简译版

对数字安全来说，生物识别技术是福还是祸？

非官方中文译文•安天技术公益翻译组 译注

文档信息			
原文名称	Are Biometrics Good or Bad for Digital Security		
原文作者	Larry Alton	原文发布日期	2018 年 6 月 8 日
作者简介	Larry Alton 是一位独立商业顾问。		
原文发布单位	InformationWeek		
原文出处	https://www.informationweek.com/strategic-cio/security-and-risk-strategy/are-biometrics-good-or-bad-for-digital-security-/a/d-id/1331991?		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

对数字安全来说，生物识别技术是福还是祸？

Larry Alton

2018 年 6 月 8 日

有人说，生物识别技术对数字安全是有益的，但是这项技术确实存在缺陷。

很多公司都很关心数字安全，无论是保护自己的信息不被竞争对手和网络犯罪分子窃取，还是保护客户免受威胁的侵害。这些公司开始考虑采用生物识别技术进行身份验证。顾名思义，生物识别技术是指根据人体某一部位的特征进行身份验证或识别，包括指纹、人脸和其他任何独特的身体特征。

通过视网膜扫描开门，或者通过耳朵的形状识别客户身份，诸如此类的想法似乎有些天方夜谭。但是，这真的是数字安全的前进方向吗？

优势

随着现代智能手机的发展，指纹识别（Touch ID）和人脸识别（Face ID）功能已经成为主流。公平地说，与传统的身份识别和验证方法相比，这些方法有一些显著的优势。

- **最明显的优势在于特征的独特性。**我们以指纹为例，世上没有完全相同的两组指纹，因此，只要成功扫描到相应的指纹，就能确认对方的身份。大多数生物识别特征都很难伪造。
- **生物识别技术便于使用。**你不必记住一大堆口令或携带证件来证实你的身份，你只需要笑一笑，眨一眨眼睛，摆弄一下耳朵或者扫一扫手指纹就可以了。创建生物识别技术也比较容易。
- **准确性。**虽然生物识别扫描仪不是 100%准确的，但几乎万无一失。最新的指纹技术综合研究发现，单指测试准确率高达 98.6%，双指测试的准确率高达 99.6%，四指（或更多）测试的准确率则高达 99.9%。
- **成本低。**虽然创建生物识别系统的成本可能很高，但从长期来看，其管理成本远低于传统系统。公司可以减少文书工作，避免所有的密码重置成本。此外，与传统系统相比，如果生物识别技术能够防止任何欺诈或滥用行为，就可以为公司节省数百

万美元的成本。

劣势

另一方面，生物识别技术也有其缺点。

- **设备局限性。**目前，智能手机是拥有生物特征识别功能的最方便和便携的设备，但是智能手机有其局限性。它的指纹扫描区较小，因此只能采集部分指纹。研究表明，由于这种固有的局限性，人们可以设计“万能指纹”来愚弄手机；目前有 5 种指纹设计能够骗过约 65%的设备。
- **特征更改。**生物识别技术依赖于唯一和持久的人体特征，但如果这些特征发生了变化呢？如果有人复制了你的特征呢？要复制虹膜或耳朵的形状可能很难，但如果有人真的复制了，你基本不可能更改你既有的、作为安全措施的特征。考虑到至少已经发生过一次大规模窃取生物识别数据的黑客攻击，这是一个严重的威胁。
- **口令重置。**传统数字安全措施的一个优点是可以远程执行；如果你发现有人盗用了你的信用卡或在线帐户，可以使用口令在个人设备上登录该帐户，将其关闭，或更改口令。但是，如果你的生物识别信息被盗，你需要亲自到现场验证身份，到那时，损害可能已经造成了。
- **系统限制。**生物识别技术仍然依赖于数据库，而数据库是很脆弱的。美国联邦调查局（FBI）已经将约一半美国人的脸部特征储存在大型数据库中；但是没有办法保证这些数据库的安全。如果有人侵入了这些数据库——无论是通过暴力破解还是猜测员工弱口令，就能访问其中的数据，进而操纵数以百万计的帐户。

生物识别技术在数字安全中的作用

生物识别技术拥有传统数字安全措施无法企及的优势，但我们不应把它视为一场全面的革命。相反，它只是多种工具中最新的一种，我们应该组合使用这些不同层次的工具来增强安全性。总的来说，任何公司都不应该“将所有鸡蛋放在一个篮子里”，任何一种安全解决方案都不太可能是万无一失的，因此我们需要使用多种解决方案，以获得最佳的保护效果。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*