

“儿童智能手表销量第一,其次是智能学习机和智能机器人。”一个商家告诉记者,这几周的销量都是平日的两倍以上。

儿童智能手表价格参差不齐,便宜的一两百、贵的近千元,功能大多雷同:向家长提供孩子的位置信息、支持双向电话、语音群聊,部分还能接收文字信息。

记者随机采访了多位购买儿童智能手表的顾客,都认为手表“很实用”。一个妈妈表示:“现在小学生几乎人手一个,家长能和孩子随时通话,也能看到孩子行走的轨迹,走哪儿家长心里都有数。”让她不满意的是,最新款的手表都升级到了4G,增加了不必要的游戏功能。至于安全风险,大多数人都表示没想过。

近日,国内最大的安全众测平台“乌云”,发布了儿童智能手表的一份报告:淘宝销量前32位的儿童智能手表,有13款存在接口越权漏洞,可导致超百万儿童被黑客实时监控,获取儿童的日常行走轨迹,实时环境声音等。“乌云”的“白帽子”还现场演示,只要得到父母的手机号,或者是进入系统平台,便可破解该手机号关联的孩子的手表,从而获取实时定位、全部行走路线。

更令人意外的是,现在很多智能手表都有通话、监听、录音等功能,通过这些漏洞,不法分子可随时听到孩子的声音,了解孩子所处的环境。若手表放在家里,也随时可录制到家长的对话,无论对于小孩和家长,都存在比较大的隐私泄漏危险。

中国儿童智能手表市场正在快速发展,根据统计,2017年第一季度,中国儿童智能手表市场出货量高达351万台,同比增长64.9%。随着手表由2G向4G升级,功能越来越多,也伴随着风险的成倍叠加。

孩子安全的第一守卫者并不是电子产品,而应该是家长,家长的监护责任是任何电子产品都不能替代的。此外,让孩子学习一些安全常识,树立孩子自我保护意识也十分必要。

智能云存储
每30秒受到1次黑客攻击

“云存储”早就不是新鲜事物,伴随着物联网的发展,越来越多的智能家电也能与手机联网,在“云端”使用存储信息。轻触“上传”“保存”,原本需要存储在实体工具中的大容量文件,只需几步就能轻松保存到网络“云端”。但随之而来的,是个人隐私数据泄露的忧虑。

数据容量动辄以TB计数的时代,网络“云”能否真正有效保障个人信息不被泄露?

昨天,记者注册多个云平台,大多数运营商在《用户协议》中承诺,“不会公开或向第三方提供用户存储在云服务上的非公开内容”,细读下去,后面一句却另有深意,“除非有下列情况”。这些免责内容,大多包含在数千字的《用户协议》中,极易忽视。

“下列情况”大多包括:用户资料遭到未授权的使用或修改,造成的有形或无形损失,运营方不承担任何直接、间接的赔偿。还有一些看似提醒实则霸道的《服务协议》描述,例如:“(运营方)有权在无需事先通知用户的情况下,采取一切认为必要的措施”。

看不见摸不着的“云盘”,真的安全吗?事实上,云盘平台一直以来都是黑客攻击的重点目标,“有些云盘,平均每30秒就受到一次黑客攻击。”一位业内人士告诉记者。

互联网安全专家佟力强提醒,选择可信度高的网络产品服务提供商,使用新技术新产品前,一定要注意看《产品用户协议》,明白自己的权利义务。一些涉及重要人身隐私财产的信息,不要轻易上传云端。在发现违法犯罪行为时,应及时向网信、公安部门举报,并留存好相关证据材料。

近半年来,关于云盘泄露个人信息的事件层出不穷,中国政法大学知识产权研究中心特约研究员李俊慧认为,当前对互联网领域相关的规定还亟须完善,云数据储存需要厘清个人、运营商和监管者的权责界线。

智能家电
一旦染毒隐私无处可藏

5月,勒索病毒爆发,仅仅2天时间就造成了全球150多个国家的20多万人受影响,高校、火车站、自助终端、邮政、加油站、医院、政府办事终端等多个领域受到侵害。很多人惊魂未定,“智能家电也有可能被病毒感染吗?”

“现在的物联网设备基本都是在‘裸奔’。”专注物联网安全投资的永洲创投创始合伙人陆一舟“语出惊人”。

他举例称:有家厂商为了检测一款空调的噪音以改进产品,就在空调里安装了收集声音的装备,这些设备可以回传众多空调的分贝数。但就是这么一个装备,很快被外部的安全专家发现了漏洞,只需要略施小计,就可以将其变成“窃听器”。

互联网安全专家肖新光则举例:现在很多人家里都买了扫地机器人,这个机器人都有麦克、摄像头等装置,也需连接网络,这就相当于是一台潜在的监控设备。一旦遭到攻击,家庭隐私也就无处可藏。

2016网络安全大会,一个解码安全团队通过攻击智能插座,实现了利用插座发布微博。他们在接入到智能家居的控制网络后,利用漏洞攻击智能插座,获得APP端的认证信息,从而远程控制智能插座,再利用协议上的漏洞,便可以通过一个智能插座来发送微博。

“现在向物联网转型的企业,多数都是白色家电企业出身。他们的安全能力严重不足,固有思维是追求硬件的标准化,而黑客就是喜欢标准化的硬件。”一位业内人士告诉记者。

【专家建议】

用区块链技术给智能家电“加锁”

看似智能的家电,在黑客攻击面前往往不堪一击。切实有效的应对之策在哪里?最新的方向是区块链技术,相比备受争议的比特币,其背后的区块链技术,被认为有望改变世界的未来。

区块链就像一个数据库账本,记载所有的交易记录。区块链完整保存所有交易记录的特点让任何人都无法从中作假。简单来说,区块链就是一台创造信任的机器、一个安全可信的保险箱,可以让互不信任的人,在没有权威中间机构的统筹下,还能愉快地进行信息互换与价值互换。这种安全、便捷的特性逐渐得到了银行与金融业的关注。

去年底,复旦大学计算机科学技术学院成立“区块链技术联合创新中心”。昨天,记者采访复旦大学软件学院副院长韩伟力教授,他表示,“区块链可以提供一种可信赖的数据服务,因此可以广泛用于各类物联网应用中,所以应用到智能家电也是可行的。”

以智能摄像头泄露隐私事件为例,如果使用区块链技术是否可以避免?韩伟力教授解释,“使用区块链技术,可以方便物联网各个节点之间建立信任关系,也即可以让用户与摄像头、甚至各个物联网节点之间的相互认证变得更加便捷。当然这需要进一步地研发相关的应用系统,从系统、使用管理共同入手,才能保障智能家电的安全,并保护用户隐私。” 本报记者 程绩

【相关链接】

智能家电缺乏国家标准

“物联网安全,消费者能做的并不多”,互联网安全专家肖新光说,“不像电脑、手机等设备具有诸如下载杀毒软件等成熟的安全措施,智能硬件无法形成交互。”

这就对物联网设备厂商提出了更高的要求,“但现在的智能家电生产商,大多都是生产‘白家电’出身,安全意识淡漠。”360创始人CEO周鸿祎在去年的网络安全大会上称,“做企业做了11年,最无奈的还是国内企业对网络安全的漠视”。

多位安全专家提出,需要通过改变规则、制定法律等办法来明确智能硬件厂商的安全责任,尤其对于隐私、数据的合理采集、合法使用及妥善保管等方面。

目前,物联网时代的基础设施并不完善,包括云平台、通讯技术、信息传输等方面的安全技术保障都还不完善,尤其对于可穿戴设备产业而言,目前更多的是在硬件的产业链技术环节进行搭建,对于系统平台方面的安全考虑并不到位。

“现在很多的终端设备,既没有密码也没有保护程序,想要获得一个传感器的控制权相当的简单。”业内人士透露。

智能家电收集用户信息,收集后都会储存在自己厂家的云端,或者租用大公司的云服务器储藏,而一些实力小的公司,会存在用户信息泄露的问题,这样就给黑客一个可乘之机。 本报记者 程绩