VoIP 點對點加密通訊技術導入國軍運用之研究

作者：中華電信研究院

副研究員涂雅晴、研究員林逸修、研究員周自強

提要

一、網路電話在有網路的環境下就能使用，就算是跨國電話也不需要另外負擔價格高昂的長途通訊費用，大幅降低電話通訊的成本，但卻有著通訊品質不佳的缺點，所以在以前的普及率一直不高。

二、隨著網路電話技術以及網路通訊的高度發展，人們的生活習慣與行動網路越來越密不可分，加上網路電話的通話品質也越來越好，使得一般使用者的接受度逐年增加，漸漸成為日常生活中最廣為使用的通訊方式。

三、便利性與安全性兩者通常很難共存，在如此便利且低成本的網路電話技術之下，隨之而來的是通訊間的安全性問題，而我們透過點對點加密技術開發 Secure VoIP App，補足網路電話在安全性上的缺失，讓使用者可以安心的使用網路電話服務。

關鍵詞：網路電話(Voice over Internet Protocol, VoIP)、點對點加密(End to End Encryption, E2EE)、秘密通訊。

前言

過往人們使用電話透過公用交換網路(Public Switched Telephone Network, PSTN)進行語音通訊。由於全球數位匯流的蓬勃發展，網路以及與其相關的技術也相對成熟且多樣化。漸漸的可以使用網路電話的數位裝置也顯然成為人們生活中不可或缺的必需品。

在網路與人密不可分的生活中，網路電話也可以提供使用者傳統電話所擁有的功能：撥打電話以及接聽電話。雖然目前網路電話的通話品質與傳統電話尚未能相比，但是卻能大幅降低使用者的語音通訊成本，不論是國內外通話，皆只需要負擔網路頻寬的費用，不再需要其他成本。以企業成本做考量的公司行號是最先接受此通話方式的族群。隨著近期網路電話技術的蓬勃發展，以及功能上的多樣性，漸漸的一般使用者也開始接受此通訊方式。因為只要擁有可連網能力的數位裝置，就能透過Facebook Messenger、Line、Skype…等即時通訊軟體，藉由網路傳送訊息以及撥打網路電話，不需要額外付出語音通訊的費用。

然而，2016年，英國廣播公司(British Broadcasting Corporation, BBC)報導國際特赦組織對市面上16款主流通訊軟體的安全性排名調查。[1]此排名根據通訊軟體是否擁有或預設使用點對

[1] Amnesty international, “Snapchat, Skype among apps not protecting users’ privacy,” Amnesty international, https://

點加密功能，是否告知使用者存在的風險等五項檢測標準作為評分依據，結果顯示並沒有任何一款通訊軟體得到滿分。此外，雖然根據評測報告顯示Line已使用點對點加密技術為使用者做安全性的把關，但是Line在2018年所發布的透明度報告中提到：Line可以在特定情況下為全球執法機關提供解密的訊息內容。[2]間接說明透過Line傳遞的文字或是語音訊息是可以被截取或是監聽的。這也表示在現代生活中廣泛被使用的網路通訊，雖然便宜又方便，卻也相對的不受保障，容易有被竊聽或從中截取訊息的風險。

鑒於以上，我們提出以點對點加密為基礎，提供使用者安全的網路通訊環境，再搭配硬體元件Slim SIM，提升手機使用的安全性，使得使用者在不安全的網路下，也可以安心地進行安全的語音通訊。

背景介紹

一、公用交換電話網路

公用交換電話網路是採用電路交換方式的通訊網路，連結起想要通訊的雙方。由於此種通訊方式是透過電路的交換，建立起一條專屬的通路直到釋放，此段時間的頻寬只能被兩端點的設備使用，所以設置成本較高，且通訊網路資源使用率也較差。但由於是建立一條雙方的專屬通道，相對來說可靠性與穩定性也較好，因此依然為目前全球通訊最大的網路。

二、網路電話

網路電話，顧名思義是透過網路來進行語音通訊，讓接收方能夠聽到傳送方的聲音，達到類似傳統電話的一種技術。網路電話會受到歡迎的主要原因與智慧型行動裝置的普及有極大的關聯。由於網路電話是運用網路作為傳輸工具，所以隨著行動網路的普及，使得網路電話的可攜性大大提升，只要具有連網能力的手機、平板甚至是電腦，皆能使用即時語音通訊的服務。

在網路電話中，對話啟動協定(Session Initiation Protocol, SIP) 是其中一種規範標準，目前廣泛的被使用且蓬勃發展，用於建立、修改以及終止語音、視訊、即時通訊…等互動式對談。[3]SIP不只可以提供即時語音通話服務，也可以為視訊等其他語音加值服務提供介接介面，是用於網路電話中最主要的協定之一。

雖然網路電話是透過網路傳遞訊息，潛在許多安全及隱私上的風險，但是我們可以將金鑰交換、加密技術應用在數位化的語音產品上，因此可以做到比傳統使用公用交換網路的電

---

www.amnesty.org/en/latest/news/2016/10/snapchat-skype-among-apps-not-protecting-users-privacy/, 2016/10/21, (2020/02/03).

[2] Line，〈LINE 發布透明度報告(2017 年 7 月至 12 月)〉，《Line Corporation》，https://linecorp.com/zh-hant/pr/news/zh-hant/2018/2167，2018/04/24，(2020/05/21)。

[3] 〈對話啟動協定〉，《維基百科》，https://zh.wikipedia.org/wiki/%E5%B0%8D%E8%A9%B1%E5%95%9F%E5%8B%95%E5%8D%94%E5%AE%9A，(2020/05/25)。

話更安全的保障。

三、網路電話伺服器(VoIP Server)

網路電話伺服器的工作類似代理者的角色，VoIP電話軟體可以透過網路撥打給VoIP電話軟體或是透過PSTN撥打給一般傳統電話，建立一條透過網路傳輸的語音通道，提供網路電話的呼叫服務，是一種使用網路協定的用戶專用交換機系統(Private Branch Exchange, PBX)。IP-PBX(IP-Private Branch Exchange)內紀錄所有的用戶以及與其相對應的SIP帳號資訊，所以能夠透過網路進行撥打傳統電話或是網路電話呼叫服務。[4]

四、D-H 金鑰交換(Diffie-Hellman Key Exchange, D-H)

D-H金鑰交換是一種金鑰交換的演算法，可以在開放的網路環境下，讓不認識的通訊雙方透過訊息交換，生成一把只有通訊雙方知道且對稱的一次性會談金鑰(Session Key)。此會談金鑰用於加密通訊雙方的訊息內容。

D-H金鑰交換是傳輸層安全性協定(Transport Layer Security, TLS)的基礎，但是有個致命的缺點，容易受到中間人攻擊(Man-in-the-Middle Attack, MITM)。[5]因為在D-H金鑰交換的過程中，缺少對通訊雙方做身分認證的機制，使得任何人都可以冒充成為通訊的參與者開始進行通訊。

五、傳輸層安全性協定

在1999年，國際技術規範組織(Internet Engineering Task Force, IETF)將安全通訊協定(Secure Sockets Layer, SSL)標準化，公布採用主從式架構(Client－serverModel)且與應用層協定無耦合性的傳輸層安全性協定，為透過網路傳輸的資訊提供一個安全的通道，保證資訊傳遞時的私密性。

資料使用傳輸層安全性協定透過網路傳遞的過程中，會先對使用者與伺服器進行單向或雙向驗證，確保資料傳輸兩端點的合法性；再透過兩端點間的金鑰交換，生成一把會談金鑰；最後再將資料透過此金鑰進行加密，直到傳輸結束。此過程可以避免資料在傳輸的過程中被竊聽或是攔截，保障網路通訊的安全及資料的完整性。

六、安全即時傳輸協議(Secure Real-time Transport Protocol, SRTP)

即時傳輸協議(Real-time Transport Protocol, RTP)是一種網路傳輸協定，詳細規範透過網路傳輸語音以及視訊的標準封包規格。[6]而安全即時傳輸協議是以即時傳輸協議為基礎，加強提供RTP傳輸封包的保密性(Confidentiality)、訊息身份驗證(Message Authentication)以及重複

---

[4] S. Khan, N. Sadiq, “Design and configuration of VoIP based PBX using asterisk server and OPNET platform,” 2017 International Electrical Engineering Congress (iEECON), 2017, pp.1-4

[5] Nan Li, “Research on Diffie-Hellman key exchange protocol,” IEEE 2nd International Conference on Computer Engineering and Technology, 2010, Volume 4, pp.634-637

[6]維基百科，〈即時傳輸協定〉，《維基百科》，https://zh.wikipedia.org/wiki/%E5%AE%9E%E6%97%B6%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE，(2020/05/25)。

傳遞(Replay Protection)之保障。之所以會有SRTP的設計架構出現，是因為一般靜態檔案傳輸時所使用的安全協定並不適用於即時串流。即時的串流資訊對於頻寬的限制高、傳送錯誤的容錯能力低、延遲性的敏感度以及終端運算能力的限制等問題，實作在過往靜態資料的傳輸協定上會不符合其需求。為了解決以上的問題，造就安全即時傳輸協議架構的誕生。除此之外，安全即時傳輸協議的架構也非常具有彈性，便於往後功能擴充以延長協議的壽命，所以非常適合用於網路電話。

七、點對點加密

近年來科技技術日益強大，消費者的隱私權意識也逐漸抬頭，而最近受到高度關注的區塊鏈技術，也是在這波重視隱私性的浪潮下產生，標榜去中心化服務，是個高度隱私及安全的技術。以網路電話服務來說，需要有個伺服器來協助處理兩端通訊的服務，既然有個服務中心的角色，那麼誰又能確保此角色不出問題呢?這樣的想法導致使用者開始注重訊息的隱私權問題，擔心本身的訊息會被有心人拿去做其他的用途。

點對點加密的出現就是讓使用者能夠擁有專屬的金鑰，當使用者雙方開始進行通訊時，會先透過系統進行金鑰交換，產生一把會談金鑰，之後的訊息從發送端至接收端之間皆會以此會談金鑰加密的方式傳送。因為只有發送端與接收端擁有此會談金鑰，並無第三方擁有，所以只有他們可以對設備上的訊息進行加密及解密。在傳輸的過程中，每個訊息封包都是獨立加密的，所以不論是提供服務的供應商或是攻擊者均難以破解，能保障訊息在傳輸途徑間的安全，防止有心人從中竄改或是竊聽訊息，是一種具備高度隱私的訊息傳遞方式。

八、線上憑證狀態協定(Online Certificate Status Protocol, OCSP)

數位憑證認證機構(Certificate Authority, CA)主要的工作是核發以及管理數位憑證，為一具公信力且受信賴的第三方。以往確認數位憑證是否有效或是已被註銷，需要從數位憑證認證機構取得憑證吊銷列表(Certificate Revocation list, CRL)，經過長時間的使用，憑證吊銷列表的檔案內容會越來越大，也使得更新週期越來越長。

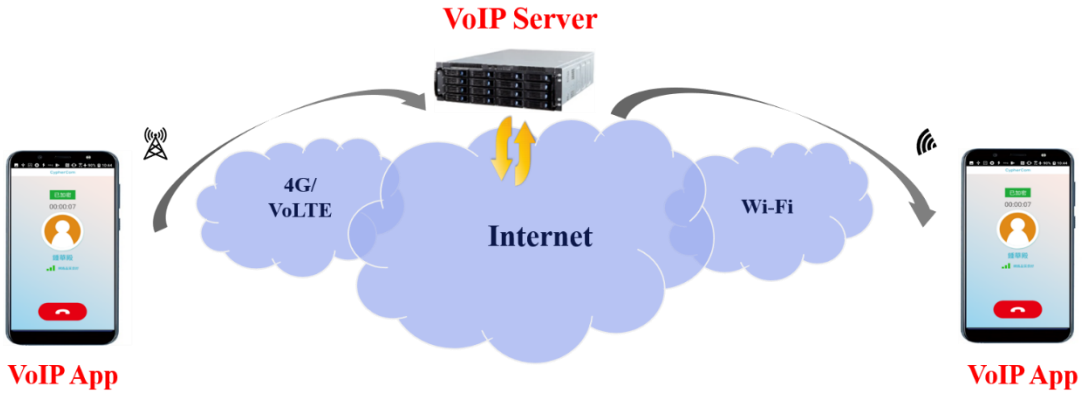
為了改善憑證吊銷列表檔案內容大以及更新週期長的問題，造就線上憑證狀態協定的出現。此協定的目的為提供線上動態憑證狀態查詢，允許單次只查詢單張憑證狀態，不再需要將冗長的憑證吊銷列表全部下載下來，避免因為更新週期長而產生安全性上的風險，讓我們能更即時的掌握憑證撤銷狀態。此外，線上憑證狀態協定可以根據使用需要來客製查詢狀態，使得應用程式在開發上擁有更多的彈性。

設計驗證與比較

在具有網路(包含Internet、4G、Wi-Fi)的環境下，使用者就可以透過網路電話進行網路通話。網路電話的基本架構如圖一，我們需要有具備網路電話服務的應用程式，如行動裝置上的即時通訊軟體，以及應用程式開發者所提供的網路電話伺服器，如此一來，我們就能透過

網路並利用網路電話應用程式進行網路通話。

圖一 網路電話基本架構圖



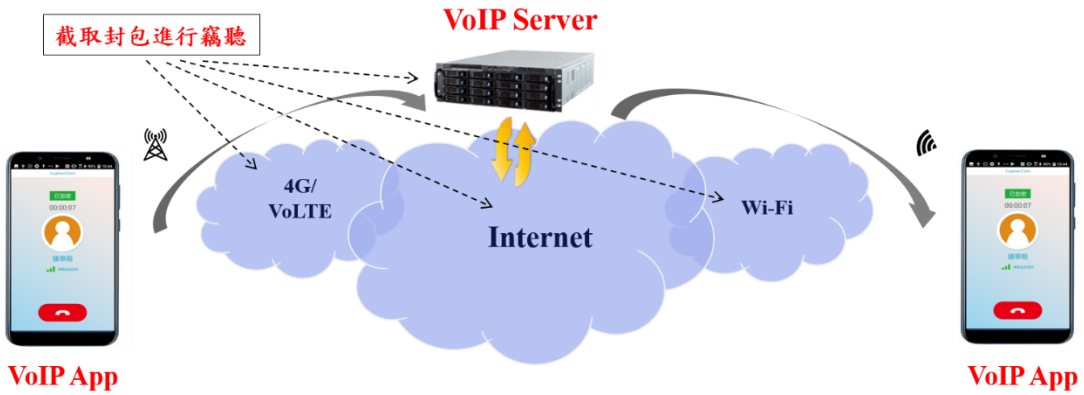
資料來源：作者繪製。

然而，在不被信賴的網路環境下，傳輸的資訊不受保障，潛在著許多隱私問題，有著極高的被竊聽風險。如圖二所示，在不安全的網路環境下，有心人士可以從多個點對通話進行竊聽與攻擊，進而獲得自己想要的訊息。所以，為了不讓使用者的訊息暴露在危險的環境中，通話的安全對網路電話來說是非常重要的。

一、網路電話的發展

隨著網路電話日益蓬勃的發展以及功能上的多樣化，慢慢地取代公用交換電話網路成為一般人最能接受的通話方式。網路電話透過各種數位技術強化了公用交換電話網路，創造出更安全的通話環境，使得普及率逐漸提高。

圖二 網路電話架構被攻擊之示意圖

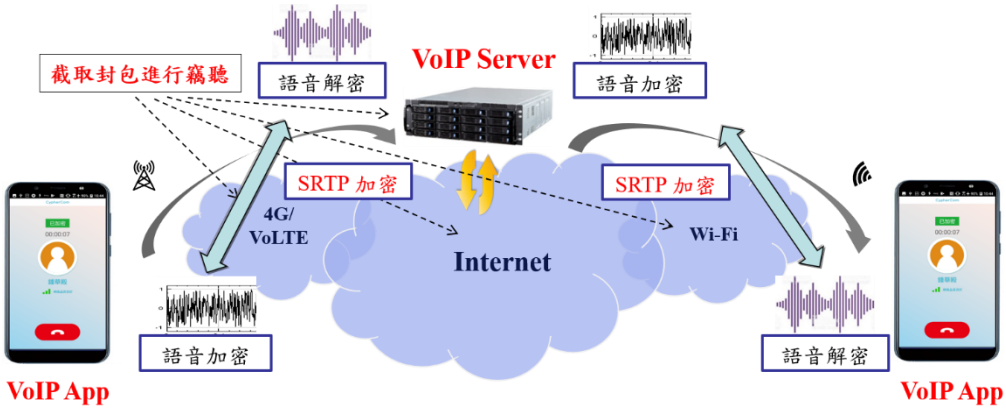


資料來源：作者繪製。

市面上充斥著許多含有網路電話功能的即時通訊軟體，為了保障使用者通話的安全，大多使用安全即時傳輸協議建立語音通訊通道，為使用者的通訊安全把關。如圖三所示，在語音訊息透過安全即時傳輸協議傳輸過程中，已加密之語音訊息經過網路電話伺服器時，會先對語音進行解密以及再加密的步驟，最後才會輾轉抵達接收端，解析成語音資訊讓接收者聽

到。在此種架構下，無法避免網路電話伺服器握有可以將使用者已加密訊息還原之金鑰的缺點，產生使用者對語音通話在網路環境上傳輸的疑慮。

圖三 使用安全即時傳輸協議之網路電話架構圖



資料來源：作者繪製。

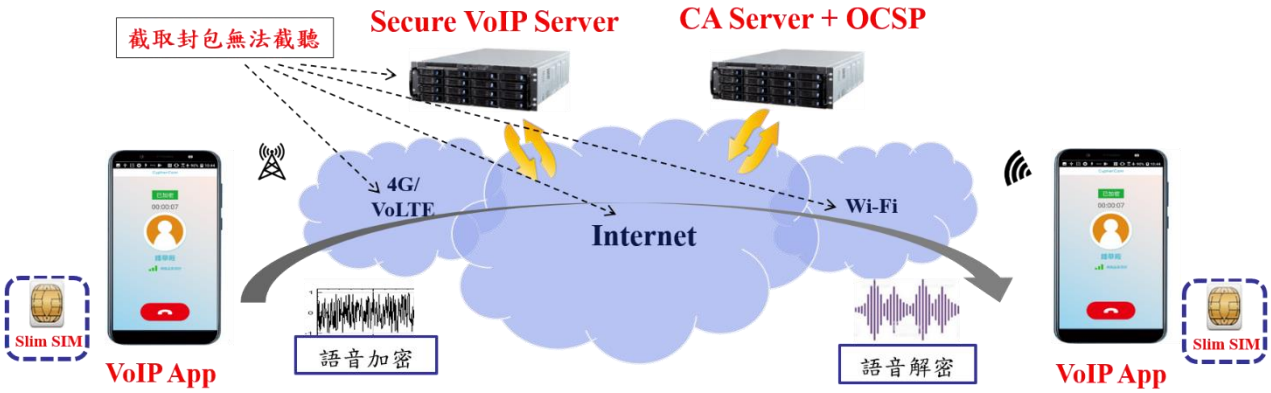
除此之外，在安全即時傳輸協議中，SIP是以明文定義的，訊號建立時才會開始進行加密，已加密封包也有可能會被有心人截取後進行竊聽。

二、服務架構與流程

為了解決上述的問題，我們實現一個以點對點加密技術為基礎，能真正針對通話兩端進行點對點加密通話的高度私密性通訊App - Secure VoIP App。此通訊App能夠讓使用者雙方的通話不經過網路電話伺服器還原加密音訊的過程，即可將加密音訊原封不動的傳遞到接收端，真正的保障使用者的通訊安全。

Secure VoIP App與點對點秘密通訊系統的架構如圖四，主要分為五個部分：

圖四 Secure VoIP App 與點對點秘密通訊系統架構圖



資料來源：作者繪製。

(一)語音加密

採用點對點加密技術，使用可防止中間人攻擊且具備向前保密機制(Forward Secrecy, FS)之ECDHE-RSA非對稱加密演算法，再加上系統時間參與金鑰交換，以防止重送攻擊(Replay

Attack)，最後協商出256位元之會談金鑰，對語音封包進行加密，強化網路電話的通訊安全。

(二)Slim SIM 硬體貼片

配發一組用於點對點秘密通訊之電話號碼，並將數位憑證以及私密金鑰存入Slim SIM中，用於計算認證身分之數位簽章，且不須更換手機SIM卡，即可整合網路電話傳輸。用於Secure VoIP App之Slim SIM已取得ICP-Brazil法規(ICP-Brazil Standard Cryptographic Module)制定的安全驗證許可證書[7]並且選用通過NIST(National Institute of Science and Technology)、FIPS(Federal Information Processing Standards)140-2 Level 3安全認證之卡片作業系統(Card Operation System, COS)。[8]

(三)VoIP App

運用雙向傳輸層安全性協定、安全即時傳輸協議，提供安全的加密網路通話功能。

(四)Secure VoIP Server

為VoIP App建立語音資料的安全傳輸通道，提供網路電話呼叫服務。

(五)CA Server、OCSP

搭配數位憑證認證機構(CA)核發憑證，且透過線上憑證狀態協定提供即時驗證憑證狀態，支援多時機點檢驗，加速身份驗證效率。

在此架構下，我們使用安全即時傳輸協議以及雙向的傳輸層安全性協定，並且選擇比D-H金鑰交換更安全的ECDHE-RSA非對稱加密演算法，使得使用者與伺服器之間能夠進行雙向驗證，也讓用於訊息點對點加密的會談金鑰可以抵禦中間人攻擊。

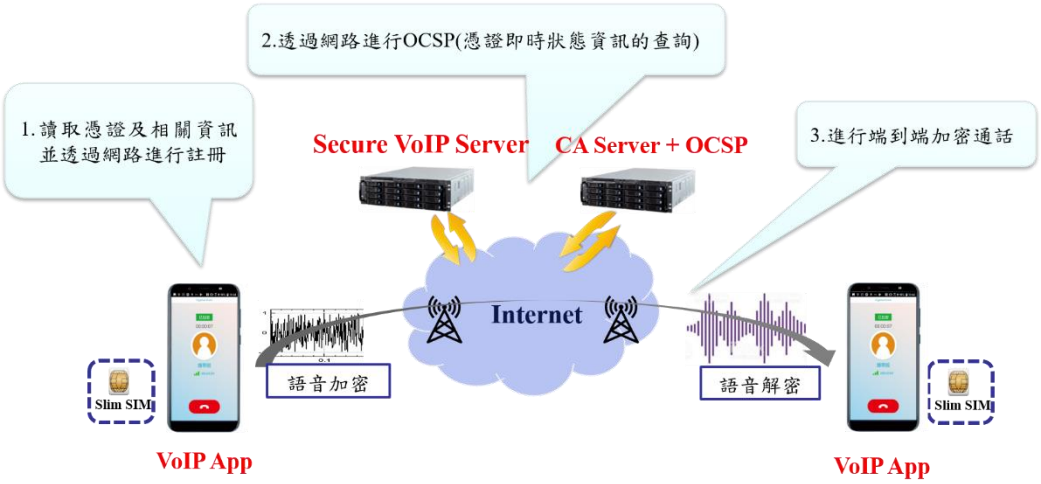
通訊雙方在金鑰交換的過程中，需要先從硬體貼片Slim SIM中取得數位憑證與其他使用者相關資訊，經過線上憑證狀態協定的使用者身分驗證後，才會開始進行產生會談金鑰的訊息交換，最後生成一把具備高度安全性的會談金鑰。

Secure VoIP App的系統架構除了解決在D-H金鑰交換過程中可能遭遇的中間人攻擊風險，也保留D-H金鑰交換的前向安全保密能力。藉此確保用於加密訊息的會談金鑰除了發送端與接收端外，不會有第三方擁有，實現真正針對通訊雙方的點對點加密技術，保障用戶訊息在不安全環境下的傳遞安全。另外，由於我們將私密金鑰與數位憑證儲存在硬體貼片Slim SIM中，所以即使是開發者也無法獲得使用者的隱私資料，也保障使用者終端設備的安全。

[7]〈太思科技集團和 Vantage IT 宣佈通過巴西國家科技與信息協會的安全許可，為 A3 證書提供行動解決方案〉，《太思科技》，https://taisys.com/news-detail?lang=zh&id=3c7bKQSUs6DmmaIIVYXds6q9J2OQStgfzQul8 BKisA，2019/12/03，(2020/05/21)。

[8]〈太思科技 SIMoME® Vault 獲得 FIPS 140-2 Level 3 驗證核可〉，《太思科技》，https://www.taisys.com/news-detail?lang=zh&id=13f00_iX_YdycsHXTkwbPVnahOHXlDwgkAyn4FJscg，2019/04/17，(2020/06/29)。

圖五 Secure VoIP App 使用流程圖



資料來源：作者繪製。

Secure VoIP App的使用流程如圖五所示，App開啟後先從Slim SIM讀取數位憑證與使用者相關的資訊。接下來，將取得的使用者相關資訊向網路電話伺服器進行註冊。註冊時，網路電話伺服器會透過數位憑證認證機構即時驗證使用者資訊。直到網路電話伺服器回覆註冊成功後，才可以開始使用Secure VoIP App的網路電話撥接功能。網路電話撥出後，即開始進行點對點加密之網路通話。

三、Secure VoIP App 與目前市面上網路電話產品之安全性比較

目前市面上充斥著許多的網路即時通訊軟體，尤其以某L即時通訊軟體(以下簡稱L App)在台灣的普及率最高，所以本篇文章以L App做為比較目標，比較結果如表一。

表一 Secure VoIP App 與 L App 的功能比較圖

項目	CHT	L App
E2EE方案	支援語音加密通訊	支援文字訊息、一對一的語音與視訊加密通訊 勝
端對端之安全加密金鑰的產生機制	有(EDCHE-RSA) 勝	有(其E2EE白皮書：ECDH key exchange algorithm)
硬體安全元件	有，使用Slim SIM 勝	無
CA Server	有，提供可靠的憑證管理 勝	無
OCSP Server	有，提供憑證即時狀態資訊的查詢服務 勝	無
帳號管理	客戶須提出申請，審核通過後才會提供憑證 勝	允許帳號綁定臉書帳號(若臉書帳號被盜，則L App帳號也不安全，近年來通訊軟體詐騙案層出不窮)
憑證停用、廢止	有 勝	無
VoIP App技術	TLS、SRTP	RTP、SRTP

資料來源：作者繪製。

以本篇主要探討的點對點之安全加密金鑰產生機制來說，L App所採用的金鑰交換機制為ECDH-RSA，雖然可以防止中間人攻擊，但是並沒有具備向前保密機制，[9]也無法確認是否具有防止重送攻擊的功能。而Secure VoIP App採用ECDHE-RSA金鑰交換機制，並使用系統時間參與金鑰交換，不僅可以防止中間人攻擊，且具備前向保密機制，也因為有添加系統時間，可以防止重送攻擊。

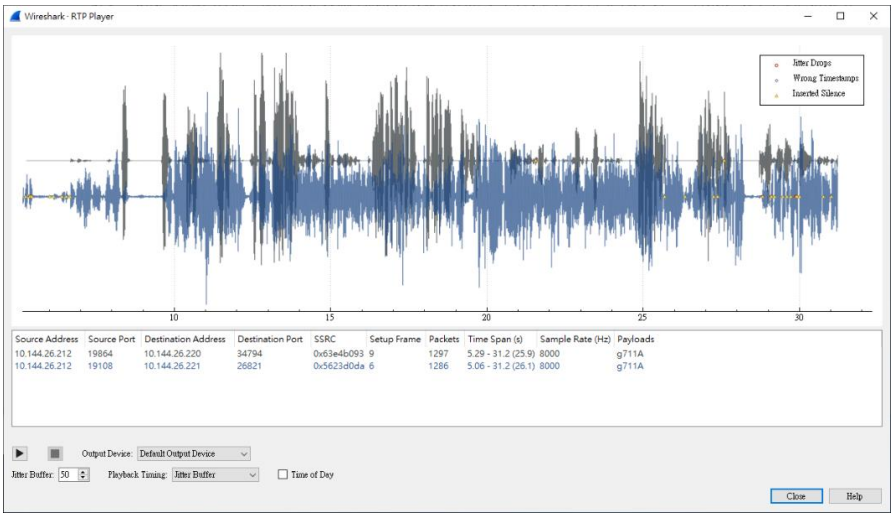
此外，Secure VoIP App採用硬體貼片Slim SIM做為憑證相關資料的儲存管理工具，以及使用CA+OCSP進行用戶帳號憑證管理，相較於L App使用的軟體憑證，以及綁定社群軟體帳號之帳號管理機制，Secure VoIP App對使用者身分驗證以及訊息的安全性相對較有保障。

四、結果驗證

為了驗證Secure VoIP App是否正確地將使用者的語音訊息加密，我們使用網路封包分析軟體－Wireshark來做檢測、截取以及分析封包內容，進而分辨語音訊息是否已經經過加密處理。

在網路傳輸環境中，若為未加密、不安全的通訊，透過Wireshark截取的語音封包分析後(如圖六)，可以明顯地看出此波形依然保持原始的語音波形，且可以清楚地播放出此語音訊息的內容，造成使用者的隱私風險。

圖六 未加密語音封包波形圖

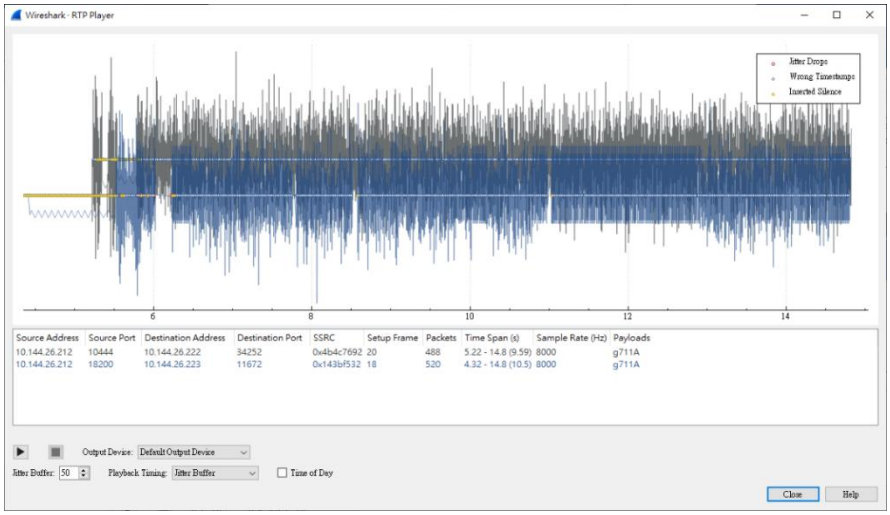


資料來源：截取 Wireshark 軟體分析畫面。

已加密的語音封包波形如圖七所示，我們可以很明顯的發現此波形圖中語音波形的振幅都差不多，顯示此音訊已被加密，且播放後只能聽到雜訊聲，無法聽出原始的語音內容。在沒有金鑰的情況下，攻擊者無法藉由此封包得知語音訊息的內容。

[9]〈傳輸層安全性協定〉，《維基百科》，https://zh.wikipedia.org/wiki/%E5%82%B3%E8%BC%B8%E5% B1%A4%E5%AE%89%E5%85%A8%E6%80%A7%E5%8D%94%E5%AE%9A，(2020/05/21)。

圖七 已加密語音封包波形圖



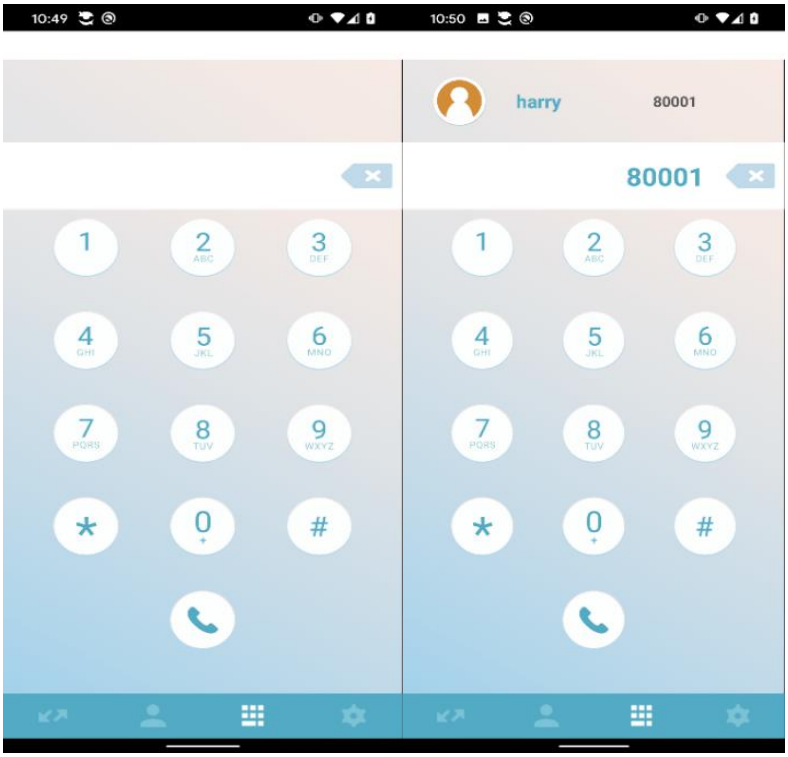
資料來源：截取 Wireshark 軟體分析畫面。

五、Secure VoIP App 發展現況

Secure VoIP App目前已完成基本的撥號功能、整合手機通訊錄功能、加密群組通訊錄下載功能、Slim SIM PIN Code修改功能…等。只要將已配發憑證及通訊門號之硬體貼片 Slim SIM 貼在原本的SIM卡上，並置入智慧型裝置，安裝Secure VoIP App 後，即可在有網路的環境下使用。

Secure VoIP App撥號功能及畫面如圖八(左)，點選撥號功能後，畫面上會顯示欲撥出的號碼如圖八(右)。

圖八 Secure VoIP App 之撥號畫面

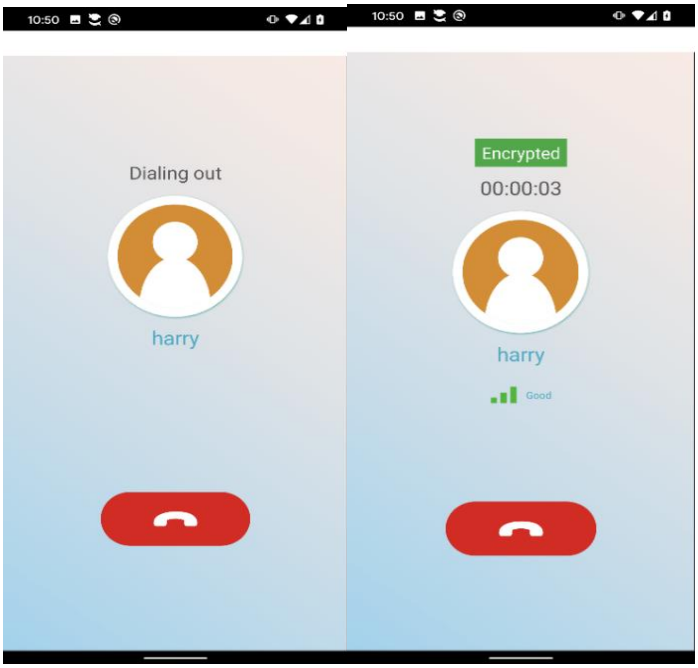


資料來源：截取 Secure VoIP App 畫面。

按下撥出後，畫面會顯示撥出中(Dialing out)如圖九(左)，當對方應答後，畫面如圖九(右)顯示通話中之通話時間，若此通電話為加密電話(Encrypted)，則顯示已加密。若欲結束通話，可按下紅色電話按鈕結束通話。

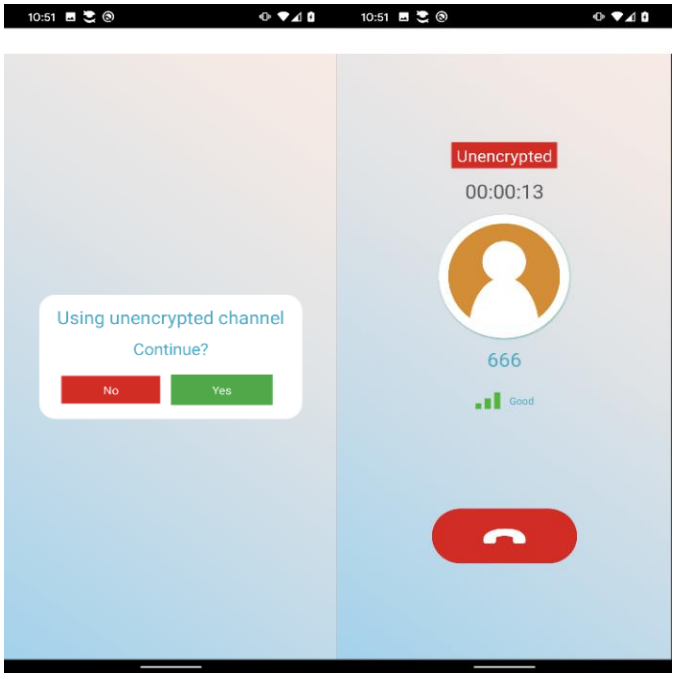
若此撥號對象不具備加密通話功能，則畫面會跳出提示，如圖十(左)，顯示此通話未使用加密通道，詢問使用者是否繼續通話。若按下是，則開始進行未加密通話，且提示使用者此通電話未加密(Unencrypted)如圖十(右)；若按下否，則結束此次通話。

圖九 Secure VoIP App 之撥號中(左)及已加密通話中(右)畫面



資料來源：截取 Secure VoIP App 畫面。

圖十 Secure VoIP App 之未加密提示(左)及未加密通話中(右)畫面



資料來源：截取 Secure VoIP App 畫面。

國軍應用

國軍內部的訊息通常都是屬於機密資訊，除了網路分為內網、外網之外，也會要求軍人在手機上安裝管制軟體，禁止手機在軍用基地內使用藍芽、照相及手機網路分享功能，防止國軍機密外洩的可能。Secure VoIP App是以高度隱私性為出發點所研發出的網路電話通訊軟體，使用點對點加密技術，即使在訊息傳遞途中遭受到第三方的攻擊時，也能保有使用者的隱私及訊息的安全性，導入國軍之SWOT分析如圖十一。

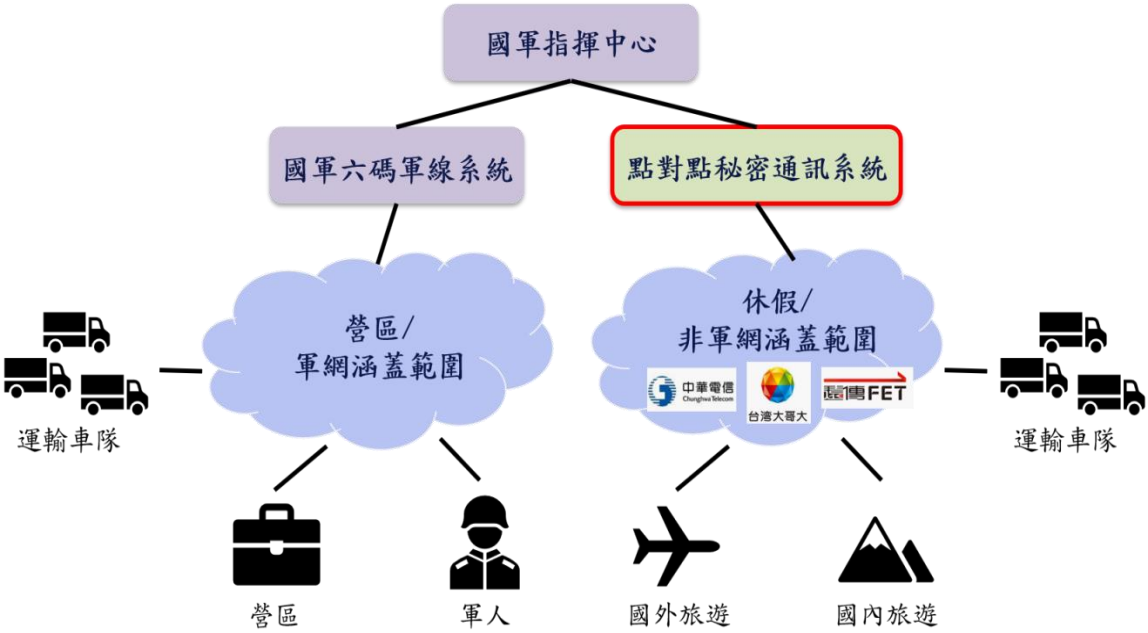
圖十一 導入國軍之 SWOT 分析圖

資料來源：作者繪製。

國軍應用Secure VoIP App之通訊架構圖如圖十二所示，點對點秘密通訊系統架設於國軍內部，雖然無法與國軍六碼軍線系統互通，卻能與之相輔相成，利用既有電信公司的網路補足軍網的不足，讓國軍的通訊再無死角。只要國軍所使用的智慧行動裝置上貼有已核發憑證之硬體貼片Slim SIM，皆可透過網際網路，撥打Slim Sim所配發之電話號碼進行秘密通訊。

點對點秘密通訊的使用並不限制於特定電信商所提供的網路，中華電信、台灣大哥大…等電信所提供之4G、5G數據上網服務以及Wi-Fi…，任何具有網際網路的環境皆可使用，就算在不安全或是不可信賴的網路環境下都可以提供服務，使得使用者在進行網路通話時，能保有隱私及安全性，非常適合用來輔助國軍在軍網以外的加密通訊需求，以保障訊息的安全性。此外，點對點秘密通訊是以網路電話為基礎的通訊方式，所以在進行通話時會受限於所在環境的網路品質。

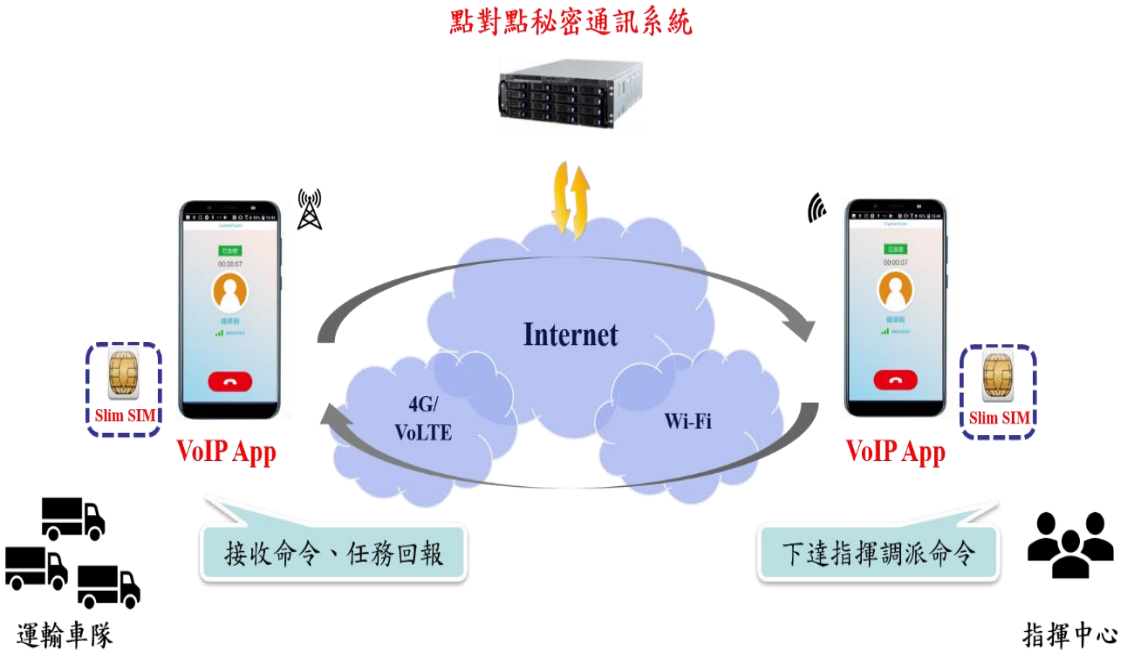
圖十二 國軍應用 Secure VoIP App 之通訊架構圖



資料來源：作者繪製。

以國軍的運輸系統為例(如圖十三)，在運輸的過程中，車隊需要接受指揮中心的調度，接收命令以及回報任務，所以在運輸車上需要具有溝通能力的設備，使得運輸車隊的駕駛、車長與指揮中心之間能做即時的溝通。若將Secure VoIP App設備安裝於運輸車上，即可做為車隊與指揮中心溝通的橋樑，享有即時通訊的便利性，也可保障訊息的安全。

圖十三 國軍的運輸系統示意圖



資料來源：作者繪製。

除此之外，Secure VoIP App也可用於公事的溝通、假日回報…等。相較於市面上擁有網路電話呼叫功能的即時通訊軟體，Secure VoIP App使用點對點加密技術，並將數位憑證等相關的使用者資訊儲存於硬體貼片Slim SIM當中，使得在傳遞途中的訊息不用擔心被第三方竊取，因為加密後的訊息除了溝通的兩端，並無第三方擁有可以將訊息解密還原的金鑰，讓國軍的訊息傳遞能更有安全保障，減少機密資訊洩漏的問題。

結論

在現代人的生活中，網路技術的發展迅速，以及智慧行動裝置的普及，造就網路電話技術的蓬勃發展，可以安裝在智慧行動裝置上的網路電話已漸漸取代傳統PSTN電話，成為目前主流的通訊方式。由於網路電話只需要在一個具有網路的環境下，就可以透過智慧行動裝置的搭配上擁有網路電話呼叫功能的即時通訊軟體，就可以透過網路進行語音通訊，是一種既省錢又方便的通訊方式。

然而，若在不安全的網路環境下，使用者透過網路電話進行語音通訊，會使得通話的安全性面臨極大的挑戰。市面上已有許多可以使用網路電話的即時通訊軟體，雖然也標榜具高度的安全性，但往往無法避免網路電話伺服器也擁有一把可以對使用者訊息解密的金鑰，進而將使用者的隱私與訊息暴露在危險之中。

Secure VoIP App以智慧行動裝置與智慧行動裝置間的點對點加密為基礎，搭配硬體元件Slim SIM，提供即時憑證狀態查詢服務，並使用傳輸層安全性協定以及安全即時傳輸協議建造出一條安全的傳輸通道，不只提供使用者安全的加密通話功能，也加強網路電話傳輸環境的整體安全，更提升手機使用的安全性，更有效的保障使用者在網路上的通訊安全，創造出一個安全的網路通訊環境。所以，當使用者使用Secure VoIP App時，不必再擔心訊息會被有心人截取或是竊聽，可以安心的使用網路電話進行即時通訊。

參考文獻

一、許士榮、蔡仁及、劉連寬、周自強、張詩郁、連啟宏、鄭復榕、林逸修、張景雄、吳冠峯，〈新型態的 VoIP 行動 App 服務整合應用 New type of VoIP Mobile App service integration application〉，《電信研究雙月刊》(桃園)，第 47 卷第 3 期，中華電信研究院，民國 106 年 9 月。

二、張峻嘉、林逸修、蔡仁及、周自強、連啟宏、劉連寬、張詩郁、何佩玲、張景雄、吳冠峯，〈IMS 虛擬分機技術 IMS Virtual Extension Technology〉，《電信研究雙月刊》(桃園)，第 49 卷第 2 期，中華電信研究院，民國 108 年 6 月。

三、邱奕勳，〈一個以 RTCP 為基礎的 VoIP 數位簽章機制 A RTCP-based Digital Signature Mechanism for VoIP〉，國立交通大學資訊管理研究所碩士論文，2008 年。

四、A. Sinaeepourfard and H.-M. Hussain, “Comparison of VoIP and PSTN services by statistical analysis,” IEEE Student Conference on Research and Development, 2011.

五、B. Goode, “Voice over Internet protocol,” Proceedings of the IEEE, vol.90, Sept. 2002.

六、C. Meyer J. Schwenk “Lessons Learned From Previous SSL/TLS Attacks-A Brief Chronology Of Attacks And Weaknesses,” IACR Cryptology ePrint Archive 2013.

七、E. Rescorla, “Diffie–Hellman Key Agreement Method,” RFC 2631, June 1999.

八、M. Baugher, D. McGrew, M. Naslund, E. Carrara and K.Norrman, “The secure real-time transport protocol (SRTP),” RFC 3711, March 2004.

九、Nan Li, “Research on Diffie-Hellman key exchange protocol,” IEEE 2nd International Conference on Computer Engineering and Technology, 2010, Volume 4.

十、S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP,” RFC 2560、6277, June 2013.

十一、S. Khan, N. Sadiq, “Design and configuration of VoIP based PBX using asterisk server and OPNET platform,” 2017 International Electrical Engineering Congress (iEECON), 2017.

十二、太思科技，〈太思科技集團和 Vantage IT 宣佈通過巴西國家科技與信息協會的安全許可，為 A3 證書提供行動解決方案〉，《太思科技》， https://taisys. com/news-detail?lang=zh&id=3c7bKQSUs6DmmaIIVYXds6q9J2OQStgfzQul8BKisA，2019/12/03，(2020/05/21)。

十三、太思科技，〈太思科技 SIMoME® Vault 獲得 FIPS 140-2 Level 3 驗證核可〉，《太思科技》，https://www.taisys.com/news-detail?lang=zh&id=13f00_iX_YdycsHXTkwbPVnahOHXlDwgkAyn4FJscg，2019/04/17，(2020/06/29)。

十四、〈對話啟動協定〉，《維基百科》，https://zh.wikipedia.org/wiki/% E5% B0%8D%E8%A9%B1%E5%95%9F%E5%8B%95%E5%8D%94%E5%AE%9A，(2020/05/25)。

十五、維基百科，〈即時傳輸協定〉，《維基百科》，https://zh.wikipedia.org/wiki/% E5%AE%9E%E6%97%B6%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE，(2020/05/25)。

十六、維基百科，〈傳輸層安全性協定〉，《維基百科》，https://zh.wikipedia.org/wiki/ %E5%82%B3%E8%BC%B8%E5%B1%A4%E5%AE%89%E5%85%A8%E6%80%A7%E5%8D%94%E5%AE%9A，(2020/05/21)。

十七、Amnesty international, “Snapchat, Skype among apps not protecting users’ privacy,” Amnesty international, https://www.amnesty.org/en/latest/news/2016/ 10/snapchat-skype-am

ong-apps-not-protecting-users-privacy/, 2016/10/21,(2020/ 02/03).

十八、BBC Newsbeat, “Facebook most secure for instant messaging services, says Amnesty,” BBC, http://www.bbc.co.uk/newsbeat/article/37717718, 2016/10/21, (2020/02/10).

十九、Line，〈LINE 發布透明度報告(2017 年 7 月至 12 月)〉，《Line Corporation》，https://linecorp.com/zh-hant/pr/news/zh-hant/2018/2167，2018/04/24，(2020/05/ 21)。

二十、Margaret Rouse, “end-to-end encryption (E2EE),” SearchSecurity, https:// searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE, July 2015, (2020/02/18).

作者簡介

學歷:國立中央大學軟體工程碩士，經歷:現任中華電信研究院匯流服務研究所副研究員。

學歷:元智大學資訊工程碩士，經歷: 現任中華電信研究院匯流服務研究所研究員。

學歷:國立交通大學資訊工程碩士，經歷: 現任中華電信研究院匯流服務研究所研究員。