增強簽入過程安全性之研究
The Study of Improving the Login Security

孫宏民* 林文彥** 詹智強**
Hung-Min Sun Wen-Yen Lin Chu-Chai Chan

*朝陽科技大學資訊管理研究所
Department of Information Management
Chaoyang University of Technology
Email: hmsun@mail.cyut.edu.tw

**朝陽科技大學工業管理研究所
Department of Industrial Engineering and Management
Chaoyang University of Technology
Email:ccchan@mail.cyut.edu.tw
s8515606@mail.cyut.edu.tw

摘要

為了保護電腦系統的資源，在現行電腦簽入的程序(Login Procedure)中，是以輸入使用者身份(Username)與密碼(Password)來防止非法者入侵系統以取得使用權。使用者身份為一公開之資訊，而密碼可能被偷看、竊取或被猜中，非法者只要輸入了正確的密碼，就可以順利入侵系統。本論文之目的，希望在不增加使用者負擔的前題下，藉由將現行的簽入程序中之身份驗證方式作一修改，以提昇電腦系統的安全度。

關鍵字: 電腦安全、簽入程序、密碼

Abstract

Login procedures are usually used to protect the resource of computer systems from illegal use. However, the password may be seen, stolen, or guessed. Once the illegal user gets the correct password, he can login and use the system resource unlimitedly. In this paper, we develop a user authentication mechanism to improve the login security.

Keywords: Computer Security, Login Procedure, Password

1. 簡介

在現行電腦中，使用簽入程序來辨識合法者，防制非法者是最常見的防護措施[9]。簽入的程序，是以輸入使用者身份與密碼來防止非法者入侵系統以取得使用權，使用者身份為一公開之資訊，而密碼則可能被偷看、竊取或被猜中，非法者只要輸入了正確的密碼，就可以順利入侵系統。

This research was supported by the National Science Council, Taiwan under grant number NSC-86-2213-E-324-002..

Dehnad [4]於 1989 年提出改善系統簽入程序安全性之研究。在現行的簽入系統中，當使用者輸入錯誤密碼時，系統會拒絕使用者進入系統，此一過程恰好給入侵者一個提示: 輸入的密碼並非正確的密碼，使得非法者依此提示，並使用試誤法(Trial and Error)去破解合法使用者的密碼。 Dehnad 為了克服此一問題，將入侵者入侵失敗的次數作為進入系統的依據之一，使進入系統的機會會隨著入侵失敗次數的增加而變小，在文獻中並以入侵者成功入侵系統所需的次數之期望值來證明 Dehnad 的方法優於傳統簽入系統的方法。

在另一方面，使用個人敲鍵特徵來辨識使用者的合法性，是另一方面的研究主題[1-3,5-8,10]。系統首先將合法者個人所輸入的使用者名稱與密碼的特徵—包括按鍵時間及按鍵延遲時間等—儲存在資料庫中，作為系統辨識使用者的依據。除非使用者身份、密碼以及特徵皆相同，否則無法取得系統使用權。

本論文的研究目的是整合 Dehnad 的方法與個人敲鍵特徵辨識法，並提出新的簽入程序以增加系統簽入程序的安全性。本文亦將分析新設計的方法之有效性，所以，我們將使用者區分為合法使用者與非法入侵者，非法入侵者又區分成已知密碼及未知密碼兩個狀況。根據這些情況，來評估各方法欲獲得系統使用權所需之簽入次數之期望值，藉此來比較本論文所提出之方法與文獻方法之間的優缺點。

2. Dehnad's Method

在傳統的簽入程序中，入侵者先前入侵系統的失敗次數並不會影響到此次進入系統的與否(僅與此次密碼是否正確有關)，因此入侵者只要輸入的使用名稱與密碼吻合，系統仍然允許使用者進入系統。 Dehnad [4]在 1989 年提出改善簽入系統的安全性之方法，以防止入侵者利用試誤法的方式來測試找出正確密碼以進入系統。 Dehnad 將入侵者入侵失敗的次數作為進入系統的依據，也就是說，入侵者只要前次輸入錯誤的密碼而被拒絕進入系統，那麼即使此次密碼是正確

的，其進入系統的機會並不會為 1 。我們以下列討論來分析 Dehnad 的理念，並將文獻中對個案的公式做推導導出通式：

傳統的簽入系統:

使用權取得條件:密碼正確則允許進入系統。

假設入侵者以隨機方式選取可能之密碼(選過不重覆)

S：所有可能之密碼空間,

$\frac{1}{|S|}$：入侵者第 i 次猜，猜中正確密碼的機率(事前機率),

ε：入侵者成功入侵系統所需的入侵次數的期望值,

$$\varepsilon=\sum_{i=1}^{s}\frac{i}{|S|}=\frac{|S|+1}{2}$$

合法者成功進入系統所需次數的期望值為: 1 。

Dehnad 的簽入方法:

使用權取得條件: 密碼正確未必被允許進入系統，須視之前輸入狀況而定，不同的狀況被允許進入系統之機率亦不同，機率值之大小如下所述。

q_0： 當首次進入或已知前次密碼已為正確但未獲進入之情況下,本次密碼亦正確時，使用者被允許進入系統的機率(例如 q_0=0.95)。

q_1： 當前次密碼不正確，但本次密碼正確時，使用者被允許進入系統的機率(例如 q_1=0.5)。

假設入侵者成功入侵系統所需的入侵次數的期望值以 ε 表示，假設僅有三組可能的密碼 S=$\{S_0,S_1,S_2\}$,且 q_0=0.95, q_1=0.5 。試想入侵者在測試密碼 S_0 時失敗，那麼他將會測試 S_1，如果又失敗將會測試 S_2，假設又失敗那他將又再測試 S_0，一再的循環測試，直到成功進入系統為止，此種方法稱為試誤法。

$$\varepsilon=1/3\left\{0.95+0.05\cdot\sum_{i=1}^{\infty}(0.5)^i\cdot(1+3i)+\sum_{i=0}^{\infty}(0.5)^{i+1}(2+3i)\right.$$

$$\left.+\sum_{i=1}^{\infty}(0.5)^i(3i)\right\}=4.1$$

在傳統的簽入方式 ε 為: $\varepsilon=\frac{|3|+1}{2}=2$,

由上可知，當|S|=3，q_0=0.95，q_1=0.5 時，使用 Dehnad 的方法較傳統簽入方式之防禦能力為佳， Dehnad 的方法下，入侵者成功入侵系統所需的入侵次數之期望值為傳統簽入方式之 2.05 倍。在此我們將 Dehnad 的公式推廣成有 k+1 種可能的密碼狀況。設密碼空間為 S = $\{s_0,s_1,s_2,.....s_k\}$ ，共有 k+1 種的密碼變化，設 $|S|=n=k+1$,

$$\varepsilon=\{q_0\times1+q_1\times2+q_1\times3+q_1\times4+...+q_1\times n+$$
$$(1-q_0)\times q_1\times(n+1)+(1-q_1)\times q_1\times(n+2)+..$$
$$..+(1-q_1)\times q_1\times2n+....\}\ /\ n$$
$$=\left\{q_0+\frac{1}{2}\cdot(n-1)\cdot[(n+2)+2\cdot n\cdot\frac{1-q_1}{q_1}]\right.$$
$$\left.+(1-q_0)\cdot[(n+1)+n\cdot\frac{1-q_1}{q_1}]\right\}/n$$

而合法者成功進入系統所需次數的期望值則為: $\frac{1}{q_0}$ 。

必須注意的是：q_1 太小會造成合法者的負擔，因有時候合法者可能不小心打錯密碼之後，下一次密碼縱使對而能獲得使用權之機率變得相對很小。

3. 敲鍵特徵辨識系統

敲鍵特徵辨識系統的觀念首先由 Gaines[5]提出，該報告利用實驗研究探討以敲鍵特徵鑑定身份之可能性。之後陸續又有許多學者提出相關之實驗與研究論點[1-3,6-8,10]。此類系統乃根據個人使用密碼時的敲鑑時間長短與敲鍵之延遲時間來鑑定身份；簡單來說所謂的敲鍵時間的長短即是按下單一密碼到放開所經過的時間；敲鍵延遲時間即是於相鄰兩密碼間所花的時間，利用此來當成允許進入系統之特徵參考依據。文獻[1-2]主要的研究目的是發展出一套良好的鑑定方法，使系統能依所收集到的特徵資料進行精確的辨識。關於鑑定能力是以 FAR(False Alarm Rate:錯誤拒絕率；系統拒絕給予合法者系統的使用權之比率)與 IPR(Imposter Pass Rate:錯誤接收率；系統給予非法者系統使用權之比率)兩個數值來評判鍵定能力的好壞。

當某一鑑定方法所獲得的 FAR 與 IPR 的值皆較其他方法為低時，表示此一鑑定方法有良好的鑑定能力可以成功的拒絕大部份的非法使用者，而且不會給合法者帶來太大的負擔: 需重新簽入的機率不大。關於測量鑑定方法是以資料庫中所收集到的合法者資料（以 R 集合表之）與使用者此時所輸入密碼所獲得的特徵值（以 T 集合表之）作一比對；換句話說即是判斷 R 與 T 的距離是否很接近，愈接近愈能確定此一使用者為合法使用者。而多接近才算接近呢?這完全取決於門檻值 (Threshold Value) 的大小。當所定的門檻值越大表示使用者輸入的特徵須與資料庫中的特徵越相似，相反則異。因此，門檻值的定訂也會影響 FAR 與 IPR 兩值。

經文獻研究的數據顯示[2]，最佳的鍵定方法所獲得的 FAR 與 IPR 如表一：

FAR	0.04	0.06	0.08	0.10	0.12	0.20	0.30
IPR	0.076	0.063	0.054	0.049	0.045	0.037	0.016

表一、最佳鍵定方法之 FAR 與 IPR

在此方法下，合法者成功進入系統所需次數的期望值則為: $\frac{1}{1-FAR}$ ，非法者若已知密碼，他能成功入侵系統所需次數的期望值則為: $\frac{1}{IPR}$ ，非法者若不知密碼，並假設他以試誤法來猜密碼，則他能成功入侵系統所需次數的期望值則為:

$$\left\{IPR+\frac{1}{2}\cdot(n-1)\cdot[(n+2)+2\cdot n\cdot\frac{1-IPR}{IPR}]\right.$$

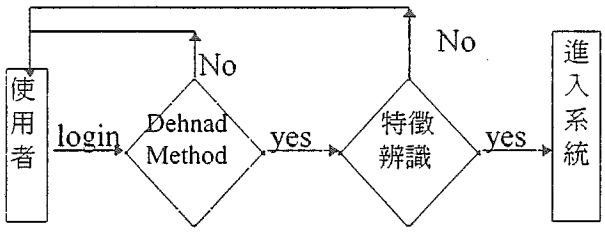
$+(1-IPR)\cdot[(n+1)+n\cdot\frac{1-IPR}{IPR}]\Big\}/n$ ，n 為密碼總數。

4. 增強簽入過程安全性之研究方法

本論文結合上述兩種方法另外發展出新的簽入過程以加強系統的安全性。在本論文中，我們共提出了四種方法，分別討論於後：

研究方法(一):

首先以 Dehnad 的方法[4]為第一道防護措失，其次以特徵辨識法[1-2]為第二道防護措失。其進行程序如下：



圖一、研究方法(一)

合法使用者:

假設當使用者已知密碼之情況下所被系統接受的機率為 q_0，當使用者通過第一防護措施後，第二道防護措施啟動，使用者鍵入的資料將被收集並與資料庫的特徵值作比對，以辨識使用者的真偽。假設 α 為第二道防護措施中合法者被拒絕進入系統的機率(即是 FAR)。

假設 $p(i)$ 為第 i 次才進入系統的機率 ，i=1…∞，則

$p(1)=q_0\cdot(1-\alpha)$, $(2)=(1-q_0\cdot(1-\alpha))\cdot q_0(1-\alpha)$, ...,

$p(k)=(1-q_0\cdot(1-\alpha))^{k-1}\cdot q_0(1-\alpha)$

期望值為 $\varepsilon'=\frac{1}{q_0(1-\alpha)}$

非法使用者:

Case I: 已知密碼者

假設第一道進入的機率為 q_0，第二道進入系統的機率為 β (即為非法者進入系統的成功機率 IPR)。假設 $p(i)$:為第 i 次進入系統之機率,i=1…∞,

$p(1)=q_0\cdot\beta$;

$p(2)=(1-q_0\beta)\cdot q_0\beta$,$p(k)=(1-q_0\beta)^{k-1}\cdot q_0\beta$

期望值為 $\varepsilon'=\frac{1}{q_0\beta}$

Case II: 未知密碼者

進入第一道系統的機率分別為 q_0 (當使用者首次輸入密碼或前次所輸入密碼為正確，且本次輸入密碼亦正確)；q_1 (當使用者本次輸入的密碼正確但前次輸入密碼錯誤之情況下)，第二道進入系統的機率為 β (即非法者進入系統的成功的機率 IPR)，|S|=n,期望值為: $\varepsilon''=\Big\{q_0\beta+\frac{1}{2}(n-1)\cdot[(n+2)+2\cdot n\cdot\frac{1-q_1\beta}{q_1\beta}]+(1-q_0\beta)\cdot[(n+1)+n\cdot\frac{1-q_1\beta}{q_1\beta}\Big\}/n$

研究方法(二)

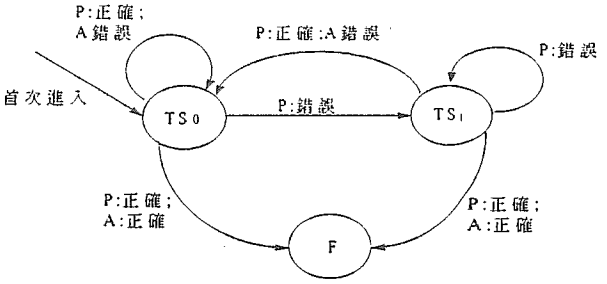
此方法結合 Dehnad 的觀念於特徵辨識系統。其進行程序如下：系統設定了三個狀態，根據目前狀態，使用者被允許進入系統之機率亦不同，這些狀態及相對之機率值敘述如下:

State TS_0 :(起始狀態)在此狀態下，系統以較寬鬆之門檻值(以 TV_0 代表)來判斷輸入之資料是否為合法使用者(輸入之密碼正確時才作判斷)。當輸入之密碼錯誤時，則將狀態轉移至 TS_1，當輸入之密碼正確，但未過門檻值，將狀態停留在 TS_0，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F。

State TS_1 :在此狀態下，系統以較嚴謹之門檻值(以 TV_1 代表)來判斷輸入之資料是否為合法使用者(輸入之密碼正確時才作判斷)。當輸入之密碼錯誤時，則狀態停留在 TS_1，當輸入之密碼正確，但未過門檻值，將狀態轉移至 TS_0，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F。

State F: (終結狀態)到達此狀態時，系統即給予使用權。

圖解如下：(P:表示密碼;A:表示密碼特徵)



圖二、研究方法(二)

合法使用者:

對合法使用者而言，只會停留在 State TS_0 及 State F 中。在 State TS_0 中獲得使用權(跳至 State F)之機率為 1-FAR_0，其中 FAR_0 為合法者在 TV_0 下之錯誤拒絕率。使 $\alpha_0=FAR_0$。則其期望值為 $\varepsilon'=\frac{1}{1-\alpha_0}$

非法使用者:

Case I:已知密碼

對已知密碼之非法使用者而言，亦只會停留在 State TS_0 及 State F 中。在 State TS_0 中獲得使用權(跳至 State F)之機率為 IPR_0，其中 IPR_0 為非法者在 TV_0

下之錯誤接受率。使 $\beta_0 = \text{IPR}_0$ 。

其期望值為 $\varepsilon' = \frac{1}{\beta_0}$

Case II:未知密碼

使用者未知密碼，並以試誤法順序嘗試所有可能之密碼。當所有密碼的變化總數為一集合 $S=\{S_0, S_1, S_2, \ldots\ldots S_k\}$。對未知密碼之非法使用者而言，若其猜中密碼，在 State TS_0 中獲得使用權(跳至 State F)之機率為 IPR_0，在 State TS_1 中獲得使用權(跳至 State F)之機率為 IPR_1，其中 IPR_0 及 IPR_1 分別為非法者在 TV_0 及 TV_1 之錯誤接受率。使 $\beta_0 = \text{IPR}_0$ ，$\beta_1 = \text{IPR}_1$ 。$|S| = n$, 期望值

$$\varepsilon'' = \left\{ \beta_0 + \frac{1}{2} \cdot [(n+2)\cdot(n-1) + 2(n-1)\cdot n \cdot \frac{1-\beta_1}{\beta_1}] + (1-\beta_0)\cdot[(n+1) + n\cdot\frac{1-\beta_1}{\beta_1}] \right\} / n$$

研究方法(三)

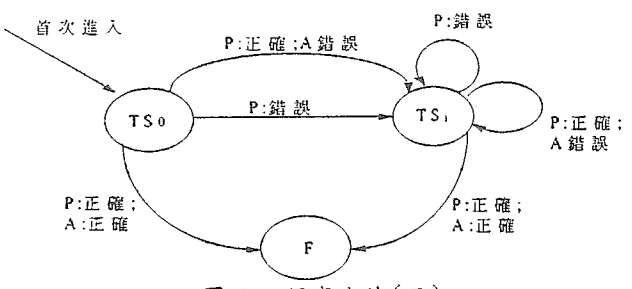
此方法為方法(二)的變化，所不同的是本方法修正了系統各狀態之間的移轉情況。系統設定了三個狀態，根據目前狀態，使用者被允許進入系統之機率亦不同，這些狀態及相對之機率值敘述如下:

State TS_0 : (起始狀態)在此狀態下，系統以較寬鬆之門檻值(以 TV_0 代表)來判斷輸入之資料是否為合法使用者(輸入之密碼正確時才作判斷)。當輸入之密碼錯誤時，則將狀態轉移至 TS_1 ，當輸入之密碼正確，但判斷為非法者，亦將狀態轉移至 TS_1 ，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F 。

State TS_1 :在此狀態下，系統以較嚴謹之門檻值(以 TV_1 代表)來判斷輸入之資料是否為合法使用者(輸入之密碼正確時才作判斷)。當輸入之密碼錯誤時，則狀態停留在 TS_1 ，當輸入之密碼正確，但判斷為非法者，亦將狀態停留在 TS_1 ，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F 。

State F: (終結狀態)到達此狀態，系統即給予使用權。

圖解如下:(P:表輸入的密碼;A:表密碼的特徵值)



圖三、研究方法(三)

合法使用者:

對合法使用者而言，在 State TS_0 中獲得使用權(跳至 State F)之機率為 1-FAR_0 ，在 State TS_1 中獲得使用權(跳至 State F)之機率為 1-FAR_1 ，其中 FAR_0 及 FAR_1 分別為合法者在 TV_0 及 TV_1 之錯誤拒絕率。使 $\alpha_0 = \text{FAR}_0$ ，$\alpha_1 = \text{FAR}_1$ 。$p(1) = 1-\alpha_0$，$p(2) = \alpha_0\cdot(1-\alpha_1)$, $p(k) = \alpha_0\cdot\alpha_1^k\cdot(1-\alpha_1)$, ➡期望值為 $\varepsilon' = \frac{\alpha_0 + (1-\alpha_1)}{1-\alpha_1}$

非法使用者:

Case I: 已知密碼

對已知密碼之非法使用者而言，在 State TS_0 中獲得使用權(跳至 State F)之機率為 IPR_0 ，在 State TS_1 中獲得使用權(跳至 State F)之機率為 IPR_1 ，其中 IPR_0 及 IPR_1 分別為非法者在 TV_0 及 TV_1 之錯誤接受率。使 $\beta_0 = \text{IPR}_0$ ，$\beta_1 = \text{IPR}_1$ 。$p(1) = \beta_0$，$p(2) = (1-\beta_0)\cdot\beta_1, \ldots, p(k) = (1-\beta_0)(1-\beta_1)^k\cdot\beta_1$ ➡期望值為 $\varepsilon' = \frac{(1-\beta_0)+\beta_1}{\beta_1}$

Case II: 未知密碼

使用者未知密碼，並以試誤法順序嘗試所有可能之密碼。當所有密碼的變化總數為一集合 $S=\{s_0, s_1, s_2, \ldots\ldots s_k\}$。對未知密碼之非法使用者而言，若其猜中密碼，在 State TS_0 中獲得使用權(跳至 State F)之機率為 IPR_0，在 State TS_1 中獲得使用權(跳至 State F)之機率為 IPR_1，其中 IPR_0 及 IPR_1 分別為非法者在 TV_0 及 TV_1 之錯誤接受率。使 $\beta_0 = \text{IPR}_0$ ，$\beta_1 = \text{IPR}_1$ 。$|S| = n$,期望值

$$\varepsilon'' = \left\{ \beta_0 + \frac{1}{2} \cdot [(n+2)\cdot(n-1) + 2(n-1)\cdot n \cdot \frac{1-\beta_1}{\beta_1}] + (1-\beta_0)\cdot[(n+1) + n\cdot\frac{1-\beta_1}{\beta_1}] \right\} / n$$

研究方法(四)

此研究方法是將方法(三)的方法再推廣，系統設定了四個狀態，根據目前狀態，使用者被允許進入系統之機率亦不同，這些狀態及相對之機率值敘述如下:

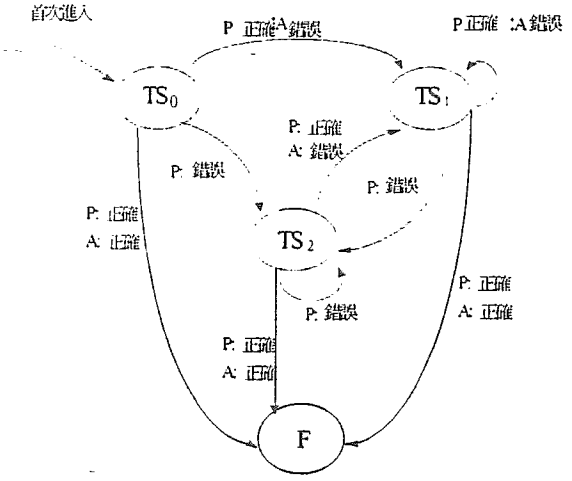
State TS_0 : (起始狀態)在此狀態下，系統以較寬鬆之門檻值(以 TV_0 代表)來判斷輸入之資料是否為合法使用者(輸入之密碼正確時才作判斷)。當輸入之密碼錯誤時，則將狀態轉移至 TS_2 ，當輸入之密碼正確，但判斷為非時，則將狀態轉移至 TS_1 ，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F 。

State TS_1:在此狀態下，系統以較嚴謹之門檻值(以 TV_1 代表)來判斷輸入之資料是否為合法使用者(輸入之密碼正確時才作判斷)。當輸入之密碼錯誤時，則狀態轉移至 TS_2，當輸入之密碼正確，但判斷為非時，將狀態停留在 TS_1，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F。

State TS_2:在此狀態下，系統以最嚴謹之門檻值(以 TV_2 代表)來判斷輸入之資料是否為合法使用者。當輸入之密碼錯誤時，則狀態停留在 TS_2，當輸入之密碼正確，但判斷為非時，將狀態轉移至 TS_1，當輸入之密碼正確，且判斷為合法者，將狀態轉移至 F。

State F: (終結狀態)到達此狀態，系統即給予使用權。

其狀態變化狀況如下:(P:表示密碼;A:表示密碼特徵)



圖四、研究方法(四)

<u>合法使用者:</u>

合法使用者在正常的狀況下並不會跳到 State TS_2。對合法使用者而言，在 State TS_0 中獲得使用權(跳至 State F)之機率為 $1\text{-}FAR_0$，在 State TS_1 中獲得使用權(跳至 State F)之機率為 $1\text{-}FAR_1$，其中 FAR_0 及 FAR_1 分別為合法者在 TV_0 及 TV_1 之錯誤拒絕率。使 $\alpha_0 = FAR_0$，$\alpha_1 = FAR_1$。假設 $p(i)$ 為第 i 次才進入系統的機率，$i=1\ldots\infty$，$p(1)=1-\alpha_0$，$p(2)=\alpha_0\cdot(1-\alpha_1)$，...，

$p(k)=\alpha_0\cdot\alpha_1^k\cdot(1-\alpha_1)$ ➡期望值為 $\varepsilon'=\dfrac{\alpha_0+(1-\alpha_1)}{1-\alpha_1}$

<u>非法使用者:</u>

Case I:已知密碼者

對已知密碼之非法使用者而言，在 State TS_0 中獲得使用權(跳至 State F)之機率為 IPR_0，在 State TS_1 中獲得使用權(跳至 State F)之機率為 IPR_1，其中 IPR_0 及 IPR_1 分別為非法者在 TV_0 及 TV_1 之錯誤接受率。使 $\beta_0 = IPR_0$，$\beta_1 = IPR_1$。假設 $p(i)$ 在第 i 次才進入系統的機率，$i=1\ldots\infty$。$p(1)=\beta_0$，$p(2)=(1-\beta_0)\cdot\beta_1$，...，

$p(k)=(1-\beta_0)(1-\beta_1)^k\cdot\beta_1$ ➡期望值為 $\varepsilon'=\dfrac{(1-\beta_0)+\beta_1}{\beta_1}$

Case II:未知密碼者

使用者未知密碼，並以試誤法順序嘗試所有可能之密碼。當所有密碼的變化總數為一集合 $S=\{s_0,s_1,s_2,\ldots\ldots s_k\}$。對未知密碼之非法使用者而言，若其猜中密碼，在 State TS_0 中獲得使用權(跳至 State F)之機率為 IPR_0，在 State TS_1 中獲得使用權(跳至 State F)之機率為 IPR_1，在 State TS_2 中獲得使用權(跳至 State F)之機率為 IPR_2，其中 IPR_0、IPR_1 及 IPR_2 分別為非法者在 TV_0、TV_1 及 TV_2 之錯誤接受率。由於利用試誤法(相鄰兩次猜測之密碼必不相同)來猜測密碼，能夠獲得使用權之情況必定是由 State TS_0 跳至 State F(第一次就猜中且特徵亦超過門檻 TV_0)或是由 State TS_2 跳至 State F(第二次以上才猜中)。因此，使 $\beta_0 = IPR_0$，$\beta_1 = IPR_2$。$|S|=n$，期望值為

$$\varepsilon''=\left\{\beta_0+\frac{1}{2}\cdot\cdot[(n+2)\cdot(n-1)+2(n-1)\cdot n\cdot\frac{1-\beta_2}{\beta_2}]+(1-\beta_0)\cdot[(n+1)+n\cdot\frac{1-\beta_2}{\beta_2}]\right\}\Big/ n$$

5.實例比較

關於比較的方法，本研究是以入侵者成功入侵系統所需的入侵次數的期望值來辨認防禦能力的好壞；也就是說期望值的次數越多表示其防禦能力越強，此外，在比較時應有同一基礎才有意義，所以我們控制讓合法者成功進入系統所需次數的期望值相近且不大於二次，以免造成使用者之負擔。由於合法者成功進入系統所需次數的期望值，是基於假設合法者不會敲錯他的密碼之狀況下來評估的。然而有時候合法者會發生打字錯誤的現象，為了不增加合法使用者的負擔，我們期望打字錯誤事件發生之後，合法者再簽入一次，仍有很高的機率能進入，這亦是我們所要控制的因子之一。

在第三節中，我們介紹了個人敲鍵特徵辨識系統的目的是要發展出一套良好的鑑定方法使系統能精確的區分出合法者與非法者，所以本研究取最佳鑑方法[2]的 FAR 與 IPR 來進行實例驗證，經由文獻的實

驗證明(如表一)，根據不同的門檻值，我們可取 FAR_0=0.04、FAR_1=0.06、FAR_2=0.08；IPR分別為 IPR_0=0.076、IPR_1=0.063與IPR_2=0.054。我們分別以密碼總數為3及密碼總數為1000為例子來比較各方法的效益，分別表列於表二及表三，其中備註欄為合法者發生打字錯誤的現象之後，再簽入一次而能夠獲得使用權之機率。

	合法者	非法者		參數	備註
		已知密碼	未知密碼		
現行方法	1	1	2		1
Dehnad	1.04	1.04	2.22	q_0=0.96、q_1=0.92	0.92
特徵辨識	1.04	13.16	38.47	FAR=0.04, IPR=0.076	0.96
方法一	1.04	13.16	39.26	q_0=1、q_1=0.98 FAR=0.04, IPR=0.076	0.94
方法二	1.04	13.16	46.41	FAR_0=0.04, IPR_0=0.076 FAR_1=0.06, IPR_1=0.063	0.94
方法三	1.04	15.67	46.41	FAR_0=0.04, IPR_0=0.076 FAR_1=0.06, IPR_1=0.063	0.94
方法四	1.04	15.67	54.15	FAR_0=0.04, IPR_0=0.076 FAR_1=0.06, IPR_1=0.063 FAR_2=0.08, IPR_2=0.054	0.92

表二、密碼總數為3時，各方法所需嘗試之期望值

	合法者	非法者		參數	備註
		已知密碼	未知密碼		
現行方法	1	1	500.5		1
Dehnad	1.04	1.04	587.41	q_0=0.96、q_1=0.92	0.92
特徵辨識	1.04	13.16	12658.39	FAR=0.04, IPR=0.076	0.96
方法一	1.04	13.16	12926.90	q_0=1、q_1=0.98 FAR=0.04, IPR=0.076	0.94
方法二	1.04	13.16	15373.31	FAR_0=0.04, IPR_0=0.076 FAR_1=0.06, IPR_1=0.063	0.94
方法三	1.04	15.67	15373.31	FAR_0=0.04, IPR_0=0.076 FAR_1=0.06, IPR_1=0.063	0.94
方法四	1.04	15.67	18018.61	FAR_0=0.04, IPR_0=0.076 FAR_1=0.06, IPR_1=0.063 FAR_2=0.08, IPR_2=0.054	0.92

表三、密碼總數為1000時，各方法所需嘗試之期望值

由表中，我們可以發現，方法四能提供較好的防禦力。這些方法皆不會因為密碼總數的增加而造成合法者成功進入系統所需次數的期望值之變化，所以不會帶給合法使用者多大的負擔，由於簽入的方式與現有之方法一樣(僅輸入使用者名稱與密碼)，不同處僅在於系統內部如何決定使用權之取得與否，從使用者的眼光來看，並不會發現有何差異，因此，這些方法適合實際應用在現今之系統上，而不需要額外的硬體支援。

6.結論

本論文整合了兩種不同的增進簽入程序安全性之方法，並提出了四種新的方法以改善簽入程序之安全性，期能在不增加合法使用者負擔下，使非法入侵者更難入侵系統。由數據分析顯示，這些方法皆有不錯的效益，而且也易於應用在實際系統中。

參考文獻

[1] 蘇雅惠，敲鍵特徵個人識別法，國立交通大學資訊管理研究所碩士論文，1992。

[2] 孫宏民，基於個人敲鍵特徵之使用者辨識與系統辨識的設計與製作，國科會專題研究計畫報告書，NSC-86-2213-E-324-002，1997。

[3] Bleha, S., Slivinsky, C., and Hussien, B., "Computer-Access Seurity Systems Using Keystroke Dynamics," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 12, No. 12, pp. 1217-1222, 1990.

[4] Dehnad, K, "A Simple Way of Improving the Login Security." Computers & Security, 7(8) , 607-611, 1989.

[5] Gaines, R., Lisowski, W., Press, S., and Shapro, N., "Authentication by Keystroke Timing: Some Preliminary Results," Rand Report R-2526-NSF. Rand Corporation, Santa Monica, CA, 1980.

[6] Garcia, J., "Personal Identification Apparatus," Patent Number 4,621,334. U. S. Patent and Tradement Office, Washington, D. C., 1986.

[7] Joyce, R., and Guta, G., "Identity Authentication Based on Keystroke latencies," *Communication of ACM*, Vol. 33, No. 2, pp. 168-176, 1990.

[8] Leggett, J., and Williams, G., "Verifying Identity via Keyboard Characteristics," *International Journal of Man-Machine Studies*, Vol. 28, No. 1, pp. 67-76, 1988.

[9] Pfleeger, C. P., *Security in Computing, Reading*, Prentice-Hall, 1989.

[10] Umphress, D., and Williams, G., "Identity Verification through Keyboard Characteristics," *International Journal of Man-Machine Studies*, Vol. 23, No. 3, pp. 263-273, 1985.