行政院國家科學委員會專題研究計畫成果簡短報告

行動資訊服務環境下安全技術之研究與製作(二)

Security of the Ubiquitous Information Service Environment (II)

計畫編號：NSC 87-2213-E-009-055

執行期限：民國 86 年 8 月 1 日至民國 87 年 7 月 31 日

主持人：曾文貴 交通大學資訊科學系副教授

一、中文摘要

近年來無線通訊技術發展迅速，『行動資訊服務』(mobile information service)的需求也大量增加。無線通訊技術是行動資訊服務的必要條件，然而無線通訊存在一些技術障礙，例如通訊頻寬太低、通訊品質不穩定、通訊易被攔截、手機功能有限等，所以以往基於有線網路所發展的資訊技術並不能直接應用到行動資訊網路上。我們總體計劃的目的是研究如何提供一整合的行動資訊服務環境，使得使用者無論在任何時間、任何地點皆可以連絡上各類資訊網路系統，輕易的取得所需的資訊。本子計劃的目的是研究行動資訊服務環境中的安全技術，包括『資料傳輸的安全』、『使用者的身分確認』、以及『廣播資料的多重安全』等。

本計劃為期三年，第一年計劃已經執行完畢，在本年度的計畫裡，我們實作一個系統（網路安全漫遊系統）來驗證我們所設計協定的安全與效率。

Abstract

Due to fast development of wireless communications, there are increasing demands on mobile information services, which are based on wireless communication. However, there are some inherent properties of wireless communications that make it difficult to apply wireline-based information technologies to wireless-based information services. For example, the wireless communications cannot use too much band-width, their communication quality is not stable, they are vulnerable to intercept, the function of the mobile handsets is restricted, etc. Therefore, the goal of our joint project is to study how to provide a mobile information service environment so that a user can access information through wireless information systems at any where and at any time. This sub-project is to research the security issues of the mobile information service environment, such as security of

data communication, authentication of users, multilevel security of broadcast data, etc.

This project has a three-year term. In this year (second), we implement a Secure Internet Roaming System (SIRS) to show that our proposed protocols are secure and efficient.

二、計畫緣由與目的

以往的行動服務大都以通訊為主，資訊服務則侷限於有線的網路上（如 Internet），以現今的發展趨勢來看，行動資訊服務（mobile information service）的需求將大量增加；簡要的說，行動資訊服務是要讓使用者不論在任何時間、任何地點皆能透過無線網路連接到資訊網路以取得必要的資訊。

有線網路的資訊服務，特別是 Internet 上的資訊服務早已蓬勃發展，我們也很自然的會想到是否可以把有線網路的資訊技術直接移轉到無線網路上，以節省研發的時間與費用，然而事情並不是那麼簡單。行動無線環境有它自己獨特的特點，例如它能使用的通訊頻寬通常很小，通訊品質也不穩定，因此無法作大量的資料傳輸；使用者手機的功能有限，因此無法作大量且複雜的運算；無線傳輸容易被攔截，因此它的安全問題就特別突出；還有因為使用者是機動的，使用者可能在地點 A 查詢資料，而查詢的資料回來時，使用者可能已經到地點 B 了。

我們的總體計劃是要研究行動資訊網路上的各相關問題，希望提供一行動資訊服務的環境以達到行動資訊服務的理想境界。本子計劃是要研究行動資訊務網路環境上的『安全問題』，包括『資料傳輸的安全』（communication security）、『使用者的身份確認』（user authen-tication）、『廣播資料的多重安全』（multilevel security of broadcast data）等。

在第一年的計劃裡，我們研究行動環境下的使用者身分確認與金匙交換，我們對現有的行動服務系統做了完整的綜合比較，並對 GSM 系統的安全問題提出改良的方法。現在執行的第二年計劃中，我們要將第一年的研究成果做成系統，我們選定的目標是網路安全漫遊系統（Secure Internet Roaming System）。Internet roaming 的概念是無論使用者 login in 到網路上的任何機器，當有其他的使用者要聯絡他時，都可以找到他。例如，使用者 A 的 home account 是在機器 M 上（他的電子郵件位址是 a@m），當他 login 到機器 N 上時，如果有新的郵件到達，郵件會自動轉到 N 機器上；還有，當使用者 B 要與使用者 A 作線上交談時，使用者 B 只要下 “talk a@m” 命令，系統會自動找到在機器 N 上的使用者 A，然後建立連線。Internet roaming 所牽涉的安全問題與行動電話系統的安全問題很類似，因此我們實作這一個系統來驗證我們所設計協定的安全與效率。

三、研究成果

我們可以把網路安全漫遊系統當成 E-mail server 的一個外掛程式。一個 E-mail server 如果要提供網路安全漫遊的功能給它的使用者，只要將網路安

全漫遊系統和 E-mail server 結合在一起，當它的使用者希望使用網路安全漫遊系統的功能，發出註冊要求時，系統會發給使用者一封特殊的 E-mail，裡面包含使用網路安全漫遊系統所需要的資訊。在使用者是此 E-mail server 的合法用戶期間（E-mail address 沒改變），上述的註冊動作只要做過一次，使用者就能繼續使用網路安全漫遊系統的功能。

我們的研究成果有三項：（一）提出一個以身分為基礎的身分認證方法；（二）提出一個以身分為基礎的金匙分配方法與（三）實作一個網路安全漫遊系統。分述如下：

(一)以身分為基礎的身分認證方法

- 起始階段

金匙分配中心（Key Distribution Center, KDC）產生兩個質數 p 和 q，令 $n= p*q$，選擇一個質數 e，並計算 d，使得 $e*d= 1 \pmod{\text{lcm}(p-1, q-1)}$，lcm 代表最大公倍數。另外，有一公開的 one-way hash function f，用來計算使用者 i 的 extended ID，其目的在避免使用者同謀的可能性。系統個公開資訊有（n, e, f），私密資訊有（p, q, d）。

- 使用者註冊階段

當使用者 i 向 KDC 註冊一個新的帳號 ID_i 時，KDC 先用 f 來計算使用者 i 的 extended ID，$EID_i= f(ID_i)$，接著計算使用者 i 的私密資訊 $S_i= EID_i^d \pmod n$ 將(n, e, f, S_i)存放在 smart card 中，透過一個安全的管道將 smart cart 送給使用者 i。

- 應用階段

當使用者 i 想要對使用者 j 證明他的身分，步驟如下：

(1) 使用者 i 產生一個隨機數 r，計算 $R= EID_i^r \pmod n$，將（ID_i, R）傳給使用者 j。

(2) 使用者 j 收到（ID_i, R）後，產生一個隨機數 x，傳給使用者 i。

(3) 使用者 i 收到 x 後，計算 $T= S_i^{(r+1)x} \pmod n$，將 T 傳給使用者 j。

(4) 使用者 j 收到 T 後做下列運算：$T^e = (R*EID_i)^x \pmod n$，如果成立則確認使用者 i 的身分是 ID_i。

(二)以身分為基礎的金匙分配方法

起始階段和使用者註冊階段和（一）幾乎完全一樣，不過系統的公開資訊多了一個 hash function h。

- 應用階段

假設 User1 與 User2 是註冊過的系統合法用戶，各自擁有系統發給的 smart card，當 User1 與 User2 希望進行祕密的通訊前，進行金匙分配以建立 session key 的步驟如下：

(1) User1 產生三個隨機數 r_1, x_1, y_1（$\gcd(x_1, y_1)= 1$），利用 extended Euclidean algorithm 計算 a_1 & b_1，使得 $a_1x_1+b_1y_1= 1$ 成立。假設 b_1 是負數，a_1 是正數，做下面的計算：

$$M_{11} = r_1(EID_2 D^{x_1} \pmod D$$

$$M_{12} = (EID_2 D^{y_1 e x_1} \pmod D$$

$$M_{13} = \left(EID_2^{-1}\right)^{v_1 e y_1} = \left(EID_2\right)^{-v_1 e y_1} \pmod D$$

$v_1= h（M_{11}, ID_1, ID_2, t）$, t 是系統時間。

將(M_{11}, M_{12}, M_{13})傳送給 User2。

(2) User2 收到(M_{11}, M_{12}, M_{13})後，利用下面的計算確認 User1 的身分：

$$\gamma_{11}^{c_1}\gamma_{12}^{e} = EID_1^{v_1} \pmod D$$

$c_1=e*v_1$。如果上式成立，則確認 User1 的身分是 ID_1，做下列計算：

$$\gamma_{14} = \gamma_{12}^{r_2} \pmod D$$

$$\gamma_{15} = \gamma_{13}^{r_2} \pmod D$$, r_2 是 User2 產生的隨機數。

將(M_{14}, M_{15})傳送給 User1。

(3) User1 收到（M_{14}, M_{15}）後，做下面的計算：

$$r_1 = (\gamma_{14})^{a_1}(\gamma_{15})^{-b_1} = (EID_2)^{v_1 e r_2} \pmod D$$

(4) 步驟(1)～(3)中，User1 與 User2 的角色對調，User2 可以得到

$$r_2 = (EID_1)^{v_2 e r_1} \pmod D$$

(5) User1 和 User2 分別計算他們的 session key K_{12} 和 K_{21} 如下：

$$b_{12} = (r_1)(EID_1)^{v_2 e \sigma_1} \pmod D$$，

$$b_{21} = (r_2)(EID_2)^{v_1 e r_2} \pmod D$$ 完成金匙分配，雙方擁有相同的 session key。

(三)實作一個網路安全漫遊系統

- 系統功能與目的

網路安全漫遊系統的目的在提供使用者一個線上交談的安全環境，不用擔心交談的內容被竊聽。使用者在不同的機器間漫遊，依然可以收到朋友的呼叫，進行線上交談；SIRS server 會直接將新郵件轉寄到使用者正在使用的機器上。簡單來說，網路安全漫遊系統的功能有兩項：（一）線上交談，（二）轉寄郵件。

目前我們先發展 SIRS 線上交談的功能，如何將 SIRS 與 E-mail servers 結合，提供轉寄電子郵件的服務暫時不討論。

- 系統架構

整個系統由三種不同的成員組成，分述如後：

(1) SIRS server：一方面要扮演金匙分配中心（KDC）的角色，處理使用者註冊的事宜。另一方面則接受使用者登入或登出，記錄使用者的最新位址，提供給其他使用者查詢。

(2) SIRS client：安裝在各地的電腦上，是使用者與系統真正接觸的界面。沒有 domain 的觀念，SIRS client 並不隸屬於任何 SIRS server。負責根據使用者提供的資訊及下達的指令，做適當的反應。

(3) disk：負責儲存使用者資訊，如 ID、私密資訊和系統參數等等，這些資料以使用者提供的密碼為金匙，加密後存放在 disk 中。所以，擁有 disk，還要配合使用者提供正確的密碼，經過解密讀取資料後，才能成功的進入系統。使用者帶者 disk 可以由不同的 SIRS client 進入系統。

- 系統協定

我們以使用者的觀點來說明 SIRS 系統運作的流程。假設 SIRS 系統中有兩台 SIRS server（Server1, Server2）提供服務，而且已經照（一）的起始階段設定好系統參數，我們令 ID 的格式為：UserName@ServerName。兩個使

用者 User1 和 User2 是好朋友，User1 向 Server1 註冊一個 UserName 為 Alice 的帳號，User2 向 Server2 註冊一個 UserName 為 Bob 的帳號，這兩個使用者從註冊帳號、登入網路到進行線上交談的過程如下。

(1) **User1** 向 **Server1** 註冊一個新帳號 **Alice**

(1.1) User1 利用一台安裝有 SIRS client 的機器與 Server1 建立連線，提出申請帳號的要求，並告知希望使用的 UserName 是 Alice。送出訊息：*"register/Alice"*。

(1.2) 收到註冊的要求後，Server1 計算此帳號(ID_1= Alice@Server1)的 extended ID，$EID_1 = f(ID_1)$。然後根據 EID_1 是否已經有人使用來決定註冊是否成功，此時 Server1 可能送出兩種訊息：

"register/0"：如果 EID_1 恰巧與其他已註冊帳號的 extended ID 相同，告知使用者註冊失敗。

"register/S_1/n/e"：如果 EID_1 與目前所有已註冊帳號的 extended ID 沒有衝突，Server1 計算其相對的私密資訊 $S_1 = EID_1^d \pmod n$ 然後將 S_1 還有系統公開的參數 n、e 傳給 SIRS client。

(1.3) SIRS client 根據收到的訊息判斷註冊是否成功，如果收到 *"register/0"* 表示註冊失敗，告知使用者申請其他帳號；收到 *"register/S_1/n/e"* 表示註冊成功，要求 User1 設定密碼，然後以此密碼為金匙，將（ID_1, S_1, n, e）加密後存到 disk 中，完成註冊的程序。

(2) 使用者 **User1** 登入/登出系統

(2.1) User1 啟動 SIRS client 登入系統的功能後，SIRS client 要求 User1 輸入密碼，以讀取 disk 中的使用者相關資訊（ID_1, S_1, n, e）。如果密碼錯誤，即使擁有 disk 也無法登入系統。

(2.2) 在得到 disk 中的使用者相關資訊後，SIRS client 就可以利用我們所提出的以身分為基礎的身分認證方法向 SIRS server 證明是合法的使用者。如果身分認證無誤，則更新此帳號的位址記錄。

(3) 建立安全通道

假設 User1 已經利用 SIRS client1 成功登入系統，User2 讓 SIRS client2 讀取 disk 中的資料後（不需要登入系統），希望與 User1 進行祕密的通訊，過程如下：

(3.1) User2 對 SIRS client2 下達指令 *"talk Alice@Server1"*。

(3.2) 根據 ID_1（Alice@Server1），SIRS client2 得知此帳號使用者的最新位址記錄由 Server1 負責維護，SIRS client2 與 Server1 建立連線後，發出查詢位址的要求：*"query/Alice"*。

(3.3) Server1 收到查詢的要求後，查詢 Alice 目前的位址記錄，將查詢的結果傳給 SIRS client2。

(3.4) SIRS clinet2 根據收到的查詢結果，判斷 Alice 是否在線上，如果收到 *"query/0"* 表示不在線上，將此訊息告知 User2。在這裡，查詢得到的結果是 Alice 在 SIRS client1，所以 SIRS client2 與 SIRS client1 建立連線。

(3.5) 如果 User1 正利用 ID_1 和其他使用者線上交談，SIRS client1 和 SIRS client2 無法建立溝通管道，將

此訊息告知 User2。如果 User1 閒置中，則 SIRS client1 與 SIRS client2 進行（二）提到的金匙分配方法建立 session key，然後利用這把 session key 加解密雙方溝通的訊息，達成安全的溝通。

四、結語與討論

在前面的章節裡我們提出了一個新的以身分為基礎的使用者身分認證方法以及一個新的以身分為基礎的金匙分配方法，並且利用這兩個方法來設計並製作一個網路安全漫遊系統（SIRS），讓使用者即使在不同的機器間漫遊，也可以收到遠端朋友的呼叫，然後進行線上交談，而且不用擔心交談的內容會被竊聽。

由於我們的系統採用以身分為基礎的密碼方法為設計的基礎，自然的，也繼承了這種密碼方法本身的好處，歸納如下：

- 使用者進行線上交談，建立 session key 的過程中不需要 SIRS server 或第三者的幫助。
- 使用者跟 SIRS server 間不需要保有私密金匙，使用者也不需要浪費記憶體去記錄其他使用者的公開金匙
- 當有新的使用者加入系統時，舊用戶不需要更動他們原有的私密資訊。
- 即使有某些使用者的私密資訊被洩漏出去，也不會影響其他用戶私密資訊的安全。

網際網路是個不安全的環境是眾所周知的事，駭客入侵網路系統時有所聞，強調網路安全是未來的趨勢，可以預見的，將來市面上的產品如果不提供安全的功能將不會被消費者所接受。

經過以上的討論，我們認為未來的工作可以朝下面幾點進行：

- 設計出一個更好的以身分為基礎的金匙分配方法。雖然我們的方法目前看來沒有安全的疑慮，實際應用也證明確實可行，不過計算量大，傳輸訊息多，傳輸的次數也多一次，這些缺點不但限制了這個方法的應用範圍，也提供給入侵者更多成功破解系統的機會。
- 以網路安全漫遊系統原本的構想而言，E-mail 安全轉寄的要求在我們的系統裡可以達成，只要 SIRS server 推導出收信人的私密資訊，然後 E-mail server 根據此私密資訊加密信件，轉寄給收信人，那麼只有擁有私密資訊的收信人才能對這封加密過的信件解密。
- 如果要讓網路安全漫遊系統提供傳送訊息的功能，我們也可以加上安全的機制，只要利用數位簽章方法，先對訊息做簽章，收到訊息的對方就能確認訊息是否是偽造的。
- 網路安全漫遊系統提供使用者間檔案傳輸的做法和線上交談的過程相同，雙方先經過金匙分配方法建立 session key 後，利用這把 session key 對檔案做加密，如此，就不用擔心檔案在傳輸的過程被人盜用了。

五、參考文獻

[1] A. SHAMIR, Identity-based

crypto-systems and signature schemes, *Proc. CRYPTO '84*, Springer-Verlag, pp. 47- 53

[2] L. M. KOHNFELDER, A Method for Certification, *Lab. Comput. Sci., Mass. Inst. Technol., Cambridge, MA*, May 1978

[3] R. BLOM, Non-Public Key Distri-bution, *Proc. Crypto '82*, 1982

[4] E. OKAMOTO and K. TANAKA, Key Distribution System Based on Identification Information, *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 4, pp. 481-485, 1989

[5] K. OHTA, Efficient identification and signature schemes, *Electron. Lett.*, vol. 24, No. 2, pp. 115- 116, Jan 1988

[6] S. TSUJII and T. ITOH, An ID-Based Cryptosystem Based on the Discrete Logarithm Problem, *IEEE Journal on Selected Areas in Communication*, Vol. 7, No. 4, pp. 467- 473, May 1989

[7] T. MATSUMOTO and H. IMAI, (Comment) Proposal for Identity-Based Key Distribution Systems, *Electron. Lett.*, 1988, 24, pp. 72-73