

密碼管理

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 密碼管理的挑戰.....	3
密碼的保安威脅	3
II. 趨勢和 IT 管治.....	4
單一密碼與多個密碼的比較	4
不同程式採用不同密碼的考慮	4
IT 管治：良好的密碼管理政策及用戶教育.....	5
III. 幫助密碼管理的技術	6
公開密碼匙基礎建設	6
單一登入	6
限用一次密碼權標	7
IV. 最佳作業實務	8
如何選擇良好的密碼	8
處理密碼時應注意事項	9
系統／保安管理員應注意事項	9
V. 總結.....	11

摘要

密碼是用戶進入電腦系統或網站時最常用的認證方法，亦是防禦未經授權接達的第一道防線，因此，積極實施良好的密碼管理政策，是維護這道防線最關鍵之處。本文旨在提供處理和管理密碼方面的指引及最佳作業實務。

I. 密碼管理的挑戰

在我們的日常生活中，有關資訊科技的事物愈來愈多，還有不斷增加而要緊記及管理的戶口和密碼。要為不同的資訊系統選擇密碼，實在令人困擾。如果同一個密碼用於所有系統，當入侵者得到這個密碼，便能夠接達所有系統。另一方面，如果在不同系統使用不同密碼，用戶便會傾向選擇方便記憶或容易被破解的密碼，甚至將密碼寫下來，對系統保安構成威脅。用戶忘記密碼的情況屢見不鮮，最終增加用戶支援和重設密碼等操作的負荷。

密碼的保安威脅

用戶要進入電腦系統，輸入密碼是最簡便的認證方法，電腦系統只需要用戶表明及確認身份。雖然實施密碼認證方法很容易，但卻會引起不少保安威脅。以下是一些合法用戶可能洩露密碼的常見保安風險：

1. 肩窺攻擊 (Shoulder attack)：當用戶輸入密碼時，旁人有機會在其肩膀後方直接觀看所鍵入字符，或非直接地從閉路電視監察，繼而竊取密碼。
2. 暴力攻擊：由於密碼的長度有限，通常只有八個文數字字符，攻擊者可用程式自動拼湊密碼，嘗試所有可能的組合直至找到有效的密碼。現今電腦的運算能力更高，成功施行暴力攻擊所需時間便大大縮短。
3. 探取攻擊：如網絡渠道沒有適當加密，只要使用網絡探取工具，密碼在網絡上被傳送時便可能被收集。另外，如使用惡性攻擊工具（例如鍵盤側錄程式），用戶在認證過程中輸入密碼時便可能被收集用戶密碼。
4. 登入仿冒攻擊：攻擊者設立仿冒的登入畫面，看似與真正的登入畫面無異。當用戶在仿冒畫面登入時，其密碼便會遭記錄或傳送給攻擊者。

如果成功進行以上所述攻擊，可幫助未經授權的用戶取得合法用戶的密碼。因此，只使用密碼作為認證方法的系統不可能分辨密碼持有人的身份有效與否。

II. 趨勢和 IT 管治

單一密碼與多個密碼的比較

從用戶角度看，不論單一密碼如何複雜，記著單一密碼比處理多個密碼容易。另外，如果單一密碼已足夠認證所有系統，用戶便會提高警覺以保護自己的密碼。可是，使用單一密碼登入所有系統在技術上並不可行，尤其在既有的系統上，或須跨越多種操作系統平台的時候更加不可行。

如果用戶只需要間中接達某些系統，他們有機會忘記這些不常用的密碼，給負責重設密碼的支援人員增加工作負荷。再者，用戶會嘗試避開繁複的程序，例如將密碼寫下來，或選擇方便記憶但容易被破解的密碼。

對攻擊者來說，單一密碼的保護性較低，當密碼被成功奪取，所有系統將自動被入侵。因此，機構決定使用單一密碼的時候，所有系統必須以相同的保安程度作出保護。

不同程式採用不同密碼的考慮

一般系統

視乎本身的功能特點和數據類型而定，不同的資訊系統有不同的保安要求。一般來說，所選擇的認證機制之複雜程度應切合其保護的資訊價值，例如內部程式處理機密資料時需要緊密的接達控制，相反而言，互聯網程式處理一般資料搜尋或會容許匿名登入。

換言之，因應系統的保安要求和所保護的資訊價值的不同，不同系統應選擇不同的密碼。如果使用單一密碼接達多個系統，所有用戶賬戶必須跟最高保安要求的系統有同樣的安全程度，否則入侵者便有機可乘入侵保護性低的系統，並且取得其它較高保安要求系統的接達權。

重要的系統和資源

在重要的系統或處理機密資料的程式中，應該實施嚴格的接達控制以防止未經授權的接達。基於風險考慮，用以接達這些重要內部系統的密碼必須跟其它的不同。

內部和對外應用程式

因機構未能完全控制外在環境，相對控制內部應用程式而言，要嚴格控制對外的應用程式並不容易。譬如用戶在沒有保安控制的公共設施、家中電腦或其它地點接達公司的互聯網程式，由於沒有保安控制，所以向外洩露密碼的風險大增。如果內部和對外程式均使用相同密碼，將會削弱內部系統的保安程度。萬一對外程式的密碼被破解，入侵者或會利用該系統作為踏板並破壞內部系統。

一般而言，內部和對外程式的重要程度不一，相對保安要求也不同，因此應實施多個密碼政策，接達內部和對外程式時不應再使用相同密碼。另外，建議的作業實務是接達重要程式或一般程式時使用不同密碼，甚至使用擁有特別權力的賬戶接達重要程式。這種作業實務已記錄在政府團體和機構廣泛採用的密碼指引中。

具備相同保安要求的系統

為了在方便和安全之間取得平衡，只要制定清晰的保安政策和賬戶使用方式，用戶使用相同密碼接達相同保安要求的程式也是可行的。舉例說，接達工作時間記錄輸入系統和申請假期系統便可使用相同密碼，原因是兩者皆是人力資源系統，並且根據相同的保安政策進行管理。

IT 管治：良好的密碼管理政策及用戶教育

如果密碼並非由中央數據庫或系統管理，要發展機制以實施不同程式使用不同密碼便很困難。因此，應在保安政策中清晰地闡述不同程式使用不同密碼的標準。由於密碼是防禦未經授權接達的第一道防線，良好的密碼管理政策是維護這道防線最有效的方法。

除此以外，用戶應學習及注意選擇和處理密碼的最佳作業實務。使用不安全的密碼可以直接影響整個系統的保安。同樣地，所有用戶須具有責任感，採取適當的步驟選擇密碼以及確保密碼的安全。

III. 幫助密碼管理的技術

要實施良好密碼管理，除了訂立保安政策和指引，以下技術將有助於推行有效又易用的密碼管理。

公開密碼匙基礎建設

公開密碼匙基礎建設（PKI）的技術採用數學算法和程序，有助於安全交易，提供數據機密性、數據完整性和認證。PKI 使用數碼證書以證明個別用戶的身份。數碼證書是一種數碼文件，為個別用戶加上公開密碼匙作為認證，就像一張個人身份證。獲信任的核證機關（CA）製作證書，並用 CA 的私人密碼匙在證書加上數碼簽署，以核實作出要求一方的身份。任何人都可使用其證書核實身份，以進入不同的應用程式，然後，程式會根據簽發證書的 CA 確認數碼證書以便核實用戶的身份。

PKI 不需要預先為所有程式作出登記，因此特別適用於連線交易和公共程式的用戶認證。用戶只要向獲信任的 CA 申請證書，便可以跟不同應用程式作出認證。

實施 PKI 時要注意的保安考慮事項如下：

1. 私人密碼匙必須加以保護並儲存在安全的地方，例如儲存在保安權標或以 PIN 作安全防護的智能咭。
2. 保安權標／智能咭的 PIN 應加上有關的密碼限制，以防止未經授權接達內部的私人密碼匙。
3. 密碼匙周期管理、發出及撤銷數碼證書、儲存及提取數碼證書和 CRLs（證書撤銷名單）時應訂立適當的程序。
4. 為私人密碼匙備份時，必須以加密形式複製及儲存，保護程度不可低於原本的私人密碼匙。
5. 因為並非所有程式皆支援 PKI，所以有機會出現不互通的情況。

單一登入

用戶使用單一登入（Single Sign-On, SSO）技術，只要跟認證伺服器辨識身份一次，便可以接達多個應用程式，包括內部和對外系統。用戶可享受選擇單一密碼以接達多個應用程式的好處，而毋須緊記不同的密碼。然而，如果認證部份被入侵，則表示用戶有接達權的所有資源均有機會被破壞。

實施 SSO 時要注意的保安考慮事項如下：

1. 由於單一認證控制用戶接達所有資源的權利，所以認證過程必須有足夠的安全措施去保護這些資源，以及滿足大部份重要應用程式的要求。應用程式的單一認證過程必須比原本的認證方法更嚴格，否則結果只會是保安程度下降。
2. 應加入第二重認證，例如保安權標和智能咭，以強化認證過程。
3. 應實施有關的密碼限制，例如最短密碼長度、密碼複雜程度、最多嘗試登入次數和更新密碼最短時間等。
4. 認證伺服器可能成為攻擊目標，因此應加強保護，令入侵者不能接達認證資料，否則當入侵者得到認證資料便可以未經授權接達所有系統。
5. 應使用審計及記錄功能以偵測和追蹤可疑的登入失敗嘗試。
6. 應採用加密方法以保護在網絡上傳輸的認證憑證。

限用一次密碼權標

另一種可幫助密碼管理是限用一次密碼權標。用戶通過雙重而又獨一無二的認證，包括他們有的權標和他們知悉的 PIN，因此不需要選擇或緊記密碼。權標會以 PIN 和另一認證方法，在每次認證過程中產生獨一無二、限用一次的密碼，然後授權接達以保護資源。實施限用一次密碼權標時要注意的保安考慮事項如下：

1. 在認證過程中，每位用戶需要一個權標，表示須另計成本。
2. 用戶須任何時候攜帶權標，如果遺失或忘記攜帶，便不能夠接達系統。如果遺失權標，甚至數小時或數天不能使用系統。反之，基於軟件接達控制系統只需要重設密碼，用戶便可登入。
3. 用戶應注意權標的實體保安，並確保權標任何時候被妥善保護。
4. 大部份限用一次密碼認證方法只會認證首次連接，其後的連接會被假設為已認證，增加被劫持的機會。
5. 保安權標可能不支援所有應用程式或伺服器。

IV. 最佳作業實務

如何選擇良好的密碼

不當密碼的例子

以下是選擇不當密碼的例子，即容易被猜中，或輕易被從互聯網下載免費的密碼破解軟件破解。

- "password" - 最容易猜到的密碼
- "administrator" - 用戶登入名稱
- "cisco" - 供應商名稱
- "peter chan" - 個人姓名
- "aaaaaaaa" - 重複同一個字母
- "abcdefgh" - 連貫字母
- "23456789" - 連貫數字
- "qwertyui" - 鍵盤上相鄰鍵碼組成的密碼
- "computer" - 在詞典中查到的單字
- "computer12" - 稍為修改過在詞典中查到的單字
- "c0mput3r" - 稍為修改過在詞典中查到的單字，例如以“0”替代“o”、“3”替代“e”。

為防止被入侵，以下是一些併湊密碼的簡單規則以供參考：

不應

1. 不應使用任何形式的登入名稱（原形、倒寫、大寫、重複等）。
2. 不應使用任何形式的本人姓氏或名字。
3. 不應使用配偶或子女的姓名。
4. 不應使用他人容易取得的其它個人資料，包括身份證號碼、車牌號碼、電話號碼、出生年月日、居所街道名稱等。
5. 不應使用由相同字母組成的密碼，例如“aaaaaa”。
6. 不應使用連貫的字母或數字，例如“abcdefgh”或“23456789”。
7. 不應使用在鍵盤上相鄰鍵碼組成的密碼，例如“qwertyui”。
8. 不應使用能夠在英語或其它外語詞典中查到的單字。
9. 不應使用能夠在英語或其它外語詞典中查到的單字的倒寫。
10. 不應使用廣為人知的縮寫，例如：HKSAR、HKMA、MTR。

11. 不應使用稍為修改以上第 1-10 點所述例子後組成的密碼。稱為修改的形式包括附加或加插數字或符號，或使用替代字符，例如以 3 替代 E、\$ 替代 S、0 替代 O。
12. 不應重新使用近期使用過的密碼。
13. 不應在不同情況下使用相同密碼；建議在不重要的情況下用一個密碼，關於敏感或重要的情況則使用另一個密碼。

應

1. 應使用至少由六個大小寫不一的字母、數字及特殊字符混合組成的密碼。
2. 應使用不容易猜到但方便用戶本人記憶的密碼，以避免將密碼寫下。
3. 應使用毋須眼看鍵盤即能快速輸入的密碼，以避免行經的人看到所輸入的內容。

處理密碼時應注意事項

不應

1. 不應寫下密碼，特別是電腦附近或存檔並寫上「密碼」二字。
2. 即使有極為充分的理由，也不應透露或出示密碼。
3. 不應在顯示器顯示密碼。
4. 不應寄出密碼，尤其是通過電郵系統寄出未加密的密碼。
5. 用戶不應揀選一些網站提供的「記憶密碼」功能，而應取消瀏覽器軟件的有關功能。
6. 不應將密碼儲存在任何媒體，除非這些媒體可阻止未獲授權人士接達（例如以獲批准的加密法來進行加密）。

應

1. 應至少每 90 天更換一次密碼。
2. 在首次登入時應更改預設或初始密碼。
3. 如果懷疑密碼已洩露，應立即更換密碼。更換密碼後，應通知系統／保安管理員，以便採取跟進行動。

系統／保安管理員應注意事項

不應

1. 不應向用戶寄出密碼，尤其是通過電郵系統寄出未加密的密碼。
2. 除非可驗證用戶的身份，否則不應代用戶披露或重新設定密碼。
3. 不應將密碼儲存在可供公開閱讀的檔案內。

應

1. 應揀選適當的賬戶初始密碼。

2. 不同的賬戶應揀選不同的初始密碼。
3. 應要求用戶在收到新的密碼後，立即更換初始密碼。
4. 應更換所有的系統預設密碼，包括安裝新系統後的服務賬戶密碼。
5. 應要求用戶至少每 90 天更換一次密碼。

系統保安功能

以下是一些操作及應用系統提供的較理想的保安功能，這些功能有助執行以上建議的部份揀選密碼準則。建議應盡可能啟動這些功能。

1. 連續登入失敗次數達到預定上限後自動暫停用戶賬戶。
2. 賬戶操作被暫停後，規定有關賬戶必須經系統／保安管理員人手調整後才能重新啟動。
3. 禁止用戶使用短於預定長度的密碼，或重新使用曾經用過的密碼。

V. 總結

密碼是用戶進入電腦系統時最常用的認證方法，卻經常成為入侵者入侵系統的目標。密碼是防禦未經授權接達的第一道防線，因此積極實施良好的密碼管理政策是維護這道防線最有效的方法。視乎本身的功能特點和數據類型，不同的資訊系統應有不同的保安要求。並使用其它接達控制機制以實施密碼管理，以減低用戶緊記大量密碼的負荷。要實施密碼管理，可採用良好保安作業實務及指引，給用戶提供關注選擇和處理密碼的培訓和教育。

另外，要實施有效的資訊保安管理，應作多方面考慮，包括實體保安、數據和應用程式保安、網絡保安，以及強化保安技術，例如防火牆、VPN 和 SSL。