一次密碼技術導入國軍網站身分認證之研究

作者/馬兆顯 中校・陳正鎔 助理教授・伍台國 博士

提要

近年來，由於資訊科技的快速發展，國軍各單位也陸續將過去傳統人工作業，改為電子化作業，建構各項資訊系統，朝向資訊化、自動化、整體化方向努力，並將各項資料轉換為電子檔，儲存於資料庫，透過各單位建置之網站與首頁，存取各項資訊，惟資料之存取，僅使用帳號、密碼之管控，致使只要進入網站，就幾進入無人之境，可輕易獲得資訊，造成洩(違)密事件的發生時有所聞，實為安全上之罅隙，故本文提出於一次密碼認證 (One-Time Password Authentication) 智慧卡，並結合認證中心 CA 之防護機制，將智慧卡應用於國軍登入電腦網站之個人身分認證，提高對資料之保密安全，期為國軍相關應用之參考。

關鍵詞：一次密碼(OTP)、智慧卡、認證中心(CA)、身分認證

壹、前言

自從資訊科技日漸普及，國軍各單位已逐漸將過去手抄謄寫之紙本資料，轉換為電子資料，並建立各項資料網站之入口，但網站入口首頁之身分辨證，一般而言大都使用帳號與密碼之管控模式，未採用加密技術，故只要竊取到使用者之帳號、密碼，即可進入網站，存取相關資料，雖然，各通資單位一再宣導要定期更換密碼，並制定密碼選取原則，避免遭人盜用，惟不經意中仍可發現電腦螢幕上、辦公桌旁，張貼個人帳號密碼，因此，即有『一次密碼認證』(OTP)、『單一簽入』(SSO)等相關技術，被提出應用於身份查核。

其中，一次密碼認證技術，於 1981 年由 L. Lamport 以密碼認證為基礎，提出一次密碼認證系統(S/Key One-Time Password Authentication System)[1]-[2]，惟所提之 S/Key scheme 易遭攻擊破壞，因此，Yeh、Shen 及 Hwang 於 2002 年另提出以改良式之一次密碼驗證安全機制[3]，運用於智慧卡之中，此乃建立電子商務線上安全交易環境，可避免有心人士的重送攻擊(Replay Attack)、欺騙攻擊(Spoofing Attack)、離線字典攻擊(Off-Line Dictionary Attack)、總體字典攻擊(Global Dictionary Attack)及訊息內容主動式揭露攻擊(Active Attack and Revelation of Message Contents)，有效提高其認證之方式，達到簡單、安全及效

率。但是，2004 年 Ku、Tsai、Tsaur[4]等人認為該三位學者所提出之論點，雖可改善 S/Key scheme[5]-[7]認證之功能，然仍有遭竊取驗證攻擊(Stolen-Verifier Attack)[8，9]之可能。

因此，本文除將保留 Yeh 等人所述系統架構之特點外，並提出 Ku 等人攻擊之防護措施，以加強系統架構與加密技術之完整性與安全性，藉此營造安全、便利之認證環境，應用於進入國軍各網站存取重要資料時之身分認證，期能有助於國軍資訊安全之要求。

本文概分為三節，第一節為前言說明；第二節分別介紹 Yeh 等人所提一次密碼驗證運用於智慧卡之安全機制系統架構，加密技術與原理，舉實例演算說明，並與不對稱式密碼技術比較，另提出改良之系統架構，解除 Ku 等人所提出之竊取認證攻擊(Stolen-Verifier Attack)，所造成之安全漏洞安全疑慮，以導入國軍網站身分認證之應用；最後闡述結論。

貳、一次密碼驗證安全機制應用於智慧卡之系統架構

所謂一次密碼驗證，顧名思義即指每次登入，均採用不同之『認證資料』進入系統，以避免遭受非法使用者的偽冒攻擊，2002 年 Yeh、Shen 及 Hwang 提出一次密碼驗證之智慧卡機制(A Secure One-Time Password Authentication Scheme Using Smart Cards)，其特點為增進 S/Key 之架構，由使用者與伺服器間進行雙向身分驗證，此系統主要分為三個階段：(一)註冊階段、(二)登入階段、(三)驗證階段。分別敘述如下：

在各階段說明前，首先將所需之名詞及參數進行定義：

U：登入網站之使用者。

S：網站之驗證伺服器。

PW：表示為使用者之密碼。

K：表示從使用者 PW 所推導傳送之私有金鑰。

SEED：表示為 S 產生之大型隨機亂數，並且分享給使用者。

N：當使用者完成註冊後，所產生之允許登入次數。

H( )：表示為雜湊函數，H^2 同等於 H(H(m))，H^3(m)即表示為 H^2(H(m))，m 為雜湊後次數。

⊕：表示為 XOR 運算元。

—>：表示為網路之一般通聯通道。

=>：表示為網路之安全通聯通道。

一、註冊階段

伺服器 S 於開始先產生一秘密大型隨機亂數 SEED(種子值)，並與使用者 U 共享之，此隨機亂數 SEED 透過秘密通道傳送給 U，此外，S 將 SEED 儲存於本身資料庫中，而 U 則儲存於智慧卡中，接著 S 再產生一隨機亂數 D_0，並計算 SEED $\oplus D_0$ 和 $H(D_0)$，將此兩算式之計算結果數值與允許登入次數值 N 傳送至 U。當 U 接收後，以互斥或(XOR)方式計算 SEED$\oplus$(SEED$\oplus D_0$)，即可從智慧卡中取出 D_0 並與接收之 $H(D_0)$進行比對，如果兩者數值相等，則表示 U 可確認是由 S 所發出之訊息，下一步為 U 輸入 PW 到智慧卡中，去獲取密鑰 K 並結合 SEED 值，並雜湊函數以計算自身之初始驗證值 $P_0=H^N(K\oplus SEED)$。U 將 P_0 值再以 XOR 方法計算 $P_0\oplus D_0$ 值，將結果傳送至 S，而 S 從接收之訊息中運用 D_0 去獲得 P_0，並確認是否為 U 所發出之訊息。另外，S 設定 U 初次成功登入 U 之次數 T 為零。此階段之簡易步驟概述如下圖一：

伺服器 Server

步驟一:

1. S產生一隨機亂數SEED, 經由安全通道傳送至U。
2. S與U分別儲存此一隨機亂數SEED。

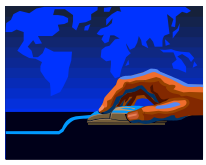
使用者 User

安全通道

伺服器 Server

步驟二:

1.S產生另一隨機亂數D_0 與N。
2.S計算SEED$\oplus D_0$ 與$H(D_0)$ 。
3.S傳送N、SEED$\oplus D_0$ 與$H(D_0)$至U。
4.U經由智慧卡中儲存之SEED計算出D_0。
5.U將D_0以雜湊函式計算並比較接收之$H(D_0)$，以驗證S之身份。



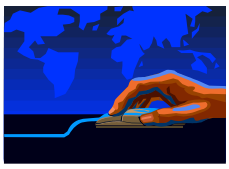
使用者 User

一般通道

伺服器 Server

步驟三:

1.U產生$P_0=H^N(K\oplus SEED)$ 。
2. U計算$P_0\oplus D_0$。
3. S接收$P_0\oplus D_0$。
4. S藉由D_0演算出P_0,以驗證U之身分。



使用者 User

一般通道

圖一　註冊階段步驟

二、登入階段

當 U 第 t 次請求登入 S 時，S 先接收 U 之請求登入，並隨機產生數值 D_t，及修正 T 值(T=t−1 次)，下一步，S 計算 SEED⊕D_t 和 H(D_t) ⊕P_{t-1} 此二數值，將計算結果及伴隨 C_t=(N-t)值傳送至 U，U 接收後，計算 P_{t-1}=H(H^{Ct}(K⊕SEED))，並將其結果從接收之 H(D_t) ⊕P_{t-1} 獲取 H(D_t)。此外，U 利用隨機亂數 SEED，從接收之 SEED⊕D_t 獲取 D_t，若獲取之雜湊數值結果同等於先前獲取之 H(D_t)，並經由雜湊函數計算 P_t=H^{Ct} (K⊕SEED)值，U 可驗證是否為為 S 所送出之訊息，U 再計算 P_t⊕D_t 值，將此 XOR 值結果傳送至 S。

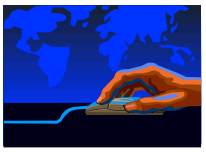
此階段之簡易步驟概述如下圖二：

伺服器

步驟一:

1. U 請求登入 S。

一般通道



使用者 User

伺服器 Server

步驟二:

1.S 隨機產生數值 D_t 及修正 T 值

2.S 計算 SEED⊕D_t 和 H(D_t)⊕P_{t-1} 值並伴隨 C_t=(N- t)值傳送至 U。

3.U 計算 P_{t-1}=H(H^{Ct}(K⊕SEED)) 。

一般通道

使用者 User

伺服器 Server

步驟三:

1. U 經由 H(D_t) ⊕P_{t-1} 獲取 D_t，並計算 H(D_t)及 Pt=H^{Ct} (K⊕SEED)，以驗證為 S 所發出之訊息。

2. U 計算 P_t⊕D_t 並傳送給 S。

一般通道

使用者 User

三、驗證階段

S 從 U 接收訊息 P_t⊕D_t，並運用 D_t 以 XOR 方式演算出 P_t，若所獲之 P_t 雜湊函數值與資料庫中儲存之 P_{t-1} 相等，則 S 可驗證為 U 所發出之訊息，並重新儲存資料庫內資訊，將 P_t 取代 P_{t-1} 及 t 取代 t-1，其概述步驟如下圖三：

伺服器 Server

1.S 接收訊息 $P_t \oplus D_t$。

2.S 運用 D_t 演算出 P_t。

3.再以 P_t 雜湊函數值比對 P_{t-1}，若其值相等則可驗證為 U 所發之訊息，並重新儲存資料庫訊息。

使用者 User

一般通道

圖三　驗證階段步驟

參、不對稱式密碼與一次密碼技術之比較

除了一次密碼技術外，較常用之認證方式為不對稱式密碼技術，所謂不對稱，是使用二把不對稱(asymmetric)的鑰匙，分別是公開鑰匙(Public Key)及私密鑰匙(Privacy Key)，發送端使用公開鑰匙將明文加密後變為密文，傳送給接收者，接受者使用私密鑰匙，再將密文解開，還原成明文，最著名之演算法為 RSA 演算法[10]，於 1978 年由 Rivest、Shamir 及 Adleman 三人所發展出來之公開鑰匙系統架構，應用廣泛，如本國內政部所使用之自然人憑證，即使用 RSA 演算法結合公開金鑰基礎建設(Public Key Infrastructure，PKI)之系統架構，將個人私密鑰匙儲存於智慧卡內部記憶體中，其金鑰長度為 1024 位元[11]。

不對稱式密碼技術，最主要之保密關鍵在於金鑰之長度，而鑰匙的長度與函數之計算複雜度呈非線性成長，長度越長，計算越繁複，故需要有取捨考量，使鑰匙之長度必須達到可抵抗暴力或總體字典攻擊，但可以小到讓一般的加/解密可執行，並且使用人必須按時更換密碼，以防遭人竊取，因此，與一次密碼技術比較，產生下列缺點：

一、定期更換並需記憶多組密碼：使用不對稱密碼技術，為防止密碼遭竊取，使用者須定期更換密碼，且若操作使用不同之系統，還必須記憶多組密碼，一旦忘記密碼，將造成作業上困惱。可是，若使用一次密碼技術，每次都隨機產生密碼，將不會有密碼忘記之缺點並減少密碼被竊之風險。

二、遭受暴力攻擊法之威脅：不對稱式密碼技術，同樣會遭受暴力攻擊法之威脅，雖然只要金鑰長度足夠，破解時間將會拉長，但相較於一次密碼技術而言，由於每次都隨機產生不同之密碼，故較不受暴力攻擊之威脅。

三、計算複雜：由於不對稱密碼技術使用之數學計算繁複，金鑰長度越長，加/解密之速度就越慢，對一般用途之作業來說，就顯得過慢。

綜合而言，一次密碼技術，在保密性、安全性及便利性都較不對稱式密碼

技術為佳，故在下節將介紹，一次密碼技術之改良系統架構，以抵抗竊取驗證攻擊法，及導入國軍網站身分認證之應用。

肆、一次密碼技術增加認證中心(Certificate Authority，CA)之改良系統架構

一、系統架構說明

由於資訊科技發展一日千里，網路應用更加無所不在，使得電子商務交易日趨頻繁，消費使用者與廠商間，不需要面對面交易，僅藉由網路媒介進行商業行為，因此，在電子商務交易中，二者彼此間如何有效認證，以確定為合法使用者及廠商所提供之正確網站，非釣魚網頁[12]-[13]，就益顯重要。

國軍之網站較不會發生虛假網站之情事，但對進入網站人員之身分確認與紀錄，卻有其必要性，尤其針對重要資料存取之網頁，應特別管制，以避免未經授權人員或有心者，可輕易獲取相關情資。

根據 BS7799 資訊管理原則及 2003 年洪隆泰等人提出金流平台之資訊安全管理探討—以 C 計畫參與銀行為例[14]，對於網際網路及電子商務之資訊安全，可歸納出有下列幾項共同特點：

(一)運用各式認證技術

使用者與廠商建構之網站間，必須相互確認雙方身分，一般使用方式為動態密碼(One Time Password，OTP) 或公開金鑰憑證技術，甚者，利用生物特徵辨識(如：指紋、虹膜等)方法進入系統[15]-[16]，其目的在於避免身分遭竊取、偽冒，達到唯一性與不可否認性。

(二)增加加密位元長度

隨著資訊科技的快速發展，各項資訊軟、硬體設備效能亦相對提升，使得利用電腦犯罪之破壞者或駭客，更容易獲取性能較佳之設備及運用便利之軟體工具，從事違法行為。所以，必須提升加密位元之長度，才能增加解密之困難。例如，我們所熟知的 RSA 加密技術[17，18]其金鑰長度從 512 位元，增加到不得小於 1024 位元。

(三)強化個人保密觀念

除了加密技術的精進改良外，實際上，一般洩密最大之原因在於人為疏失，目前社會上，詐騙案件層出不窮，上從達官顯貴、高等知識份子；下至販夫走卒、一般百姓，都有被詐騙之情事發生，他們利用人性的弱點，不斷翻新的詐騙技術，騙取受害者，以獲不法利益。在國防單位，也有為了金錢利益，竊取重要軍事機密或資料販賣，如過去曾發生某軍事情報單位軍官，受金錢誘惑，

竊取單位機密資料，提供中共參考，最後，終被查獲，身敗名裂。所以，應加強個人保密教育與法制觀念，進以提升自制能力與自我要求之紀律，防止軍機洩漏[19，20]。

綜觀上述三點而言，第二、三項為規則訂定及個人觀念教育問題，因此，本文將就第一項『運用各式認證技術』，延續前文一次密碼驗證之智慧卡 (A Secure One-Time Password Authentication Scheme Using Smart Cards)並結合認證中心(Certificate Authority) 機制，提出一改良系統架構，加以探討並導入國軍網站身分認證，此架構可分為下列三個階段：1.註冊階段 2.登入階段 3.驗證階段。主要針對伺服器 S 與認證中心 CA 之部分說明，伺服器 S 與使用者 U 之間認證程序及各項參數說明同前文。

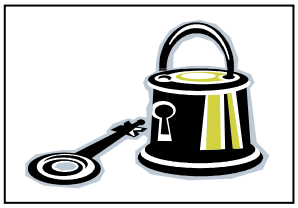
1.註冊階段

S 於首先產生與和 CA 之一共享秘密大型隨機亂數 SEED，並且經由秘密通道傳輸至 U 和 CA，S 與 CA 將 SEED 儲存於自身資料庫中，而 U 則儲存於智慧卡中，接著由 U 計算 $P_0=H^N(K\oplus SEED)$且傳送至 S 儲存後，再由 S 傳送至 CA 資料庫中儲存。此階段簡易步驟概述如下圖四：

伺服器 Server

1. S產生一隨機亂數SEED,經由安全通道傳送至U和CA。
2.S 與 CA 分別儲存此一隨機亂數 SEED。

安全通道



認證中心 CA

圖四　認證中心註冊階段

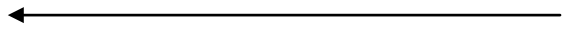
2.登入階段

當 U 第 t 次登入 S 時，待 S 接收 U 之登入請求，S 隨即產生隨機數值 D_t 與 R_t，另當 U 將相關數值計算完畢且回傳 S 後，S 將 $P_{t-1}\oplus P_tR_t\oplus SEED$ 及 $R_t\oplus SEED$ 傳送至 CA 中心。CA 中心運用 SEED 計算 $R_t\oplus SEED$ 可得知 R_t，再運用 $P_{t-1}=P_0$ 計算 $P_{t-1}\oplus P_tR_t\oplus SEED$ 亦可獲得 P_t，此階段簡易步驟概述如下圖五：

伺服器 Server

步驟一：

1. U 第 t 次登入 S，S 接收 U 之登入請求。
2.S 產生隨機數值 D_t 與 R_t。



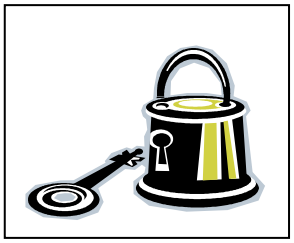
一般通道

使用者 User

伺服器 Server

步驟二：

1. S 計算 $P_{t-1}\oplus P_tR_t\oplus$SEED 及 $R_t\oplus$ SEED 傳送至 CA 中心。
2. CA 利用 SEED 計算獲得 R_t。
3. CA 利用 P_{t-1} 與 R_t 計算獲得 P_t。



認證中心 CA

一般通道

圖五　認證中心登入階段步驟

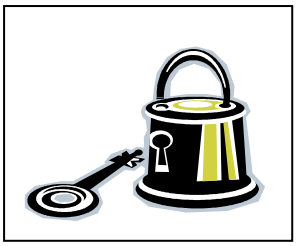
3.驗證階段

CA 利用雜湊函式計算 P_t 後便可獲得 P_{t-1}，對照 S 所傳送之 P_{t-1}，可確認是否為 S 所發出之訊息，接著 CA 將訊息 $P_{t-1}\oplus H(R_t)\oplus$SEED 回傳給 S，S 可運用 SEED 與 P_{t-1} 計算出 $H(R_t)$，以確認是否為 CA 所發出之訊息，且 S 紀錄所有之驗證值 P_t 及登入次數 C，此階段簡易步驟概述如下圖六：

伺服器 Server

步驟一：

1. CA 利用雜湊函式計算 P_t 後，便可獲得 P_{t-1}。
2. 比對 S 所傳送之 P_{t-1}，以驗認是否為 S 所發出之訊息。

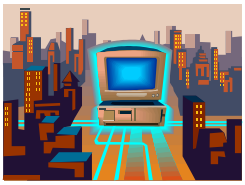


認證中心 CA

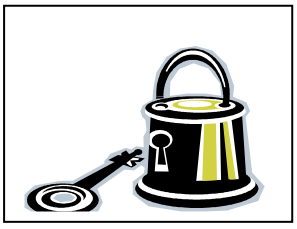
一般通道

步驟二：

1. CA 將訊息 $P_{t-1}\oplus H(R_t)\oplus$SEED 值回傳給 S。
2. S 運用 SEED 與 P_{t-1} 計算出 $H(R_t)$，以驗證是否為 CA 所發出之訊息。
3. S 紀錄所有之驗證值 P_t 及登入次數 C。



伺服器 Server



認證中心 CA

一般通道

圖六　認證中心認證階段步驟

二、系統架構分析

在原系統架構下，使用一次密碼鑑別機制，藉由雙方之挑戰訊息及回應訊息，達採雙方認證之目的，可防範下列攻擊：

(一)伺服器偽冒攻擊

在註冊階段，S 經由安全通道，傳送 SEED 值，藉由此值運算 S 能夠被認證，在登入階段時，則透過 SEED 及 P_{t-1} 被使用者 U 認證，故攻擊者無法在註冊階段重複攔截，偽冒伺服器通過認證。

(二)重複攻擊

由於 U 每次登入， S 每次均產生不同之隨機數，亦產生不同之密碼，攻擊者無法偽裝及預測下一次 KEY 值，即使竊取一次 KEY 值，重複傳送該筆資料，也無法通過 S 之認證。

(三)離線字典攻擊

一般通行碼鑑別機制，主要之秘密在於使用者之 KEY 值，通常使用者選擇較簡單熟悉之密碼(如：個人出生年月日、電話號碼、身分證字號等)，以便記憶，攻擊者能夠利用使用者各種可能之秘密推測發現其正確之密碼，但在此系統架構下，由 S 產生一大型隨機亂數，用以保護使用者之密碼，且攻擊者同時獲得 K 及 SEED 值，非常困難，故可避免離線字典攻擊。

雖然，一次密碼驗證之安全機制，可防範上述伺服器偽冒等方式攻擊，但仍有遭受竊取驗證攻擊(Stolen-Verifier Attack)[4]之可能性，因此，對一次密碼驗證技術，產生安全威脅。

所謂竊取驗證攻擊，是有心者透過偽冒手段，竊取網路線上交易使用者之驗證值，進而猜測出使用者之密碼，獲取相關重要資料或不法利益，以下介紹竊取驗證攻擊法之步驟。

竊取驗證攻擊法：假設使用者 U 完成第 t 次登入，破壞之第三者則竊取每一個或開始使用之 P_i，且 $1 \leqq i \leqq t$。而破壞者利用 P_i，可從擷取之 $P_i \oplus D_i$ 獲得 D_i，再利用 D_i，從擷取之 $SEED \oplus D_i$ 獲得 SEED。另外，由於 $P_i=H^{Ci}(K \oplus SEED)$，所以，破壞者透過 SEED 與 P_i 可猜測密碼 PW'及推算出符合之密鑰 K'，再計算 $P_i'=H^{Ci}(K' \oplus SEED)$。假使計算後之 P_i'同等於竊取之 P_i 值，則破壞者亦可推導出密鑰 K=(K')，即表示可以正確猜測出 U 之 PW=(PW')。

於是破壞者即可輕易產生 P_j，此時 $t+1 \leqq j \leqq N$，經由使用 K 和 SEED，可偽冒模擬 U 登入 S，或偽冒 S 與 U 交談，欺騙 U，然而破壞者已知 SEED，且 $1 \leqq k \leqq N$，可從驗證訊息之傳送或從 U 第 k 次一開始於登入階段步驟二之傳送，這兩個項目中推算獲取時序密鑰 D_k，由此即可破解 Yeh 等人所提一次密碼驗證機制。

因此，在本文所提出之改良架構下，除可避免上述原系統之各項攻擊行為外，還能抵抗竊取驗證攻擊，此系統架構，主要是增加認證中心及查驗所有記錄，現就此二項利弊得失分析如後：

(一)增加認證中心

利用上述架構，在註冊階段時，S 產生一秘密之大型隨機亂數值 SEED，此數值由 S 以秘密通道分別傳送給 U 及 CA 共享，隨後，於登入階段時，S 另新產生一隨數值 R_t，原有 D_t 數值利用於 S 與 U 之間運算，而新產生之 R_t 數值則僅運用於 S 與 CA 之間運算，使 S 與 U 及 S 與 CA 間，雙方各自相互驗證，U 與 CA 彼此之間無直接交互關係。

此舉最主要之目的有二項，第一為藉由第三者驗證中心，提升系統架構之公正性與確認性，當使用者身分被偽冒或遭竊取時，S 透過 CA 中介驗證，以查驗確定其身分，此為三方認證，較雙方認證更加嚴謹。其二為增加系統架構之安全性，因於登入階段除沿用原有之 SEED 及 D_t 數值外，並額外新產生一隨機亂數值 R_t，使 S 與 U 所運用之參數值與 S 與 CA 所利用之參數值不同，且 S 與 CA 間，可以 SSL 加密方式之機制傳輸，不易為有心者所竊取，所以，必須同時截獲此二項參數值，再使用竊取驗證攻擊法才可能破解。

(二)查驗所有紀錄

當完成驗證階段時，原系統架構為 S 將會更新資料庫 P_t 及 C 之數值，在本文所提之改良的方法架構中，資料庫將不予以更新，而是將每次登入紀錄全部儲存，並在驗證時，須逐一比對所有紀錄。

此法目的為增加系統資料完整性，由於資料庫內紀錄所有之驗證值 P_t 及登入次數 C，使得有心第三者須蒐集所有驗證紀錄，才可能實施攻擊與破壞。

雖然，此系統架構可有效防範上述各項攻擊，但也產生下列缺點：

1.預算成本之增加：由於增加認證中心，相對就必需增加設施裝備，不但增加預算成本外，還需要消耗人力處理及負責維護軟、硬體等相關事宜。

2.降低系統之效能：基於系統架構新增了 CA，所以增加了系統的複雜性，並且需要驗證所有記錄，除必須耗用記憶體資料儲存空間及增加系統計算能力外，還必須增加網路流量，可能會導致降低了系統之效能，因此，同意登錄之次數宜有所限制，並建議針對存取或閱覽重要資料之網站，採取實施此法管控。

綜合前列所述，比較原有及改良後之系統架構，整理出表一。

表一　原有系統與改良後系統架構比較表

比較項目	原有系統架構			改良後系統架構		
	低	中	高	低	中	高
安全性		V				V
確認性		V				V
公正性	V	—			—	V
系統效能		—	V	V	—	
系統複雜度	V	—			—	V
預算成本	V	—			—	V

（註解：1.安全性－係指資料訊息於傳遞過程中，遭到竊取及破解之難易程度，低代表易遭到破解；中代表尚可；高代表不易遭到破解。2.確認性－係指 S 與 U 間身份之確認程度，低代表無法確認；中表可確認；高代表確認性良好，不易遭受偽冒。3.公正性－係表示 U 與 S 產生糾紛時，藉由第三認證中心，判別真相，低表示不具公正性；高表示較具公正性。4.系統效能－係指系統處理雙方身份驗證時之運算效果能力，低代表消耗較多系統資源處理；高代表消耗較少系統資源。5.系統複雜度－係指系統變更原有架構後，造成實際建構系統上之困難複雜程度，低表示建構程度較易；高表示建構較困難。6.預算成本－係表示系統架構不同，所需之預算成本，低表示耗用成本較低；高表示消耗成本較高。7.—－表示無，空欄位。）

伍、導入國軍網站身分認證之應用

國軍近年來，利用資訊設施，處理公務執行作業，已經變成不可或缺之工具設備，如果資訊設備故障、網路不通，許多事務即無法迅速完善處理，甚至停擺，由此對資訊設備之依賴可見一斑。也因資訊化作業，既迅速又便利，且資料處理量龐大，若稍不謹慎小心，即有安全洩密之虞，其損失與破壞更甚於一般。

另外，由於科技不斷進步，加之儲存媒體製程技術日益精進，體積越做越小，記憶容量卻越來越大，如大家所熟知之隨身硬碟或大拇哥等裝備，輕薄短小，攜帶方便，透過 USB 介面，即可輕易下載大量資訊，故肇生洩密案件時有所聞，嚴重影響國防安全及國軍形象，所以，資通安全是國軍當前持續重點工作之一。

資通安全，主要在保護儲存在記憶媒體之資料及運用網路或其他方式傳送

資訊時之安全，以達到所謂資料保密性(Data Confidentiality)資料完整性（Data Integrity）、身分鑑別性(Authentication)及不可否認性(Nonrepudiation)等幾項目標特性，為求資通安全，大致可分為下列三點措施：

一、使用者之認證

利用一般通行密碼、IC 卡、SSO、OTP 及生物特徵等方式，鑑別使用者身分。惟各單位資訊化日趨普遍，網站及網域增加速度如雨後春筍般，從政戰、人事、情報、作戰、後勤、資通到其他相關服務應用系統，每登入一個網站可能就要一個帳號密碼，且介面整合不易，對任何一個單位而言，無論在作業上、管理上都十分困難，此種困擾稱為網路藤蔓症(Web Sprawl)[21]，造成一般常見現象就是如前文所述將帳號密碼紀錄於便條紙上，張貼於電腦螢幕旁，或是登入所有網站均採用同一帳號密碼，亦或者將所有人帳號密碼，統一交付一個幕僚保管，如此說來，密碼即是明碼，毫無秘密可言，所以，需選擇一個適當的認證方法與技術，以利人員身分認證，保護資料的安全。

二、資訊存取控制

資料存取控制是單位資料存取的安全政策制定，用以規範單位資料合法人員的存取，避免非法人員進入，如人事單位人員只能合法存取與其職務相關之網頁資料，不可隨意登入存取作戰部門之資料；另外，應設定相關人員權限，不同職務層級不同，權限設定也不相同，如主官(管)使用權限即高於一般幕僚參謀權限。

三、紀錄稽核追蹤

除了事前的身分認證鑑別，作業中的存取控制外，還應特別注意追蹤並紀錄保留事件訊息或存取紀錄，一旦發生不尋常或非法之資料存取事件，可供事後查詢紀錄或即時提供身份線索，協助追查犯罪，俾利事後系統安全漏洞之防堵及相關政策檢討調整。

以上所述措施，除第二點資訊存取控制，屬於政策訂定之外，在此，我們可利用本文所提一次密碼驗證智慧卡技術結合 CA 之機制，應用於國軍網站身分之認證，達到使用者之認證及記錄稽核追蹤之目的。舉例說明，針對儲存重要情資、人事、演習資料、兵力駐地等相關機敏資料之網頁，僅開放相關人員瀏覽，並核發相關人員智慧卡。而 CA 及 S，則建置於總部(或司令部機房)，使用者完成首次註冊後，爾後每次需進入網頁存取資料時，先發出個人鑑別需求，經由 S 及 U 雙方認證通過後，始得登入存取，且每次都由 S 產生不同密碼，加以認證授權。

U 每次登入時，發出個人識別名稱鑑別需求，S 傳回每筆挑戰訊息(challenge)

與「一次性驗證值」，U 處理程序便依據回覆之鑑別秘密計算鑑別秘密雜湊函數值，並以此鑑別秘密函數值加密挑戰訊息以作為回應訊息(response)，如回應訊息之衍生值與「一次性驗證值」相符，可確認回覆鑑別秘密的正確性，也證明 U 輸入正確之通行碼。相對而言，唯有 U 所註冊之 S 才可提出正確之「一次性驗證值」，若回應訊息與「一次性驗證值」不相符，則可懷疑該挑戰訊息與「一次性驗證值」來自偽冒的 S，也就是無法通過此一雙方認證機制。另外，U 每次登入，S 均與 CA 產生另一認證紀錄，以作為公正第三者之查驗，因此，不易為有心之破壞者所攻擊，也不會因智慧卡遺失而造成立即洩密之顧慮。假若資料遭竊也可由 S 之完整紀錄追查可能登入存取之使用者，可有效提昇人員認證、資料存取之安全。

陸、國軍導入此技術之效益分析

一次密碼驗證技術如導入國軍網站身分認證，可為國軍帶來幾項效益，分述如下：

一、降低資料外洩風險

在國軍強調資訊化、數位化的同時，隨著科技一日千里的發展，各單位個人電腦的普及化、資通網路結構的精進以及國軍網際網路的快速成長，使得資訊傳播與應用無遠弗界。甚至基層營、連級單位都使用資訊設施，每日都有大量官兵在國軍廣域網路或單位區域網路上執行各項作業，存取各種資料，而這些資訊有些是儲存在南、北二地不同單位的電腦上。雖然大部分的士官兵使用者都是合法地存取資料，但仍有非法入侵與存取其它電腦中資料的情事發生，尤其，對岸不斷發展訊息戰，我們應隨保持警戒與機動，防範其資訊戰之入侵攻擊。

當然，除了來自外部的攻擊外，內部人員也有入侵系統的可能，此種情況最易被忽略與不注意，這些攻擊大部分想從中獲得利益，也可能只是發洩個人的不滿或是惡作劇以造成組織運作的紛亂，但卻可能促使資訊系統架構或組織內部的重大傷害。

而資料之存取，首先在於人員之認證，本技術提供一個安全的認證方式，藉由每次進入網站存取資料時，產生不同之密碼辨證合法人員，避免非相關及不合法人員進入系統，獲取資料，並記錄存取人員身分，以備查驗，可以有效降低資料外洩之風險，提高系統之安全性。

二、具有長期投資效益

在國防預算日益緊縮的今日，比起面對龐大國外軍售動輒千億預算之沉重

壓力相較下，花費不多之預算，建構使用本機制作業，但卻能帶來保障國軍資訊系統安全，可謂物美價廉。並且利用本技術智慧卡可以結合其他軟體介面，將單位營區內門禁管制、上下班打卡紀錄，乃至圖書館書籍借閱，統一整合運用，使其發揮最大之效能，故就預算成本角度來看，可算是極佳之投資報酬，具長期投資效益。

三、減少官兵作業負擔

由於國軍各單位都有發展不同之資訊應用系統，每當進入不同的網站或系統時，就可能需要不同之密碼，許多士官兵或幕僚人員，可能記憶多組帳號密碼，甚者，以筆記本、電腦紀錄不同之帳號密碼或如前文所述將多組密碼張貼於電腦螢幕旁，故使用之密碼越多，就越易遺忘不常使用之系統密碼或是彼此混淆，且稍有不慎，也越容易造成帳號密碼洩漏，遭非法人員竊取使用，存取相關資料。

因此，使用一次密碼驗證技術，對使用者(士官兵)而言，可以不用記憶多組密碼，避免密碼洩漏或遺忘，減少士官兵作業負擔，並促進資訊安全；對系統管理人員而言，可大量減少因使用者忘記密碼，無法進入系統所造成過多人為疏失之處置作業，系統管理人員可專心致力於系統維護調校工作或處理突發狀況，有效提高系統管理人員之作業效能。

柒、結論

資訊科技越發達，使用越便利，人們對他們就越依賴，然而，便利性與安全性往往是背道而馳，現今，國軍正朝向資訊化發展，相對而言，資通安全的正確觀念與紀律，也應不斷提升與要求，如何在精進相關技術下，既可達到其便利性，又能獲得其安全性，並取得二者間之平衡與協調，是我們努力的方向與目標。

本文所提出之一次密碼驗證智慧卡結合認證中心機制加密技術，為加強 Yeh 等人所述改良式之一次密碼驗證安全機制之安全性，可防範 Ku 等人所提之竊取驗證攻擊(Stolen-Verifier Attack)法，並藉以導入國軍重要網站身分之認證，避免以往將密碼隨意張貼明顯處或僅使用一組密碼進入所有系統，能降低資料外洩之風險，增加身分認證之可靠性與安全度。除此之外，在未來研究方向上，我們將朝向如何精進加密技術，降低成本及網路通聯流量，以提升整體效能等方面持續努力。

註釋

1.L. Lamport, “Password Authentication with Insecure Communication,” Commun. ACM, vol.24, N0.11, pp.770-772, 1981.
2.N. Haller, “The S/Key(TM) One-Time Password System,” Proc. Internet Society Symposium on Network and Distributed System Security, pp.151-158, 1994.
3.T. C. Yeh, H. Y. Shen, and J. J. Hwang, “A Secure One-Time Password Authentication Scheme Using Smart Cards ,” IEICE Trans. Commun. ,vol.E85-B, no.11, pp.2515-2518, Nov. 2002.
4.W. C. Ku, H. C. Tsai, and M. J. Tsaur, “Stolen-Verifier Attack on an Efficient Smartcard-Based One-Time Password Authentication Scheme ,” IEICE Trans. Commun. , vol.E87-B, no.8, pp.2374-2376, Aug. 2004.
5.N. M. Haller, “A One-Time Password System ,” RFC 1938, May 1996.
6.N. M. Haller, “On Internet Authentication,” RFC 1704, Oct. 1994.
7.N. M. Haller, “The S/Key One-Time Password System,” RFC 1760, Feb. 1995.
8.C. L. Lin, H. M. Sun and T. Hwang, “Attacks and Solutions on Strong-Password Authentication,” IEICE Trans. Commun. , vol.E84-B, no.9, pp.2622-2627, Sept. 2001.
9.C. M. Chen and W. C. Ku, “Stolen-Verifier Attack on Two New Strong-Password Authentication Protocols,” IEICE Trans. Commun. , vol.E85-B, no.11, pp.2519-2521, Nov. 2002.
10.William Stallings 著，巫坤品，王青青譯，「密碼學與網路與網路安全－原理與實務」第三版，碁峰資訊股份有限公司發行，pp.291-300，2005。
11.http://moica.nat.gov.tw/html/index.htm.
12.Gunter Ollmann, “The Phishing Guide Understanding & Preventing Phishing Attacks ,” NGS Software Insight Security Research, September 2003.
13.黃麗芳等，「利用 ElGamal 演算法防範虛假網站安全機制之研究」，國立台北大學資訊管理學系研討會，2005。
14.洪隆泰，耿慶瑞，「金流平台之資訊安全管理探討—以 C 計畫參與銀行為例」，國立台北科技大學商業自動化與管理研究所碩士論文，2003。
15.http://www.aotusoft.net/tech/jishu_2.htm.
16.http://www.sinobiometrics.com/chinese/iris.htm.
17.Wang, G. , Bao, F. , Zhou, J. , Deng, R. H, Comments on“A practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem," Knowledge and Data Engineering, IEEE Transactions, vol. 16, pp.1309-1311, 2004.

18.Yuuki TOMOEDA, Hideyuki MIYAKE, Atsushi SHIMBO and Shinichi KAWAMURA, “An SPA-Based Extension of Schindler's Timing Attack against RSA Using CRT,” IEICE, vol.E88-A, no.1, pp.147-153, Jan. 2005.
19.http://times.hinet.net/SpecialTopic/940622-card/2172819.htm.
20.http://www.ettoday.com/2005/07/07/10846-1813806.htm.
21.http://www.speechfriendly.org/cgi-local/nyt.cgi/http://www.ebizq.net/news/4086.html