立法院「資訊應用系統大型主機動態密碼系統」簡介

壹、前言

時光回溯到 94 年 3 月，多家金融機構發生電腦遭駭客植入木馬之事件，引發身分竊取問題的高度矚目。檢視資安廠商多年來的報告，身份竊取不約而同地已成注意的焦點。

據國外知名防毒 M 公司 96 年報告指出，93 年 1 月到 95 年 5 月間，用來獲取使用者帳號密碼的鍵盤測錄程式(Key logger)增加 2.5 倍，而去(97)年下半年在台最猖獗的前 3 個惡意程式，有 2 個是專偷線上遊戲的帳號密碼。爲對抗身份竊取所可能帶來的損失，業者紛紛提出解決方案，其中的「動態密碼鎖」技術便應運而生。

傳統固定密碼，被駭客竊取後，就可以冒用進行交易。而動態密碼每次產生的密碼都不相同，且僅一次有效，採用特定演算法，以變動的時間、次數或輸入內容等參數，爲基本元素「Seed」，經演算得到的結果，轉換成密碼，由於 Seed 具有變動性，每次產生的密碼不同，因此稱之爲 One Time Password(OTP)或「動態密碼」。

依據本院資訊安全存取控之政策，大型主機作業系統之特殊權限帳號必須定期更換，且要建立分持制度，以保障本院重要資訊應用系統的安全性，爰此而引進 RSA 動態密碼解決方案，在原有的用戶帳號密碼認證機制之外，再增加一次性密碼輸入，藉由雙因素認證，解決身份竊取問題。

貳、工作原理

動態密碼鑰匙正面有液晶螢幕，每 60 秒隨機產生 Pass Code，其生命週期 60 秒。動態密碼產生時，產生器硬體並沒有與電腦連線，欲登入的電腦系統是如何確認密碼的正確、有效性？

鑰匙內含高精度之計時電路，具備唯一硬體序號，計時電路於出廠時皆精確校正程序，確保每次產生之 Pass Code 與伺服器一致，核發前，管理人員會先將該硬體序號輸入動態密碼伺服器中，並對應至欲使用此機制之帳號。

用此帳號登入系統時，動態密碼伺服器便會接管認證，於輸入正確使用者名稱、動態密碼後，即可完成驗證，登入成功後該密碼便會視爲已用過，並自動捨棄不可再用。

因爲每支鑰匙皆有不同硬體序號，有不同的硬體計時同步線路，不同之 Pass Code 演算法，對應伺服器中不同之密碼產生器，所以不同的人拿不同的鑰匙，所產生的 Pass Code 也就不同，且能確保每一支鑰匙於產生一組 Pass Code 以後不會連續產生一模一樣的號碼。也因爲該 Pass Code 於 60 秒鐘內或已登入成功後便會被丟棄視爲無效，即便密碼被駭客盜走也無法逞其惡意入侵之能事。

如果該硬體鑰匙被有心人士奪走，且嘗試破解其中的Pass Code演算法，這該如何是好？

鑰匙遺失或遭人偷竊，可立刻通報系統管理員，將該其註銷，登入將被阻攔無法得逞，且該系統的設計理念採用不可逆之原理規劃，無法以反向軟體工程得逞，該鑰匙一經拆解，即自動失效，形同報廢，再造、複製亦無作用。

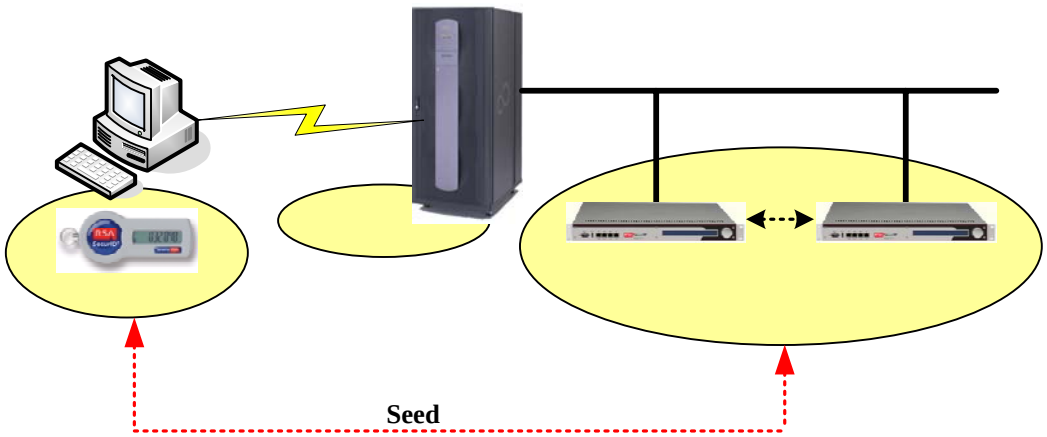
參、系統架構

本院採用 RSA SecurID 雙因素認證系統，使用者需同時提供兩種辨認方式，一是 RSA SecurID 認證裝置(Token)，二是密碼，經 RSA 伺服器認證符合後才可進入系統，密碼採用 Time-based 演算法，密碼 60 秒變動，提供迅速、簡單和高度可靠的身分確認方式，確保資訊安全。

RSA SecurID 認證系統是由三個主要部份所組成：

1. 認證裝置(RSA Authentication Authenticators)。
2. 認證管理伺服器(RSA Authentication Manager)。
3. 認證代理程式(RSA Authentication Agents)。

架構如圖示：



一、 認證裝置(RSA Authentication Authenticators)

RSA SecurID 認證裝置能夠辨識使用者身份，開啓存取受保護資源的途徑，每個 Token 會隨機產生 Seed value，每 60 秒變更並顯示一組號碼，該號碼只能在此一分鐘使用，且必須結合使用者的個人識別碼或密碼，Token 的動態特性使得身份無法被竊取。

二、 認證代理程式(RSA Authentication Agents)

RSA 認證代理程式介於使用者以及任何需要保護的網路資源之間，當使用者試圖存取特定資源時，Agent 將存取要求轉給 RSA Server。

三、 認證管理伺服器(RSA Authentication Manager)

RSA 認證管理伺服器結合了高效能的認證引擎和集中式管理能力，接收到存取請求後，RSA 認證管理伺服器會運用和 Token 一樣的演算法來檢查輸入的 Token 碼，如果兩個因素中的任何一個有誤，使用者會被要求重新輸入正確的資訊，三次錯誤後，會被系統鎖住，直到管理者重啓帳號爲止。

四、 優點(Advantages)

本院大型主機資訊系統運用此動態密碼系統架構，可用來保護特殊權限帳號，防止帳號遭竊取，可有效阻絕駭客盜取帳號，優點歸納如下：

(一)、 足夠安全性

有不可預測、不可重複、一次使用等特性，密碼若不慎被截取，不僅無法利用前次輸入的密碼再進行交易，pin code 的驗證上也無法過關，更可藉由管理端設定終止，有效防堵木馬程式，提昇安全性。

(二)、 使用門檻低

不需在使用者電腦上安裝安控軟體，也不需要製作憑證(CA)金鑰，更不用再執行憑證展期手續，或另外安裝讀卡機，依照鑰匙上所顯示之號碼搭配 pin code，即可開用。

(三)、 便利性高

鑰匙隨身攜帶，不需要與電腦連結，可防止木馬盜用、防止密碼側錄等程式的攻擊。

肆、系統功能

本院 ISMS 嚴格規範 Admin 密碼長度不得少於 8 位，且須定期更換，藉由動態密碼安全認證系統，可同時整合本院大型主機帳號管理稽核機制，以增加主機系統的安全性且可避免增加系統管理者及使用者記憶密碼之負荷，強化通行密碼之安全性，系統功能如下：

一、 支援 HA 架構，主系統與備援系統均可同時提供認證服務。
二、 硬體設備故障無法運作時，可轉由主機作業系統直接作密碼認證，不影響使用者登入作業。
三、 紀錄檔(log)能與主機作業系統登入紀錄檔勾稽，由伺服器管理及紀錄所有的登入行爲，且提供管理者相關報表。
四、 可承載 50,000 個使用者。
五、 提供 DR 的工具及還原程序，備援系統可升級爲主系統。
六、 每秒可處理 180 APS(Authentication Per Second)個使用者認證程序以上。

七、 提供 LDAP 匯入及同步工具，可自 Microsoft Active Director/ SunOne Directory Server/ Novell eDirectory 目錄伺服器匯入帳號。

八、 管理方式：

(一) 可由 RSA local host 管理介面直接操作。

(二) 利用專屬管理軟體，透過動態密碼認證才能來進行遠端的管理，以提升安全性。

九、 可依據組織中每位管理人員所具有的權限來分派職責管理使用者群組，並提供管理介面來管理並建立管理者角色。

十、 具備網路設備廠商整合認證測試，預留整合、擴充空間：

(一) Cisco、F5、Juniper、Fortinet。

(二) Novell、Windows、Oracle ERP、Oracle DB、Solaris。

十一、 AES 128bits 演算加密：

(一) 硬體 Token：在 LCD 螢幕上，每 60 秒自動變更密碼。

(二) 軟體 Token：支援.NET、J2EE、及 CE 等平台。

伍、效益與展望

本院在引進 OTP 技術方案之後資訊安全業已獲得更進一步的提升，可從技術、管理、稽核、使用及價值等面向之效益說明：

一、 技術：

(一)支援多種平台標準技術協定。

(二)一次性密碼、雙因素驗證技術、金鑰與伺服器同步技術、集中控管、HA 架構。

二、 管理：

(一)避免帳號盜竊。

(二)資訊人員毋須維護複雜的身份識別存放區。

(三)簡化管理，減輕 IT 管理負擔－簡化對關鍵系統的存取，讓存取的安全性堅不可摧，並減輕 IT 管理者的負擔。

三、 稽核：

(一)降低洩漏的風險性。

(二)可避免無意間授與用戶存取敏感資料的權限之風險。

四、 使用：

(一)學習適應門檻低。

(二)使用者無須記住多組帳號與密碼。保障帳號密碼安全。

(三)避免帳號被盜用所引發的訴訟爭端。

(四)不再有密碼遺忘的困擾。

五、 價值：

(一)具備彈性擴充與異質平台整合能力，可保障既有投資。

(二)確保帳號存取安全，避免重要資料盜竊。

(三)降低商務中斷的風險－提供金融級資安建設。

(四)整合應用－VPN、Radius、Citrix、IIS/Tomcat Filter、Windows 網域登入、Outlook Web Access、客製化 ID/Pass 網頁升級。

道高一尺、魔高一丈，資安工作無止盡，應時保資安意識、技術之更新，以防微杜漸。本院的動態密碼系統，已爲大型主機系統環境奠下基礎的安全機制，無論在人員控管、技術層次、管理面向、法規遵循等，均已邁向成熟的曲線。

權限管控議題上，動態密碼機制乃一資安試金石，本院將繼續朝向系統整合的路線，由動態密碼的驗證模式延伸至其他資訊應用系統，並結合本院各類資訊應用系統，以 SOA 架構深崁入軟體內層，充分滿足實體的動態密碼管控機制、與多樣化、變異的軟體管控需求，使多因素驗證與更完善的單一簽出簽入的驗證機制能全面實踐，達到登入無障礙、資安無罣礙、人人有信心、業務有保障之高水準資訊環境。

（本文由立法院資訊處 提供）