東海科學第三卷：81–95
90 年 7 月

一個適用於無線網路環境的安全通道之建立

林祝興* 王保利*

摘 要

在本文中，我們探討如何建立一個適用於無線網路的安全通道。我們利用了 Diffie-Hellman 交談金鑰交換協定配合 Interlock Protocol 建構起這一項通道；透過 WAP 瀏覽器 API 呼叫底層加解密程式(我們採用 Rijndael)，達成安全傳輸。而這項設計可以確保使用者與伺服器之間能夠做到安全的溝通，使得使用者與伺服器彼此傳遞的資訊不致外漏，讓有心之人有機可乘。我們並將所提方法實作於無線網路環境中。

關鍵詞：WAP、VPN、WML、Key-Exchange Protocol、Interlock Protocol、Man-in-the-middle Attack

一、簡 介

網際網路的來臨，『全民上網』已經是必然的趨勢；而電腦也已儼然成為家家戶戶的生活必備品。而民眾不單單只要求電腦上網，而且能更方便隨身物品，如：個人數位助理(PDA：Personal Digital Assistant)、手機(Mobile Phone)，能夠立即上網；即所謂的無線通訊數據上網。根據 eTForecasts 的研究報告[2,3]，2000 年時無線上網人口(4,000 萬)僅佔全球上網人口(4 億 1,400 萬)的 9.6%，但到了 2005 年時，無線上網人口(7.3 億)將佔全球上網人口(11.7 億萬)的 62%之多。屆時西歐的無線上網人口佔該地上網人口比例更高達 68%，美國則僅有 39%。而在 2003 年日本的手機上網數也將和 PC 上網人數旗鼓相當[26,27,28]。

原有的電子商務市場能夠獲得民眾的認可，是因為民眾相信網路消費能夠保證安全；而在更方便的無線網路市場，又提供了更便利的方式利用手邊的行動裝置上網消費。所以，更刺激了民眾消費的意願。但是，目前在無線上網裝置上，受限於無線硬體裝置的計算能力，並不能達成安全的消費平台。本文在行動裝置有限的硬體設備下，設計出一個具有效率且安全的系統，來達成安全通訊環境，使得人們在瀏覽 WAP 網頁以及傳送訊息時，能

* 東海大學資訊工程與科學系 E-mail: chlin@mail.thu.edu.tw

夠安全無虞的完成通訊，進而完成無線網路交易，提昇行動網路消費的意願。

首先，我們採用現今普及於消費市場的 PDA 為主要的測試平台。在眾多的機種中大致上可以依據所配置的作業系統區分為四大種類，並列舉出幾種具代表性的機台：

1. Palm OS：以 Palm Inc.[5][6]研發的作業系統 Palm OS 為主體。目前流通於市面上的機種大致配備的作業系統版本為 Version 3.1 與 Version 3.5+；而代表性的幾種為 Palm III、Palm IIIc、Palm V、Palm Vx、Visor[7] Prism、TRG Pro[8]。
2. Windows CE：由 Microsoft Corporation [10]針對個人數位助理特性，專案研發的作業系統；以此作業系統為主體的主機，不僅功能強大、針對多媒體做支援、彩色平台、配備高容量記憶體等眾多好處。因此，微軟公司更直接暱稱它為「口袋型電腦(Pocket PC)」，確實一點也不為過。代表機種為：Compaq IPAQ H3630[11]。
3. EPOC：EPOC [8]這個作業系統是由 Symbian[12]所提出來的。由通訊大廠如 Ericsson、Nokia、Matsushita、Motorola 以及 Psion 所共同訂定出的無線通訊標準。主要針對行動通訊設備輕、薄、短、小的特性所設計出來的作業系統；使其主機的特性能有更高的效能、耗費更少的電力、更短的指令回應時間。其主要代表的主機為：Ericsson R380s、Nokia 9210。
4. 其他：不似之前提及的三大類，此項分類的機種都是配備封閉式的作業系統；通常主機在出廠時，廠商直接將該主機的基本功能寫入該主機的記憶體內，而使用者無法像 1、2、3 類，能夠將自己所需的功能以程式化的方式載入記憶體。所以此類的主機在功能面上不及以上提及的三大類；而提供的需求以針對特定功能為主。如翻譯機，股票機等。

在本篇論文中，我們將提出一套適合於無線網路之安全通訊的機制；同時把這套理論應用於電子商務當中，“Mobile Security”[18,19]是我們最終所要達成的目標--能夠有效而安全無虞的存取浩瀚網路的資源。現在，我們有了 PDA，接下來就是需要建置於其上的應用程式—無線網際網路瀏覽器。針對這個前提，我們勾勒出這個架構於無線通訊設備平台上的瀏覽器應用程式的基本需求—1.安全、2.效能、3.方便。

1. 安全：我們使用對稱式加密系統(Symmetric Cryptography[22])，將 WAP Site 所送出

的資料均予以加密，再做傳送的動作，確保資訊的安全；同樣地，使用者使用此瀏覽器瀏覽網頁時，如果遇到需要傳送資料的情形，系統也會透過對應主機的API(Application Programming Interface)呼叫加密程式處理訊息，達到資訊安全的目的。

2. 效能：受限於主機的硬體設備，無法即時處理高運算量的資料。故採用對稱式密碼法可以有效減低對主機計算能力的依賴性，達到快速運算的目的，同時兼顧資料訊息的安全。
3. 方便：PDA 又被暱稱為『口袋機』，可知 PDA 為方便的數位裝置。因此，以此平台作為設計的對象，更能提高原本的附加價值，達到數位資訊即時化的目的。

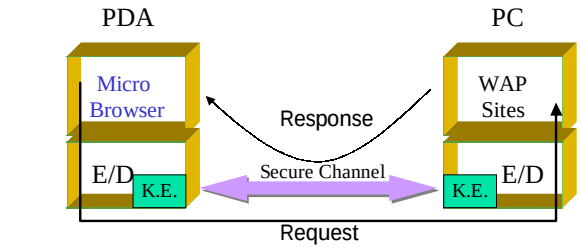
我們將本文所提之方法付諸實作。表一中列出開發環境規格表。在第二節中，我們說明系統架構；第三節介紹作業流程；第四節作安全性及效能分析；第五節作一個簡單結論。

PDA--PalmVx 主機規格	
作業系統	Palm OS Software v. 3.5
記憶體容量	8MB 記憶體大概可以儲存一萬筆地址、五年的行事曆、三千筆待辦事項、三千筆記事、四百筆電子郵件。還有其他的外掛軟體。
快閃記憶體	可下載最新版的 Palm OS 軟體來更新。
本機工作電腦規格	
Server	COMPAQ AP500
發展環境	
程式工具	CodeWarrior Lite for Palm OS

表一：開發環境規格表

二、系統架構與流程

本篇文章主要是在 Palm OS System 上設計一個建構於 WAP 瀏覽器上的安全通道。這個瀏覽器可經由無線傳輸開啟在 Web Server 端的任何一個使用 WML(Wireless Markup Language)網頁。而在網頁開啟與傳輸的過程中，所有的資訊在兼具安全及效能前提下，達到安全通訊的目的。



圖一：系統整體架構圖

1 系統設計：存在於 PC 端的 WAP 網站(使用 WML 語言編纂)，以及使用者端之手持無線設備(在此，我們以可程式設計的開放平台 Palm OS 的 PDA 為主：以 Palm Vx-8MB RAM 為例)。

2 系統元件：

(1) 微瀏覽器：此瀏覽器嵌入由我們設計的對稱式加解密演算法(Symmetric Cryptography)，在此我們採用區塊式密碼法(Block Cipher— Rijndael[34])，來瀏覽經由 WML 語言編纂過的 WAP 網頁。

(2) 對稱式密碼法：由 *NIST(*National Institute of Standards and Technology)所選出的下一代 *AES(*Advanced Encryption Standard[1])所建議的加、解密法。

(3) 金鑰交換：在完成加、解密之前，我們必須達成通訊雙方加、解密金鑰交換，在此時，我們採用 Diffie-Hellman[22]交談金鑰(session Key)交換技術；完成金鑰交換之後，即可用此交談金鑰做下一步驟的加解密金鑰。但是，在金鑰交換的同時，我們以 Interlock Protocol 輔助，以確保安全性。

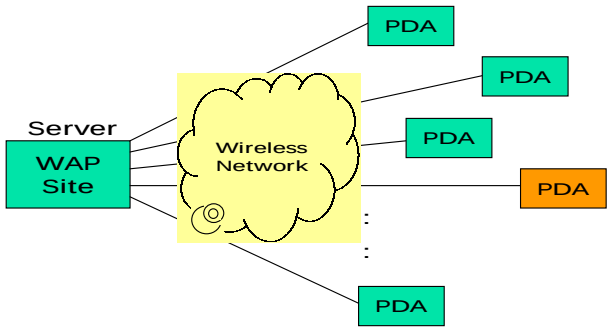
三、系統流程

我們將系統流程分成四階段(4 phases)，依此四個階段詳細的介紹：

1. Connection Phase：

在浩瀚的無線網際網路中，同一時間可能有多台無線裝置對此網伺服器作網頁存取的動作；而且，當任何一台無線裝置作連結時，會在 Server 端作第一次觸發(trigger)的

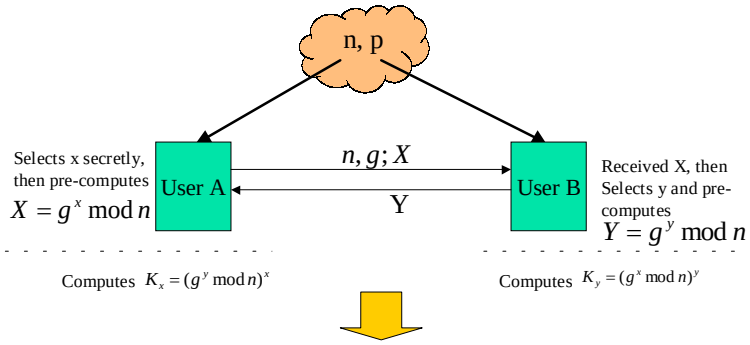
動作。此時，我們假設取其中一台無線存取裝置(PDA)作為例子。



圖二：Connecting Phase 圖示

2. Key-Exchange Phase：

a. Diffie-Hellman 交談金鑰交換系統簡介：



圖三：Diffie-Hellman 交談金鑰交換協定

(1) 首先使用者 *A* 與使用者 *B* 相互溝通，確認雙方在公開領域選擇兩個質數 *n* 和 *p*，而使得*(n-1)/2* 與*(p-1)/2* 亦為質數。並且使用者 *A* 先隨機選擇一個亂數 *x* 並且計算 $X = g^x \bmod n$，並且將 *n*、*g*、*X* 送給 *B*。

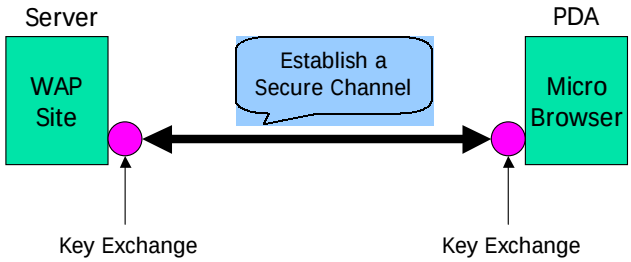
(2) 同樣地，使用者 *B* 亦先以共同資訊*(n, g)*以及自己隨機選擇的亂數 *y*，並計算出的公開金鑰 $Y = g^y \bmod n$；並將此計算之後的數值，傳送給 *A*。

(3) 使用者 *A* 收到訊息之後，以自己的秘密亂數 *x* 加以計算，求得 $K_x = (g^y \bmod n)^x = g^{yx} \bmod n$，並將此數作為下次與使用者 *B* 加、解密訊息之

交談金鑰。

(4) 同樣地，使用者 *B* 也本身的秘密亂數 *y* 和使用者 *A* 所傳來的數值加以計算，求得 $K_y = (g^x \bmod n)^y = g^{xy} \bmod n$，並將此結果，作為下次與使用者 *A* 通訊時，加、解密的交談金鑰(此時金鑰與使用者 *A* 為相同，我們共同稱之為 *K*)。如此一來，通訊雙方就能產生相用的一把交談金鑰。

b. 系統應用：



圖四：Key-Exchange Phase 圖示

在這個步驟，我們執行這個系統最重要的關鍵—金鑰交換。此時，Client 端選擇一個隨機亂數 R_{PDA}，再加上 Client 端 PDA 的 PDA 機碼(Machine_Code，此機碼合法性為唯一，當在下載無線網際網路瀏覽器時，在 Server 提供的網頁(web pages)填入；此時 Server 取得)。將兩者連接，再經過單向雜湊函數(One-Way Hash Function)作轉換，得到結果，即為 Client 端的秘密金鑰(假設為 x)，然後 Client 端再以此序列計算出屬於本身的公開金鑰(假設為 X，$X \neq x$)，再將此 X 送於 Server 端。

$$H_{value\_c}$$
$$= Hash(R_{PDA}, Machine\_Code)$$
$$x = H_{value\_c}$$
$$X = g^x \bmod n$$

同理，當有 PDA 作連結的同時，此觸發動作讓 Server 本身呼叫亂數產生器產生一個屬於該事件的亂數(R_{server})。此亂數結合 Server 本身的時間(*Client_Login_Server_Time*)，再經過一次雜湊函數(*One-Way Hash Function*)，作為 Server 端本身的秘密金鑰(*y*)，再以此秘密金鑰計算出屬於此 Server 對應此 PDA 的公開金鑰(假設為 Y，$Y \neq y$)。再將此公開金鑰 Y 送於 Client 端[20]。

$$H_{value\_s} = Hash(R_{server}, Client\_Login\_Server\_Time)$$

$$y = H_{value\_s}$$

$$Y = g^{y} \bmod n$$

當 Client 端收到由 Server 端送來的公開金鑰 *Y*，便以此公開金鑰結合自己的的秘密金鑰作運算，得到結果，即為彼此之間(Client-Server)作相互溝通的交談金鑰(K_C)。

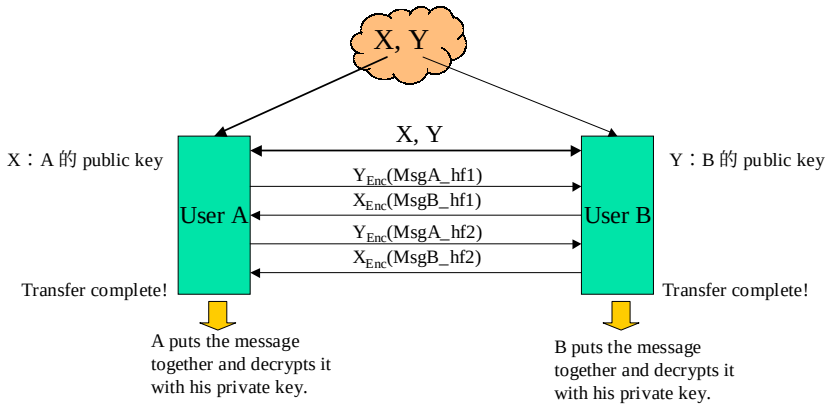
$$K_C = (Y)^{x} = (g^{y} \bmod n)^{x}$$
$$= g^{yx} \bmod n$$

同理，Server 端也做類似的處理(交談金鑰：K_S)：

$$K_S = (X)^{y} = (g^{x} \bmod n)^{y}$$
$$= g^{xy} \bmod n$$

但是，因為 Diffie-Hellman 的交談金鑰交換會遭遇到中間人的攻擊(Man-in-the-middle Attack)[22]，所以我們結合了連鎖協定(Interlock Protocol[22])作安全的保護。同樣的，簡介 Interlock Protocol：

Interlock Protocol 是由 Ron Rivest 和 Adi Shamir 所共同提出來的，主要目的是為了防止 Diffie-Hellman 在金鑰交換時產生中間人攻擊，我們使用此協定加以輔助；使得使用者 *A*、*B* 在產生秘密金鑰時，能有一個更安全的溝通管道。



圖五：使用 Interlock Protocol 訊息交換

(1) 使用者 *A*，*B* 分別在公開領域取得對方的公開金鑰 *X*、*Y*(此公開金鑰與

Diffie-Hellman 中的金鑰相同；若經由 *A*，*B* 互傳亦可)。

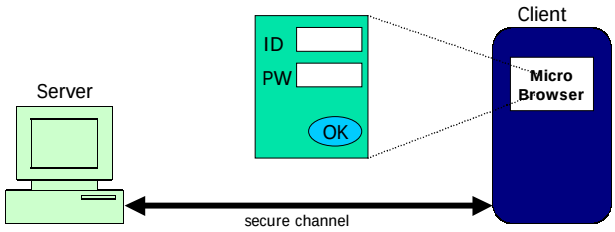
(2) *A* 得到對方的公開金鑰之後，以 *B* 的公開金鑰對接下來要傳送的訊息加以加密；並且將密文分成兩部分，一次傳送一半的密文。

(3) 同樣的，使用者 *B* 也將對方 *A* 的公開金鑰拿來加密接下來要傳送的訊息，並且同樣分成兩部分，一次也僅止於傳送一部份。

(4) 雙方經過兩次傳送之後，得到完整的訊息密文；此時，將密文拼湊，然後用自己的私密金鑰，針對此份密文加以解密(x_{Dec}[MsgB],y_{Dec}[MsgA])，就能獲得完整的訊息。

如此一來，不但完成了 PDA 與 WAP Site 之間的金鑰交換，同時也確保了彼此之間交談金鑰的安全性。

3. Logon Phase：



圖六：Logon Phase 圖示

當完成以上兩個步驟後(Connection Phase、Key-Exchange Phase)，這個使用者對這台伺服器已經完成安全通道的建置；倘若這個使用者想發送訊息(如：訂單、文件)給伺服器，就必須再完成登入(Login)伺服器的動作。在此，我們區分為新帳號註冊及登入以及舊帳號登入：

(1) 新帳號註冊及登入：

新帳號註冊所必填的欄位為：該 Client 端 PDA 的 *Machine_Code*(可比對與最初所填入的資料是否相同？)、該使用者的 *ID* (與 *login* 時相同)、*Password*。完成表格後，以已交換完後的交談金鑰加密後送出。之後，該 Server 將其密文解密，然後儲存在對應的資料庫。

Client 端做以下步驟，並將最後結果送出(*Login_Msg*)：

$ID = ID$

$PW = MD5(password)$

$Login\_Msg = Enc_{Session\_key}(ID, PW, Machine\_Code)$

Server 端收到訊息後, 以與 Client 端共同的交談金鑰解開, 並作資料庫儲存的動作：

$Dec_{Session\_key}(Login\_Msg)$

$= Dec_{Session\_key}(Enc_{Session\_key}(ID, PW, Machine\_Code))$

$= (ID, PW, Machine\_Code)$

(2) 舊使用者登入：

將 (*ID*, *PW*, *Machine_Code*)加密送出, 比對資料庫；如果對應該 *ID* 的 *Machine_Code* 不同, 予以增加該 *ID* 所對應的 *Machine_Code*(即一個使用者可以對應多個 *Machine_Code*, 只不過該新的 PDA 必須安裝我們設計的無線網際網路瀏覽器應用程式)。

4. Transmission Phase：

在這個 Phase 中, 我們採用的關鍵技術是使用對稱式加密法—Rijndael Cryptography Algorithm；在此, 先作 Rijndael 簡介及說明：

Rijndael 是在 *AES* 的選拔中, 經過多次的角逐, 與其他演算法的相互競爭, 最後脫穎而出, 作為下一代加密演算法的標準。而 Rijndael 本身是一個經過反覆運算的加密演算法, 允許可變動的資料區塊(block)以及金鑰長度(key length), 而資料區塊以及金鑰長度的變動都是各自獨立的。

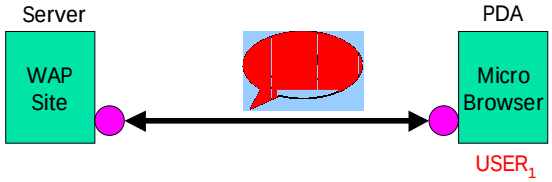
優點：

(1) 在 Rijndael 本身的設計上, 回合與回合之間的轉換是可以採用平行處理, 以提昇執行效率。

(2) Rijndael 可以實作在較低配備的主機上, 並且以相當快速的速度作運算, 頗符合 PDA 這種低速運算設備。

(3) 加密法不採用算數運算(arithmetic operations), 所以不會因為不同的處理器架構(big-endian or little-endian)而有所差異。

(4) 不使用其他加密元件(如：S-boxes)；亦不易種入暗門程式(trapdoor)。



圖七：Transmission Phase 圖示

現在，假設使用者有一份填寫完成的訂單(Document)欲送達 Server 端做訂購的動作，吾人如何確保此份訂單的資訊能夠安全的送達 Server 端呢？假設訂單資訊為 *Document*，此時，系統會呼叫底層的對稱式演算法(我們採用 Rijndael)作加密的動作；依循以下的步驟：

$$Ciphertext\_Doc_{Info} = Enc_{Sym}(Document, ID)$$

將此已經加密過的訂單密文，送至 Server 端；此時，Server 收到後，以 Client 相同的對稱式演算法解密，即可解出此份訂單，得到訂單內容：

$$\begin{aligned} &Plaintext\_Doc_{Info} \\ &= Dec_{Sym}(Enc_{Sym}(Document, ID)) \\ &= (Document, ID) \end{aligned}$$

四、安全及效能分析

1. 攻擊方法分析[14,15,21,23,24,25]：

(1) 針對 Connection Phase 作攻擊：

此步驟是為了 Client 端與 Server 端建立一個獨立的連結通道，而每個 Client 的身分都代表一個獨立的個體，與伺服器連接時，分別各自產生了一個獨立通道，故偽裝攻擊此伺服器無法成功。

(2) 針對 Key-Exchange Phase：

(2.1)交談金鑰交換前：

在金鑰交換前，各自的 Client 並未擁有任何相關的資訊(如：隨機亂數)；所以，此攻擊者並沒有任何攻擊目標。

(2.2)交談金鑰交換過程中：

我們系統採用了 Interlock Protocol 杜絕中間人的攻擊；因此防範了此一

攻擊行為。

(2.3)交談金鑰交換完成後：

假設攻擊者為 *H*，欲對其中一個 Client，假設為 $Client_i$，做出攻擊行為。在這個 Key-Exchange Phase 中，攻擊者必須猜測出 $Client_i$ 的相關資訊(R_i, *Machine_Code*)：

(2.3.1)猜出 *Machine_Code*：

在 $Client_i$ 下載無線網際網路瀏覽器時，可能因為某些原 因，導致 *Machine_Code* 外流；或者此攻擊者攻擊儲存這個儲存 $Client_i$ 的 *Machine_Code* 資料庫伺服器，導致獲得任何 $Client_i$ 的 *achine_Code*。所以，此項參數可能外流。

(2.3.2)猜出 $Client_i$ 亂數 R_i：

但是，往回看看我們所採用的金鑰交換的協定，是經過單向雜湊函數所運算，送出的資訊又是經由採用離散對數的方式所包裝；故，要解出原始的資訊，必須先要遭遇離散對數(Discrete Logarithm)的難題，而後，又必須面臨單向雜湊函數的問題，可謂「計算時間內不可行(Computing Infeasible)」。故此項攻擊實屬不可行。

(3) 針對 Logon Phase：

所有資料都是經由 Connection Phase 完成連結，Key-Exchange Phase 完成金鑰交換而建立而成的安全通道；一切訊息都經過加密完成，然後傳送。而傳送的交談金鑰，是由離散對數形式加密，所以，欲破解密文以獲得登入者的 *ID* 及 *PW*，就必須先破解離散對數的演算法，困難度同(2.3.2)。

$$Login\_Msg = Enc_{Session\_key}(ID, PW, Mach\_Code)$$

$$Session\_key = g^{xy} \bmod n$$

(4) 針對 Transmission Phase：

欲破解經由對稱式加密法—Rijndael，所加、解密的任何訊息，首先必須突破我們設計的前三個 Phases 之後，才有可能接觸到由 Rijndael 所加解密的任何訊息。而有關於對稱式加密法--Rijndael 的安全，請參考文件「*AES Proposal：Rijndael*」[35]有詳細說明，在此並不贅述。

2. 在效能分析上，我們對訂單、文件加解密的方式是採用對稱式加密法。使用對稱式加密法的考量點，歸因於加解密的速率比其他演算法加、解密的速率快上數十甚至數百倍[13,22]。所以，對於受制於低速硬體配備的 PDA 而言，不啻是一個最好的選擇；縮短加、解密時間，就等於縮短了使用者等待的時間，而對於現行網際網路計費制的現在，就等於縮短了連線時間，也替消費者節省不少金錢支出。

五、結　語

網際網路盛行的現在，伴隨而來的，是讓使用者能夠以更方便的方式隨手上網，因此「Mobile Security」是一個重要的課題；而這也是我們這篇文章所要探討的目標。因此，設計出一個能夠在浩瀚網際網路中，提供一個能夠確保使用者身分不被冒用、使用者與網站伺服器之間所傳輸的訊息不會被竊聽、被竄改的「安全通道」。如此一來，在往後的無線電子交易(Mobile Commerce)，都能夠在以安全為前提的狀態下，達到方便又迅速的交易環境。

參考文獻

[1] Advanced Encryption Standard, http://csrc.nist.gov/encryption/aes/

[2] Institute for Information Industry, http://www.find.org.tw/home.asp

[3] eTForecasts Co., http://www.etforecasts.com/

[4] ICOA, Inc.,http://www.openwap.org/

[5] Palm, Inc, http://www.palm.com/

[6] Palm OS, http://www.palmos.com/

[7] Handspring, Inc. http://www.handspring.com/

[8] TRG Pro Product, Inc http://www.TRGPro.com/

[9] EPOC Product, www.epocworld.com/

[10] Microsoft Corporation, http://www.microsoft.com/

[11] COMPAQ Co., http://www.compaq.com/

[12] Symbian Limited, http://www.symbian.com/

[13] Lacy, J.B., Mitchell, D.P., and Schell, W.M. (1993) “CryptoLib: Cryptography in

Software," *UNIX Security Symposium IV Proceedings*, USENIX Association, pp 1-17.

[14] Cox, D. (1995) "Wireless network access for personal communications," *IEEE Comm. Magazine*, **30**(12), December.

[15] Maughan, D., Schertler, M., Schneider, M., and Turner, J. (1998) "Internet security association and key management protocol (ISAKMP)," draft-ietf-ipsec-isakmp-10.txt July.

[16] Montengro, G., and Dawkins, S. (1998) "Wireless networking for the MNCRS," draft-montenegro-mncrs-00.txt, August.

[17] Myles, A., Johnson, D., and Perkins, C. (1995) "A mobile host protocol supporting route optimization and authentication," *IEEE J. Selected Areas in Commun.* **13**(5), June, pp. 839-849.

[18] Solomon, J. (1998) *Mobile IP: The Internet Unplugged*, Prentice Hall, Englewood Cliffs.

[19] Bird, R. *et al*. (1991) "Systematic design of two-party authentication protocols," *Proc. Crypto. 91*. Santa Barbara, CA, Aug., pp. 44-61; also available as "Advance in Cryptology," in *Lecture Notes in Computer Science*, J. Feigenbaum, Ed. New York: SpringerVerlag, Vol 576.

[20] Denning, D.E., and Sacco, G. M. (1981) "Timestamps in key distribution systems," *Commun. ACM* **24**(8), pp. 533-536.

[21] Needham, R.M., and Schroeder, M.D. (1978) "Using encryption for authentication in large networks of computers." *Commun. ACM* **21**(12) pp. 993-998.

[22] Schneier, B. (1994) *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Whily & Sons, Inc..

[23] Maurer, U.M. (1991) "Perfect cryptographic security from partially independent channels," *Proc. 23rd ACM Symposium on Theory of Computing*, pp. 561-571.

[24] Merkle., R.C. (1978) "Secure communication over insecure channels.," *Comm. ACM* **21**(4), pp. 294-299.

[25] Geffe, P.R. (1973) "How to protect data with ciphers that are really hard to break," *Electronics* **46**, pp. 99-101.Scourias, J. (1997) *Overview of the Global System for Mobile Communications*.

[27] Winch, R. (1993) *Telecommunication Transmission Systems*, Mc-Graw-Hill, New York.

[28] 林一平 (1998) "Introduction to Mobile Network Management," 維科.

[29] "Wireless Application Protocol Architecture Specification", WAP Forum, April 30, 1998,

URL: htttp://www.wapforum.org/

[30] “Wireless Application Environment Overview”, WAP Forum, Nov. 4, 1999, URL: htttp://www.wapforum.org/

[31] “Wireless Datagram Protocol Specification”, WAP Forum, Nov. 5, 1999, URL: htttp://www.wapforum.org/

[32] “Wireless Markup Language”, WAP Forum, Nov. 4, 1999, URL: htttp://www.wapforum.org/

[33] “Internetworking between the PLMN supporting GPRS and Packet Data Netowrk (PDN)”, GSM 09.61

[34] Daemen, J., and Rijmen, V. (1999) *“AES Proposal：Rijndael”*, Document Version 2, Mar, 9.

Building Secure Communication Channels in Wireless Environment

Chu-Hsing Lin* Poly Wang*

Abstract

In this paper, we study the problem of how to build a secure communication channel in wireless environment. We apply the Diffie-Hellman key exchange agreement and the Interlock Protocol to construct secure channels. From WAP browser, the API calls for encryption and decryption modules (Rijndael algorithm) to fulfill the security requirement. By using the proposed method, a client user and the server can transmit data securely via an insecure path. We also implement the proposed scheme in a wireless environment, which is getting much more attention.

Keywords: WAP、VPN、WML、Key-Exchange Protocol、Interlock Protocol、Man-in-the-middle Attack.

* Laboratory of Information Security, Department of Computer Sciences and Information Engineering, Tunghai University, Taichung 407, TAIWAN. Email: chlin@mail.thu.edu.tw