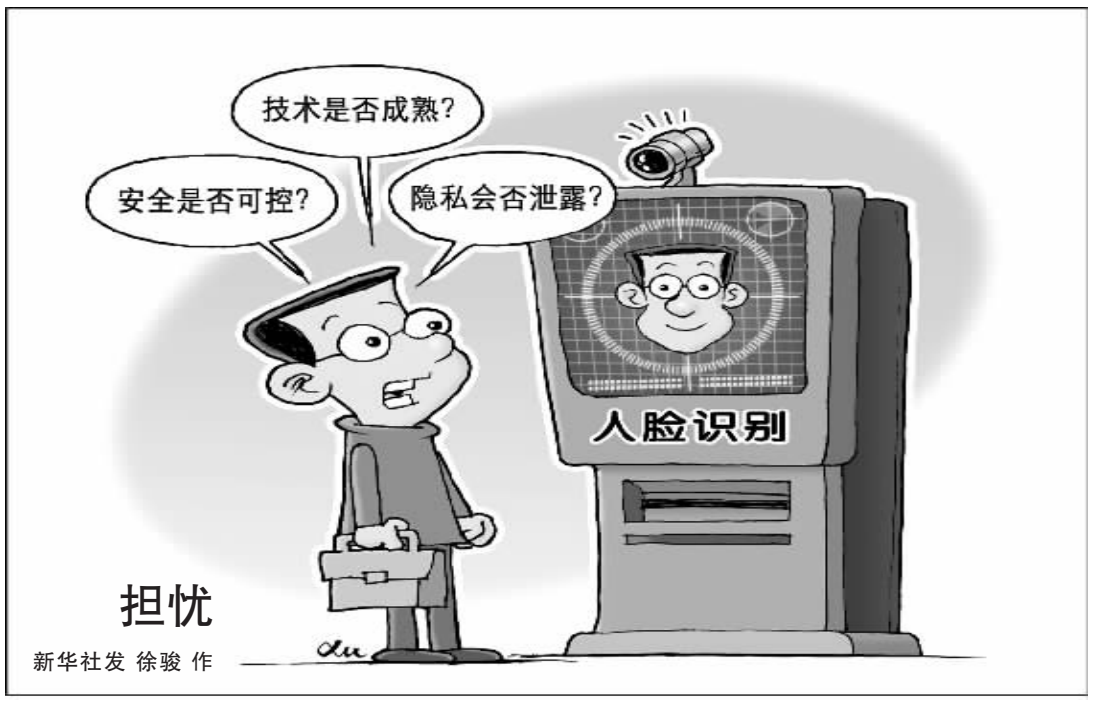
刷脸时代 你的“脸”还安全吗



担忧

新华社发 徐骏 作

2 分半破解人脸识别门禁 打印照片 10 秒解锁手机

人脸解锁、刷脸取款、刷脸买单、刷脸寄快递、刷脸住店、刷脸坐高铁……在正在到来的这个“看脸”时代,你的“脸”安全吗?

2 分半钟破解人脸识别门禁,彩色打印人脸照片 10 秒钟解锁手机……“黑客”们的一场场现场秀提醒消费者:人脸识别等生物识别技术可能潜藏安全风险和隐私问题,刷脸要谨慎,毕竟,“丢了密码可以重新设置,脸丢了就找不回来了”。

窃取关键人物的指纹、虹膜、声音(声纹)甚至人脸信息,突破警卫森严的宝库偷天换日,这是电影大片里的情节。

在刚刚结束的 GeekPwn2017 国际安全极客大赛上,白帽黑客们现场上演“谍中谍”,短短几分钟甚至几秒钟就能轻松攻破人脸识别、虹膜识别、指纹识别等生物识别系统。

评委在一台人脸识别门禁系统中录入自己的脸,只有这张脸才能打开门禁。浙江大学计算机系毕业的女黑客 tyy 用了不到 2 分 30 秒就成功通过了刷脸机。tyy 解释说,她通过 wifi 进入门禁系统,利用系统漏洞,直接获取控制权限,修改人脸信息,也就是把设备中存储的评委人脸换成了自己的脸。

更令人感到不安的是,来自百度安全实验室的“小灰灰”和高树鹏,用了不到 10 秒,就用一张打印的照片在一定光线环境下解锁了一部手机。“理论上,只要拍到一张手机主人的清晰照片就可以解锁了。”现场评委、霸众信息首席技术官徐昊说。

“现场演示攻击并不是要制造恐慌,而是通过发现漏洞,督促厂商改进技术、修复漏洞。”GeekPwn 大赛发起和创办人王琦说,大赛会将发现的漏洞反馈给厂商,让越来越多的企业和公众关注技术安全。

越智能是否越脆弱

“每个人只有十个指纹、两个虹膜、一张脸,这些暴露在外的信息一旦被破解,就是严重威胁。”白帽黑客“小灰灰”的话说出了大众的心声:看起来高大上又方便的人脸识别技术安全吗?智能度越高的产品,安全会不会越脆弱?

——技术是否成熟?很多公司都宣称其人脸识别准确率超过 99%,对此,长期研究机器学习的西安交通大学电信学院特聘教授龚怡宏介绍,这指的是在一些世界知名人脸数据库比对中取得的成绩,但在现实运用中,这种准确度要大打折扣。人群样本更大,不同光线、姿态、分辨率等条件都可能给机器识别带来困难。

——安全是否可控?小偷有没有可能用假脸欺骗门禁进入小区?金融罪犯会不会用“仿冒人脸”登录银行系统窃取钱财?

在业界专家看来,这是一种技术“攻防战”。目前很多人脸识别公司都加大了在活体检测上的技术投入,确保系统检测到的是一个“活人”,提高对攻击的防御能力。以人脸取款为例,农业银行上海分行个人金融部经理杨晟栋告诉记者,人脸取款采用红外双目摄像头活体检测技术,同时对脸部细微动作和微表情进行检测,识别度远高于手机摄像头,假脸或者照片都不可能骗过系统。

——隐私会否泄露?上海市信息安全行业协会会长、众人科技董事长谈剑峰说:“生物特征是唯一特征,但这反而可能是不安全的。密码丢失后可以设置一个新的,但有大量生物特征信息的服务器一旦受到攻击,数据库被拿走,你不可能再有第二张脸。”

多重验证 尽快立法防止“人脸裸奔”

专家表示,任何技术都是在攻防的过程中不断演变升级,最终在安全性和便捷性之间达到平衡。“世界上没有完美的技术,如果在特定的场景下,一项新技术的准确度能够满足要求,错误带来的风险可以承受,那它就是有价值的。”奇虎 360 公司副总裁、新加坡国立大学教授颜水成说。

王琦提醒,不管是厂商还是消费者,都不要出于赶时髦或者追捧概念去使用一些尚未成熟的技术。消费者在社交、互联网等场景刷脸要慎重,尤其不要把脸作为关键信息的“钥匙”。

中科院自动化所生物识别与安全技术研究中心主任李子青等专家建议,从安全层面考虑,人脸识别最好跟多种验证方式交叉使用,尤其是对安全要求极高的金融场景。比如,为了防止照片、视频播放、3D 头套等假脸攻击,银行刷脸取款都同时进行人脸识别、手机号码或身份证验证、密码验证三层防护。

尽管很多厂商宣称自己对采集的照片和人脸生物特征会进行脱敏处理,但在商汤科技联合创始人杨帆看来,保护用户隐私不仅需要企业自律,更需要政府引导行业建立统一标准,筑起保护用户隐私的堤坝。目前,欧洲监管机构已在即将出台的数据保护法规中嵌入了一套原则,规定包括“脸纹”在内的生物信息属于其所有者,使用这些信息需要征得本人同意。

“点点滴滴的个人隐私汇集起来就是国家信息安全。”在谈剑峰等业内人士看来,最重要的是立法保护公民隐私,以及确定人脸识别等技术的使用边界。“我国应尽快建立生物识别的法律和技术标准,比如什么地方能用,怎么使用;用什么技术采集、达到什么样的安全级别、采集多少个点位的特征、信息要做多少层加密,这些都需要通过立法尽快明确。”

(据新华社电)