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。

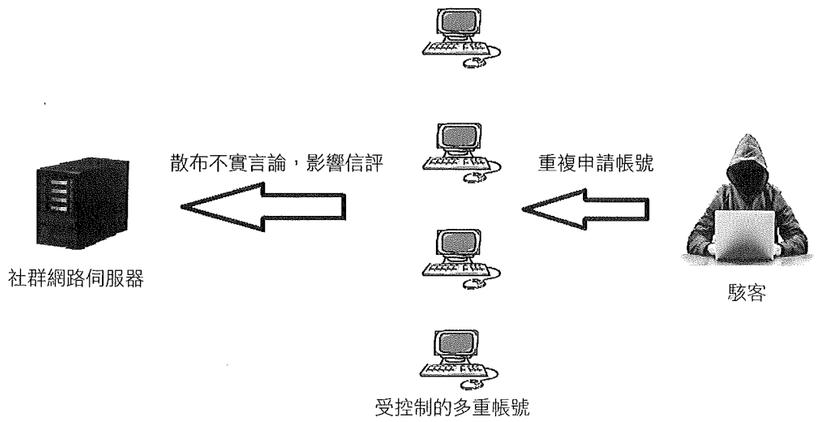
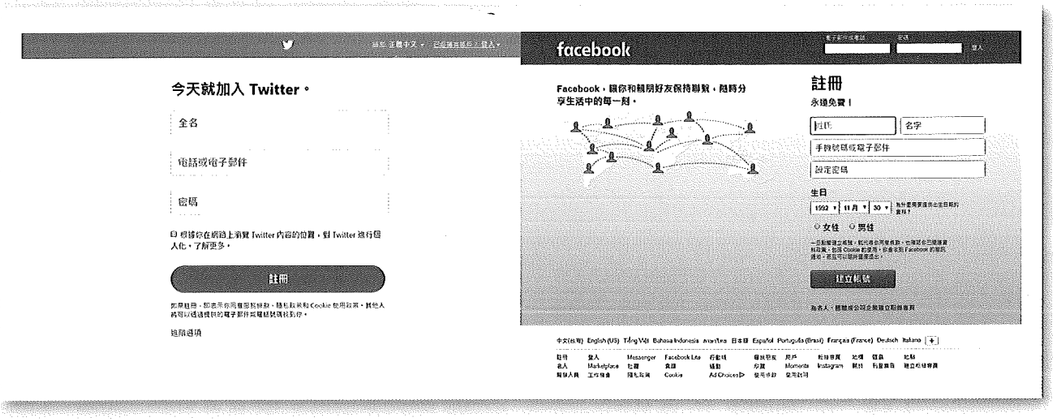


圖 1　女巫攻擊概觀



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。

「無踰我園」誘人深入

臺灣警察專科學校前校長　陳連禎

《詩經・鄭風・將仲子》描寫戀愛中男女的互動情境，十分有趣，值得現代人賞析。原文摘述如下：

將仲子兮！無踰我里，無折我樹杞，豈敢愛之？畏我父母。仲可懷也，父母之言，亦可畏也！將仲子兮！無踰我園，無折我樹檀，豈敢愛之？畏人之多言。仲可懷也，人之多言，亦可畏也！