話密碼的藝術：安全有沒有，進門第一道鎖便知有沒有

社團法人台灣 E 化資安分析管理協會
(ESAM, https://www.esam.io/)

中央警察大學-資訊密碼暨建構實驗室(ICCL)

==========

＜本文作者：

1. 社團法人台灣 E 化資安分析管理協會(ESAM, https://www.esam.io/)；

2. 中央警察大學資訊密碼暨建構實驗室（ICCL），1998 年 12 月成立，目前由王旭正教授領軍，並致力於資訊安全、情資安全與鑑識科學，資料隱藏與資料快速搜尋之研究，以為人們於網際網路(Internet)世界探索的安全保障（https://sites.google.com/site/iccltogether/）。＞

==========

摘要

現今使用者大量使用資訊設備與服務，不可避免地得記住相關的帳號、密碼。然而隨著所需記住的密碼愈來愈多，使得使用者也愈容易忘記密碼。若使用者未能建立良好的密碼使用習慣，就會傾向於使用易於破解的密碼或是懶人密碼等，導致密碼的強度不夠而容易被破解。近年來政府推行「政府組態基準」(Government Configuration Baseline，簡稱 GCB)，目的在於建立一致性安全設定，包括對於密碼有明確的要求，藉以降低資通安全風險。然而對密碼安全的要求提高，使用者在不易記住密碼的情況下，有時就會選擇將密碼存在記事本或便條紙等方式，反而更容易造成密碼外洩的風險發生。因此，我們需要更有效率的記錄密碼方式，本文將透過介紹密碼的設定原則與密碼管理軟體 KeePass Password Safe 的操作使用，協助讀者們能運用密碼管理軟體減少密碼外洩的風險，並藉此建立良好的密碼使用習慣。

壹、前言

現代的人身處資訊時代，與電腦網路的關係密切，也使得現代人有一大堆的帳號、密碼要記。電腦作業系統有登入密碼，電子郵件也有密碼，各個網站的會員帳號、密碼，多的不

勝枚舉。為了安全起見，不同的帳號還得配用不同的密碼，甚至於各網站本身也會強制要求使用者設定的密碼規則。據新聞報導而言，每個人平均所使用的密碼數量已經從 2007 年的 25 個，到 2020 年時預計會成長到 207 個！隨著所需記憶的密碼增加，懶人密碼更是大受歡迎。如據報載澳洲在 17 個政府機構中有超過 5,000 個密碼都包含 password 這幾個字母，搭配數字組合，如 password1234。這使得密碼太過於被攻擊者猜中，進行可能導致重要資訊外洩。

而近年來政府推行「政府組態基準」(Government Configuration Baseline，簡稱 GCB)，目的在於建立一致性安全設定(如密碼長度、更新期限等)，以降低資通訊設備成為駭客入侵管道。其中「密碼必須符合複雜性需求」則是要求密碼必須符合下列最小需求:

- 不包含使用者的帳戶名稱全名中, 超過兩個以上的連續字元.
- 長度至少為 8 個字元
- 包含下列四種字元中的三種:
  - 英文大寫字元 (A 到 Z)
  - 英文小寫字元 (a 到 z).
  - 10 進位數字 (0 到 9).
  - 特殊符號 (例如: !、$、#、%)

此外，還加上電腦開機密碼需 90 天更換 1 次，電腦開機密碼不能使用跟前 3 次相同的密碼。這使得使用者要記住現行使用的密碼的難度增加不少。

不少使用者為了記下密碼，就是將這此密碼訊息寫在筆記本內，或甚至像電影《一級玩家》的執行長將密碼用便條紙貼在座位旁，如此不僅有遺失的風險，被盜用的機率更是極高。更進一步的做法是記錄在電腦中的文字檔、Excel 檔等，然而這種方式還是有外洩的風險，尤其是密碼多是明文方式儲存，使用者在查找密碼時，有心人從使用者背後就能直接看到密碼。因此我們需要更好的紀錄密碼方式，那就是使用密碼管理軟體來協助我們紀錄與使用密碼。

密碼管理軟體相當於把所有的密碼鎖在一個保險櫃裡，只要記住一組保險櫃的密碼就可以查到其他組的密碼，其弱點則是保險櫃的密碼如果被破解的話，則所有的密碼就會因此暴露。但是只要使用者採用的主要密碼是屬於高強度的隨機密碼，那麼只要這個密碼保管好，就能夠同時保護好其他密碼的安全。

參、政府組態基準

組態基準，也就是針對作業系統、資通訊設備與主要操作的軟體進行相關組態設定的要求。美國系統與網路安全協會（SANS Institute）與網路安全中心（Center for Internet Security, CIS）常年在資安防護的規劃上所發展出的 CIS Controls for Effective Cyber Defense，其中安全組態設定（security configuration）一直是重要的一環，在最近的 7.1 版中，安全組態設定更被視為最基本的控制要求。而至於「政府組態基準」就是我國針對各公務機關所制定的安全組態設定規範。

我國在 2013 年時，行政院國家資通安全會報就開始逐步要求中央部會在 Windows 7 或 IE8 的環境導入 GCB；在 2014 年與 2015 年間增加 Windows Server 2008、Red Hat RHEL、Windows 8.1 與 IE11；2016 年時則開始推廣 GCB 到各部會所屬三、四級機關與地方政府。

在 GCB 中，有關密碼的部分包括增加密碼的長度與複雜度，密碼最長使用期限、最小密碼長度、強制執行密碼歷程記錄等，簡介如下：

- 密碼必須符合複雜性需求：決定密碼是否必須符合複雜性需求，包含
  - 不包含使用者帳戶名稱全名
  - 長度至少為 6 個字元
  - 包含「英文大、小寫字元」、「數字」及「特殊符號」四種字元中的三種
- 密碼最長使用期限：決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)，目前要求為 90 天以內。
- 最小密碼長度：決定使用者帳戶的密碼可包含的最少字元數，目前要求為 8 個字元以上。但若是為伺服器的話，則建議為 12 個字元以上。
- 強制執行密碼歷程記錄：設定新密碼或密碼更改時，不得與前幾次之使用者密碼相同，讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性，目前的要求為 3 次以上。

綜合所述，這樣的密碼的確可讓惡意攻擊者不易猜到，但我們也可發現除了要建立不好記的密碼外，我們還得準備 4 組以上的密碼來因應每 3 個月要固定更換。對於欠缺密碼管理的使用者來說，這無疑是一種折磨，也因此使用者就可能會採用記事本等方式來紀錄密碼，結果反而讓當初導入 GCB 的用意失去意義。

肆、密碼設定原則

密碼要怎麼設才會安全？什麼樣會是一個好密碼？依據常見的密碼設定原則如下：

- 至少包含一個英文小寫字母
- 至少包含一個英文大寫字母
- 至少包含一個數字
- 至少包含一個特殊符號(如標點符號或是@#|>*
- 至少 8 個字元以上
- 字典所找不到的字，最好是沒有任何意義的組成

同時，所設定的密碼最好不要與個人資料有關，例如英文姓名加上出生年月日，或是直接使用身分證字號的密碼都很容易會被有心的駭客破解。僅管這套規則的實行與宣導已超過 10 年以上，然而還是常見使用者未遵守規則。如密碼管理軟體公司 NordPass 在 2020 年時公布了 200 個最常見的密碼排名（https://nordpass.com/most-common-passwords-list/），最常見的密碼前十名如下：

- 123456
- 123456789
- picture1
- password
- 12345678
- 111111
- 123123
- 12345
- 1234567890
- senha

可見到，儘管已到了 2020 年，許多脆弱的密碼還仍然被使用，如「123456」、「password」和“111111”等。6 個數字可以產生的組合約 1 百萬組，看起來很多，但若以現在的電腦速度來看，大概不到 1 秒就可被暴力（brute-force）破解。密碼若設為 8 個字元的組合，如「password」，約有 2000 億組的組合，要破解就需要一段時間。但不幸地，「password」是常見密碼，也是有意義的單字。所以攻擊者不會採用暴力破解的方式，而是會採用字典法（dictionary）破解，也就是將常見的密碼彙整成字典檔來進行破解，以牛津英文字典約收錄 30 萬個詞彙來說，破解時間同樣不到 1 秒。

不過近幾年來，對於密碼的規則也進行了反思，像是當初於美國國家標準與技術研究所（National Institute of Standards and Technology, NIST）任職時，建立密碼規則的 Bill Burr 先生，也在幾年前公開說抱歉讓大家設下難懂且難記的密碼。其實 Bill Burr 所建立的密碼規則並非錯誤，愈是複雜的密碼就愈難被猜中，納入英文大小寫、數字與特殊符號也讓進行暴力破解的難度增加不少。但是愈是複雜，使用者就愈難記，就愈會傾向省力的方式，例如將密碼「password」改為「P@ssw0rd」來符合規則，若是需要增加長度或是定時更新密碼時，就可能改為「P@ssw0rd1」或是「P@ssw0rd2」來因應，也因此有些密碼破解軟體就會採用類似的方式來攻擊。

那麼現在的密碼原則是什麼呢？依據 NIST 後來針對密碼設定指南的修改，就是將字符規則的變化改為以密碼長度為主。畢竟當密碼設定如 4 組無特別關聯的單字組合「newpathtodaywear」會比「IbWMs#qq」來得容易記憶，安全性也還不差。網路也有人以顯示卡上的 GPU 來進行密碼破解，如圖 1 所示（資料來源：http://www.yourdestinationnow.com/2020/07/brute-force-password-guessing-picture.html）。使用 GPU 的密碼破解速度比 CPU 更快，可高達每秒 3 千萬組，以上述的密碼「IbWMs#qq」來看，破解時間約需 7 年；而「newpathtodaywear」的 16 個字元則是要用到 $4.6*10^7$ 年的時間才能破解。

想知道你所使用的密碼會不會很容易被破解嗎？也可以利用「How Secure Is My Password？」（https://howsecureismypassword.net/）來測試看看，將密碼輸入後，就會立即顯示使用破解你的密碼需要花費多少時間，網站的背景色也會依密碼的安全度高底來變化。我們將「newpathtodaywear」輸入這個網站後，顯示所時間約為 3 萬 4 千年。而「IbWMs#qq」呢？則是 2 小時！

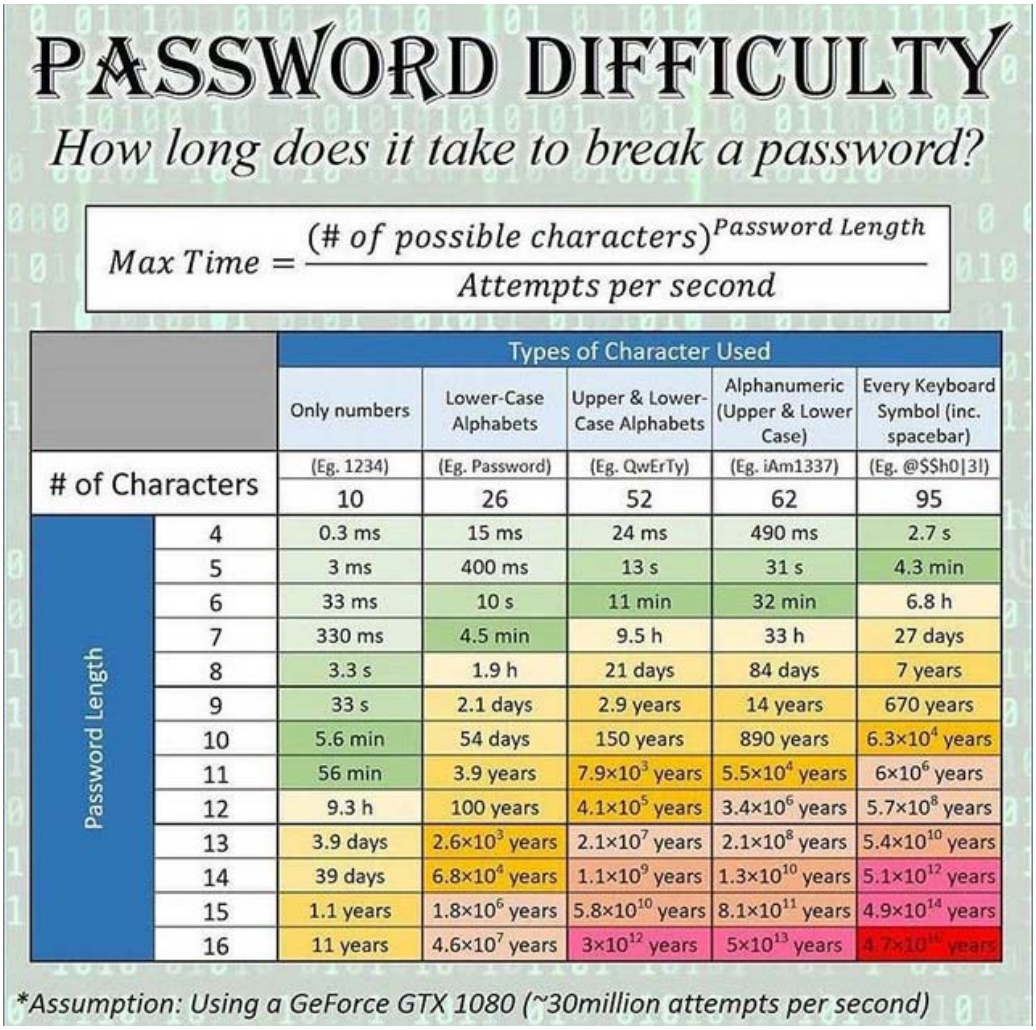

圖 1：以 GeForce GTX 1080 破解密碼

圖 2：評估密碼破解的時間

伍、密碼管理工具

有關密碼管理工具一樣是有商業軟體與開源軟體，在此我們介紹的開源軟體中相當有名的 KeePass Password Safe（以下簡稱 KeePass）。目前 KeePass 的最新版為 2.47（2021 年 1 月 9 日發布），可由其官網（https://keepass.info/）下載安裝檔或是使用免安裝（Portable）的版本。這套軟體由 Dominik Reichl 所開發，從 2003 年 11 月 16 日至今也歷經了十幾年，開放原始碼的特性，簡單易用的介面也使得這套軟體相當受到歡迎，並且還有許多開發者因應不同的環境來建不同的版本。

Keepass 程式所佔空間很小，解壓縮也才不到 6MB，很容易就可將整個程式含資料檔案都放在隨身碟上帶著走，其特點摘錄如下：

- Keepass 是開放原始碼軟體，可自由使用，亦可不需要安裝。
- Keepass 以一組隨機產生的主密碼保護資料，而且，其主密碼還可以採用密碼加密鑰文件的方式，就將加密鑰文存到 USB 隨身碟或是另外的儲存媒體中。
- Keepass 的檔案以當今最先進的加密演算法 AES 進行加密，或是使用效能較佳的 ChaCha20。
- 資料庫中儲存的密碼可以分類管理。
- 程式還支持 TAN（Transaction Authentication Number，網路銀行交易確認碼）密碼管理，幫您自動排除以使用過的密碼。
- KeePass 可以輸出成多種格式，包括 TXT，HTML，XML 及 CSV 等不同的檔案。
- 程式提供數種不同的輸入方法，以方便輸入帳號及密碼。KeePass 中的密碼，可用拖曳的

方式直接輸入至網頁或其他的任何視窗中，並且還可以設定成自動輸入。

- 程式還提供其他的功能，包括密碼產生器、密碼品質測試、自動上鎖、資料庫搜尋、匯入及匯出資料庫等等。
- KeePass Password Safe 同時支援外掛，允許經由許多其他的外掛程式擴充功能。

KeePass 類似一個管理資料庫的軟體，如圖 3 所示。啟動後可先建立自己的密碼資料庫，並建立及記住如何開啟這個資料庫的最重要「一組」密碼即可，或者與目前的 Windows 帳號綁定，如圖 4 所示。之後就可以利用 KeePass 提供的功能來建立各種登入帳號與密碼，並可透過 KeePass 來協助產生亂數密碼，如圖 5 與圖 6 所示，就可以不用擔心記不住這些複雜密碼了。

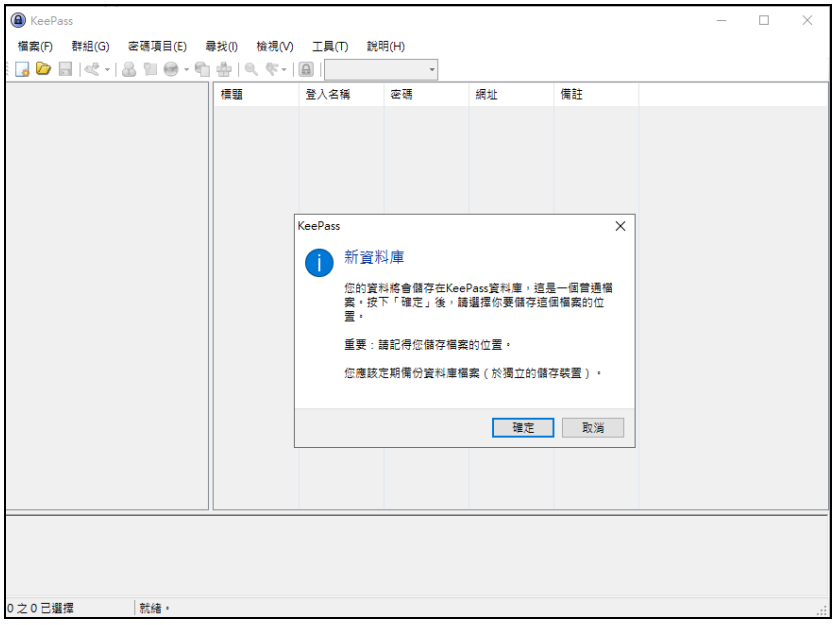

圖 3：KeePass 的執行畫面

圖 4：以 KeePass 建立密碼資料庫的畫面

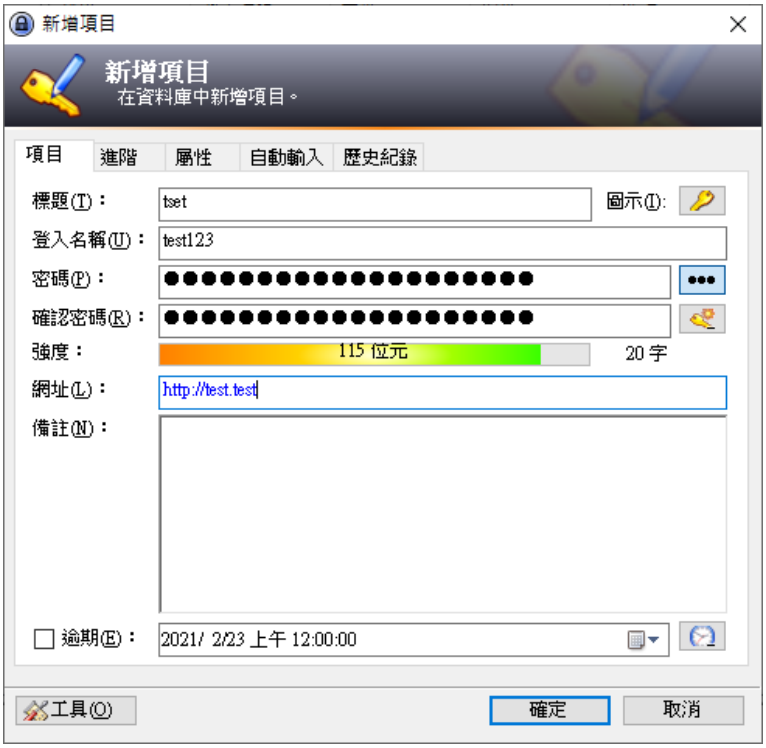

圖 5：以 KeePass 新增帳號與密碼資料

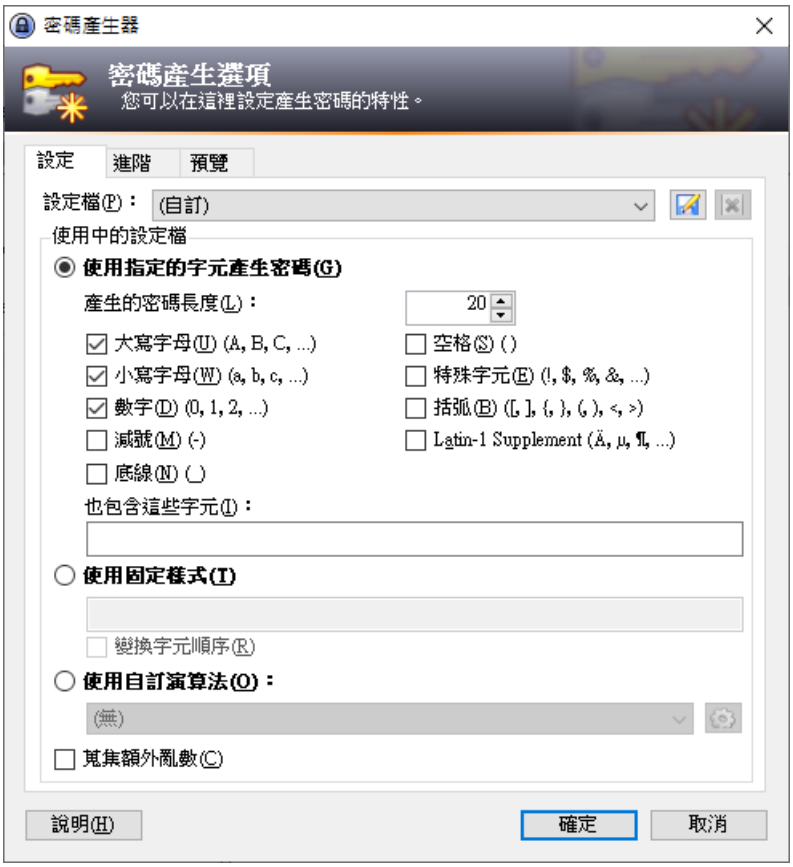

圖 6：使用 KeePass 產生亂數密碼

使用 KeePass 的優點之一，就是當需要取用這些密碼時，不用再開啟原本的設定畫面，而是可以直接在對應的項目上按滑鼠右鍵取用登入帳號或密碼，若有先指定要輸入的頁面欄位就也可以執行自動輸入，如圖 7 所示。因此，即使身邊還有其他人在，也能避免密碼外洩的問題發生。

此外，我們可以透過 KeePass 對於密碼強度的檢驗，評估我們的密碼是否足夠安全，如圖 8 所示。並可針對資料庫中的密碼來檢測是否有相似度過高的問題，如圖 9 所示，減少密碼的相似度可避免當某一密碼不小心外洩時，也不致於被有心人猜測出其他組的密碼。

除了 KeePass 外，還有不少 KeePass 的衍生軟體，如 KeePassXC，除了 Windows 版本外，還提供 Linux 與 Mac OS X 的版本。此外還有像是 Bitwarden（https://bitwarden.com/）也是備受好評的密碼管理軟體。

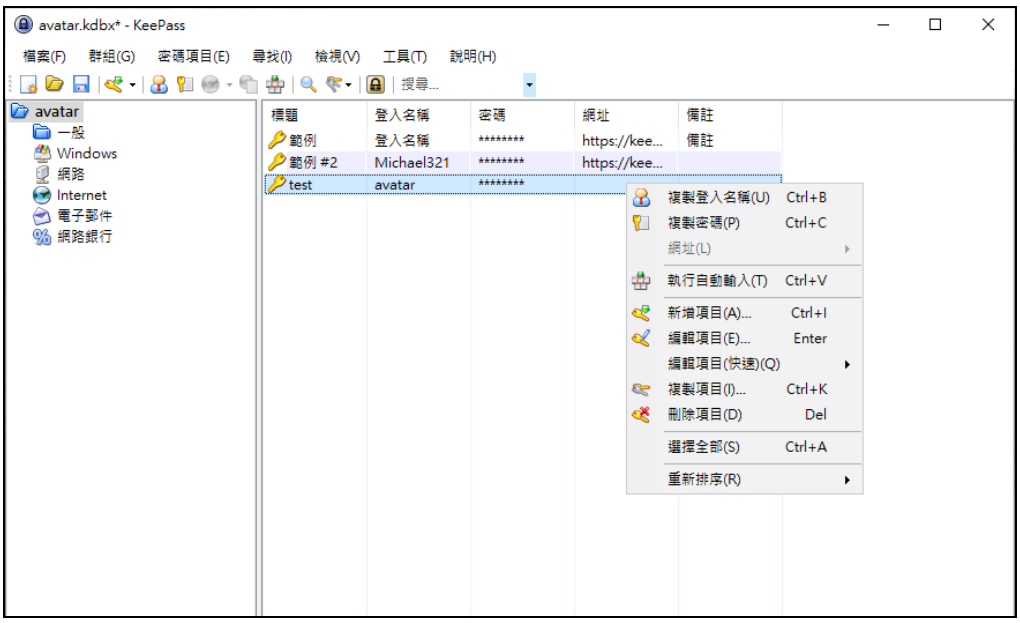

圖 7：使用 KeePass 複製密碼使用

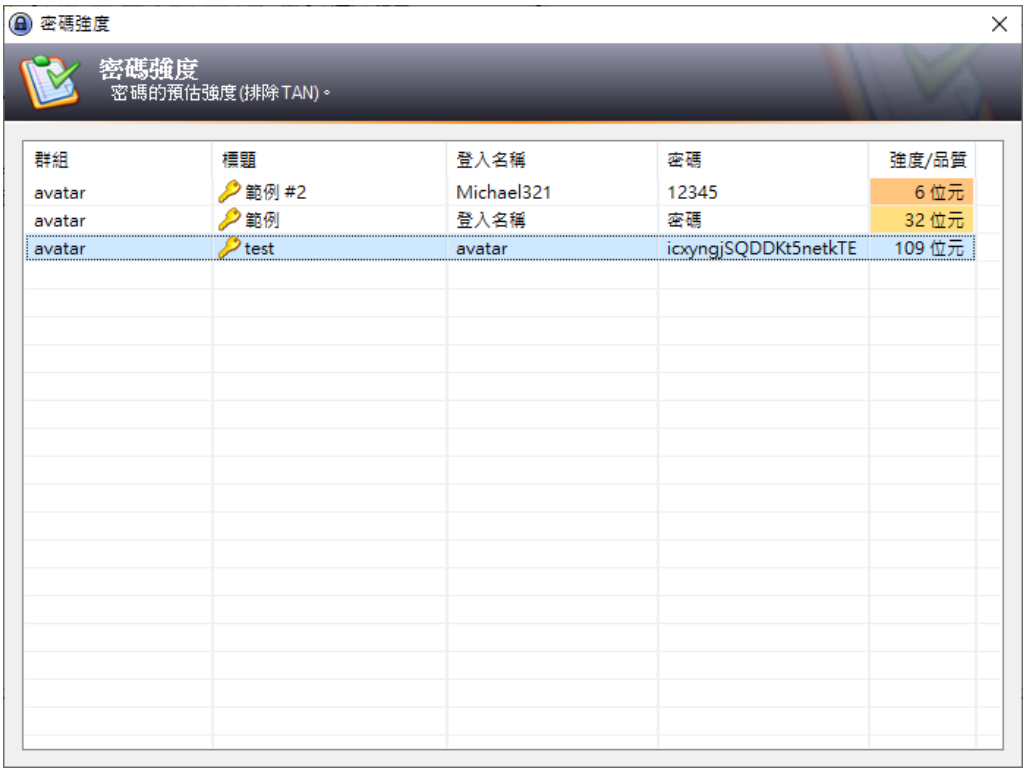

圖 8：KeePass 對密碼的預估強度

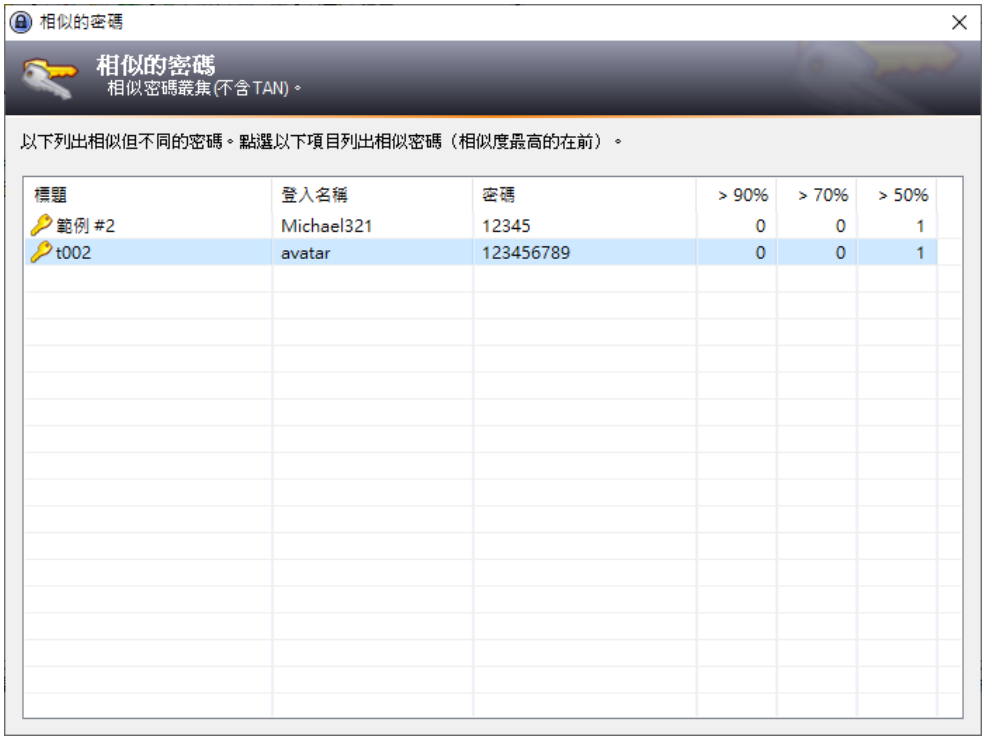

圖 9：KeePass 可找出相似的密碼

保護了密碼的安全，但我們也要注意密碼管理軟體本身的安全性，不能因為使用了密碼管理軟體就百分百相信絕對安全。在 2015 年時，一名安全研究人員就發現在 KeePass 2.28、2.29 與 2.30 版時，可透過 DLL 注入的方式，從執行中的 KeePass 中竊取儲存於記憶體中的帳號與密碼，並建立了 KeeFarce 程式來驗證確實可行。而在 2016 年二月時，KeePass 2.4.1 版本被發現是透過 http，而不是較安全的 https 來連結 KeePass 伺服器進行更新，可能會因此遭受中間人攻擊（Man-in-the-middle, MitM）。到了 2019 年時，有資訊安全研究人員 Adrian Bednarek 針對 1Password、Dashlane、KeePass 與 LastPass 等知名密碼管理軟體進行檢測，發現這些軟體確實能保障使用者的機密資訊，但還是會將一些機密訊息以明文方式留在記憶體中，若攻擊者已入侵到使用者的電腦中時，是有可能從記憶體中取得這些機密訊息。即使到最近的 2020 年時，KeePass 還被發現可以透過刻意建立的 CSV 檔來執行任意的指令。

不僅是 KeePass，即使是 Bitwarden 或是商業軟體如 1Password、Lastpass 也都曾經被發現漏洞，因此使用密碼管理軟體時，還是要注意相關的更新，以避免因潛在的漏洞導致機密資訊的外洩。

陸、情境模擬

安樂任職於台安公司已有數年的時間。最近因台安公司的資深網管工程師派調國外，在新任網管工程師尚未到任之際，公司指派安樂先接手公司的資訊系統。安樂甫一接手就發現公司內部有不少的資訊系統，每套系統都有各自的帳號密碼，且為了符合相關資訊安全規定，密碼不僅要符合複雜度規定，也要定期更換。對於安樂來說，自己本身所需的手機密碼、提款卡密碼、數個購物網站密碼、電子郵件帳號密碼等就有不少組了。現在還得加上公司資訊

系統的密碼，就有數十組的密碼需要記憶。為了方便記憶及安全起見，安樂想了個方法，就是將密碼大多設為 P@ssw0rd，後面再加上要連線的系統 IP，例如要使用的使用是 192.168.10.11，那麼密碼就是 P@ssw0rd11，至於其他以數字為主的密碼，就全部出生年月日做為密碼，並把這些密碼直接存在電腦的記事本內。

某日，台安公司發現多個系統遭受勒索病毒攻擊，更有常用的檔案伺服器資料被勒索軟體加密，經清查後發現多數的攻擊竟然是使用安樂的帳號與密碼來發動的。為此，公司請來專業資安人員來進行調查，經初步調查後發現攻擊來源的確來自安樂的電腦，且安樂的電腦也被安裝了遠端控制軟體。經過專業資安人員進一步的調查後，發現攻擊者最初是由公司的網站取得當時聯絡人，也就是安樂的電子郵件，再透過字典攻擊法進行密碼破解，由於安樂常用的密碼 P@ssw0rd 早已是常見的懶人密碼，攻擊者僅需透過這組密碼加上數字組合，就能快速破解這組密碼，因而成功入侵安樂的電子郵件帳號，並取得安樂帳號下所有聯絡人的往來信件的資料。

攻擊者過濾安樂的電子郵件後，找出安樂曾經向之前網管人員詢問過如何遠端登入公司 VPN 網路的信件與要設定的帳號及密碼，就以安樂的帳號成功登入公司的 VPN 網路，並進一步登入到安樂在公司使用的電腦，在安樂的電腦中安裝遠端控制軟體方便日後進行遠端操作。同時，攻擊者在安樂的電腦中找尋所有的機密訊息，而毫無保護的密碼檔就這樣輕易落入攻擊者的手裡，如圖 10 所示。攻擊者並以這些資訊來對公司的各項系統發動勒索病毒攻擊。安樂身為公司網管人員，因此在所有的系統上都有建立帳號，其中檔案伺服器更是使用網路芳鄰的 SMB（Server Message Block）協定來進行分享，因此攻擊者一旦使用的是安樂的帳號，就能對系統有效發動攻擊，並透過 SMB 協定成功將檔案伺服器上的資料進行加密。而這些帳號密碼的洩露，不僅使得公司系統遭受攻擊，攻擊者還一併掌握了安樂其他常用的系統，甚至於手機與提款卡的密碼等，使得安樂得花上不少時間來一一處理密碼修改的問題。

經歷這次的事件後，身為系統管理者的安樂深刻體會到密碼安全的重要性。密碼的安全不僅是在於設定足夠長度的密碼，更應注意密碼保管的安全性。若這次的事件發生前，安樂能將所管理的密碼使用密碼管理軟體保管好，如圖 11 所示。那麼攻擊者就不易取得其他系統的帳號密碼，更加難以對檔案伺服器發動勒索病毒攻擊。並且安樂也反省不應為了方便使用懶人密碼，造成個人資料外洩，而是應更加注意密碼的設定與定期修改，並且透過密碼管理軟體就妥善保存。也惟有建立良好的密碼設定與使用習慣，才能避免密碼被破解或重要資訊外洩，並成為合格的網管人員。

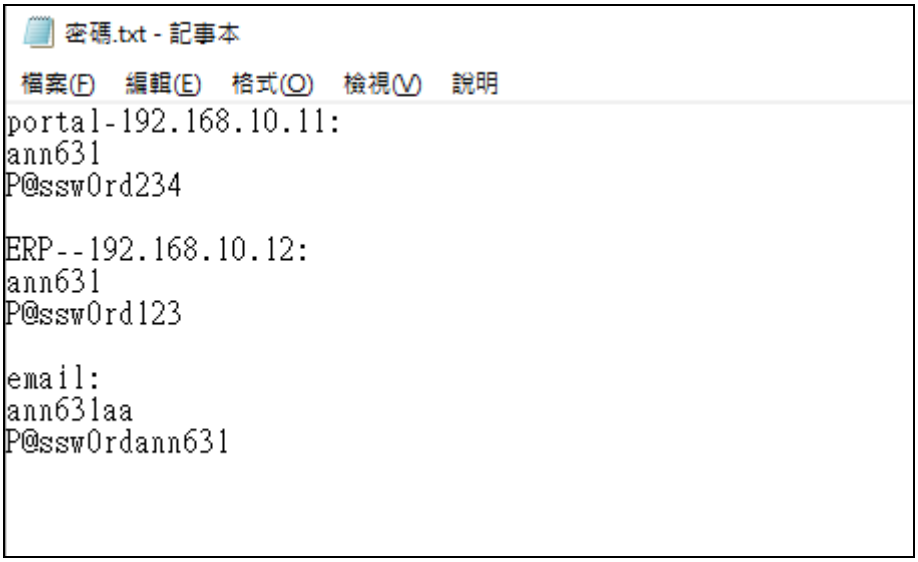

圖 10：安樂的密碼紀錄文件

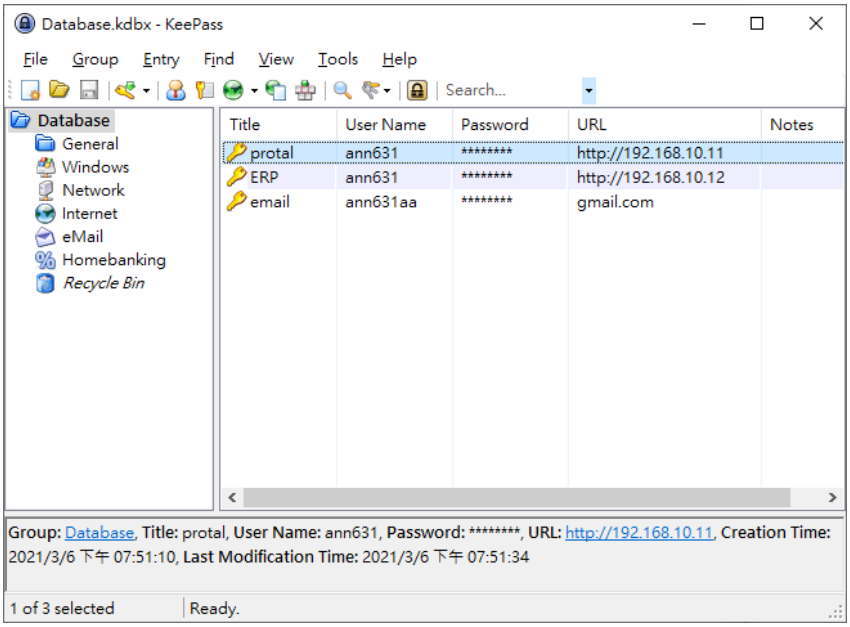

圖 11：安樂改用密碼管理軟體紀錄密碼

柒、結論

現代人每天都會面對到許多資訊設備與系統，要記憶的密碼也愈來愈多，而為了避免輕易被破解，對於密碼的要求也更趨嚴格。但為了安全起見，多組帳號密碼雖然麻煩但確實有必要。然而就人性而言，太多的密碼就愈容易傾向於設定懶人密碼，導致原本要求建立安全密碼的本意落空。因此，本文中就密碼設定原則進行說明，由過去傳統與現代的密碼設定方式，我們得知密碼的安全並不是在於多重字元的變化，而是更需關注密碼的長度。讀者們可透過這些密碼設定的原則來自行評估及檢測密碼的安全性，並建立起如何設定安全密碼的概念。而對於密碼繁雜且不易記憶的問題，我們則在本文中介紹 KeePass 這套開源的密碼管理軟體，透過 KeePass 的運用，我們將所需記憶的重要密碼減少至「一組」！ 且 透 過

KeePass 的使用，即使需當眾開啟密碼檔，也無需擔心密碼外洩。而對需要定期更換密碼的人來說，KeePass 不僅能協助使用者紀錄多筆密碼，並能協助強化密碼的安全性，不用擔心無法記住各個資訊系統複雜的密碼，讓我們在使用眾多網路服務時更加安全。