Face ID Security

2017 年 11 月

苹果官方说训练用来识别和抵制欺骗的神经网络，可以防止用照片或面具解锁手机的行为。越南研究人员研制 3D 面具破解 iPhoneX 的 Face ID，被打脸了，那么 Face ID 到底安全吗？下面，我们来看看官方的 Face ID 指南。

看一眼手机就可以安全地解锁 iPhone X，face ID 技术由 TrueDepth camera 系统提供安全认证，使用了先进的技术来精确地绘制面部集合图形。Face ID 通过检测识别人的方向，使用神经网络来进行匹配和反欺骗，然后就可以解锁 iPhone 了。Face ID 可以自动适应面部的变化，并且确保识别人生物数据的安全和隐私。

Face ID and passcodes

使用 Face ID 之前，首先有设置 iPhone X，那么就需要密码来解锁设备。当 Face ID 检测并匹配到识别人的脸，iPhone X 就会直接解锁设备。Face ID 让用户无须频繁输入又长又复杂的密码。然而 Face ID 并没有取代密码，只有提供一种更加方便的解锁方式。强密码是 iOS 设备加密保护的重要基础，在很多情况下，仍然需要输入密码：

- ✓ 设备刚开机或重启过。
- ✓ 设备超过 48 小时没有被解锁。
- ✓ 在过去的 156 个小时内，密码没有没用来解锁设备，并且过去 4 小时内 Face ID 也没有被用来解锁设备。
- ✓ 设备收到远程锁屏命令。
- ✓ 5 次面部识别未成功。
- ✓ 同时按下音量键和侧键 2 秒发起关机或者 SOS 请求后。

当开启 Face ID 后，按下侧键或者设备进入休眠状态都会马上进入锁定状态。每次唤醒，Face ID 需要面部匹配或者输入密码。随便一个人用自己的 Face ID 解锁你

手机的概率是 1/1000000，随机的一个人用 Touch ID 解锁你手机的概率是 1/50000。所以 Face ID 会比 Touch ID 更安全。Face ID 只允许连续验证 5 次（在验证不成功的情况下），这也增强了安全性。

对长得比较像的双胞胎、表兄弟（姐妹）和 13 岁以下的儿童，这个 false match 的概率是不一样的，因为并没有发现他们面部特征的不同。如果对此有担心，我们建议使用密码进行认证。

Face ID 安全

Face ID 设计之初是为了确认用户 attention，提供低误配率的健壮的认证方式，缓解数字和物理欺骗。当 iPhone X 唤醒或需要进行 Face ID 识别时，TrueDepth camera 能自动寻找识别人的面部。当检测到面部时，Face ID 通过检测眼睛是否睁开和是否注视着设备来确认 attention 和 intent 来解锁。当 VoiceOver 开启后，Face ID 不能同时使用。当确认了识别人的面部后，TrueDepth camera 会读取超过 3 万个红外点来组成面部的深度图。这些数据用来穿件 2D 图像和深度图序列，这些数据经过数字签名然后发送给 Secure Enclave 模块。

为了应对数字和物理欺骗，TrueDepth camera 会将 2D 图形和深度图序列随机化，并创建特定设备的随机模式。A11 仿生学处理器的神经引擎把这些数据转化成数字的表示，并与之前注册的面部数据进行比较。这些注册的面部数据本身也是获取的面部数据的数学表示。

面部匹配是在用神经网络训练过的 Secure Enclave 内执行的，开发的面部匹配神经网络使用了超过 10 亿图片，包括研究中收集的 IR 和深度图片等。Face ID 的设计就考虑了用户戴帽子、围巾、眼镜、隐形眼镜和太阳镜的情况。另外一个用来抵制欺骗的神经网络可以抵御用照片或面具用来解锁手机的尝试。含有面部数据的数学表示的 Face ID 数据经过加密，只能通过 Secure Enclave 访问。所以这些数据不会离开设备，也不会发送给 Apple，也不会保存到设备备份中。

在正常的操作中，Face ID 数据的保存、加密都只给 Secure Enclave 使用。

✓ 在注册过程中面部的数学表示的计算；

- ✓ 计算的面部的数学表示用来解锁设备过程中，如果 Face ID 认为这些数据在以后的匹配中有用。

在正常操作中获取的面部图像是不保存的，一旦计算进行注册或者与 Face ID 数据进行对比后就会丢弃。

Face ID 如何解锁 iOS 设备

Face ID 关闭后，当设备锁定后，最高等级的数据保护的密钥就被丢弃了。那个等级的文件和 keychain 不输入密码就无法解锁设备。开启 Face ID 后，当设备锁定后，这些密钥是不会被丢弃的，他们被封装在 Secure Enclave 中的 Face ID 子系统的密钥中。当用户尝试解锁设备时，如果 Face ID 认出了用户的脸，就提供密钥来解封这些数据保护密钥，该设备就被解锁了。这个过程通过要求数据保护和 Face ID 子系统的协作对解锁设备提供了额外的安全保护。

当设备重启时，Face ID 要用来解锁设备的密钥丢失了，当符合要求密码认证的条件下，Secure Enclave 就会丢弃密钥。为了改善解锁的性能，并且跟上人脸的变化，Face ID 扩展了它所存储的数学表示。成功解锁设备后，在数据被丢弃前，Face ID 可能会用新计算出的数学表示来进行多次额外的解锁。如果 Face ID 没有识别出用户，但是匹配质量高于一个特定的阀值，而且匹配识别后，用户马上输入了密码，Face ID 就会把这个新计算出的数学表示加入到注册 Face ID 数据中去。这个如果 Face ID 多次解锁失败，并且用户停止匹配，那么这个新的 Face ID 数据就会被丢弃。这个扩展的过程允许 Face ID 跟上头发、化妆等带来的变化，而且可以减小错误匹配率。

Face ID 和 Apple Pay

Face ID 可以用在 Apple Pay 中进行简单和安全的支付。为了在 Apple store 中使用 Face ID 进行支付认证，首先要连续两次按侧键确认支付的 intent。然后把 iPhone X 放到无接触的支付读卡器附近，就可以用 Face ID 认证了。如果想要

Face ID 认证中选择不同的支付方式，需要再认证一次，但是不需要连续两次按侧键。如果连续两次按侧键后 60 秒内没有完成支付，需要再次连续两次按侧键来确认 intent。

Face ID Diagnostics

Face ID 数据不会离开设备，也不会备份到 icloud 和其他地方。如果用 Face ID 联系 AppleCare 寻求支持，那么可能会被问到是否愿意提供 Apple diagnostic 信息，包括 Face ID Diagnostics 数据。使用 Face ID Diagnostics 需要 Apple 的数字签名认证，这与软件更新个性化过程用到的是一样的。认证之后，需要激活 Face ID Diagnostics 并开始设置。作为设置 Face ID Diagnostics 的一部分，已注册的 Face ID 会被删除，并要求重新注册 Face ID。
iPhone X 会开始记录 7 天内尝试认证获取的图片，iPhone X 不会保存之后的图片。Face ID Diagnostics 不会自动发送数据给 Apple。在发送给 Apple 之前，用户可以检查、批准 Face ID Diagnostics 数据，包括 diagnostics 模式下收集的注册和解锁图片。Face ID Diagnostics 会上传用户批准的 Face ID Diagnostics 图片，数据在上传前会加密，在上传完毕后会马上从手机上删除。用户拒绝上传的图片会马上删除掉。如果用户不能通过检查图片和上传批准的图片来决定 Face ID Diagnostics 会话时间，Face ID Diagnostics 会在 90 天后自动结束，所有 diagnostic 图片都会从 iPhone X 上删除。用户可以随时关闭 Face ID Diagnostics 服务，一旦关闭，所有本地图片就会立刻删除。

Face ID 的其他用途

第三方应用可以用系统提供的 API 来要求用户用 Face ID 或者密码来认证，支持 Touch ID 的应用自动支持 Face ID。在使用 Face ID 时，只有在认证成功时，应用才会收到通知，应用不能访问 Face ID 和相关的数据。密钥链（Keychain）也可以用 Face ID 来保护，只有在面部匹配或用设备密码时才由 Secure Enclave

发放。应用开发者也有相应的 API 在解锁 keychain 前来验证密码是否以前被设置过。应用开发者可以：

- ✓ 要求认证 API 的操作不依赖于应用的密码或设备的密码。可以查询面部是否注册过，允许 Face ID 作为安全敏感型应用的第二个认证因子。
- ✓ 生成和使用 Face ID 保护的 Secure Enclave 中的 ECC 密钥。在 Secure Enclave 授权使用后，与这些密钥相关的操作都在 Secure Enclave 内进行。

用户也可以配置 Face ID 用于 iTunes，App store，iBooks store 等的购买，无须输入 Apple ID 密码。在 iOS 11 和之后的版本中，Face ID 保护的 Secure Enclave ECC 密钥通过对 store 请求进行签名的方式对用户授权购买行为。

英文原文：

https://images.apple.com/business/docs/FaceID_Security_Guide.pdf