使用智慧卡與指紋及以身分碼為基礎的通行碼鑑別機制之安全分析

李明政 (Ming-Jheng Li)　　阮夙姿* (Justie Su-tzu Juan)
國立暨南國際大學資訊工程學系
{s3321908, jsjuan} @ ncnu.edu.tw

摘要

網際網路發展迅速的現今，使用者身份的確認是一個非常重要的議題。而通行碼鑑別機制是用來防止非法使用者進入計算機系統最重要的第一道防線。自 1991 年開始，許多學者將 Shamir 所提出的，以身分碼為基礎之密碼系統的觀念與智慧卡做結合，達到遠端使用者身份確認的安全需求。在 2002 年，一種使用智慧卡之以指紋為基礎的遠端鑑別機制被提出。此法利用智慧卡並結合指紋辨識的技術，使得傳統認卡不認人的觀念，變成既認卡又認人。前述系統在結合 Shamir 所提出的以身份碼為基礎之密碼系統後，於 2003 年，使用智慧卡與指紋及以身分碼為基礎的通行碼鑑別機制隨後被提出，本文中稱其為 Kim-Lee-Yoo 之鑑別機制。此系統分為使用以臨時數為基礎，及以時戳為基礎的兩種機制，皆可抵禦重送攻擊。此外，此鑑別機制宣稱能抵禦偽造攻擊。

本論文主要指出，Kim-Lee-Yoo 之鑑別機制，並無法抵禦偽造攻擊。

關鍵字：以身分碼為基礎之架構 (ID-based scheme)、指紋 (Fingerprint)、通行碼鑑別 (Password authentication)、智慧卡 (Smart card)、偽造攻擊 (Impersonation attack)、密碼系統安全分析 (Cryptanalysis)。

一、緒論

近年來，隨著網際網路的興起，電腦與電腦之間都可以藉由彼此互連於網路，達到資料傳輸與資源共享的目的。使用者只要在家中上網，或是在外透過公眾網路設備，即可與遠端系統做資料傳輸與資源分享。然而，只有合法的使用者，才具有存取遠端系統的權限。因此，在現今分散式電腦網路的環境中，使用者身份之確認是一個非常重要的課題。然而，如何判別合法使用者的身份？遠端通行碼鑑別機制 (Remote Password Authentication System, RPAS) 無疑是最有效，也最常被採用的作法 [21, 22]。使用者在進入系統之前，必須先利用通行碼鑑別 (password authentication) 系統來證明自己是合法使用者。

傳統的遠端通行碼確認系統中，每一位合法的系統使用者均各自擁有專屬的身份碼 (以下簡稱 *ID*)，以及一組只有使用者知道的通行碼 (以下簡稱 *PW*)。當使用者向系統中心註冊後，系統中心會建立並儲存一份通行碼表 (password table)。而檔案所儲存的內容為合法使用者 *ID* 以及相對應的 *PW* 資訊。當使用者 i (以下簡稱 U_i) 欲登入並存取計算機系統的資源時，U_i 必須首先將自己的身份碼 ID_i 以及相對應之通行碼 PW_i 輸入至系統中。系統中心則會比對通行碼表中的 ID_i 以及所對應的 PW_i，核對 U_i 輸入的 (ID_i, PW_i) 是否等於通行碼表中的 (ID_i, PW_i)。若結果為真，則允許 U_i 進入系統，否則拒絕 U_i 的登入與存取。雖然這樣的系統具有簡單且容易實行的優點，但仍有缺點，例如：系統中儲存的通行碼表容易具有安全漏洞。換句話說，一但通行碼表的資料外洩，或是攻擊者入侵電腦竄改通行碼表的內容，則系統的安全性將遭受到非常嚴重的威脅。

1981 年，學者 Lamport 提出一種遠端使用者通行碼確認方法 [10]。雖然 Lamport 的方法具有防範重送攻擊 (replay attacks) 的優點，但由於系統內部仍然必須儲存一份作為驗證用的通行碼表。同樣地，一但通行碼表洩露，或攻擊者入侵系統竄改檔案內容，則系統安全仍將遭受嚴重威脅。在 1984 年，Shamir 首先提出以身分碼為基礎之密碼系統 (ID-based cryptography) [16]。在此系統架構中，將不再需要儲存通行碼表以及不再需要可信賴的第三者 (trusted third party)。自 1991 年開始，許多學者將 Shamir 所提出的以身分碼為基礎之密碼系統的觀念與智慧卡 (smart card) [11, 13] 做結合，達到遠端使用者身份確認的安全需求 [1, 3, 6, 20, 23]。利用以身分碼為基礎之方法結合智慧卡的應用，使得遠端使用者鑑別機制具有多項優點，包括不需做金鑰交換、不需儲存通行碼表這個檔案、不需可信賴的第三者，並可有效防範重送攻擊。

近幾年，以智慧卡為基礎之遠端使用者鑑別機制，大致可分類為利用 RSA [14] 公開金鑰密碼系統為基礎之方法 [20, 23]；和使用 ElGamal [5] 公開金鑰密碼系統為基礎之方法 [7, 12]；以及利用單向雜湊函數 (one-way hash function) 的遠端使用者鑑別機制 [18]。

Lee，Ryn 及 Yoo 三位學者，於 2002 年首先提出一種使用智慧卡之以指紋為基礎的遠端鑑別機制 (a fingerprint-based remote user authentication scheme using smart cards) [12]。此法利用智

* *Correspondence to*: Justie S.-T. Juan; email: jsjuan@csie.ncnu.edu.tw

慧卡並結合指紋辨識的技術，使得傳統認卡不認人的觀念，變成既認卡又認人。就算攻擊者非法取得使用者的通行碼以及智慧卡，若不是卡片的專屬擁有者，仍然無法順利通過遠端系統驗證。近年來，許多相關的研究，也陸續的被提出 [2, 4, 9]。隨後，在 2003 年，Kim，Lee 及 Yoo 三位學者，將 Lee 等人的鑑別機制架構，結合 Shamir 所提出的，以身分碼為基礎之密碼系統，而提出使用智慧卡與指紋及以身分碼為基礎的通行碼鑑別機制 (ID-based password authentication scheme using smart cards and fingerprints) [8]。本文中稱其為 Kim-Lee-Yoo 之鑑別機制。在此系統中，作者又將其系統分為使用以臨時數為基礎 (nonce-based)，和使用以時戳為基礎 (timestamp-based) 的兩種機制，並說明其可抵禦重送攻擊。此外，此系統也宣稱能抵禦偽造攻擊 (impersonation attack)。然而，此鑑別機制卻有安全上的缺失 [15]。

本論文中，有別於 [15] 的攻擊方式，我們將利用重新註冊一個新的 $ID_a = ID_i^k \bmod n$ 以針對 U_i 作偽造攻擊。以此指出 Kim-Lee-Yoo 之鑑別機制並無法抵禦偽造攻擊。類似的攻擊方法曾被成功的使用於其他文獻中 [17]。在下一節中，我們首先回顧 Kim 等人所提出的 Kim-Lee-Yoo 之鑑別機制。緊接著，針對 Kim-Lee-Yoo 之鑑別機制，我們在第三節中提出一個偽造攻擊。由於對於以臨時數為基礎時，此機制之偽造攻擊；與對於以時戳為基礎時，此機制之偽造攻擊的方法相似。因此在第三節中，我們將只針對以時戳為基礎之機制作說明。讀者當可仿此法而推得對於以時戳為基礎時，此機制之偽造攻擊的方法。最後，本論文於第四節提出結論與未來研究方向。

二、Kim-Lee-Yoo 之鑑別機制

在本節中，我們首先將回顧 Kim，Lee 及 Yoo 三位學者所提出的，使用智慧卡與指紋及以身分碼為基礎的通行碼鑑別機制 [8]。在此系統中，又可分為使用以臨時數為基礎，及以時戳為基礎的兩種機制。由於下一節我們只針對以時戳為基礎的機制做分析，因此本節亦只提出以時戳為基礎的 Kim-Lee-Yoo 之鑑別機制。在此鑑別機制的架構中，主要包含三個階段：(1) 註冊階段 (The registration phase)； (2) 登入階段 (The login phase)；以及 (3) 驗證階段 (The verification phase)。下列將簡述 Kim-Lee-Yoo 之鑑別機制：

【參數定義】

在本論文中，所使用到的參數定義，將如下所示：

***S*, U_i**：系統中心以及使用者 i；
***ID*$_i$**：U_i 的身分 (識別) 碼；
***PW*$_i$**：U_i 的私密通行碼；
n：一個質數 (prime)；
g：Z_n 中序 (order) 為 $n-1$ 的元素；
SK*, *PK：系統中心的私密及公開金鑰，$PK = g^{SK} \bmod n$；
***f*(*x*, *y*)**：一個輸入為 x, y 的單向雜湊函數 (one-way hash function)；
T：時間戳記 (timestamp)；
***CID*$_i$**：U_i 的智慧卡編號；
ΔT：系統中心規定之合理的傳送延遲時間差。

【註冊階段】

在此階段中，一個新的使用者 U_i 首先提交他的身份碼 ID_i 以及通行碼 PW_i 給系統中心，並且進行註冊。此註冊階段步驟如下：

1. 一個新的使用者 U_i 首先選擇屬於他的身份碼 ID_i 以及通行碼 PW_i，透過安全通道，傳給系統中心 S，並且進行註冊。
2. 隨後，系統中心產生 U_i 的智慧卡編號 CID_i，並計算：

$$S_i = ID_i^{SK} \bmod n$$
$$h_i = g^{PW_i \cdot SK} \bmod n = PK^{PW_i} \bmod n$$

3. 最後，系統中心儲存 $n, g, f, ID_i, CID_i, S_i, h_i$ 至 U_i 的智慧卡中，並將智慧卡發送給 U_i。U_i 在接收到智慧卡之後，隨即註冊本身的指紋至智慧卡中。

【登入階段】

當使用者 U_i 在時間 T_1 欲登入系統時，首先 U_i 必須將他的智慧卡插入讀卡機中，隨後輸入他的身份碼 ID_i 以及通行碼 PW_i，並輸入指紋。如果指紋輸入鑑別成功，則智慧卡進行下列步驟：

1. 使用輸入指紋的細小座標 (coordinate of minutia)，產生一個隨機亂數 r。在此，由於每次指紋輸入所產生的細小座標皆會不相同。因此當使用者每次登入時，所產生的 r 值也不同，所以我們可把此值看成是一種單次使用的隨機亂數 (one-time random number)。
2. 隨後，智慧卡計算：

$$X_i = g^{r \cdot PW_i} \bmod n$$
$$Y_i = S_i \cdot h_i^{r \cdot f(CID_i, T_1)} \bmod n$$

3. 最後，傳送 $M = \{ID_i, CID_i, X_i, Y_i, T_1\}$ 給遠端系統。

【驗證階段】

當系統中心 S 在時間戳記為 T_2 的時間，接收到使用者的登入要求 $M = \{ID_i, CID_i, X_i, Y_i, T_1\}$ 之後，系統中心透過下列步驟，驗證登入使用者之合法性：

1. 首先，系統中心分別鑑別使用者 U_i 的身份碼 ID_i 以及智慧卡編號 CID_i 的合法性。如果 ID_i 與 CID_i 個別驗證皆正確，則接受登入要求，反之則拒絕。
2. 隨後，系統中心核對登入時間戳記 T_1，如果 $(T_2 - T_1) > \Delta T$ ，則系統拒絕登入要求。
3. 系統中心確認下列方程式：

$$Y_i^{SK^{-1}} = ID_i \cdot X_i^{f(CID_i, T_1)} \bmod n$$

如果正確，則系統中心接受登入要求，反之則拒絕。

4. 最後，使用者在客戶端輸入通行碼 PW_i 至智慧卡，智慧卡隨即計算下列方程式：

$$h_i' = PK^{PW_i} \bmod n$$

並確認下列方程式：

$$h_i = h_i' \bmod n$$

如果正確，則登入系統完成，反之則拒絕。

三、Kim-Lee-Yoo 之鑑別機制的安全分析

在此節中，我們將針對上一節所描述的 Kim-Lee-Yoo 之鑑別機制，作安全性分析且提出偽造攻擊。所謂偽造攻擊，即為許多使用者在未知其他合法使用者的通行碼 PW 之下，模仿其他的合法使用者的身份，且能成功的登入系統。

接下來，我們將說明利用離線 (off-line) 的方式，偽造攻擊 Kim-Lee-Yoo 之鑑別機制。在此，離線的方式即為不需進行插入智慧卡動作的登入階段，而是在遠端自行計算仿造的登入要求 M'，並發送給系統中心 S，直接進行系統中心驗證階段 (驗證階段之步驟 1 至 3)。由於合法使用者 U_i 的身份碼 ID_i 包含在歷次提出的合法登入要求 M 中，因此假定攻擊者 U_a 可在 U_i 發送登入要求 M 時，利用竊聽 (eavesdrop) 的方式，獲知欲攻擊的目標 U_i 之身份碼 ID_i。隨後，即可利用此獲取的身份碼 ID_i 進行偽造攻擊。

假設有一個攻擊者 U_a，在未知合法使用者 U_i 的通行碼 PW_i 之情形下，欲偽裝成 U_i 登入此系統，則可透過下列步驟進行偽造攻擊：

1. 攻擊者 U_a 隨機產生一整數 k，並利用事前所竊聽到的 ID_i，計算屬於 U_a 的身份碼 ID_a：

$$ID_a = ID_i^k \bmod n$$

2. 接下來，攻擊者 U_a 將計算後所得知的 ID_a 對系統中心 S 進行註冊階段 (PW_a 可任意給)，則 U_a 即可獲得系統中心 S 所計算的：

$$S_a = ID_a^{SK} \bmod n$$

由註冊階段 2 可知，$S_i = ID_i^{SK} \bmod n$ ，因此攻擊者 U_a 便可簡單的計算出：

$$S_i = (S_a)^{1/k} \bmod n$$

3. 攻擊者 U_a 在獲知合法使用者 U_i 的 S_i 之後，隨即計算：

$$X_i' = ID_i \bmod n$$
$$Y_i' = S_i \cdot S_i^{f(CID_a, T_1)} \bmod n \qquad (1)$$

4. 最後，攻擊者 U_a 利用遠端離線方式，並未經過登入階段，而直接傳送仿造的登入要求 $M' = \{ID_i, CID_a, X_i', Y_i', T_1\}$ 給系統中心 S，進行系統中心驗證階段。如此一來，攻擊者 U_a 便可透過下列驗證方程式，成功通過驗證階段 3：

$$\begin{aligned}(Y_i')^{SK^{-1}} &= (S_i \cdot S_i^{f(CID_a, T_1)})^{SK^{-1}} \\ &= (ID_i^{SK} \cdot ID_i^{SK \cdot f(CID_a, T_1)})^{SK^{-1}} \\ &= ID_i \cdot ID_i^{f(CID_a, T_1)} \\ &= ID_i \cdot X_i'^{f(CID_a, T_1)} (\bmod n) \qquad (2)\end{aligned}$$

根據上述結果得知，U_a 可成功通過系統中心驗證階段，且成功的模仿合法使用者 U_i 登入系統。由於我們的攻擊是使用遠端離線方式進行攻擊，無需進行驗證階段 4 的通行碼驗證步驟，因此即使未知 U_i 之私密通行碼 PW_i 仍可成功登入系統。此外，由於在 Kim-Lee-Yoo 之鑑別機制中，系統並未儲存任何使用者的身份碼 ID 與智慧卡編號 CID 的相對應關聯資訊。因此，在我們所提出的偽造攻擊步驟 4 中，攻擊者 U_a 只需要將自己的 CID_a 置入仿造的登入要求 M'，即可成功通過系統中心驗證階段。然而，即使系統中心儲存 ID 與 CID 的關聯資訊，我們的攻擊仍然可行。我們只需要在竊聽登入要求 $M = \{ID_i, CID_i, X_i, Y_i, T_1\}$ 的過程中，額外擷取使用者 U_i 的智慧卡編號 CID_i，並將其替換方程式 (1) 中的 CID_a 以便計算出 Y_i'，爾後送出登入要求 $M'' = \{ID_i, CID_i, X_i',$

Y_i', T_1} 即可。如此一來，在驗證階段 3 中之方程式仍可確認正確 (將方程式 (2) 中之 CID_a 以 CID_i 替換即可)。

四、結論與未來研究方向

Kim 等人基於 Lee 等人所提出的使用智慧卡之以指紋為基礎的遠端鑑別機制，並結合 Shamir 所提出的以身分碼為基礎之密碼系統，在 2003 年提出一種新的遠端鑑別機制，稱為使用智慧卡與指紋及以身分碼為基礎的通行碼鑑別機制。此機制利用以臨時數為基礎，及以時戳為基礎的兩種方式，皆可抵禦重送攻擊。此外，此鑑別機制也宣稱，能夠安全的抵禦蓄意攻擊者的偽造攻擊。然而，在本論文的安全分析之下，我們證明 Kim-Lee-Yoo 之鑑別機制，並不如其宣稱的安全。我們透過竊聽的手段，獲取合法使用者 U_i 的身份碼 ID_i 及智慧卡編號 CID_i (若系統中心沒有儲存 ID 與 CID 的關聯資訊，則不需要知道 CID_i)，並依此另行註冊 ID_a，進而換算出 U_i 的 S_i。隨後，將 S_i 利用離線的方式，自行計算出仿造的登入要求 M'，便可成功的通過系統中心驗證階段，達成偽造攻擊。由此可知，Kim-Lee-Yoo 之鑑別機制並無法抵禦偽造攻擊。然此系統之原始創意確有其獨到之處，未來我們將再深入研究，設法修改此鑑別機制，使其確實能達到可抵禦偽造攻擊之目的，並且進一步的更形完備。

參考文獻

[1] C.K. Chan and L.M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, No. 4, 2000, pp. 992-993.

[2] C.K. Chan and L.M. Cheng, "Cryptanalysis of a timestamp-based password authentication scheme," *Computers and Security*, Vol. 21, No. 1, 2002, pp. 74-76.

[3] C.C. Chang and S.J. Hwang, "Using smart cards to authentication remote passwords," *Computer Mathematics with Applications*, Vol. 26, No. 7, 1993, pp. 19-27.

[4] C.C. Chang and I.C. Lin, "Remarks of fingerprint-based remote user authentication scheme using smart cards," *ACM Operating Systems Review*, Vol. 38, No. 3, 2004, pp. 91-96.

[5] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transaction on Information Theory*, Vol. IT-31, No. 4, 1985, pp. 469-472.

[6] T. Hwang, Y. Chen and C.S. Laih, "Non-interactive password authentications without password table," in *Proceedings of IEEE Region 10th Conference on Computer and Communication System*, Hong Kong, 1990, pp. 429-431.

[7] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, No. 1, 2000, pp. 28-30.

[8] H.S. Kim, S.W. Lee and K.Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *ACM Operating Systems Review*, Vol. 37, No. 4 , 2003, pp. 32-41.

[9] W.C. Ku, S.T. Chang and M.H. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards," *Electronics Letters*, Vol. 41, No. 5, 2004, pp. 240-241.

[10] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, Vol. 24, No. 11, 1981, pp. 770-772.

[11] C.C. Lee, M.S. Hwang and W.P. Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, Vol. 36, No. 3, 2002, pp. 46-52.

[12] J.K. Lee, S.R. Ryn and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronics Letters*, Vol. 38, No. 12, 2002, pp. 554-555.

[13] P. Peyret, G. Lisimaque and T.Y. Chua, "Smart cards provide very high security and flexibility in subscribers management," *IEEE Transactions on Consumer Electronics*, Vol. 36, No. 3, 1990, pp. 744-752.

[14] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.

[15] M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," *ACM Operating Systems Review*, Vol. 38, No. 2, 2004, pp. 73-75.

[16] A. Shamir, "Identity-based cryptosystems and signature scheme," in *Proceedings of CRYPTO '84, LNCS 196*, Springer-Verlag, 1986, pp.47-53.

[17] J.J. Shen, C.W. Lin and M.S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, 2003, pp. 414-416.

[18] H.M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, No. 4, 2000, pp. 958-961.

[19] H.M. Sun and H.T. Yeh, "Further cryptanalysis of a password authentication scheme with smart cards," *IEICE Transactions and Communications E86-B*, 2003, pp. 1412-1415.

[20] S.J. Wang and J.F. Chang, "Smart card based secure password authentication scheme," *Computers and Security*, Vol. 15, No. 3, 1996, pp. 231-237.

[21] T. Wu, "The secure remote password protocol," in *Proceedings of the 1998 Internet Society Network and Distributed System Security*

Symposium, 1998, pp. 97-111.
[22] T.C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communications*, Vol. 18, No. 12, 1995, pp. 959-963.
[23] W.H. Yang and S.P. Shieh, "Password authentication schemes with smart cards," *Computers and Security*, Vol. 18, No. 8, 1999, pp. 727-733.