香港仔
LION ROCK DAILY
Facebook
lionrockdaily香港仔 www.lionrockdaily.com | 2023.10.27 | 星期五

P.11 減辣後首開新盤 香港仔樓車位價
P.15 美槍械教官 射殺22人逃遁

中大揭近300個App存漏洞 涉金融消費等領域

用硬照可過關 商用掃面高危

隨着人臉識別技術的應用越來越普遍，不少流動裝置、應用程式或賬戶操作，也透過掃描人臉就能啟動，但有關的安全問題亦引人關注，更有不法分子盜用用戶的個人資料和硬照後「偷天換日」，成功通過人臉識別進入系統。香港中文大學研究人臉識別系統設計中的弱點，發現全球18,000多個流動應用程式中，近300個存在安全漏洞，在一些情況下以硬照進行人臉識別亦能瞞天過海，登入iOS及Android流動裝置。學者建議，供應商採用多種方法加強驗證流動應用的防護，以及適當加密，用家也不能盡信由客戶端傳回的結果。

■中大團隊的研究發現，近300個人臉識別應用程式存在安全漏洞。

人臉識別一直被視為最安全的生物識別技術，但由中大工程學院信息工程學系教授劉永昌領導的研究團隊，深入分析檢測市場上18個人臉識別服務供應商提供的流動應用模組，發現其中11個存在安全漏洞，其共同點是黑客可利用這些設計漏洞繞過活體檢測，冒用他人身份開立賬戶或盜取資料。

研究團隊撰寫應用程式，以自動化分析方法，掃描18,000多個流動應用程式，發現當中有294個使用了含安全漏洞的人臉識別應用模組。劉永昌表示，隨着人工智慧的快速發展和電腦視覺技術的不斷突破，人臉識別技術已完成商業化落地，而這些存在漏洞的流動應用程式，滲透到金融、消費、生活、教育等各個領域，關於金融方面的流動應用程式更佔39%。

黑客在一些情況下，只需使用「受害者」的照片與身份資料，便可完成人臉驗證。此外，劉永昌指出，現時為防止黑客盜用他人圖像進行身份欺騙或建立傀儡賬戶，大部分人臉識別系統要求用戶在建立賬戶時完成眨眼、搖頭等動作，甚至有系統需要進行紅外活體檢測，目的是確保真人完成人臉驗證手續而非硬照，但仍防不勝防，有不法分子會通過3D列印面具或deepfake（深度偽造）等手段，利用機器學習模型弱點攻破人臉識別系統。

對填補人臉識別的漏洞，劉永昌認為須由人臉識別的開發者或者發行者着手，應以多種方法加強流動應用的防護，如程式加固和動態反調試等，以及將所有流動應用、第三方模組、雲服務器之間傳輸的人臉識別相關數據進行適當的加密。

劉永昌強調，市民作為使用者也不應坐以待斃，使用人臉識別登入前，先確認這個網站或者軟件是否安全，盡量降低個人資訊的洩露風險。

全球86%高校Wi-Fi不安全

另外，不少僱主為員工提供企業級Wi-Fi及VPN服務，以方便他們利用流動裝置如手提電腦或手機工作。中大工程學院信息工程學系助理教授周思驍領導的研究團隊，就多個主流企業級Wi-Fi及VPN服務進行深入分析及測試。在企業級Wi-Fi方面，世界各地2,000多所高等院校的7,000多份Wi-Fi用戶手冊，86%學校有至少一項操作系統指示用戶採用不安全的Wi-Fi設定。

在VPN產品方面，研究團隊測試全球132個被採用的VPN，並在其中63個找出之前未被發現的嚴重漏洞，讓黑客可以在用戶不知情的情況下盜取其密碼。周思驍提醒，市民千萬不要盲目點擊「確定」、「連線」和「接受」等按鈕，遇到可疑的情況，應向所屬單位的資訊科技管理員報告及查詢。

使用人臉識別服務的安全建議

- 盡可能在雲端驗證人臉識別信息，切勿完全相信由客戶端傳回的結果。
- 應以多種方法加強流動應用的防護，如程式加固和動態反調試等。
- 將所有流動應用、第三方模組、雲服務器之間傳輸的人臉識別相關數據進行適當的加密。

使用Wi-Fi及VPN的安全建議

廠商

廠商要對產品進行徹底的測試，以防止可能會引致安全風險的缺陷。

資訊科技管理員

在編寫使用手冊時，需要考慮可能會發生的意外，並教導使用者如何正確地處理這些狀況。

使用者

盲目點擊「確定」、「連線」和「接受」等按鈕，通常不是一種有效保護網絡安全和個人資料的做法。在點擊按鈕之前，應試着去了解潛在的影響，不要因為貪圖一時的方便而後悔莫及。

資料來源：香港中文大學

編輯部: 2873 8233 傳真: 2552 6161 廣告部: 2873 9888 3708 3888 發行中心: 2873 9889 承印: 三友印務有限公司 地址: 香港仔田灣海旁道7號興偉中心2–3樓