OTP 隨機認證秘密基礎應用於行動網管

邱泰源[1*]、方仁威[2] 、劉興華[3]
[1]中華電信企業客戶分公司、[2]健行科技大學資訊管理學系、[3]聲威網際科技股份有限公司
[1]rick7651@gmail.com、[2]andrewfung60@uch.edu.tw、[3]davidliu@hivocal.com.tw

摘要

近年來手機應用朝向多元發展，涉及資訊安全高度安全性的行動商務模式，諸如：行動 FTP、企業 EIP、行動網路商銀等應用，使用者需要高度安全性的保護。現今，行動上網方式選擇眾多，企業資訊人員使用行動網管的人數正與日倍增，造就行動安全的議題被逐漸關注。目前許多資訊人員將智慧型手機作為行動網管之主要可攜式設備，如：Router、Switch 的管理工具，無論公務出差或是下班時間面臨緊急事務都能即時處理，達到「不在辦公室、也能辦公事」的行動辦公室精神，確實將行動商務徹底實踐。據國際賽門鐵克 Symantec 研究指出，隨著攻擊者手法精進已可透過網路病毒及網頁語法偵測用戶端電腦資訊並藉此竄改網路設備之系統設定檔，將使用者網路連線導向危險區域；藉此顯示網路設備常用的以密碼為基礎之身份認證機制無法有效的防範攻擊者攻擊，為此，改善此一資訊安全風險為刻不容緩的課題。

本研究將藉由建置單次通行密碼系統(OTP)於手機，藉由身份認證雙因子鑑別的核心概念獲得系統合法授權，增強行動網管的安全性以保護網路設備，並改善使用者通行碼遭受病毒攻擊、網路攻擊問題。系統設計以不改變使用者操作為前提，建置採三層式架構方式，兼顧安全控管、獨立運作與擴充性較佳等特性，故本研究可為企業建構行動網管電子商務平台之實作參考。

關鍵詞：單次通行密碼(One-time password)、雙因子鑑別(Two-factor authentication)、三層式架構(Three-tier Architecture)。

* 通訊作者 (Corresponding author.): 邱泰源, rick7651@gmail.com

壹、前言

在現今資訊科技的日益精進下，企業 IT 部門的系統管理人員對於網路設備的管理方式不同以往，最大的差異即是將網路設備的系統設定頁面對外開放，讓系統管理人員不論外出公差、節慶休假等非處於辦公室情況，皆可藉由瀏覽器(Internet Explorer，簡稱 IE)針對該企業網路設備進行系統設定及調校，隨時隨地掌握企業內部網路設備的即時狀態，以達到「不在辦公室，也能辦公事」的行動辦公室精神[8][9]。

然而在享受科技所帶來的便利同時也隱藏著相當的資訊安全風險，根據 Sid Stamm Indiana University & Zulfikar Ramzan Symantec, Inc., (2006)[6]發表的技術文件報告指出，說明攻擊者可輕易透過惡意程式更改使用者網路設備設定，並進一步發展其他形式的攻擊，如：分散式阻斷服務攻擊(Distributed Denial of Service attack，簡稱 DDoS)、病毒(Virus)、身份竊盜(Identity theft)等形式攻擊。使用者只要經由該設備連上一個含有惡意 JavaScript 的陷阱網站，該電腦即可能被設置惡意軟體，攻擊者就能透過 JavaScript 獲得使用者連線資訊進而侵入網路設備，修改該設備的政策(Policy)或是系統設定(Configuration)，將不知情的使用者導向其他釣魚網站。而從報告中追溯攻擊者入侵的癥結點，發現網路設備所採用的使用者身份認證機制明顯不夠健全，令攻擊者能夠藉由此弱點修改系統設定，使其損失慘重。

為了解決上述問題，我們將在智慧型手機上建置一套單次通行密碼(One-time password，簡稱 OTP)安全系統，由內而外保護現行企業內部網路設備；用戶端操作介面將以密碼為基礎，提高使用安全性及便利性；而網路設備部份，以不變更網路設備的系統設計為前提，將 OTP 使用者認證機制以外在保護方式與現有網路設備相互結合，降低資訊安全風險與成本，達到低成本、高安全之目的[4][14]。

貳、文獻探討

現行使用者身份鑑別方法十分多元，例如最常見的以密碼為基礎的認證機制、對稱式密碼學方法、公開金鑰密碼學方法等；而 Furnell et al., (2000)學者[1]提及一般在使用者身份鑑別考量到使用者操作便利性及系統建置與維護成本，多數供應商在使用者身份鑑別都會以密碼為基礎作為身份認證機制。這樣的方式雖然可以提升使用者的便利性及降低供應商系統建置成本，但以密碼為基礎的使用者身份認證機制在安全性考量仍有木馬病毒、鍵盤側錄等資訊安全疑慮。

2.1 以密碼為基礎的認證機制

「使用者身份認證」是檢查欲登入系統的使用者是否可提供正確身份識別過程。現行的使用者認證機制大部份是以使用者「帳號」配合使用者「密碼」的方式共同運行，一般來說，使用者會向系統端註冊一組帳號和密碼做為日後登入系統的身份認證。通

常，帳號是用來識別使用者身份，可能由系統訂定亦可由使用者自行選擇；而密碼則是對應該位使用者之身份鑑別，由使用者自行選擇一連續大/小字串、數字、特殊符號的相互組合，在此稱為「個人化通行碼」；而此方法現今已被普遍運用於各式各樣的資訊系統中。

2.2 應用挑戰與回應的認證機制

前述以密碼為基礎或搭配單向雜湊函數的使用者認證皆屬於弱認證的方法，因系統進行認證每次傳送的訊息皆相同，攻擊者便可利用舊訊息來假冒某位使用者以獲得該使用者的操作權限，此種攻擊方式即是重送攻擊(Replay attack)。而在較安全的使用者認證系統中，將前述的以密碼為基礎的方法做為修改，讓系統於每次身份認證的過程中，用戶端與系統端之間傳輸的認證資訊皆不同；換句話說，也就是每次傳輸的訊息都是唯一(Unique)的，因此重送攻擊便無法得逞。

2.3 單次通行密碼

「單次通行密碼」的發展係從學者 Leslie (1981)發表的“Password Authentication with Insecure Communication”論文[5]，在 1981 年提出至今已逾卅年，其特性是送往系統端進行驗證的通行碼，即 OTP，只限使用一次，而此 OTP 認證碼使用過後立即失效；如此 OTP 認證碼遭受重複使用亦無法獲得系統的存取，藉此保護系統所提供服務之安全性，也保護使用者身份不易因此遭受盜用，其種類如表一所示。

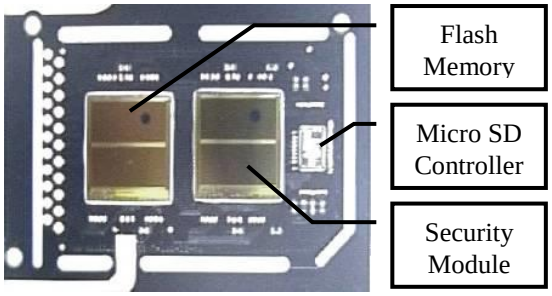
表一：單次通行密碼種類

連線方式	離線式鑑別裝置	連線式鑑別裝置
認證方式	事件基礎 (Event-Based)	挑戰與回應 (Challenge and Response)
	時間基礎 (Time-Based)	

2.4 Micro SD 鑑別裝置

現行大部份挑戰與回應型 OTP 身份鑑別都是透過鑑別裝置的使用即符合「您所知道的」與「您所擁有的」兩項雙因子鑑別條件；於研究中，我們將透過智慧型手機的開發實現「您所擁有的」條件，本研究採用動信科技股份有限公司(Go-Trust)所生產的「SDencrypter Micro SD 記憶卡」作為 OTP 身份認證 Token [10]。此款記憶卡具有如一般 Micro SD 記憶卡一樣的外觀及 4G 的快閃記憶體，容量方面已符合本研究認證秘密及運算函數儲存所需條件；而整個加解密過程完全在 SDencrypter 安全模組中進行，而記憶卡的設計上使用全球國安等級的 Common Criteria EAL 5+認證的高安全性防護儲存於晶片中，儲存的 OTP 認證碼及相關認證秘密不被竊取。此裝置設計內部主要由三個部份組成，可參閱圖一說明，包括快閃記憶體(Flash Memory)、安全模組(Security Module)

及記憶卡控制器(Micro SD Controller)等設計。



圖一：SDencrypter Micro SD 製作示意圖

參、應用於行動網管之使用者認證機制設計

在 2011 年,美國 EMC 公司受到 APT 攻擊,其中,包括該公司 OTP Token 產品 SecurID 的雙因子認證技術資料遭到外洩。本研究將探討此癥結點，引用兩項國際專利及一項延伸專利，改善現行使用者身份認證驗證值遭受揭露的問題。

3.1 可驗證的數位秘密之分割與回復

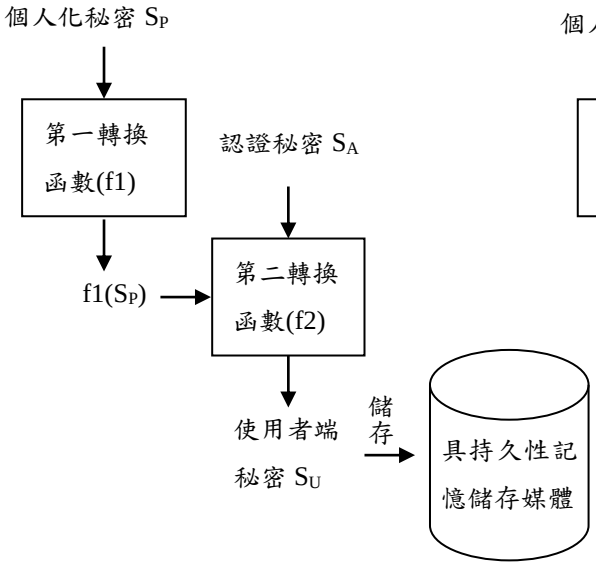
黃景彰學者 2003 年提出「可驗證的數位秘密之分割與回復」的方法，可參見中華民國專利第 I255121 號文件的內容[12]，同為美國專利可參見第 7596704 號之文件[2]，其標題為「Partition and Recovery of a Verifiable Digital Secret」(Jing-Jang Hwang, 2009)。此專利技術特性，為同時安全地保護電腦產生的秘密及個人所選擇之秘密，主要提供用戶端在秘密遺失或被竊的資訊安全風險情況下，依然可保障資料的安全。

3.2 隨機認證秘密基礎專利技術

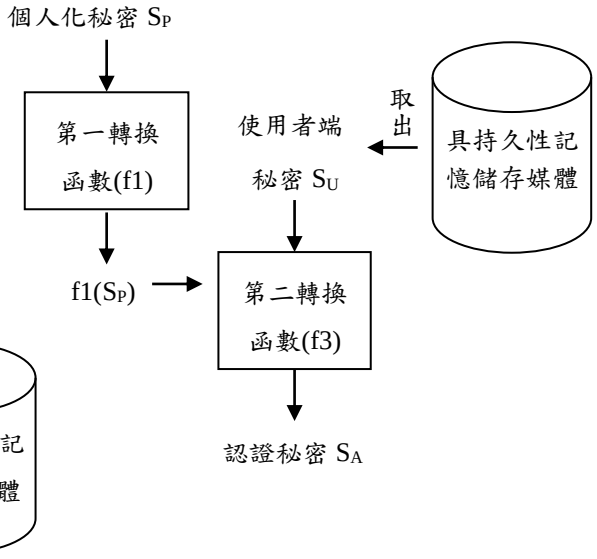
黃景彰學者 2005 年提出「藉由連結隨機產生的認證秘密與個人化秘密的使用者認證方法」為中華民國專利第 I293529 號[13]，同為美國專利公開號可參見 No.2006/0036857 之文件[3]，其標題為「User Authentication by Linking Randomly-Generated Authentication Secret with User-Chosen Secret Password」(Jing-Jang Hwang, 2006)。

在系統中，此方法以一個「強認證秘密」取代傳統挑戰與回應方法中的通行碼，此強認證秘密可以是一個由虛擬亂數產生器所產生的數值，以符號 S_A 表示之。在用戶端中，此方法使用了兩個使用者秘密來取代認證秘密；第一使用者秘密稱為是「個人所選擇之秘密」，以 S_P 表示之，它可以是一個使用者所選擇的密碼或其他使用者之選擇；第二使用者秘密則稱為「用戶端秘密」，以 S_U 表示之，用戶端秘密是經由分割認證秘密 S 之計算所獲得的輸出值，並且存放於持久性記憶體中，如圖二、圖三分別表示了認證秘

密分割與回復的過程。



圖二：認證秘密分割過程



圖三：認證秘密回復過程

3.3 使用者身份認證延伸專利技術

在上述說明完「可驗證秘密基礎專利技術」與「隨機認證秘密基礎專利技術兩種基礎技術」兩項基礎專利技術後，另由許義昌等學者於 2009 年藉此基礎專利技術從中延伸出「利用可重複之第一通行密碼及不重複之第二通行密碼來組合成單次通行密碼的使用者鑑別技術與系統」專利技術[11]，此認證方法為中華民國專利申請案之文件，其公開號為第 201034423 號。

此專利是藉由單次通行密碼的使用者鑑別技術與系統為概念，其中，用戶端登入時輸入個人化通行碼，另一所用到的每一個單次通行密碼皆是一個亂數，而電腦系統端所用到的對應於每一個單次通行密碼之驗證值則是它的一個雜湊值。在此概念中，登入的過程包含一套「同步推移程序」，在產生下一次登入所用到的單次通行密碼及系統端所對應的驗證值之後，才允許使用者登入。此專利除沿襲保有基礎專利的安全性外，延伸專利更有創新的方法使其安全性提升，並且設計更為彈性，使用更為廣泛。

肆、系統設計與實作

本研究依據前面(應用於行動網管之使用者認證機制設計)所述應用於行動網管之使用者認證機制為基礎，並配合文獻探討中闡述現行及傳統的使用者身份認證所面臨之問題做為修整，以此方向在系統建置時將由內而外做全盤的系統分析及設計，增強使用者身份認證以保護網路設備系統設定及企業內部重要資訊，不令網路攻擊者有機可乘，藉此改善現行網路設備之身份認證安全性問題。

4.1 系統發展平台與工具

作業系統：Windows XP

開發平台：Microsoft Mobile 7.0

開發環境：Microsoft Visual Studio 2008

相關技術：Visual C++、MFC

相關設備：參閱表二說明

表二：系統發展相關設備說明

相關裝置/伺服器	用途說明
智慧型手機 (含記憶卡)	用戶端OTP使用者身份鑑別裝置，負責OTP使用者身份認證。
Redirect Server	負責轉址傳遞用戶端與系統端之間的資訊自動轉址的伺服器。
Authentication Server	負責驗證用戶端登入時所傳來的OTP認證，根據OTP認證碼正確與否以決定允許或拒絕使用者之登入。
Router	經由OTP系統認證為合法使用者所登入之網路設備。

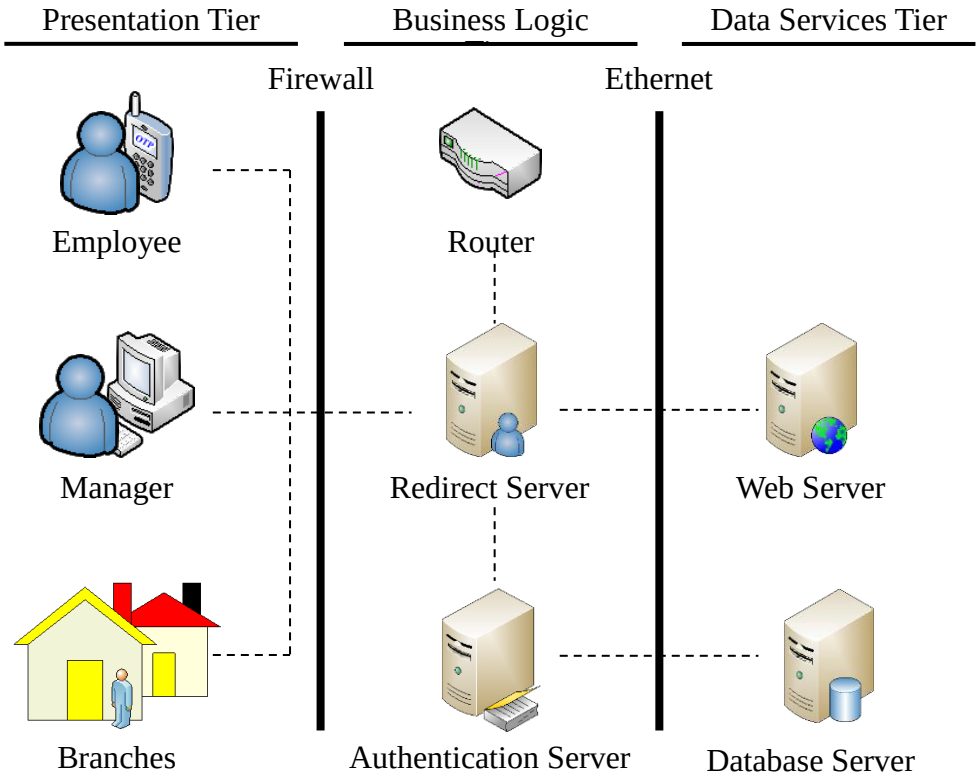
4.2 系統架構圖

本研究系統係以 Voth 等學者於1998年提出的三層式架構(Three-Tier)為設計主軸[7]，詳如圖四所示，根據本研究系統設計需求為主要考量的三項要點如下：

(一) 獨立分工：系統規劃應考慮整個應用系統之工作負荷，由三層式架構下的群組各自負擔，合力完成整個工作，使得各自均有充裕應付之能力。

(二) 安全控管：如果我們需要修改營運規則，於修改完畢後，只需安裝於應用伺服器即可，不需要去修改用戶端程式。

(三) 擴充性佳：鑒於應用系統常隨時間及情勢狀況而有所變動，因此在架構上增減應設計彈性及功能修改。



圖四：OTP 系統三層式網路架構圖

4.3 系統限制

由於本研究所設計之 OTP 系統應用環境包括智慧型手機、網路設備及相關應用伺服器等硬體設備皆有其限制，在智慧型手機部份有二：(1)無線傳輸及電力供給等兩部份，目前智慧型手機的無線傳輸方式選擇眾多，其訊號傳輸之穩定性及速率等相關問題；(2)智慧型手機在使用上亦有電力供給的需求，而電力供給穩定性及其運算效能差異性等問題；就目前上述問題皆非本研究之重點，故在系統實作上將相關問題列入參考，爭酌考量。網路設備部分，目前在網路設備的組態設定呈現上，以網頁方式呈現較為常見，故本研究亦是以網頁方式作為探討；如設備的組態設定是以其他方式呈現，如：命令提示字元、超級終端機等，不列入本研究探討。

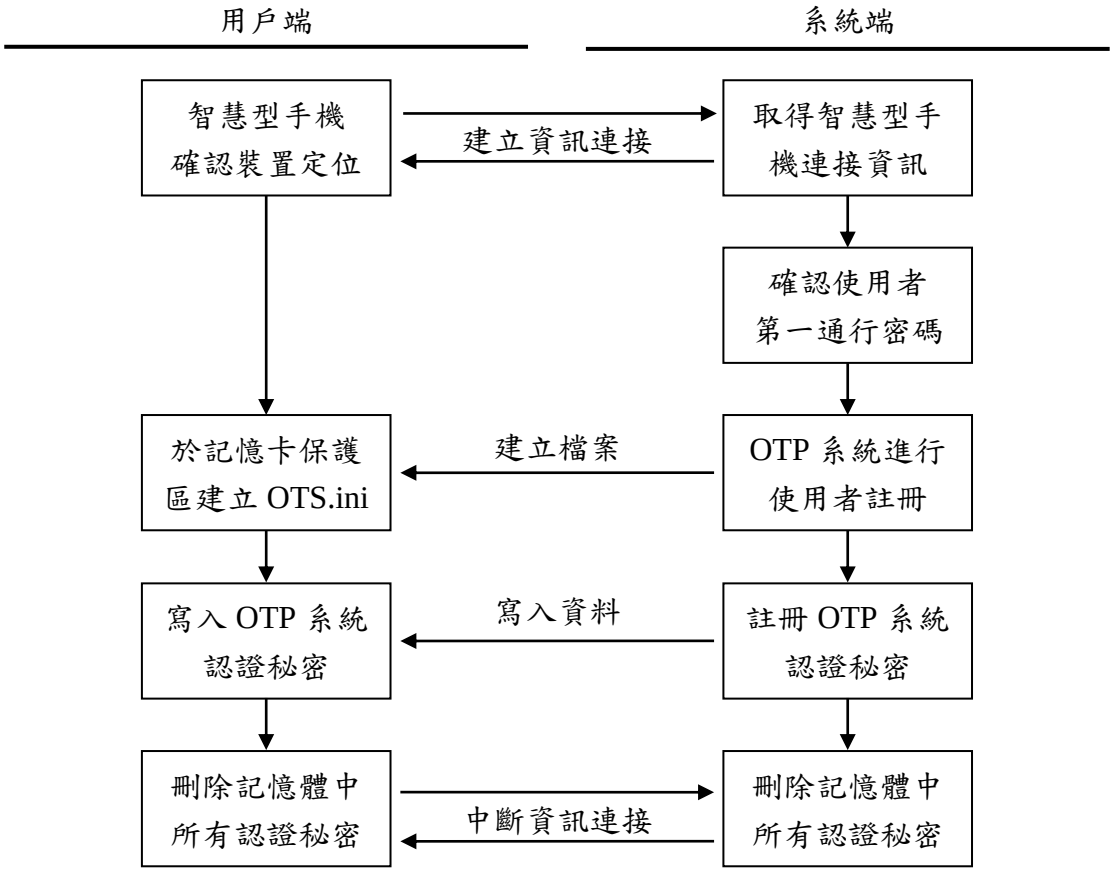
4.4 系統註冊流程

使用者在第一次使用 OTP 系統前，須先交由系統管理員執行註冊動作，以便系統管理員將使用者個人資料及認證資訊寫入於 Micro SD 記憶卡保護區內，以防止認證秘密遭受揭露，系統操作介面如圖五所示。

圖五：OTP 使用者身份註冊

註冊過程主要將「使用者識別名稱」、「系統端識別名稱」、「第二通行密碼」、「用戶端驗證值」等認證秘密寫入 Micro SD 記憶卡保護區內的組態設定檔，防止資料遭受未經授權的竄改，系統註冊流程可詳圖六所示。

系統管理員為使用者進行系統註冊後，將認證秘密寫入 Micro SD 記憶卡保護區 OTS.ini 組態設定檔中，使用者即可將此記憶卡安裝至智慧型手機使用，藉由智慧型手機執行 OTP 系統進行登入，存取 OTP 系統服務。

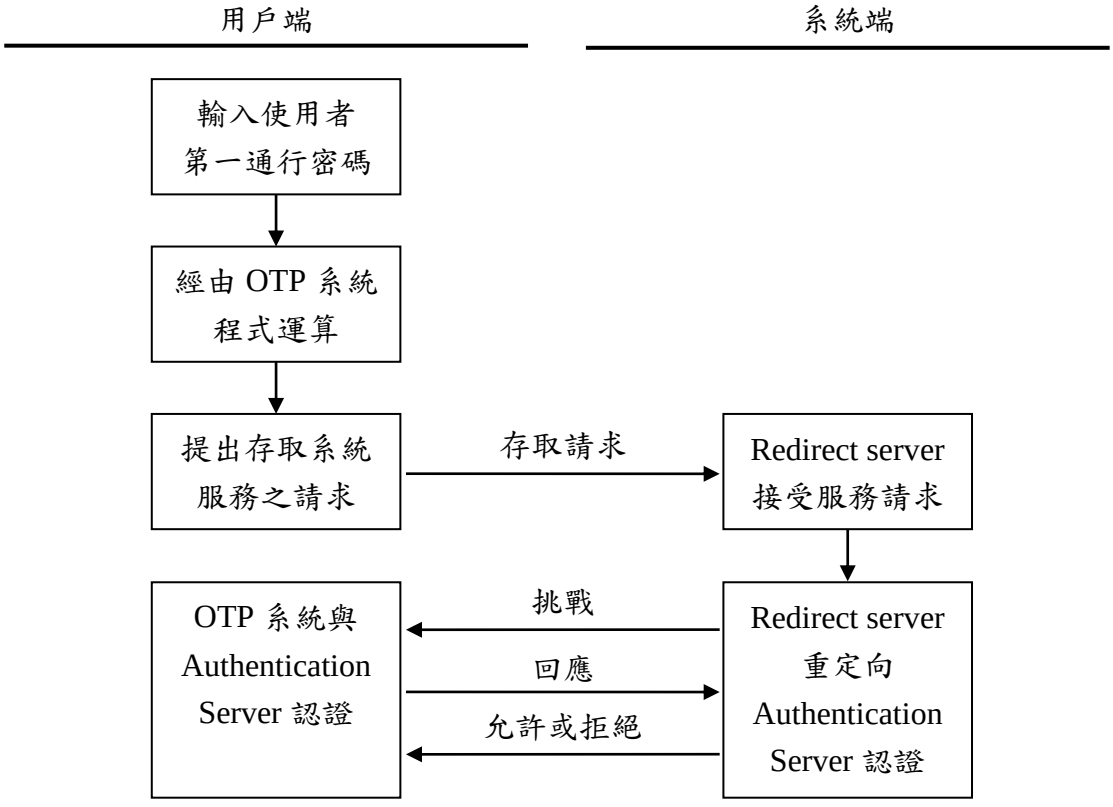


圖六：OTP 系統註冊流程圖

4.5 使用者秘密更新流程

如使用者的需要更改第一通行密碼，則須交由系統管理員處理，因使用者註冊時已將所有認證秘密皆儲存於 Micro SD 記憶卡保護區中，使用者並無法自行開啟記憶卡的保護區，此設計是保護認證秘密資料遭受未經授權竄改，亦是保護資料不會因電腦病毒或其他外在威脅而揭露認證秘密，故使用者無法自行修改系統認證秘密，須交由系統管理員重新註冊動作。

OTP 系統重新註冊會將 Micro SD 記憶卡保護區中所有認證資料重新改寫，上述已說明記憶卡保護區內無法藉由一般系統開啟將資料逐一刪除，所以僅能透過開卡程式將舊有認證秘密相關資訊完全清除，整體驗證流程詳如圖七所示，唯有此方法能夠將保護區內資訊完全清除。即使使用者在一般使用上無意將 Micor SD 記憶卡格式化，亦不影響 Micro SD 記憶卡保護區任何資料，因記憶卡快閃記憶體區域與保護區兩邊是各自獨立的區域。



圖七：驗證伺服器與用戶端進行挑戰與回應流程

4.6 安全分析及效益分析

(一) 安全分析：

本研究實作 OTP 系統並非僅針對使用者身份認證安全性不足問題，係由系統建置開始即分析與規劃，從網路設備安全性至使用者身份認證、用戶端與系統端認證秘密的傳輸防護、可能的第三方監聽及特洛伊木馬等常見資安議題，並從文獻探討中整理如表三所闡述，可分電腦病毒、網路攻擊與人為因素等三類考量範圍，將極力改善 OTP 使用者認證系統可能面臨各項風險，以下將逐一說明：

表三：可改善風險彙整表

分類	可能面臨攻擊	本研究改善方式
電腦病毒	木馬程式 (Trojan horse)	OTP系統設計包含雙因子鑑別概念，即使「您所知道」的部分遭受竊取，攻擊者尚缺少「您所擁有」的部分，仍然無法回復數位秘密部分以進行登入。
	重送攻擊 (Replay attack)	系統設計採用OTP機制，令用戶端每次所發出的認證訊息皆不相同，即使攻擊者進行重送攻擊亦無法登入系統。
	訊息監聽 (Sniffing)	用戶端與系統端所有的認證訊息皆是經由單向雜湊函數傳輸，該函數擁有不可逆推的特性，對此攻擊可有效遏止。
	猜測攻擊 (Guessing attack)	本研究所採用的單向函數雜湊在計算上是具有不可逆的特性，故用戶端驗證資訊若無揭露並不會影響系統安全。
網路攻擊	分散式阻斷服務攻擊 (DDoS)	系統端有三層式系統架構並配合Redirect server加以管制連線，而用戶端部份則有自我驗證模式，雙重系統防護。
	偽裝攻擊 (Impersonation attack)	系統基於雙因子機制，攻擊者頂多擷取資訊並偽裝「您所知道」的部分，並無法模仿「您所擁有」的用戶端秘密，以保護數位秘密。
人為因素	通行密碼揭露 (Password leak)	如使用者意外揭露個人密碼，對於系統而言僅是揭露數位秘密一部份，但攻擊者仍然無法取得裝置中的秘密種子。
	手機遺失 (Lost Phone)	攻擊者無法輕易破解記憶卡裝置所保護的秘密種子，亦無使用者的個人密碼，使用者有充分時間可辦理裝置遺失。

(二) 效益分析：

1、 用戶端效益：

(1) 使用者無需改變登入習慣：使用者進行 OTP 系統操作時與傳統使用者身份認證登入方式相同，依照畫面指示逐一指令即可登入。

(2) 使用者登入無時間、空間限制：系統管理人員可藉由智慧型手機上，工作無需侷限於企業內部或是特定網段下進行管理，可提供極大的便利性。

2、 系統端效益：

(1) 系統對於設備提供完整包容性：OTP 系統是以外在方式在保護網路設備，使其不受外在威脅，無需再與網路設備供應商做交涉，增加企業成本。

(2) 網路設備擴充彈性佳：因應企業發展，新增設備只要安置於商業邏輯層中，並且將網路設備組態設定頁面與 Redirect Server 相互對應即可。

伍、結論

本研究探討、研析現行網路設備所使用之使用者認證方式、系統使用架構及各電信業者所提供傳輸加密模式等，皆是我們所研究並考量之範圍，針對上述所說明現行網路設備情況及現有架構的不足問題將予以改善。

根據討論結果，我們納入使用者需求、系統管理人員及系統實際應用後所提升之安全性做一統整與比較，探討本研究建置的 OTP 系統結果，確實是兼具安全性、便利性、低成本考量的系統實作。本研究亦根據文獻探討中歸納出現行網路設備常見使用鑑別機制，在可接受的成本下，從安全性、使用性、成本效益等三項構面整理於表四，並以下列英文符號分別表示各種鑑別方法[4][14]：

A：應用挑戰與回應的認證機制

B：具單次性通行碼特性的認證機制

C：藉由連結隨機產生的鑑別秘密與個人化秘密的使用者鑑別

D：本論文研究 OTP 使用者認證機制

表四：各種鑑別方法及構面比較表

構面	類別	A	B	C	D
安全性	資料庫遭竊後風險	—	—	—	可以降低
	重送攻擊	可以抵抗	可以抵抗	可以抵抗	可以抵抗
	字典攻擊	據分析後難以抵抗	可以抵抗	可以抵抗	可以抵抗
	木馬攻擊	據分析後難以抵抗	可以抵抗	可以抵抗	可以抵抗
	社交工程攻擊	—	—	可以輔助	可以輔助
	可能的線上攻擊	—	—	可以輔助	可以輔助
使用性	使用者輸入資訊	通行碼及個人識別名稱	通行碼及登入碼	通行碼及系統識別名稱	通行碼及系統識別名稱
	使用者攜帶裝置	無需裝置	鑑別裝置	Micro SD 記憶卡	Micro SD 記憶卡
成本效益	使用者持有成本	無需添購新設備	鑑別裝置	Micro SD 記憶卡	Micro SD 記憶卡
	系統建置與管理成本	做為比較標準	次高(視產品而定)	稍高(三個轉換函數)	稍高(三個轉換函數)
	系統運算成本	對稱式密碼函數	視產品而定	對稱式密碼函數	對稱式密碼函數

參考文獻

[1] S. M. Furnell, P.S Dowland, H.M Illingworth and P.L Reynolds, "Authentication and Supervision: A Survey of User Attitudes", *Computers & Security*, Volume 19, Issue 6, pp. 529 – 539, October 2000.

[2] J. J. Hwang, *Partition and Recovery of a Verifiable Digital Secret*, US patent pending, Patent No. 7596704, 2009.

[3] J. J. Hwang, *User Authentication by Linking Randomly-Generated Authentication Secret with User-Chosen Secret Password*, US patent pending, Application Publication No. 2006/0036857, 2006.

[4] ISO/IEC 27001: 2005, *Information technology – Security techniques – Information security management systems – Requirements*, 2005.

[5] L. Leslie, "Password Authentication with Insecure Communication", *Communications of the ACM*, Volume 24, Number 11, pp. 770 - 772, November 1981.

[6] S. Stamm, Z. Ramzan Symantec and M. Jakobsson, "Drive-By Pharming", Technical Report, no. TR641: Drive-By Pharming, Dec. 2006.

[7] G. R. Voth, C. Kindel and J. Fujioka, *Distributed Application Develoment for three-tier architectures: Microsoft on Windows DNA*, IEEE Internet Computing, 1998.

[8] 行政院經濟部，"*華文電子商務發展行動計畫 (核定本)*"，2010。

[9] 吳院長聽取經濟部"*推動華文電子商務發展執行成效報告*"，http://info.gio.gov.tw，2011。

[10] 動信科技股份有限公司，"SDencrypter Micro SD 卡"，http://www.go-trust.com/cht/products_4.html，2010。

[11] 許義昌、劉興華、黃景彰，"*利用可重複之第一通行密碼及不重複之第二通行密碼來組合成單次通行密碼的使用者鑑別技術與系統*"，中華民國專利申請公開號第：201034423 號，2009。

[12] 黃景彰，"*可驗證之數位秘密之分割與回復*"，中華民國發明專利第：I255121 號，2003。

[13] 黃景彰，"*藉由隨機連結產生的鑑別秘密與個人化秘密的使用者鑑別*"，中華民國發明專利第：I293529 號，2005。

[14] 經濟部標準檢驗局，"*資訊技術－安全技術－資訊安全管理之作業規範*"，CNS 12971，1999。