被破解的“人脸识别”,“刷脸”究竟安全吗?

“人脸识别”的安全问题已经来了

9月13日凌晨,苹果发布新品iPhone X,新功能“Face ID”尤为引人瞩目。以后,无论是解锁iPhone X还是用其进行支付,用户只要看一眼手机就可以了。

不仅如此,多所高校在今年9月入学季尝试了“刷脸”注册;肯德基有餐厅上线了“刷脸”支付;“京东之家”有门店实现了“人即钱包”;甚至有公厕用上了人脸识别厕纸机,靠脸取纸巾;更别说银行的“刷脸”转账了。

支付宝刷脸取件

“刷脸”的时代说来就来

一大波“刷脸”场景出现,当不少人沉浸在“人脸识别”的惊喜中时,也有人发出疑问:“刷脸”安全吗?

最近一段时间,“人脸识别”技术在各地应用的新闻屡见不鲜。继北京天坛公园安装“人脸识别”厕纸机后,8月31日,广西壮族自治区南宁市一家公园也采用了“人脸识别”厕纸机;9月7日,江苏省徐州市一家公共厕所同样装上了“人脸识别”厕纸机。北京市住建委9月8日表示,为解决保障房违规转租转借现象,继去年在海淀区金隅翡丽小区推行“人脸识别”门禁系统试点基础上,今年进一步在全市所有公租房小区推广。北京、武汉等地的火车站也开始启用“刷脸进站”设备。

《法制日报》记者在网上搜索发现,目前在门禁、考勤等方面应用“人脸识别”技术已经十分广泛。然而,任何新技术都可能是双刃剑。“黑科技”在带来更多惊喜和便利的同时,其潜藏的安全隐患也不容忽视。

尴尬的使用体验

9月18日14时,《法制日报》记者来到北京市通州万达广场的京东之家体验“刷脸”支付。记者选中商品后来到支付柜台,店员优先推荐扫码支付。在记者表明要体验“刷脸”支付后,店员劝道:“这个技术还不太成熟,步骤比较烦琐,我们自己试了很多次,都不成功。之前也有顾客来尝试,没有支付成功。”记者执意表示愿意尝试后,店员才指导记者通过京东App扫码开通了“刷脸”支付功能,但是最终卡在了支付页面,无法付款。店员的电脑端也显示记者没有支付成功。记者随后多次退出App程序,尝试重启进入该功能,但都失败了。

同样作为使用者的北京师范大学大四学生墨桑(化名),对于“刷脸”的使用感受也是一言难尽。

墨桑对《法制日报》记者说:“说是化妆或者戴眼镜都不会有影响,但是戴眼镜的话,在录入时要对戴眼镜和不戴眼镜的图像各录入一遍,传说‘亲妈都认不出来的时候,机器还能认出来’。”

在墨桑看来,如果正常识别,速度还是挺快的,但并非每次都如愿。“如果学生卡、学号都不能够与图像识别系统匹配,还有最后一招,就是对着那个机器大声喊出自己的名字。第三种开启方式让我们很尴尬,虽然这种情况不多,但是已经出现了”。

在便捷性上,墨桑说:“识别系统本来就只是为了提高安全性的,不是为了更方便。虽然没有做过调查,但是听同学说安全性反而降低了,而且现在出公寓也要刷卡,谈不上便利。也许以后会改进,一次只放一个人进入,不过这也太麻烦了。”

杂乱的产品市场

和国外的“人脸识别”技术多应用于安防领域不同,在我国,“人脸识别”技术主要应用于企业的考勤门禁、物业小区的安全防护和金融领域的开户认证等,其中金融领域的应用占比较多。不过,目前比较常见的“人脸识别”技术主要出现在考勤机等应用上。

《法制日报》记者以购买者的身份采访了北京市一家专业从事“人脸识别”设备销售的企业,并现场测试了一台集“门禁”“考勤”为一体的多功能考勤机。

在现场,记者首先进行人脸照片录入,主要对人脸的眼眶、鼻区以及嘴部三块区域进行图像采集。录入之后,记者站在机器前进行识别,只要一进入摄像头可照范围之内立即就被识别成功。不过,记者摘下眼镜或者更换眼镜以及调整眼镜佩戴角度后,考勤机无法识别成功。此外,用照片比对,该设备依然无法识别。

据工作人员介绍,目前“人脸识别”考勤机的价位从数百元到上万元不等,价格越高,识别的精确度越高。记者测试的这款产品是最畅销的千元机,只要脸部采集到的数据能吻合到六成以上,便能认定是同一人。不过相对而言,由于采集时拍摄下来的一些特征相对单一,所以精确度也会受到影响。

在问答平台“知乎”上,一位网友回答了“目前人脸识别技术最大的挑战是什么”这一问题,其答案获得最高赞。这位网友告诉记者,淘宝上卖的“人脸识别”锁不能保证绝对安全。记者询问这种产品是否有可能被3D仿真面具欺骗?这位网友说,这种情况可能发生。

记者随后在淘宝上搜索“3D面具”“乳胶面具”,发现这种产品也有不少,有的面具不仅改变了容貌,而且改变了脸部的骨骼结构,戴上之后多有以假乱真的效果。

被破解的“人脸识别”

尽管“人脸识别”产品的客服人员声称一般不易被破解,但现实生活中已然出现了破解实例。破解“人脸识别”的实例,要从一次网约车经历说起。

一名市民通过网约车App下单。很快,车到了,但车辆、司机的信息均与手机客户端上显示的信息不符。为了赶紧回家,这名市民也顾不上太多,就直接上车了。结果,车开出去不到一分钟,司机就扭头对这名市民说要取消订单。尽管这名市民一再拒绝,但司机还是坚持把她送回原处,让她重新打出租车。

没有办法,这名市民只能再次用这款网约车软件叫车,结果发现来接他的还是那名司机。司机说:“你要么就打个出租车回去,只要你还用这个软件约车,叫到的还是我的车。”

这名市民当时就纳闷了,为什么会这样?一番打听后,这名市民才知道,附近有一个由30多名“黑车”司机组成的车队,每名司机都有一堆虚假的司机账号,上百个虚假账号由同一个人来统一接单,然后通过电台调度车辆去接人。因此,不管用户打到哪个号,都会调同一名司机去接人。

没错,“高大上”的“人脸识别”技术就这样被一群“黑车”师傅给黑了。

以上故事是在Freebuf(国内关注度最高的全球互联网安全媒体平台)主办的FIT2017互联网安全创新大会上,平安科技安全研究员高亭宇在一场“关于人脸识别技术应用风险”主题演讲中的一段描述。

在采访过程中,甚至有业内人士这样表示,“不是3D打印不行,如果用一台精密的打印机,破解‘人脸识别’同样不在话下”。

“除了一般的考勤、账号安全App之外,大量的银行、P2P金融企业的App已经介入使用了‘人脸识别’技术,其中金融行业在使用‘人脸识别’技术时的安全性明显高于一般应用;当‘人脸识别’技术涉及关键业务时,安全防护水准往往更高。”高亭宇说,比如他在测试国内某P2P金融的客户端时,尝试“人脸识别”解锁失败数次后,该App就检测出了可能存在恶意破解的情况,强制使用银行卡信息、手机短信等其他方式来完成认证。

高亭宇在现场强调了一点,除了“人脸识别”技术在手机上的应用缺陷之外,许多问题导致的原因都是开发者在调用第三方“人脸识别”服务时,没有严格按照一个安全的规范来做,接入流程不够严谨,甚至经常出现为了提高用户体验而舍弃安全性的做法,这样的做法在技术实力不强的小公司十分常见,最终导致的结果就是,让用户把密码写在了自己的脸上。⑬3

据新华社