# 基於 RFID 的點對點 VoIP 語音通訊系統

柯志鴻
長榮大學資訊管理學系
kech@mail.cjcu.edu.tw

吳任航
長榮大學資訊管理學系
r26911013@mailst.cjcu.edu.tw

## 摘要

由於網際網路的普及與較低的電信費率，人們逐漸使用網際網路進行更便利且更即時的連絡。即時通訊和網路語音通訊兩個最具代表性，其中 MSN 和 Skype 已成為人們最普遍使用的工具。然而，這些軟體並非絕對安全，例如，沒有嚴謹的加密或根本沒有加密，因此衍生出隱私與安全問題。所以，如何確保使用者能安全地使用軟體進行通話或傳訊，而且不會被第三者竊取，便是一個重要議題。本研究採用微軟.Net 平台和 P2P 網路技術，以及 AES 與 RSA 演算法，實作一個安全且效率高的 VoIP 通訊系統。而且，我們使用 Mifare Card 去儲存聯絡人和金鑰等各種資訊，以便增加隨身攜帶的便利性。

關鍵詞：網路語言通訊、點對點、Mifare 卡、密碼學

# 壹、緒論

自古以來，人與人之間的通信都希望能跨越時間、空間來達成遠距通訊。從早期的飛鴿傳書，到電報的發明，再到本世紀的手持行動通訊以及網路通訊皆是以此為目標。然而，隨著傳統電話、手機的費率持續居高不下，許多個人或企業用戶轉趨以網路文字通訊或視訊，如當紅的 MSN 和 Skype，等方式來達到低成本的遠距通訊。根據調查，商務應用環境中，企業與客戶之間最常使用的溝通方式即屬 Skype，因其具有優越的連線能力，以及簡易使用等優點。截至目前為止，全球已有 80%以上的企業員工[4]，使用 MSN 和 Skype 這類的即時訊息軟體(IM)和網路語音電話(VoIP)來進行聯絡與溝通。

對企業而言，使用免費的軟體是趨勢也是優勢，然而此類的軟體卻存在安全性、穩定性等多項隱憂。以市占率達 7 成[11]的 Skype 為例，因其傳輸是採 P2P 模式，且得在不經終端使用者同意的情況下，直接升級某裝有 Skype 的 PC 或崁入式話機為超級節點，做為 P2P 中繼站的角色。這些超級節點成了中繼站以後，可負責傳遞任何在防火牆背後的節點資料，導致通話內容可能被第三者截取的情形。另外，電信法[12]明文規定電信業者得提供監聽技術，提供給檢警單位做合法監聽[7]。此類合法的監聽軟體容易被駭客重製或仿冒，以及流入黑市或者分享平台上供人免費下載。這樣一來，日後駭客只要加以封裝，利用一些詐騙方式，騙取使用者執行後門檔案，即可將現行的 VoIP 軟體的上網閘道全面指向偽裝的超級節點，進而達到不法監聽的目的。以著名的 Skype 軟體為例，雖然官方聲稱採用獨特的加密手法，然而近來的研究指出，即使經過加密處理，還是有 50%~90%的辨識率，使得 VoIP 的安全性再度受到挑戰[13]。

當然，其他仍有多項缺點存在，如 MSN 無故自動封鎖聯絡人[1]，此情況下使用者毫無自主權且有一種被侵犯隱私權的恐懼；Skype 全球當機的服務不穩定性情形[2]，卻又無法獲得營運商的擔保。這些皆因軟體是免費提供給所有使用者，營運商有權利為著系統穩定性和安全性，不經通知就直接對資料庫做維護。但事實上每個人都不知道資料放在遠端的資料中心安全性為何，或者營運商會拿這些個人資料用在那些範圍。例如近年來發生的免空浩劫新聞，即是因國家介入，導致全球使用者的檔案被強制沒收。近年來，隨著這類事件陸續浮出檯面，隱私權問題逐漸被各國政府和人權團體重視。除各國已有相關訴訟進行外，企業老闆不禁自問：我的商業機密安全嗎？表 1 即是市面上常見的三種 VOIP 軟體，它們各項屬性的比較如表所列，有著不同的加密能力、通話品質和安全性，而認證機制皆採中央伺服器的方式，因此都存在上述的某些缺點。

本研究的主要目的是設計一套安全且能自主服務的網路語音通話軟體(VOIP)，讓所有能上網的使用者均能自主性地與自行建立的聯絡人進行通話。而且，所開發的軟體採用 AES(Advanced Encryption Standard)與 RSA 混合式的加密演算法，將音訊內容加密傳送，並藉由點對點網路技術（簡稱 P2P）建構可靠、安全的傳輸拓樸網路。如此一來，就不需要擔心資料竊聽問題[3]，也不需要擔心服務提供者伺服器壞掉，或者伺服器網路不通時造成的困難。另外，本軟體加入一個創新的作法，就是利用非接觸式智慧卡－Mifare Card 來儲存個人識別資訊及聯絡人資料，類似「智慧型電話卡」功能，它除了能

提供使用者安全性高的通訊環境外，更具有容易攜帶的便利性。其中對於金鑰管理，是直接藉由 Mifare Card 出廠時的獨一識別特性來建立 RSA 非對稱式加密金鑰，來識別使用者的合法性。而 AES 加密具有效率高的特點，因此適合被用來作為語音資料加密的基礎。這些資料都藉由 Mifare Card 本身的物理區段鎖定特性，安全的存放在卡片上。即使卡片遺失，不知道卡片密碼的人也是無從取得這些敏感資料。因此，本研究所開發的免費網路語音通話軟體(VoIP)，將能帶給使用者安全、穩定、方便的通訊環境。

本論文後續的內容為，第二章描述開發境及相關研究，系統的分析與設計細節在第三章。至於第四章則是系統的實作與測試，最後的結論與未來工作在第五章。

表 1：目前市面上常見的公眾 VoIP 軟體比較表

| 項目 | Skype | MSN | FreeTalk |
|---|---|---|---|
| 使用人數 | 高 | 中 | 低 |
| 加密能力 | 中 | 高(SSL) | 無 |
| 通話品質 | 高 | 中 | 低 |
| 商用電話機 | 有 | 無 | 無 |
| 傳輸方式 | DHT 網路<br>超級節點 | 公開 IP：P2P<br>私有 IP：中央伺服器 | 中央伺服器 |
| 安全性 | 低<br>超級節點可能是詐騙節點 | 中<br>直接用戶端 P2P<br>中央伺服器轉送 | 中<br>一律透過中央伺服器轉送 |

## 貳、環境與相關研究

本章節除了介紹基本的開發環境外，也將針對建置安全的語音通訊軟體所需的理論及技術加以探討，其中包括：即時語音傳輸通訊協定、網路安全模型、密碼學技術。

一、 開發工具與環境

本研究使用商業軟體 Windows Server 來架設 ASP.Net 稽核伺服器，使用商業軟體 Windows 7 來作為軟體執行平台。而開發工具則使用免費的 Visual Studio Express 版來研發通訊軟體客戶端與稽核伺服器所需的 SOAP Web 服務。稽核伺服器將個人資料以 XML 型態儲存在硬碟上。同時，我們使用 Mifare Card 來儲存個人識別資訊及聯絡人資料，搭配瑞晶資訊提供的 RM100-MIC 教學模組，進行系統實作。

二、即時語音傳輸通訊協定，包括狀態資訊技術、文字即時訊息、和語音框架資料傳輸

(一) 狀態資訊技術：2000 年即時傳訊與定位協定工作小組（Instant Messaging and Presence Protocol Working Group;簡稱為 IMPP WG），希望能完成共通的即時傳訊與定位協定（Instant Messaging and Presence Protocol；簡稱為 IMPP），制定了 RFC 2778 和 RFC 2779[9]。隨後在 2006 年被微軟和 Yahoo 公司所採用，兩家公司並達成業務上的合作，統一雙方的即時通訊系統，使得訊息得以在不同的企業中做聯邦傳送。狀態資訊服務通訊協定的相關文件，包含有：RFC 3265、RFC 3856、RFC 3857、RFC 3858。其中 RFC 3858 使用 XML 語言來傳遞狀態

資訊，正是本研究所採用的標準。

(二) 網路安全模型：對於網路安全的部份，RFC 2828 有效地將安全攻擊區分為被動式攻擊(Passive Attacks)與主動式攻擊(Active Attacks)。被動式攻擊的本質就是竊聽或監視傳輸中的線路，攻擊者的目標就是取得傳輸中的資訊。兩種典型的被動式攻擊是解讀訊息內容(Release of Message Contents)和流量分析(Traffic Analysis)。被動式攻擊通常很難被偵測到，因為攻擊者並不會更動資料，使用加密的方式，可以預防這類攻擊。因此，在處理被動式攻擊時，強調的是預防，而不是偵測。而主動式攻擊涉及資料的竄改與假造，它的攻擊方式分為下列四種，偽裝(Masquerade)、重送(Replay) 、修改訊息(Modificaiton of Messages)、讓服務失敗(Denial of Service)。主動式攻擊無法完全被預防，必需採取偵測方式，並且將被破壞或拖延的系統修復。要達到保護資訊傳輸不受攻擊者的破壞，通常採用兩種作法，一是在資料轉換時，對資訊加密；二是利用加密鑰匙讓攻擊者無法得知機密訊息[8]。

(三) 密碼學技術：密碼系統(Cryptosystem)就是將原先的明文(Plaintext)，即原始訊息，經由某種轉換而成另一偽裝形式，稱之為密文(Ciphertext)，即編碼過的訊息。唯有經過授權的人才可將其還原，這種將明文轉成密文的過程稱為加密(Encryption)；反之，將密文轉回明文的過程稱為解密(Decryption)。為防止明文輕易被未授權的人獲知內容，發送者必須選擇一個參數用來轉換明文成為不同的密文，而這個參數就叫做加密金鑰(Encryption Key)；相對地，接收者用來解開密文的參數則叫做解密金鑰(Decryption Key)。由許多加密架構所組成的學問就稱為密碼學(Cryptography)，這樣的架構我們稱之為密碼系統(Cryptography System)，或密碼(Cipher)。金鑰密碼系統可分為私密金鑰密碼系統(Private-Key Cryptosystems)與公開金鑰密碼系統(Public-Key Cryptosystems)[10]。本研究用到兩項加密演算法，AES 演算法和 RSA 演算法。其中，AES 演算法是一種私密金鑰密碼系統。私密金鑰密碼系統，其特色是加、解密都是同一把金鑰，所以不知道金鑰的第三者，將無法得知加密後資料的內容。其優點是加密與解密的速度較快(與公開金鑰密碼系統相比)，並且具備簡潔的程式碼，設計簡單易懂。缺點是，當使用者欲和他人通訊，必須與對方分享一把金鑰，因此如果人數多的時候，使用者就得分別維護許多把的秘密金鑰，造成管理金鑰上的問題。RSA 演算法則是屬於公開金鑰密碼系統，能避免對稱式密碼系統在太多人知道密碼時所造成管理上的問題，而其加解密是使用不同的兩把鑰匙[10]。

## 參、系統的分析與設計

本研究所探討的即時語音軟體，主要是以 P2P[6]作為系統架構，並利用 Mifare 卡來記錄節點資訊，試圖去改善單一伺服器在管理與維護上的高成本、當機產生服務中斷，以及資料易被截取等缺點。設計此種 P2P 的即時語音通訊，必須解決下列幾項問題。

- 電腦和 Mifare 卡片間的資料交換：由於 Mifare 只支援有限的儲存空間，因此如何將所需的資料，如個人基本資料，所有聯絡人的資料，連絡的網路位址，加密

金鑰等，利用資料封裝或壓縮的方式儲存在卡片，將是最基本且需解決的問題。

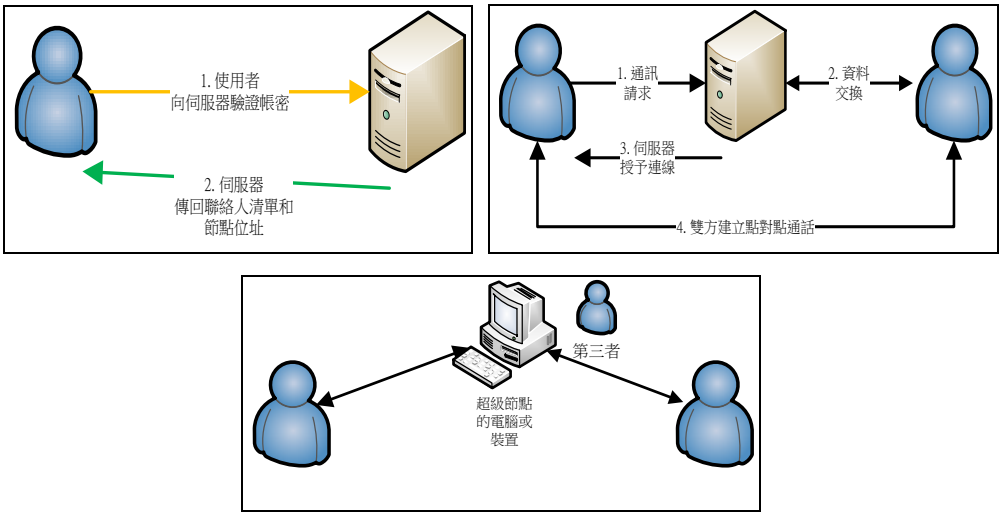
- 如何自動發現網路上的節點：由於使用者可能會將卡片攜至其他電腦使用，或者家裡的上網 IP 可能會被 ISP 在撥接時變更。因此，如何自動發現處於浮動 IP 的節點，便需要有一種找尋的機制。
- 點對點語音傳輸品質：根據 VoIP 標準，兩端點的連線品質要在 200ms 回應時間以內，聲音聽起來才不會有回音的情形發生。然而，另一方面因為需要對封包作加解密，又會產生額外的封包量。所以，如何在兼具安全性與聲音品質上取得平衡點，也是本研究必須克服的問題。
- 加密安全與速度：由於 AES 加密具有效率高的特點，RSA 簽章具有身份不可偽造的特點，但卻比傳統 DES 慢上 100 倍。因此，如何在加密的安全與效能上取得平衡，也是進行本研究所需解決的議題。
- 黑名單功能：若封鎖某一聯絡人時，應能自動拒絕其連線請求。

一、系統分析

(一) 現行軟體

現行的 VOIP 語音通訊軟體，主要是以 Client-Server(主從式)架構的方式設計，大多數軟體的運作流程如下所述。

- 使用者開啟軟體，輸入帳號與密碼登入系統，伺服器回傳所有的聯絡人清單及節點的 IP 位址，如圖 1(a)所示。
- 使用者挑選一個聯絡人進行通話或文字訊息，此時，伺服器會扮演仲介者的角色，提供雙方節點必要的資訊，細部流程如圖 1(b)所示。
- 在通訊軟體如 Skype，若節點間的網路發生大量延遲或遭防火牆阻擋時，而網路上有可高速轉送的超級節點，兩端點的流量將會導向超級節點，如圖 1(c)。



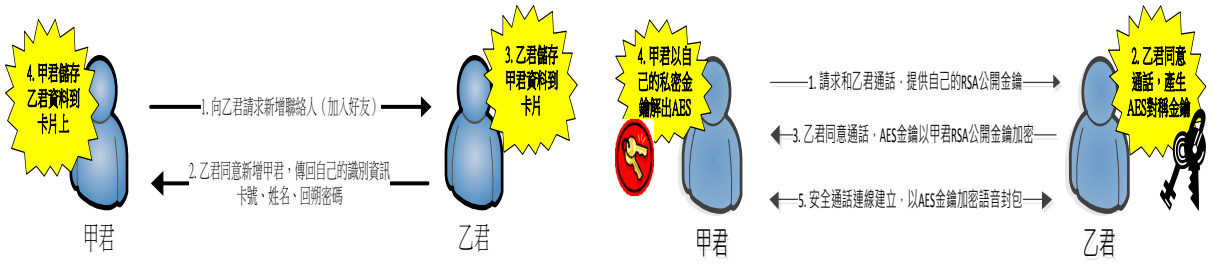

(a) 登入及接收聯絡人資料　　(b) 選取聯絡人進行通話　(c) 利用超級節點進行通訊

圖 1：現行語音通訊軟體的運作方式

值得一提的是，現行的語音通話傳輸不是沒有加密，就是加密極為簡單，容易被有心人士利用並攔截資料。尤其是網路中的「超級節點」這種角色，讓安全性顯得更脆弱，駭客可以藉由重製或偽裝成超級節點來監聽通訊內容。

(二) 本研究作法—基於 RFID 的點對點 VoIP 語音通訊系統

語音通訊較容易遭受的威脅主要在保密性，所以本研究針對此一重要議題，提出有效的改良方法，在通訊的過程中使用安全的加密機制，讓使用者透過 Mifare Card 儲存對方網際網路位址，藉以順利找到對方。而整張 Mifare Card 利用其內建的安全技術，保護所儲存的資料。當新卡片建立時，使用者會被要求輸入一組密碼，來做為卡片的解密金鑰，沒有這組金鑰就無法解密，卡片就無法開啟，因此資料的保密性極高。然而，此種作法由於沒有中央伺服器做為對稱式金鑰轉發，因此需考量對稱式金鑰在兩節點之間如何安全的產生。基本上，我們是採用「大腸包小腸」的方式，將 AES 對稱式金鑰包裝在 RSA 公開金鑰的內部，以確保這組對稱式金鑰的安全不被第三者知悉。另外，可利用每張 Mifare Card 的獨一性來製造全球獨一的 RSA 非對稱式金鑰。圖 2 是本研究所開發的語音通訊軟體的基本運作方式。




(a) 聯絡人清單的運作　　(b) 語音通話的運作

圖 2：本研究語音通訊軟體的運作方式

二、系統架構與功能設計

(一) 系統規劃

本系統在建構即時通訊軟體時，考量以下幾個重要因素：

1. 系統的安全性：如何讓封包在網路中傳遞具備保密性，使用良好的加密演算法是必要的。AES 演算法的金鑰長度是可變的，並且可以抵抗目前現有的密碼攻擊法，執行效率比DES佳，加解密相當快速，程式碼簡潔又適用於各種平台，因此被本研究所採用。另外，為了確保AES金鑰在節點之間交換時的安全，本研究採用RSA公開加密金鑰系統，將產生的AES金鑰加密後傳輸，以便能減少網路頻寬的消耗，並且又能提供即時的語音通話品質。為了確保系統的便利性與使用容易性，我們將使用者的私密金鑰，及聯絡人的資訊，存放於Mifare Card 裡，讓使用者隨身帶著走，提高便利性。由於Mifare Card是以一組金鑰加密記憶體的資料，存取卡片時須提供登入密碼，若輸入錯誤則無法存取資料。

2. 可靠的加密及認證機制：本系統將聲音經過數位化處理後，傳輸資料內容以AES對稱式加密形式發送，全程採UDP協定。為了避免在傳輸過程可能會有網路攔截之虞，因此在雙方電腦交涉產生共用對稱金鑰時，將在外層做RSA非對稱式加密，保證這組金鑰產生的安全。因為訊息是在客戶端加密後傳送，所以，即使攻擊者在傳送過程、或者在即時通訊伺服器進行監

聽或竊取，都無法得知語音的內容，因此確保通訊的絕對安全。

3. 系統的創新與成本考量：結合 Mifare Card 應用於系統，需要搭配讀卡機，方可執行。考量創新帶來的成本，選擇使用最普遍使用又價格便宜的Mifare Card傳統版，搭配非接觸式讀卡機，來實現系統。

4. 採用開放原始碼來開發系統：本研究使用已被廣泛使用的.Net平台與其IDE工具，開發即時通訊軟體的客戶端程式，開發好的軟體具有跨平台的優點。而軟體可在微軟的Windows平台上執行，日後若有需求，稍微經過修改即可用於行動裝置。因此，本系統可以提供使用者在原有的作業系統下執行使用，對於已熟悉操作Windows 作業系統的使用者來說相當方便。客戶端程式將以一個單一檔案的封裝方式呈現，使用者在使用時，不需特別安裝。系統在執行階段會自動解封裝使用，符合綠色軟體的精神。

5. 完全無中央伺服器形式的點對點通話：本研究採用XMPP技術建置語音通話系統，本系統將不依賴中央伺服器，而是節點直接發起連線給另一節點。在新增完成對方的位址資訊、並設定好加密後，日後即可直接通話。考量浮動IP節點的部份，本研究允許聯絡人位址以IP或DNS的方式儲存聯絡人電腦的FQDN。浮動IP電腦可向DDNS服務提供者，如DynDNS或No-IP等取得免費的動態網址來使用。簡單地說，本研究將中央伺服器的「聯絡人列表」直接儲存在使用者節點的持有卡片上，而通話的加密金鑰則仰賴當下動態產生。另外也不透過中繼站來做封包轉送，防止竊聽或詐欺行為發生。

6. 開發人性化的即時語音通訊軟體：基於微軟的 Windows 作業系統具人性化、易於使用者操作、且普遍被大多數使用者使用的情況等考量，加上Mifare Card 與讀卡機亦是在Windows 平台底下操作執行，所以，本研究所開發的VoIP通訊軟體，是在Windows 平台的環境執行。讓使用者減少在學習操作上所花費的時間，提高使用者的接受度。

(二) 系統架構

本系統主要分為五個子系統，分別為 Mifare Card 讀寫元件、Socket 網路傳輸元件、音訊錄放元件、音訊壓縮元件、資料加密元件，如圖 3 所示。另外，獨立開發一套簡易的稽核伺服器，提供商業用途上的稽核使用。

1. Mifare Card 讀寫元件：在 Mifare Card 讀寫元件的部份，主要提供資料與 Mifare Card 之間的傳輸方法。讓軟體能透過 COM 連接埠，從卡片讀取原始二進位資料，並轉換為高階資料供使用者讀取。此元件包含身分驗證登入、並提供讀取、寫入功能。
2. Socket 網路傳輸元件：主要是將數據資料封裝成網路資料流，並且提供點對點的非同步資料傳輸模型。由於同步資料雖然開發較容易，然而若遇上連線障礙，使用者沒有其他選擇。本研究選擇以非同步模式開發，除提供使用者良好的使用經驗外，還提供驗證檢核等功能。

3. 音訊錄放元件：在音訊錄放元件上，將會存取系統的 API 介面，以取得錄製音訊與撥放音訊原始串流的方法，來錄製、播放使用者的聲音。這些錄製、播放的音訊乃是經 PCM 取樣（或還原）的原始資料，將交由音訊壓縮元件去做壓縮（或解壓縮），以降低實際網路傳輸的所需頻寬。

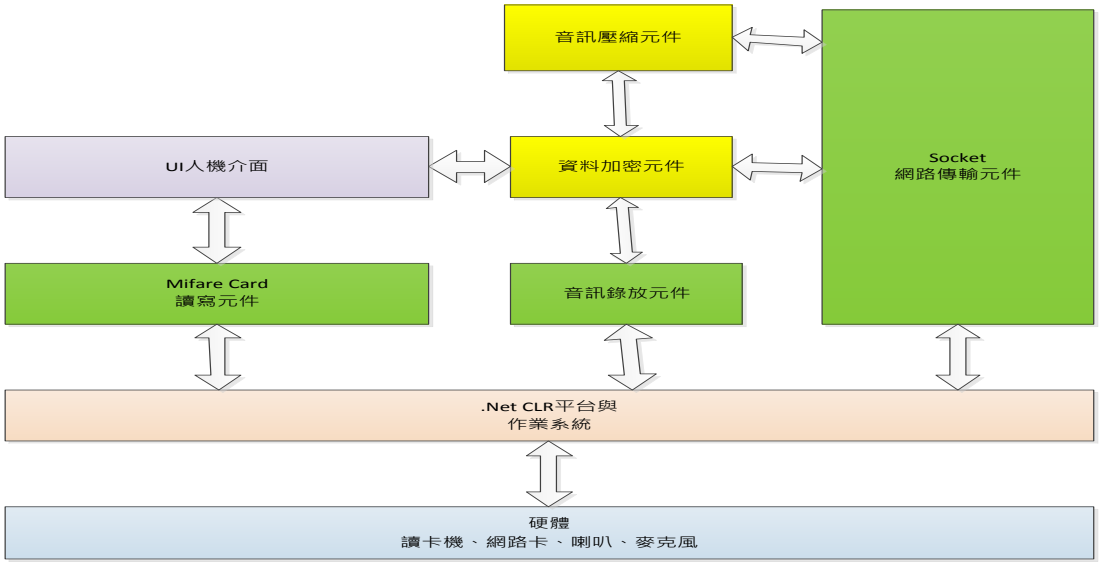



圖 3：系統架構示意圖

4. 音訊壓縮元件：音訊壓縮元件，將針對傳入的原始 PCM 音訊做壓縮，或解壓縮的處理，使得網路頻寬消耗能有效降低。經過壓縮後的二進位資料將交給加密系統做處理。另外收到對方傳來的數位資料，則經過解壓縮後，重新還原為聲音。
5. 資料加密元件：資料加密元件的部份，主要是在兩個節點的傳輸過程中，扮演資料加密的角色，可分為兩大類：控制資料、語音資料加密。控制資料部分，將依照兩個節點每次開啟軟體時所產生的動態 RSA 金鑰，做軟體控制資料傳輸用。語音資料部分，藉由控制資料與另一端電腦，彼此協定所使用的共同金鑰，再將語音資料經過 AES 加密後，交由網路元件傳輸。
6. 稽核伺服器：利用 Web 服務以 SOAP 傳輸協定[5]的方式，設計一稽核伺服器系統。在商業用途上可以記錄通話時間、對象，以及備份聯絡人資訊等。可對卡片做簡易的管理與稽查。

(三) 系統功能設計

系統功能分成兩大部分，其一是通訊軟體主體，另一是稽核伺服器端服務。

1. 通訊軟體主體：它又可分為卡片維護、聯絡人管理、個人資料設定、語音通話、系統設定、資料壓縮及加密。

(1) 卡片維護：通訊軟體的卡片作業模組，具備下列功能。

a. 卡片初始化：如同新硬碟需要格式化一般，使用者新買來一張 Mifare 空白卡，需要進行初始化以便使用，其中包括設定存取的密碼、對卡片記憶體的每一分區做權限設定，以及儲存聯絡人與持卡人的種種資

訊，如顯示名稱、電腦節點位址、還原密碼等。

b. 備份卡片資料庫：考量卡片可能會遺失，本系統設計一項功能，允許使用者備份目前的「正卡」卡片資料到「副卡」。在備份時會提示輸入還原密碼，以便日後做還原卡片資料用。

c. 還原卡片：日後若「正卡」遺失，只要拿出「副卡」，並輸入正確的還原密碼，「副卡」將會自動解密，並被升級還原回「正卡」。而所有聯絡人資料皆不須重新設定，且因金鑰也被一併還原，所以聯絡人那方不須另外重建一次，日後使用者能用所還原的正卡再做一次備份。

(2) 聯絡人管理：聯絡人功能要有新增、修改、刪除三個基本功能。

a. 新增聯絡人：在新增聯絡人時，可以選擇直接指定對方的 IP 或 FQDN 位址，或讓系統利用廣播封包去搜尋網路上所有節點。在雙方完成交握驗證後，系統自動新增一筆聯絡人資訊到 Mifare Card 內，包含對方的顯示名稱、對方的網路位址、災難還原密碼等，如圖 4 所示。日後即可直接選取聯絡人來撥號通話。

b. 修改聯絡人：修改功能可讓使用者修改聯絡人的名稱或 IP 位址，但不能修改對方的還原密碼，因為這組密碼是作為還原識別用。

c. 刪除聯絡人：進行聯絡人的刪除動作。

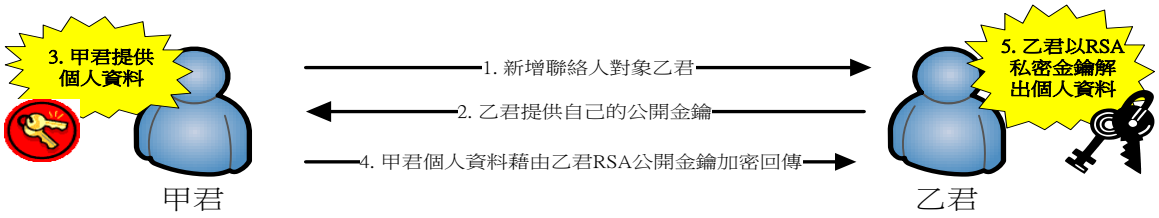



圖 4：新增聯絡人運作流程

(3) 個人資料設定：在開卡時輸入的個人資料，例如顯示名稱，或者主機位址，可藉由修改個人資料介面進行修改。修改後的資料將自動更新到所有聯絡人，若聯絡人不在線上，待對方上線後即自動更新他的卡片資料。

(4) 語音通話：語音通話有撥號、接聽功能，點選某一聯絡人後，即可進行語音撥號。若聯絡方占線時，需等候對方掛斷才可撥入。而連絡方將會出現有插撥，可選擇接聽或掛斷。

(5) 系統設定：可讓使用者設定音效設置、稽核伺服器位址。

a. 音效設置功能：選擇喜好的音訊編碼技術，以及選擇音效設備。音訊編碼部分可選擇 G.711 或者不壓縮；錄音裝置部分使用者可選擇不同的錄音麥克風裝置、放音揚聲器裝置。

b. 稽核伺服器註冊：對於商業環境將會需要記錄外點業務，或者 SOHO 家庭辦公室、衛星工廠之間的通話時，就需要一種稽核機制，來記錄

通話起訖時間、發話與受話對象。另外，在員工遺失卡片時，能提供快速的損壞還原機制。

(6) 資料壓縮及加密：又可分語音資料壓縮及解壓縮、語音資料加密、解密。

a. 語音資料壓縮及解壓縮：由於原始語音的資料量很大，為防止因頻寬不足而造成聲音不清楚或模糊的狀況，所以需要經過壓縮編碼再傳輸，接收後再進行解壓縮。本研究採用行之有年的 G.711 編碼技術來壓縮/解壓縮資料。

b. 語音資料加密：系統將 PCM 編碼後的語音資料，經過 AES 加密演算法，加密成密文資訊。資料加密功能能夠在每次軟體啟動時，動態產生 RSA 加解密金鑰配對，並在每次通話起始前，產生信任的對稱式 AES 金鑰。語音加密的金鑰，在每次通話時都不同。通話起始前雙方已採用控制封包交涉出一組 AES 金鑰。這個隨機產生的 AES 金鑰能防止封包遭攔截時，在短時間內被破解。這組 AES 金鑰將交由網路控制元件去扮演雙方電腦的交易協調角色。

c. 語音資料解密：系統可以將所接收的加密二進位資料，利用 AES 金鑰解密成可讀的二進位資料。

2. 稽核伺服器：主要提供在商業環境中的通話稽核使用，利用 ASP.Net 和 Web 服務，接收來自通訊軟體客戶端的記錄請求，其中包含兩項主要的功能。

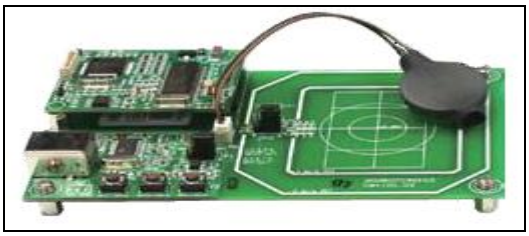
(1) 記錄：當客戶端新增聯絡人或與人通話時，做稽核記錄並存檔到資料庫。

(2) 還原卡片：當客戶端遺失卡片時，提供方法讓客戶端在最短時間內還原。

## 肆、系統實作

本系統採用物件導向開發(OOP)來整合建置，考量整體操作方便性及 Mifare Card 讀卡機驅動程式的支援能力，選擇微軟產品為開發平台。系統開發及執行環境規劃如下：

- 客戶端：作業系統平台為 Microsoft Windows 7 Enterprise，開發工具是 Microsoft Visual Basic 2010 Express，執行平台為 .Net Framework，Mifare Card 讀寫操作為瑞晶資訊的 RFID 套件(RM100)
- 伺服器端：作業系統平台為 Microsoft Windows Server 2008 R2 Web，開發工具是 Microsoft Visual Web Developer 2010 Express，執行環境和編譯器為 .Net Framework，網站伺服器元件為 IIS 7.5。



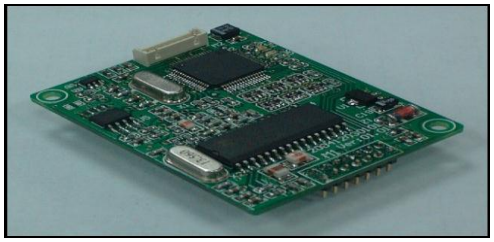


圖 5：瑞晶資訊，RM100-MIC 模組

一、系統環境介紹

本系統的 VoIP 軟體在 Windows 環境下開發及執行，並經由 USB 連結 Mifare Card 讀卡機，由序列埠命令方式進行控制。另外，利用瑞晶資訊提供的 SDK 對 RM100 讀卡機(如圖 5)作相關的讀寫命令。透過非同步呼叫的方式，使得程式得以平行處理的方式操作卡片，最後將這些指令集封裝成類別與函數方便管理。

二、實作成果

1. 登入存取卡片內容：將卡片放置在讀卡機上，並輸入卡片密碼，如圖 6。
2. 卡片初始化：將卡片放置於讀卡機上，點選「新卡」按鈕，即會出現卡片作業選項，如圖 7。選擇「註冊新卡」按鈕，即可依照所設定的卡片密碼、名稱、網路位址、資料還原密碼，來寫入卡片。

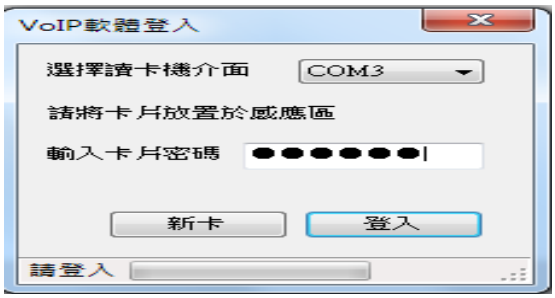



圖 6：軟體登入畫面


圖 7：卡片初始化

3. 聯絡人列表：成功登入後，系統會讀取卡片資料，並顯示在聯絡人清單中如圖 8。
4. 聯絡人管理：點選「聯絡人」選單，即可出現管理按鈕，如圖 9，可進行聯絡人的新增、修改和刪除等動作。


圖 8：聯絡人列表

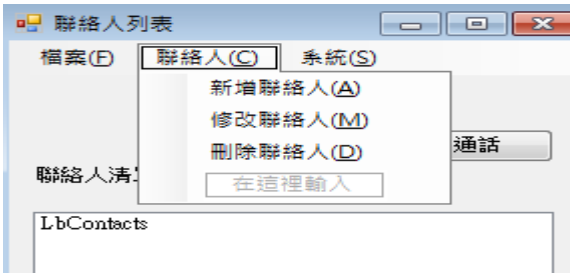



圖 9：聯絡人管理

5. 新增聯絡人：點選「聯絡人」選單，點選「新增聯絡人」即可新增，如圖 10，聯絡人一方會收到請求訊息
6. 進行通話：從聯絡人清單中選取某位聯絡人，再點選「通話」按鈕，即可和聯絡人通話，如圖 11。

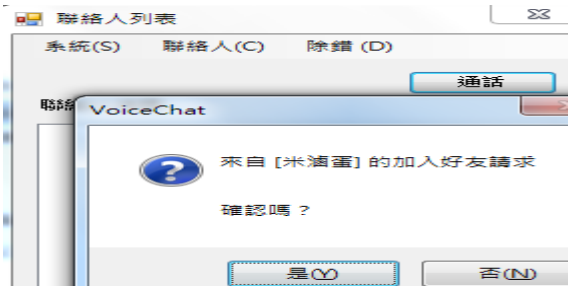



圖 10：新增聯絡人視窗

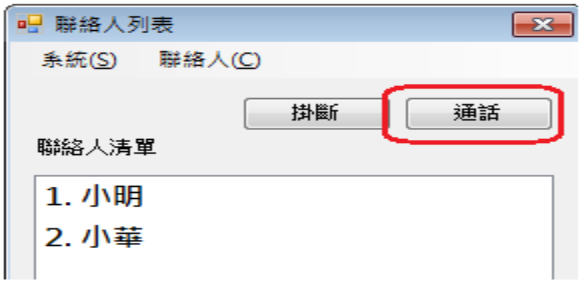



圖 11：與聯絡人通話

7. 卡片資料維護：可藉由卡片維護功能，備份卡片，或者將此卡作廢。如圖 12。
8. 密碼變更：可以藉由「變更密碼」功能，更改登入卡片的密碼。如圖 13。

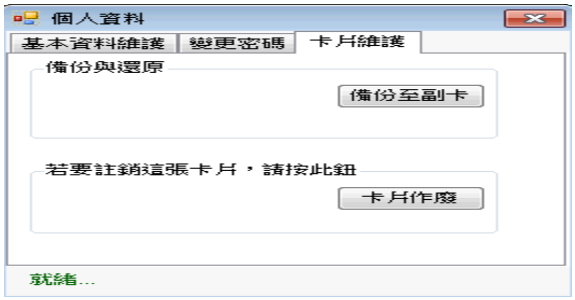



圖 12：卡片維護—備份卡片、報廢卡片

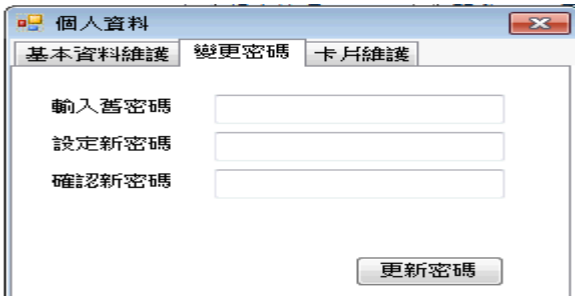



圖 13：變更卡片存取密碼

9. 稽核伺服器端查詢：可以藉由瀏覽器，存取稽核伺服器的網頁，查詢哪些已註冊的卡片，及其所增建的聯絡人清單、通聯記錄等。如圖 14 至 16。

| | | 卡片編號 | 顯示名稱 | 慣用主機位址 | 最後更新 |
|---|---|---|---|---|---|
| 檢視聯絡人 | 通聯記錄 | 2222 | nana | naa | 2012/3/30 上午 11:05:00 |
| 檢視聯絡人 | 通聯記錄 | 1887618332 | 米滷蛋 | MiniEgg.no-ip.org | 2012/3/30 下午 09:37:00 |
| 檢視聯絡人 | 通聯記錄 | 1887622108 | 洋蔥頭 | WhatsIron.no-ip.org | 2012/3/30 下午 09:37:00 |

圖 14：檢視註冊卡片列表

1887618332 查詢

| 編號 | 聯絡人卡號 | 聯絡人名稱 | 聯絡人位址 | 最後更新 |
|---|---|---|---|---|
| 1 | 1887622108 | 洋蔥頭 | WhatsIron.no-ip.org | 2012/3/30 上午 11:27:16 |

圖 15：檢視持卡人的聯絡人名冊

1887618332 查詢

| 紀錄ID | 受話人卡號 | 受話人名稱 | 通話時間(秒) | 起始時間 |
|---|---|---|---|---|
| 9 | 1887622108 | 洋蔥頭 | 354 | 2012/4/2 下午 04:45:19 |
| 8 | 1887622108 | 洋蔥頭 | 167 | 2012/4/2 下午 04:35:12 |

圖 16：檢視聯絡人間的通聯紀錄

三、系統操作流程圖：圖 17 是本軟體的系統操作流程圖。

四、資料傳遞流程圖：圖 18 是本軟體在通話進行中的資料傳遞流程圖。

本研究所實作的語音通訊軟體，在完成時進行了基本的的通訊測試。主要是針對兩位欲進行通話的使用者，小明和小華，在通話進行中刻意將小明的軟體，以除錯的方式

植入錯誤的 AES 加密金鑰。此時，立刻造成小華一方講的話，在小明一方聽起來完全是雜訊；而小明那方所講的話，在小華一方也是雜訊。這樣的結果主要是因本研究採取與坊間各項軟體有別的壓縮加密演算法，也就是以原始語音經過 G.711 編碼器壓縮後，再以 AES 加密技術加密數據資料而成。所以，若沒有正確的解密密碼，自然會得到無意義的語音壓縮資料而不是原始聲音，如雙方喇叭所聽到的雜音一樣。即便以超級電腦來解讀此一 AES 密碼，也因無法取得原始正確音訊資料的明文對照，而不知解開的資料是正確與否。此種測試結果證實，本研究所開發的軟體提供安全的即時語音通訊。

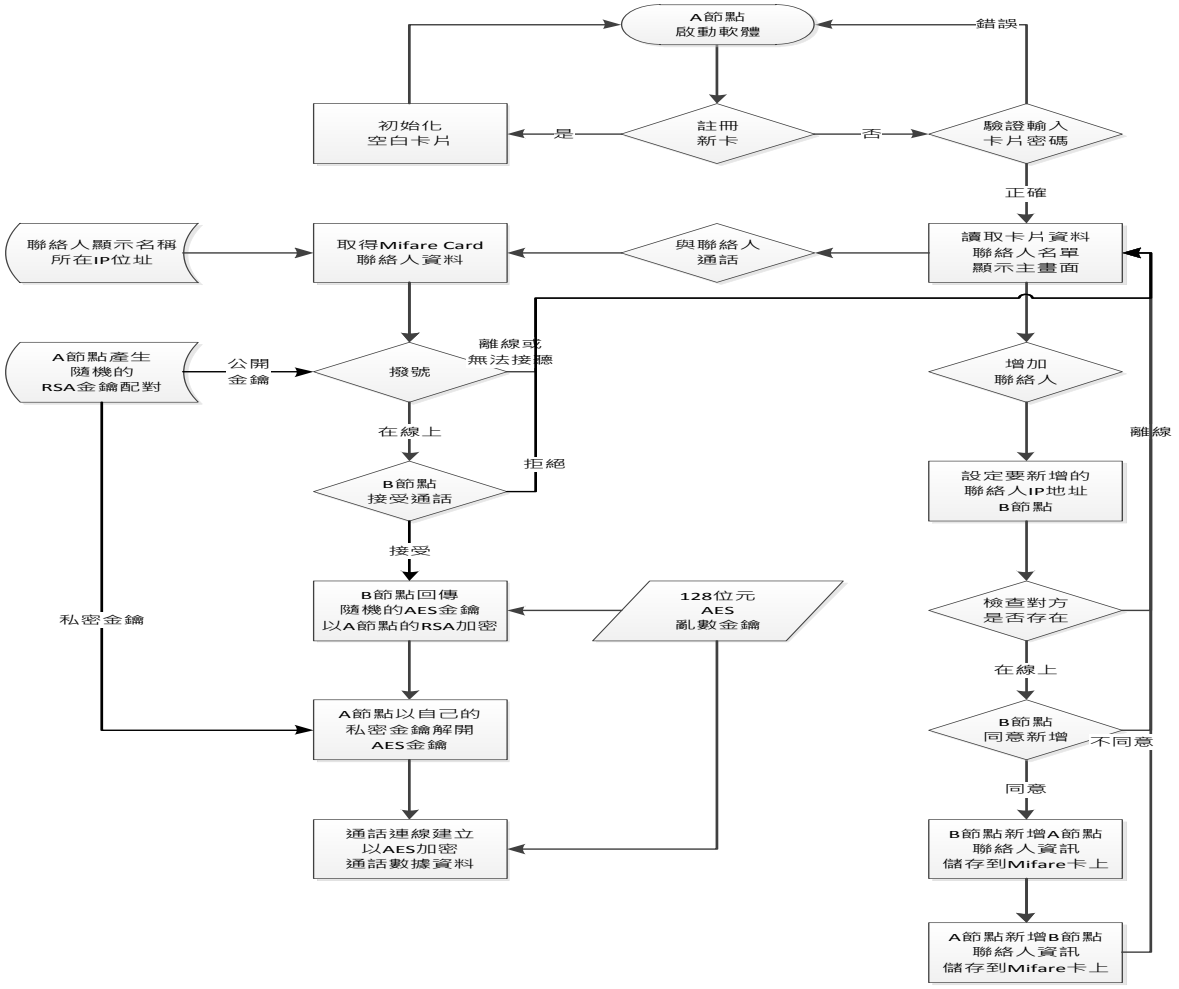



圖 17：系統操作流程圖

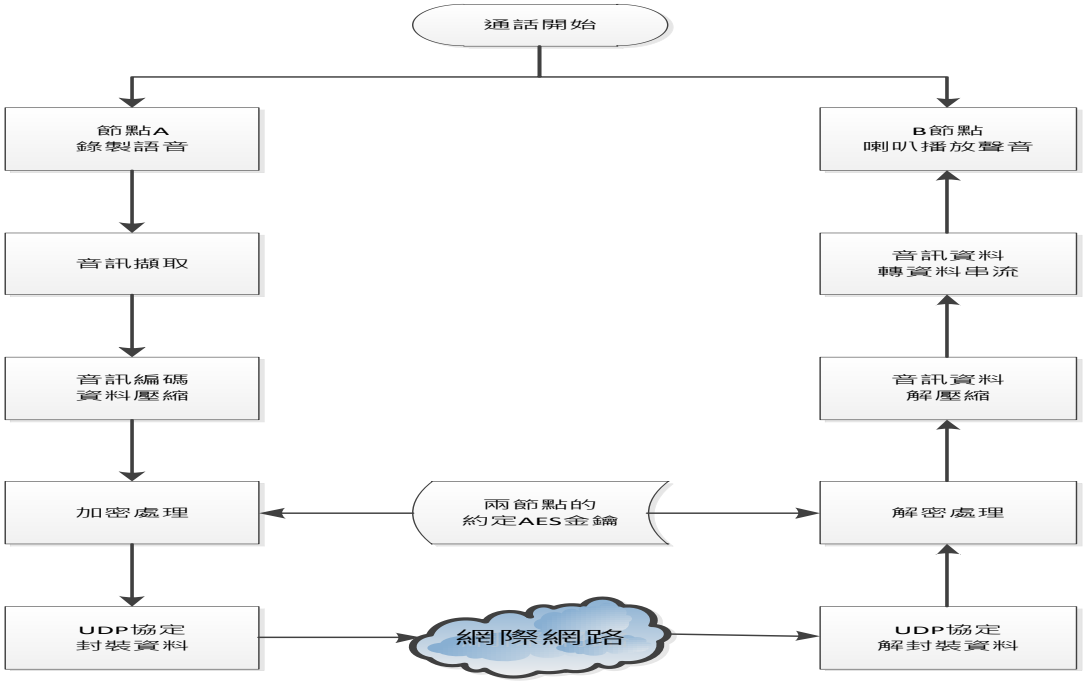



圖 18：通話時的資料傳遞流程圖

## 伍、結論與未來工作

本研究針對目前主流市場的主從式 VoIP 服務架構進行改良，並設計一套安全的網路語音通話軟體。我們採用雙重加密演算法，RSA 與 AES，來兼顧資料傳輸過程的安全性和即時性。此外，也設計了稽核伺服器來管理聯絡人和還原資料用。此一軟體具備的優點有：(1) 語音加密後傳送，內容無法被竊聽；(2) 使用 Mifare Card 儲存聯絡人資訊，增加安全性、自主性及可攜性；(3) 不需要中央伺服器及中繼節點，能解決網路依賴性問題；(4) 利用 G.711 編碼，即使在低頻寬下也能表現良好音質；(5) 低成本的系統開發。本軟體在未來仍有多項工作可繼續進行：(1) 群組通話功能；(2) 傳輸檔案的功能；(3) 解除使用者必須有真實 IP 的限制；(4) 改為較新的 Mifare Plus 卡進行實作[14]。

## 參考文獻


1. MSN 怪怪自動封鎖人？微軟官方論壇教學，
   http://www.nownews.com/2011/02/21/11622-2690706.htm
2. Skype 故障原因：軟體臭蟲引起超級節點超載連鎖反應，
   http://www.ithome.com.tw/itadm/article.php?c=65271
3. Skype 前景成疑：微軟新專利可竊聽 VoIP 通話，
   http://news.cnyes.com/Content/20110628/KDXHJNQQ9QNM6.shtml
4. TWCERT 專欄,2006,即時通訊軟體使用建議與相關安全防護
5. 朱政杰(民 97),以 SOAP 為基礎的異質平台監控系統研究
6. 郭麗淑(民 93),以 P2P 為基礎的移動式即時通訊

7. 彭俊豪(民 98),以 SIP 為基礎提供合法監聽之功能
8. 楊中皇(民 95),網路安全理論與實務。台北：金禾資訊
9. 劉建志(民 95)，細說即時傳訊，取自：http://www.itmag.org.tw/magazine/article_single_26.htm
10. 賴溪松、韓亮、張真誠(民 93),近代密碼學及其應用,旗標出版
11. 全球即時通訊市場統計 2011-Q2，http://www.opswat.com/sites/default/files/OPSWAT-Market-Share-Report-June-2011.pdf
12. 電信法, http://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=186&sn_f=1067
13. Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on Fon-iks, White, A.M. Matthews, A.R. Snow, K.Z. Monrose, F. Page(s): 3 – 18, Digital Object Identifier : 10.1109/SP.2011.34
14. Reverse-Engineering a Cryptographic RFID Tag, Karsten Nohl and David Evans, University of Virginia; Starbug and Henryk Plötz, Chaos Computer Club, Berlin, USENIX Security '08 Refereed Paper Pp. 185–193 of the Proceedings

# Peer-to-Peer VOIP System Based on RFID

Chih-Horng Ke

Department of Information Management, Chang Jung Christian University

kech@mail.cjcu.edu.tw

Jen-Hang Wu

Department of Information Management, Chang Jung Christian University

r26911013@mailst.cjcu.edu.tw

## Abstract

Due to the popularity of the network and the lower rates of telecommunications, people gradually contact with each other via the internet in a more convenient and more immediate way. The two most representatives are the IM and VoIP, and MSN(IM-type) and Skype(VOIP-type) have become the popular communication tools. However, these software are not absolutely safe, for example, there is no strict encryption or no encryption at all, thus they cause a lot of issues of privacy and security. So, how to guarantee that users can safely use the software for calling or messaging and would not be intercepted by others is an important issue. In this study, we use the Microsoft .Net platform and P2P technology, as well as AES and RSA algorithms, to implement a safe and efficient VoIP communication system. Moreover, we use the Mifare Card to store the information of contacts and security key in order to increase the convenience of carrying.

Keywords: Voice over IP, Point-to-Point, Mifare Card, Cryptography