密碼安全性原則困擾的是駭客還是自己？

※本文摘錄自法務部調查局 106 年 11 月份清流雙月刊

◎陳彥銘（資訊工業策進會工程師）

密碼複雜度的設計原來是錯的？當初的發起者已公開坦承錯誤。與其規定英文、數字、特殊符號等組成複雜度，不如追求密碼長度，方便使用又確保安全。

資安事件層出不窮

網路 E 世代的來臨，使用網路雲端服務已經是日常生活中的一部分，舉凡社群網站（例如臉書）、Google 服務（例如信箱、雲端硬碟），或是購物網站、網路銀行等；這些雲端服務提供了使用者便利性，卻也帶來了資安上的風險。

近年來重大資安事件接連爆發，連大型的企業組織也不能倖免，例如 yahoo 就曾於 2013 年爆發 10 億筆帳號資料外洩，而 Apple 也曾因為 iCloud 身分驗證機制的安全缺陷造成多位好萊塢女星私密照外洩，而這些資安事件皆是帳戶身分驗證的環節出了問題。

密碼複雜度高就是安全？ 發明人卻後悔了！

身分驗證是存取網路服務的第一步，也是保護個人資訊安全的最基本機制。據統計，民眾最常用的密碼包含：123456、123456789、password、qwerty（鍵盤上的橫排）等，而為了強化帳戶的安全性，防止帳戶被有心人士盜用，許多單位會訂定密碼安全性規範，避免密碼被輕易破解。以微軟伺服器作業系統所設定的密碼複雜度原則為例，其要求為不包含使用者的帳戶名稱或全名的重要資訊，且必須包

含下列 4 種字元中的 3 種：英文大寫字元（A 到 Z）、英文小寫字元（a 到 z）、10 個基本數字（0 到 9），以及非英文字母字元（例如!、$、#、%）。照此設定方式，再加上最小密碼長度設定為 8 個字元的話，確保至少 218,340,105,584,896 不同單一密碼的可能性，目的是避免密碼被惡意人士用暴力窮舉法輕易破解。

這種密碼設定方式開始流行，起因於 2003 年美國國家標準技術研究所（NIST,National Institute of Standards and Technology）所制定的一份文件附錄，有趣的是，撰寫該安全密碼最佳實踐原則的作者 Bill Burr 近日接受華爾街日報訪問時卻直言當初所制定的方式並不十分恰當，並為此造成使用者的不便感到抱歉（“Much of what I did I now regret.”）。他並不是在鼓勵使用容易被破解的密碼，而是因為當初撰寫時沒有考量到人類的惰性問題，太複雜的密碼組成要求不僅徒增困擾且可能還有反效果。

與其追求字符複雜度，
不如擁抱字串長度

其實早在 Bill Burr 接受訪問之前，NIST 已變成強調密碼長度而非組成複雜度，只要密碼長度足夠，即使是一串簡單的英文字元所組成的密碼，其排列組合的可能性數量就已足夠。且考慮到一般民眾為了使用方便好記又符合複雜度要求的密碼，常常會利用鍵盤排列（例如!@#$QWERasdf）、象形文字（例如將 s 取代成 5，或是將 a 取代成@）等手法來設計密碼，這也是為什麼 P@55w0rd 也會登上密碼使用排行榜上的前段班。

而對駭客而言，為了節省破解時間，一開始會先利用「慣用密碼紀錄表」來進行密碼破解，故其實“P@5 5w0 r d”比“ilovemycompany”這類簡單規則組成的字串更能輕易被破解。但要

特別注意的是，使用簡單組成規則的前提是字串長度要夠長（建議至少 12 個字元），可能性數目才足夠。

改變使用密碼的壞習慣

理論上，密碼組成字符愈複雜確實會提升破解的難度，但因為使用的對象是人而非機器，人類的創造力可以無限，但記憶力卻是有限，無法記憶過於複雜的密碼，為了配合複雜度要求反而容易產生其他不安全的使用行為，導致變得更不安全。例如，好不容易創造了一組好記又複雜的密碼，所以在各種網路服務都使用同一組帳號密碼，一招打天下的概念，卻也讓駭客相對省事，拍賣網站淘寶網就曾於 2015 年被駭客利用從他處取得的 9,900 萬筆帳密資料進行比對測試，發現有近兩成的帳戶真實存在，部分帳號因此被用來進行詐騙。用戶可以將重要服務（例如網路銀行）的帳密跟一般服務（例如會員電子報）所使用的帳密有所區隔，至少可以減少帳密外洩的危害程度。

另一種常見的密碼安全性政策是要求更換密碼的頻率，例如 90 天內強迫更換密碼，且限制密碼不可重複使用；這些規定立意良善，出發點是為了避免用戶仍重複使用那幾個愛用的密碼，但所謂上有政策下有對策，例如用戶就會在密碼尾數加上字元 1，下次變更時尾數則變成 2，依此類推，如此一來就喪失了變更密碼的本意。頻繁變更密碼的要求也是在考驗用戶的記憶力，於是有些用戶就將密碼抄錄於紙本或存在電腦桌面的檔案裡，甚至整理成一個 Excel 檔記錄各個密碼，心存僥倖的心理使然，反而變成更不安全。

為了應付現今各種網路服務制定的各種帳號密碼要求，目前市面上已有業者開發出密碼代管服務，用戶只要記憶一個「超級密碼」，登入該服務後就能存取及管理所有的密碼紀錄。筆者認為一般民眾可能不需要那麼專業的密碼管理服務，但最低限度也不能將密碼寫下來

放到抽屜裡藏著，可以自製陽春版的密碼雲端儲存機制，把密碼紀錄檔案寄送到自己的雲端信箱（例如 Gmail）以隨時查詢，至少存取前還有一層身分驗證的保護，且是免費並能兼顧易用性。

結語

臺北捷運初期宣導搭乘手扶梯應「右側站立，左側通行」的政策，即使十年前就已經改為「緊握扶手，站穩踏階」，但人類的創造力可以無限，但記憶力卻是有限，密碼設定與其追求字符複雜度，不如擁抱字串長度。一般民眾養成的習慣已經改不過來。目前密碼複雜度要求已成為「顯學」，即使當初的作者坦承錯誤，但現實風向已經「回不去了」，用戶也必須自我學習，改變使用密碼的壞習慣。資訊安全與使用便利性常常是背道而馳的設計理念，系統開發人員必須找到一個平衡點，並依機密程度、業務影響層級及法規要求等面向評估系統安全等級，以訂出適切的密碼安全政策。