**真相揭秘：手机的指纹解锁真的安全吗？**

　　每个人的指纹都是独一无二的，但纽约大学及密歇根州立大学的研究人员发现，两枚指纹之间的局部特征普遍存在相似性，因此手机或其它设备上的那些基于指纹的安全系统，要比想象中的脆弱的多。



　　系统的漏洞在于，用于身份验证功能的指纹传感器并不会捕捉用户指纹的完整图形，相反，它扫描储存的只有指纹的部分区域，而且许多手机还允许用户在系统里录入多个手指的指纹。

　　只要用户的指纹与系统里保存的区域指纹相匹配，手机就会解锁。据研究人员推测，不同人的指纹区域之间可能存在足够的相似性，足以用来制造出虚假的“超级指纹”，从而骗过手机的指纹传感器。

　　该研究的合著者，密歇根州立大学计算机科学与工程系教授Arun Ross表示，许多电子设备比如智能手机均开始将指纹传感器用于用户身份验证，但手机上的指纹传感器尺寸很小，扫描录入的只有一部分指纹。为了弥补这个不足，电子设备通常会在注册过程中，要求用户录入单个手指指纹的不同区域点，以确保其中至少有一个会在身份的识别过程中与获取到的指纹图像成功匹配。而正是这一点使得情况不妙。

　　“由于指纹传感器的尺寸变小，提高传感器的分辨率就显得十分必要，这样才能捕捉到额外的特征点，”Arun Ross说道，“如果不提高分辨率，那么将不可避免地损害到用户指纹的独特性。研究过程中的实证分析也证实了这一点。”



　　Ross表示，研究团队目前正致力于如何解决这个突出的漏洞。其中包括需要开发出有效的反电子欺骗技术；在用户注册时谨慎挑选指纹的数量和类型；提高小型传感器的分辨率以便于提取更多特征点；提高利用了节点与纹理的识别技术；以及设计更有效的综合方案，从而将用户的多个指纹区域结合起来。

　　纽约大学计算机科学和工程研究组组长Nasir Memon称，“超级指纹”有点类似于一个黑客，试图用1234这种通用密码来破解PIN码（手机SIM卡的个人识别码）。

　　Memon表示：“1234这个密码大约有40%的几率是正确的，据我们估计，这个正确率有点高。”

　　国家科学基金会资助研究人员对8200枚指纹进行分析试验。通过商业指纹验证软件，研究人员每批次抽取800枚指纹，结果显示平均有92枚具备成为“超级指纹”的潜在可能性。（他们将“超级指纹”设计为在随机抽取的每个批次中，至少能够匹配于其中4%的虚假指纹。）



　　相反地，在800份完整的试验样本中，研究人员只发现了一枚完整的可用作“超级指纹”的人造指纹。Memon表示，“这并不奇怪，匹配部分指纹的成功率要比匹配一整枚指纹的高得多，然而大部分设备用来匹配的都是部分指纹。

　　研究人员对取自真实指纹图像的“超级指纹”的特征进行分析，建立了一个算法用于创建合成“超级指纹”。实验表明，人造的合成指纹匹配的可能性更高，与某些真实的指纹相比反而更能骗过安全识别系统。而由真实指纹结合制成的“超级指纹”成功匹配了系统中26%-65%的用户指纹，其成功率取决于用户储存了多少指纹图像，并设定了每次最多尝试匹配5次的限制。

　　用户在手机里录入的指纹越多，安全系统就越脆弱。

　　研究人员强调他们的工作是在模拟环境下完成的，但需要注意的是，人造指纹技术的发展以及将电子指纹转移到实体的技术，可能导致攻击生物识别设备的可能性提高，这是一个很严重的问题。

　　由于“超级指纹”的高匹配度，设计值得信赖的基于指纹识别的身份认证系统正面临挑战，亟需加强方案的设计，从而利用多种因素进行身份验证，以提高系统的安全性。研究人员认为，这项研究将会影响未来安全系统设计的方向。同时，Memon表示，目前使用密码解锁手机仍是安全的。