運動手環 APP 洩漏你的行蹤

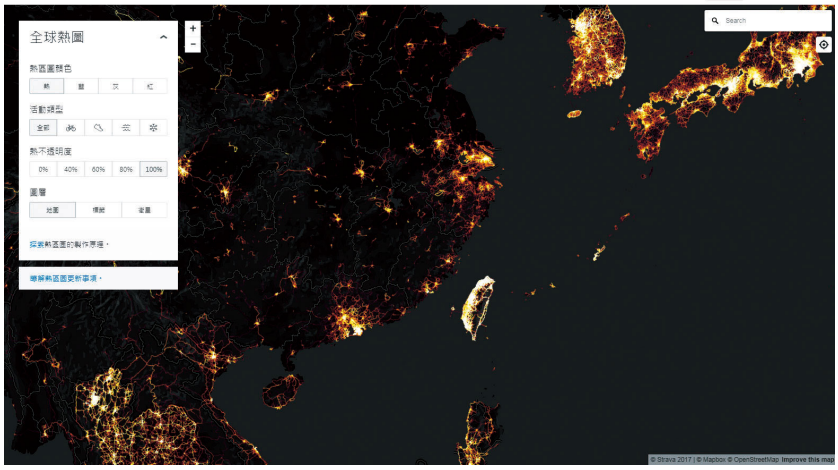
■ 陳姿陵

在運動風氣盛行下，美國 GPS 定位公司 Starva Labs 推出可使用於運動手環之智慧型 APP 後，大受歡迎；該公司將過去 2 年從全球用戶蒐集來的大數據，繪製成一份健身追蹤地圖（又名「全球熱圖（Global Heat Map）」）並於 2017 年 11 月間上網公布，其上顯示出全球超過十億條跑步和騎車健身路線，卻引爆各國秘密軍事基地被曝光的危機。

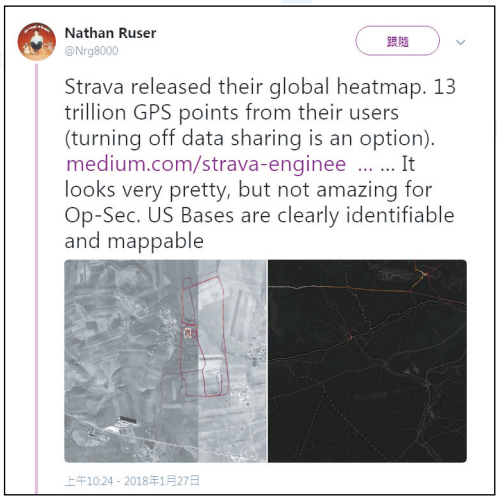
現今科技日新月異，「雲端」、「WIFI」與「APP」等技術或軟體相繼問世，現代人生活已離不開科技；隨處可見的個人電腦以及智慧型手機，在無線網路的進步下，其資訊傳播速度更有大幅度的躍進，例如：智慧型手機加上網路便是個人的 GPS 定位系統；當透過 Google Map 或其他地圖系統，便可使用衛星導航之功能；加上手機內建的相機鏡頭，便可隨時隨地上傳相片或影片，透過社群網站可與全世界朋友們分享生活點滴。然而在如此的便利的環境下，卻也暗藏了許多個人隱私遭侵入及國家機密遭窺視之危機。

近期網友熱烈關注一款智慧型手機應用程式（APP），是由美國 GPS 衛星定位追蹤公司 Strava Labs 所推出，號稱「運動員的社群網路應用程式」，可呈現穿戴此電子產品的全球用戶騎單車、跑步、游泳、滑雪時行經的所有路線的地圖熱點。光線越強的地方，代表在此地記錄跑步或騎單車的用戶越多，臺灣亦不乏熱中使用此款 APP 的用戶。有位澳洲大學生魯瑟（Nathan Ruser），在研究「熱圖」公布的路徑後，意外發現在中東戰亂地區有部分光線很強，由於中東當地人會使用這種高科技運動手環的人應該很少，故推測「熱圖」已

智慧型裝置加上網路便具備 GPS 定位功能，透過地圖系統可使用衛星導航功能，加上內建的相機鏡頭，可隨時隨地上傳相片或影片，與全朋友們分享生活點滴。



Strava Labs 推出的 APP 可記錄用戶使用路線，光線越強的地方，代表在此地記錄的用戶越多。（資料來源：畫面截自 Strava 官方網站全球熱圖，https://www.strava.com/heatmap#5.53/117.68908/27.41221/hot/all）



澳洲大學生魯瑟在研究「熱圖」公布的路徑後，推測「熱圖」暴露美國海外秘密的軍事基地。（資料來源：畫面截自 Nathan Ruser Twitter，https://twitter.com/Nrg8000/status/957318498102865920/photo/1?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fori.upmedia.mg%2Fnews_info.php%3FSerialNo%3D34361）

暴露了美國海外秘密的軍事基地；而依據「熱圖」所暴露全球各地敏感的軍事基地中，赫然發現臺灣某軍事基地在其中。

另依據媒體報導，美國國防部長馬提斯（Jim Mattis）在獲悉健身 APP 洩漏軍隊機密消息後，開始考慮禁止士兵使用帶有 GPS 定位手機入部隊的可能性。新加坡國防部更於 Starva 軟體洩密曝光後，即刻於 2018 年 2 月 2 日在國防部網站發布新聞，禁止軍人使用健身手環。新加坡此等效率頗值得我政府借鏡。

保密工作對個人及國家安全有著相當大的影響，無論平時或戰時均應落實執行管控措施，尤其負責國防安全之國軍弟兄更應留意。由於手機 APP 或智慧手環有定位功能，國軍官兵進入營區需先關閉。在營外，用戶 APP 內有可關閉上傳數據的功能，應瞭解相關隱私設定，以確保個人行蹤不會被洩漏。

除了前述 APP 外，來路不明的 WIFI 連結，極有可能隨時遭駭客入侵盜取資料及操控，而不明連結網址引誘點擊，易讓使用之行動電話遭歹徒入侵利用，致使個人資料遭竊取及偷拍。此外，在公共場所隨意使用商站提供免費或未經加密認證的無線網路（WIFI）進行金融交易、購買商品等動作，易使手機內的資料遭有心人士盜用，潛存被詐騙風險。

據統計，資安漏洞大都來自於人為的破壞與疏忽，故最有效的資安防護政策，就是個人養成良好的資安保密習慣。例如：落實實體隔離、機密資訊儲存使用加密軟體、不因吸引人的主旨標題而開啟來路不明的電子郵件、公務不家辦，唯有如此才能將資安風險降到最低。

在近年間駭客入侵國內外關鍵基礎設施事件增多、企業遭網路勒索病毒攻擊事件愈來愈頻繁，而且智慧型手機用戶不斷創新高的情況下，不論是政府為提高施政品質、企業追求營業額或個人享受科技便利之同時，對於資通安全更要提高警覺，以慎防秘密於無意間流出。

行政院施俊吉副院長於 3 月 1 日在資安成果展開幕典禮中表示：在金融科技快速進步與普及的趨勢下，強化資安防護已成為政府當前重要課題。政府會保持高度的警覺心，並抱持逆水行舟的精神，在資安工作上不斷精進努力，但唯有全國民眾的大力支持，資安防護工作才能臻於完備。

謹慎使用無線網路（WIFI），避免手機內的資料遭有心人士盜用。

社群網站的女巫攻擊

■ 法務部調查局資通安全處　雷喻翔

等紅綠燈時回覆 FB 上的留言，或給友人按個讚；在通勤路上滑手機，瞧瞧動態時報裡頭的最新消息，這些情景於日常生活中再熟悉不過，其中卻隱藏著信賴風險？

社群網路的生態系統

近幾年由於臉書（Facebook）、推特（Twitter）及 Youtube 等社群網路的興起，影響了人際之間的交流，並產生了史無前例的大量網路資料。大量的資料流帶來大量的使用人潮，而且藉由社群網路提供的應用程式介面（Application Programming Interface），第三方應用軟體可以輕易地與社群軟體互動，例如使用者在行動裝置下載了新的餐廳推薦軟體，無須重新申請新帳號，而是直接使用原本已經擁有的社群網路帳號登入，如此，便可享用便捷的服務並與社群網路的親朋好友分享資訊。透過上述簡便的方式，社群網路逐步結合金融、餐飲、交通等原本獨立的服務，建構出一套完整的使用者「生態系統」。

隨著社群網路的風行，攻擊這套生態系統的意圖也隨之增加。一個惡意的使用者可以在社群網路上註冊多組帳號，並從中製造錯誤的訊息、刻意張貼不實的評論誤導風向、影響網路的投票結果，用以破壞社群網路建構出的信賴機制。此類型的攻擊手法就是典型的「女巫攻擊」。

目前眾多第三方應用軟體可以輕易地與社群軟體互動，無須重新申請新帳號。（圖片來源：截自臺北市政府網路市民登入畫面，https://citizen.taipei/MP.aspx；大臺北公車會員登入畫面，https://ebus.gov.taipei/）

女巫攻擊

女巫攻擊乍看之下讓人摸不著頭緒，它是源自於 1970 年代出版的一本美國小說，小說書名便是女巫（Sybil）。書中的女主角人格混亂，一個人同時擁有 16 種不同的角色，於是電腦科學家便以此命名，將「意圖以多組不同帳號來顛覆社群網路的使用者行為」定名為女巫攻擊。圖 1 描述女巫攻擊概觀：惡意使用者先藉由申請大量的帳號創造出看似毫無關聯的獨立實體，接著再向社群網路伺服器發動不實攻訐以達成駭客的目的。

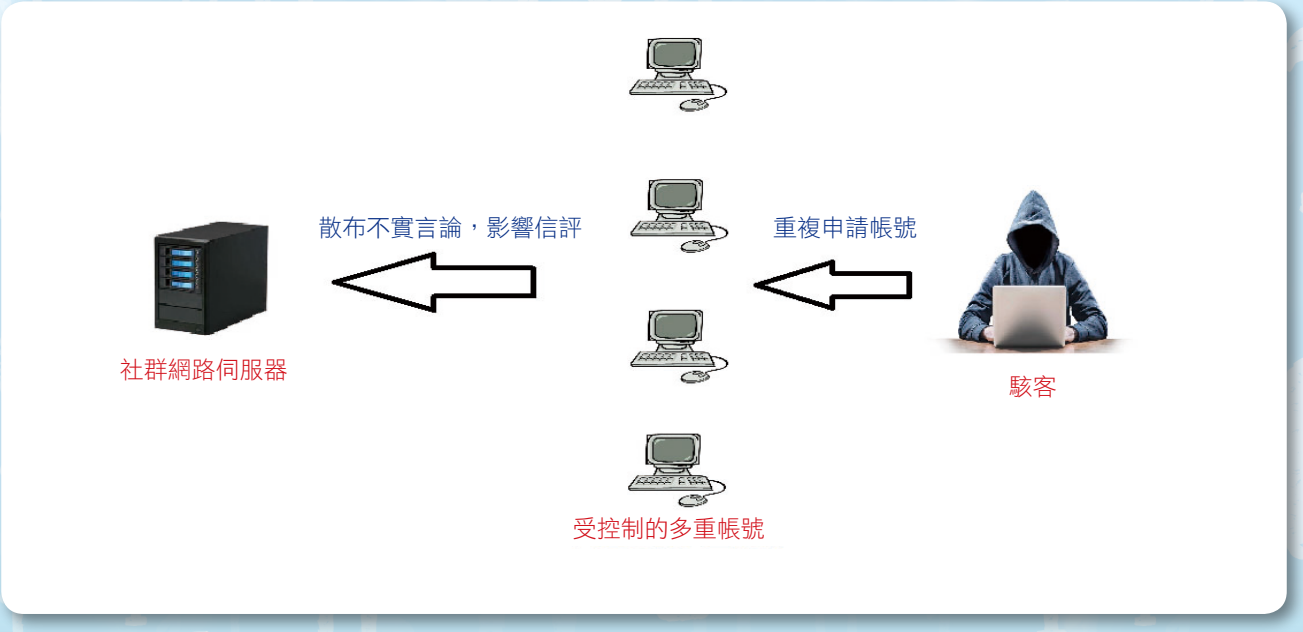


圖 1　女巫攻擊概觀

社群網站帳號申請僅需簡單的電子郵件或手機號碼進行認證，易遭有心人士利用。（圖片來源：截自臉書、推特，https://twitter.com/signup?lang=zh-tw、https://zh-tw.facebook.com/）

在理想情形下，一個使用者應當只有唯一的一個帳號，此虛擬帳號雖然隱匿了部分的個人隱私，但是實際上就是這位使用者於社群網路上真實身分的投射。然而現實的情況卻非如此，諸如臉書、推特的帳號申請管道僅依賴簡單的電子郵件認證，雖然初衷是為了減少使用者申請帳號的繁瑣手續，但同時也提供有心人士操作的管道。

女巫攻擊不似傳統以病毒、木馬為武器的資安攻擊手法，對於家庭或辦公室電腦的破壞沒有立即的侵略性，但對社群網路來說，就「安全」及「信任」方面將產生巨大的影響。常見的例子如下：在網路電子投票中，惡意的使用者可以利用多個 IP 位址作假，用以取得想要的支持目標；又例如以詐騙消費者為目的之虛設公司會利用女巫攻擊獲得 Google 搜索排名，以提升該公司的信譽及公信力。

因應之道

有鑑於此，資訊安全研究者相繼提出可能的解決方式，一種最簡單的方法是採用可信賴的第三方代理機構來驗證每一

個使用者提出的申請。這個機構必須擁有毫無疑問的公信力，對於使用者的申請進行嚴格審核，降低偽裝身分的機率。審核方式可以分成直接或是間接審核：直接方式是由公正機關直接對使用者進行身分查核，確定不是重複申請且該身分與使用者實體是「一對一」對應後，始能發出認證書；間接審核的對象不是個人，而是機構，當該機構從公正機關獲得認證書後，它可以扮演公正機關的角色，對個人申請進行驗證。

兩種方式各有其優缺點，直接審核的優點，是可以更加嚴密地掌握申請者的身分，一旦有可疑事件發生，可以提供完整的反向查詢，申請人的真實身分無從隱蔽。相反地，間接審核無法第一時間提供申請人的詳細身分，必須經過一層層遞迴地查找後才得以掌握目標。直接審核的缺點，則是單一可受信賴的公正機關將面臨資源管理和網路通訊的瓶頸，當所有申請都集中於單一機構時，整體的服務品質受限於網路頻寬及伺服器處理速度，有可能遭到阻斷服務攻擊（Denial-of-Service attack），進而耗盡系統網路資源。如同面對社交工程或其他資安攻擊手法，很難有一種完美的架構可以百分之百抵擋變化多端的駭客入侵，女巫攻擊也無法單靠一種解決方案便可一勞永逸，這也是專家學者們仍然持續投入研究的原因。

物聯網及車聯網的衝擊

女巫攻擊除了危害社群網路以外，對於新興的物聯網（Internet of Things）或是車聯網（Vehicular Networks）也同樣帶來危害。兩者都是由多部機器或汽車經由彼此之間共同認定的通訊協定所架構出的網路，一旦有多個惡意分子混入其中，企圖夾雜錯誤的訊息，這種行為無疑就是典型的女巫攻擊。

科技大廠及各國際車廠競相加入研發無人車，在可預見的未來，無人車將在各大城市滿街跑，車與車之間的通訊便是車聯網的應用。想像一下以下狀況：車輛之間依靠彼此的車流量回報來判斷最佳路徑，如果有一群被操控的車輛故意回報錯誤的車流量資訊，整個交通網路將大受影響，其嚴重性不言可喻。

結語

社群網路帶來了便利，同時也帶來了更多不確定性，如果原本被認為是正確的資訊一夕之間反被判定是錯誤資訊，輕則影響社群網路的公證力，更甚者錯誤訊息的傳遞會造成實體社會的惶恐不安。然而，女巫攻擊目前尚無完美的解決方案，除了依靠公正機關的把關外，最重要的是網路使用者的判斷力，當遇到可疑訊息時，需要有縝密的思考跟多方求證，切勿「眼見為憑」全盤接收。就如面對社交工程的釣魚手法，**根本解決之道仍是使用者的使用習慣**，這是再多的網路防火牆跟防毒軟體都比不上的。