行動通訊軟體 LINE 的安全設計探討

何煒華
東吳大學資訊管理系
副教授
e-mail：
whhe@csim.scu.edu.tw

秦裕國
東吳大學資訊管理系
研究生
e-mail：
jackiechin123@gmail.com

摘要

行動即時通訊軟體在現今社會當中，已經成為忙碌生活當中溝通與資訊交換的最重要媒介，過往有許多針對此一現象的研究。因為行動即時通訊軟體的普及與便利性、廣泛性，許多原先透過電話、簡訊甚至電子郵件進行冒用、詐騙、甚至社交工程的不法行為紛紛轉移到這個全新且廣泛被使用的通訊機制上。面對不斷升高的資安風險，行動即時通訊軟體供應商也不斷透過版本更新，增進安全控制來防護，本研究以最具指標意義的行動即時通訊軟體軟體 LINE 作為研究的標的，研究並分類其安全控制措施，探討設計的有效性，希望能提供使用者在使用行動即時通訊軟體時對於自身安全防護的實質參考。

關鍵詞：安全控制、資訊安全、風險

Abstract

The mobile instant message (MIM) software has become the most important medium of communication and information exchange means at nowadays. There are many researches about this phenomenon in the past. Because of the popularity, convenience and extensiveness of MIM, many wrongful or illegal fraud behavior such as phone call, messages, and social engineer attack all move on to this brand new and widely used platform. Faced with the rapid rising risk of information security, the MIM software provider also increase its security controls for protection through software update continuously. In this paer, we are trying to survey and classify the security controls of the most significant MIM – LINE, and give users some substantive references about security issues when using MIM.

Keywords: Security Controls, Information Security, Risk

1. 前言

本文探討當外在資安風險增加與即時通訊軟體不斷改進安全控管機制的情況下，將安全控制措施進行分類研究，探討這些安全性的設定所能夠防護的範圍，如敏感性資料的揭露、網路詐騙的防範、線上交易的安全防護等等，期望能提昇使用者對於安全設定的認知，進而找出適當的方式以有效降低經由即時通訊軟體所造成的資安事件的風險。

2. 研究背景與動機

2.1 即時通訊軟體

即時通訊軟體 (Instant Messaging, IM) 是一個即時的訊息傳遞系統，兩人或多人透過網際網路的鏈結，使用文字、語音、圖片、檔案、或視訊進行交流。即時通訊軟體不同與傳統的電子郵件，它的會話交談是即時進行的，進行對話的雙方，就好比是面對面的交談一樣，也因為這樣的即時特性，即時通訊軟體對我們的工作、生活以及其他的各種層面，產生了重大的改變。

即時通訊軟體最早是出現在個人電腦上，由於其便利性、即時性，受到歡迎的即時通訊軟體非常的多，包含了 Windows Live Messenger (MSN)、AOL、Skype、Whatsapp、Yahoo! Messenger、QQ、WeChat、LINE、Jabber 等等，所有的即時通訊軟體都來自於芬蘭 Jarkko Oikarinen 於 1988 年所設計的 IRC (Internet Relay Chat) 軟體的啟發，原先 IRC 設計的初衷是希望使用者在閱讀電子布告欄文章的同時也能即時的建立群組討論與談，軟體應用持續創新演變至今，除了群組討論的功能外，即時通訊軟體更注重人與人之間一對一的即時交談。

在所有即時通訊軟體當中，ICQ 是最早被發表的，ICQ 取其英文發音的諧音 I Seek You 為名，其作者為四名以色列青年，並且在剛發表短短半年的期間就擁有了超過 85 萬的註冊用戶，即時通訊軟體所帶來的便利性以及對大眾的吸引程度可見一斑。[38]

2.2 行動即時通訊軟體

隨著網際網路與行動裝置的日益普及，伴隨著後 PC 時代的來臨，在 2010 年以後，個人電腦的市場佔有率在整個消費性電子市場中逐漸的下降，取而代之的是更便於攜帶的行動裝置，於此同時，即時通訊軟體的主要運作平台重心也隨之轉移，我們稱之為行動即時通訊軟體(Mobile Instant Message, MIM)。在所有的行動即時通訊軟體當中，2011 年 6 月在日本所推出的 LINE 即時通訊軟體，支援了包含行動裝置以及個人電腦在內的九種作業系統[27]，並在日本以及東南亞地區發展快速。在台灣，更被喻為是市場上最受矚目的智慧型手機應用程式之一，2013 年 1 月 LINE 的使用人數正式突破一億人大關，截至 2014 年 10 月，LINE 於全球更擁有了超過 5 億 6 千萬註冊使用者，其中包含約 1 億 7 千萬活躍使用者，在這當中，有 1700 萬的活躍使用者來於自台灣[38]。

也因為 LINE 在台灣非常受到歡迎，許多的傳統的詐欺行為，例如電話詐欺、信件、簡訊詐欺等等，也紛紛轉移陣地來到這個幾乎所有人都普遍使用的即時通訊軟體上面，在這個情況下，使用者在使用即時通訊軟體時對資訊安全的認知以及軟體所提供的安全防護機制就顯得更為重要。

2.3 行動即時通訊軟體相關議題

行動即時通訊軟體因為普及率高、使用率高，它對於我們的生活，產生了重大的改變，而行動通訊軟體以行動裝置作為主要的載具，必須搭配不間斷的網路服務進行交談，截至 2014 年八月為止，台灣的行動上網(3G+4G)已經超過 988 萬用戶數，對比過去所做的統計資料顯示，上網人口中，使用行動上網的人口比率，從 2012 年的 26%成長到了 2014 年八月的 47%，在這麼普及的行動網路與行動即時通訊軟體使用率下，許多學者紛紛提出了許多有關行動即時通訊軟體行為議題的研究項目，包含研究中高齡使用者對即時通訊軟體的使用偏好[7]，以及對即時通訊軟體滿意度的相關研究[9]，更有大量的研究是圍繞在行動即時通訊軟體的使用者忠誠度相關議題上[40]或是探討影響消費者採用何種行動通訊軟體的決策因素及使用意圖[11][15][16]，更有一些研究是透過 Stafford 等人於 2010 所進行的科技依賴研究作為基礎[35]，探討社會互動、情感因素、以及大眾對即時通訊軟體的依賴來自於哪些因素，研究結果顯示，使用者使用行動即時通訊時會產生人、樂趣、訊息與工作四方面的依賴，並且增進使用者在朋友、同事及家人三方面的歸屬感[12]。

在這當中，在日本、台灣、以及東南亞地區最為普及的行動通訊軟體 LINE，因為行動網路的快速發展與普及，加上 LINE 的許多創新設計，例如貼圖訊息、貼圖付費機制、結合遊戲與行動通訊軟體本身等等，讓 LINE 迅速的席捲了整個東亞市場，許多學者也探討了這些創新設計對於使用者使用意圖的影響[2][17]，然而這些針對消費者選擇使用行動通訊軟體的意圖或趨勢的探討與研究雖然很多，但是針對資訊安全相關議題的文章卻非常稀少。

由於網路的蓬勃發展，透過網路進行詐騙、入侵、竊取資料的案例時有所聞；2013 年 7 月，位於日本渋谷號稱擁有最安全伺服器的 LINE，遭到台灣北科大學生透過系統漏洞入侵竊取了 169 萬筆使用者資料，內容包含了旗下 NAVER 入口網站各項服務的會員帳號、電子郵件信箱、Hash 加密的密碼與帳號暱稱，有關單位花費了好幾個月的時間才追查出駭客的身分並且修補漏洞[25]；2014 年 6 月，雖然 LINE 官方方在三發出聲明表示 LINE 的通訊過程均透過 RSA 2048 位元的加密，韓國、台灣以及泰國政府[23][36][37]曾表示已有能力攔截用戶的對話紀錄；詐騙集團利用流行的 Line 即時通訊軟體，以傳訊息「裝熟」或「恫嚇」方式，讓人點選其附上的連結網址，一連結就被植入並啟動木馬程式，利用被害人名義使用小額付款功能；警政署統計 2014 年一月到九月，電腦網路犯罪案件高達一萬五千三百一十七件，比去年同期多七千二百九十三件，增加百分之九十。其中 LINE 帳號被盜用登錄報警次數一千七百七十八件、透過 LINE 進行詐騙代買點數等犯罪一千八百二十件。警政署刑事警察局科技研發科科長邱紹洲表示，2014 年 LINE 詐騙案件暴增，主要是因 LINE 電腦版可透過電子郵件及臉書帳號登入，不少個人電腦上的木馬

程式會從鍵盤上盜取用戶帳號、密碼，臉書和 LINE 一起「失守」。

2.4 LINE

在為數眾多的即時通訊軟體，具有指標性質的 LINE 能夠在短時間內擁有大量的註冊使用者，很大一部分的原因，除了使用者對即時通訊的需求以外，更多的使用者是因為 LINE 成功導入整合各項的應用程式、遊戲的加值服務與可使用代幣購買表情貼圖。截至 2015 年 12 月為止，LINE 已經發表了除了即時通訊軟體本身以外的 16 種應用程式與 14 款遊戲[27]，這些周邊的應用程式不但支援了主要的行動裝置平台，而且其內容所包含的範圍非常廣泛，例如常用工具、製作賀卡、攝錄影、影像處理、防毒防駭、來電與簡訊過濾、以及線上諮詢服務等等。此外，更有為數眾多的虛擬商品可以由 LINE 本身的的線上商店 LINE STORE 進行購買，使用者可以選擇使用 LINE 所提供的支付工具 LINE PAY，透過綁定信用卡資料、預先儲值、接受好友轉帳進行虛擬商品的購買。LINE 的附屬遊戲部分更是充分的結合了 LINE 通訊軟體的特性，透過遊戲，線上呼朋引伴結合虛擬人物與贈送代幣，讓越來越多的使用者受到吸引，願意註冊使用 LINE。

根據 ARO 的一項統計報表[圖 1]指出，在 2012 年 11 月到 2013 年 1 月，與美國行動流量監控先驅 Arbitron 公司合作，經過 500 多位智慧型手機用戶的同意，在其智慧型手機中安裝應用程式，藉以偵測使用行為，取得包含使用時間、內容、方式、應用程式、網路瀏覽、手機作業系統、通信業者分佈等資訊。無論以月或是週為單位來看，LINE 都是到達率最高的應用程式 APP[18]，在這當中，有 80.6%的使用者至少每週會使用 LINE 一次，而排名第二的則是 Facebook，每週到達率達到 72.5%。

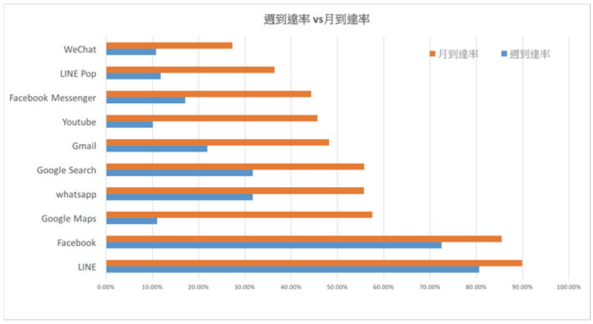

圖 1：行動裝置 APP 到達率比較圖
資料來源：ARO Mobile Audience eXplorer [18]

此外月到達率前十名之行動裝置 APP 中，有四項均為「訊息」類別，顯示使用者對訊息傳遞功能非常重視。因此，LINE 也很積極的擴增即時通訊軟體的使用範疇，使用者除了可以傳遞文字、圖片訊息外，更可以透過中繼主機，不必考慮對方使用的裝置平台，即時的與聯絡人進行視訊或是語音通話。LINE 的功能強大，涉及的範圍也很廣泛，對於裝置的權限要求也因為各項應用各有不同，在此情況之下，隱私以及安全性的相關議題就有必要受到更多的重視。

截至 2015 年 9 月為止，目前全球透過通訊軟體 LINE 傳送與接收的訊息次數，高達 170 億次，並且根據尼爾森最新的「LINE 使用行為研究與市場觀察」報告當中發現，97%的通訊軟體使用者都有使用 LINE，其中更高達 88%是每天都使用的重度族群[30]。然而伴隨著使用者不斷攀升，使用量不斷提高的同時，外部的風險也正不斷的升高，雖然各大行動通訊軟體業者不斷的透過程式更新，提昇了安全設定的等級，加強了安全控管的作為，但有心人士、駭客、詐騙集團等等，均不會輕易放過這個為數眾多的使用者集合。

3. 文獻探討

3.1 即時通訊軟體

即時通訊軟體(Instant Messenger, IM),在最早的時候，只是運用於軍方的無線電通訊系統，廣泛的使用在各種緊急情況的處理，當網際網路興起之後，BBS 交談成為許多人用來溝通聯絡的方式之一。 1988 年芬蘭 Jarkko Oikarinen 建立了一個基於網際網路的聊天站，稱之為 IRC (Internet Relay Chat)系統，使用者可以即時的針對文章進行討論，即時的文字通訊從此廣受歡迎。

隸屬於 Mirabilis 公司的四位二十多歲以色列工程師，在 1996 年 11 月共同開發了 名為 ICQ 的一套軟體，並且開放大眾免費下載使用，開展了即時通訊軟體的世界[18]。許多即時通訊軟體，包括 LINE、WeChat、ICQ、Facebook Messenger 、 MSN Messenger 、 Yahoo! Messenger、Skype、Miranda IM、QIP 和 Trillian 等[5]，就在這樣的風潮下誕生了。

3.2 即時通訊服務

網際網路工程任務小組(The Internet Engineering Task Force , IETF)成立了名為即時傳訊與定位協定的工作小組(Instant Messaging and Presence Protocol Working Group, IMPP WG)以能完成共通的即時傳訊與定位協定(Instant Messaging and Presence Protocol , IMPP)[6]為目標，並且提出即時通訊服務標準規範 RFC 2778，制定了：

(1) 即時訊息服務(Instant Messaging Service)
(2) 現狀資訊服務(Presence Service)

3.3 即時通訊協定

網際網路工程任務小組當初所提出的即時傳訊與定位協定(IMPP, Instant Messaging and Presence Protocol)成為目前所有主流即時通訊協定 SIMPLE 以及 XMPP 所參考的主要架構。

網際網路工程任務小組於 2002 年提出了一個名為 SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) 的 RFC3428 標準，主要是以 SIP(Session Initiation Protocol)為基礎的即時通訊協定，其中 SIP 本身主要用途為溝通、管理與停止媒體對話程序，對話程序是由傳送特定資料的通訊協定來加以完成，例如 RTP(Real-time Transport Protocol，即時傳輸協定)，建立多媒體對話的通道後，隨即利用 SDP(Session Description Protocol)此一會議描述協定來完成兩端交換對話資訊的功能。當溝通協調完成之後，可利用 RTP 來傳送多媒體(例如視訊、語音)封包，非常適合用來發展多媒體通訊的即時服務[6]。

3.4 即時通訊軟體面臨的資安威脅

即時通訊軟體最主要面臨的資安威脅就是透過即時通訊軟體傳遞的詐騙簡訊連結，這些詐騙的連結，經過使用者點擊後可能會在使用者的手機中植入惡意程式，對使用者造成危害。

近年來，簡訊詐騙的情況有逐漸攀升的趨勢，台灣手機用戶的受害情況相當驚人。根據趨勢科技的觀察，台灣近期詐騙簡訊網址氾濫，光這一個月內就成功騙取了近 89 萬次的點擊數，且最高紀錄一天內就出現 10 筆簡訊惡意網址! [20]

圖 2 透過簡訊傳送的詐騙連結
資料來源：趨勢科技新聞[20]

這些詐騙簡訊內的網址[圖 2]，會嘗試安裝惡意程式到受害者手機內，除了透過私下替受害者註冊小額付款騙取金錢之外，還有可能會竊取受害者手機內的通訊錄、通話紀錄甚至個人資料，導致受害者親友通通淪陷，成為有心人士下一波再次詐騙金錢或竊取資料的對象！

趨勢科技同時也發現，近期流行的詐騙簡訊內容，其手法與變形過程大致如下[20]：

- 裝熟假冒好友，佯裝手機不見或是猜猜我是誰，要求「代收驗證碼」，騙取被害人的個資後，冒名購買物品或是遊戲點數卡，造成被害者的金錢損失。
- 偽造「快遞通知單」或「宅急便」，要求點擊網址以「簽收電子憑證」，點擊後，若手機位開啟任何防護措施，會自動安裝應用程式 APK，造成金錢損失。
- 謊稱您正申請「網路支付水電費 OOOO 元，若懷疑被冒用可查看憑證」，要求點擊網址，安裝 APK 後造成金錢損失。
- 目前最新的詐騙內容則是「網拍取貨」，內容為：「OOO 先生，你的 OO 網拍商品已經送達門市，寄件代碼 http://goo.gl/uq****」，要求點擊網址，同樣是自動安裝 APK 後造成金錢損失
- 更甚者，更有結合時事，例如風災捐款，搶救某某候選人等等詐騙手法。

此外，若使用者安裝的 LINE 通訊軟體並未定時更新，也很可能會受到透過圖片夾帶病毒檔案方式的攻擊，攻擊者選定已知 ID 的目

標後，傳送夾帶惡意程式的圖片給對方，當對方開啟圖片閱讀時，惡意程式就成功的植入了被害人的手機當中。

刑事局統計民國 103 年 1 至 4 月共發生 497 件手機簡訊詐騙事件、財損金額高達 315 萬 293 元，凸顯出手機資安意識的重要。手機用戶應儘速建立正確資安觀念，除了對不明簡訊內容應提高警覺、多方確認是否安全後再點擊之外，更應立即安裝手機安全防護軟體。

此外，若由非官方認可或是認證的渠道下載安裝的通訊軟體，或手機內的行動即時通訊軟體遭到惡意的置換、竄改，亟有可能在看似正常的通訊軟體當中潛藏著伺機監控、竊取、竄改資料的木馬程式或是惡意軟體。

3.5 行動裝置平台面臨的資安威脅

行動即時通訊軟體因為運行在行動裝置上，所以帶來了更即時與便利的服務，使用者間彼此的溝通也更加的快速，但是在便利快捷的同時，裝置平台本身卻有可能成為駭客覬覦的攻擊目標。

知名資安廠商 Cryptography Research 與 McAfee 於 2012/4 發布研究結果指出， Apple iOS，存有難以修補的安全弱點[4]。研究結果顯示，手機作業系統所使用的加密傳輸機制是可以被破解的，這對仰賴網路通訊完成訊息交換機制的即時通訊軟體來說，實在是必須要密切提防與加強安全控管的重要議題。Cryptography Research 在實際展示時，側錄手機所傳輸的網路購物、網路銀行以及登入企業 VPN 之封包後，破解加密機制並分析封包內容，取得封包內所含之信用卡卡號、銀行及公司帳號密碼等機敏資訊並成功登入。

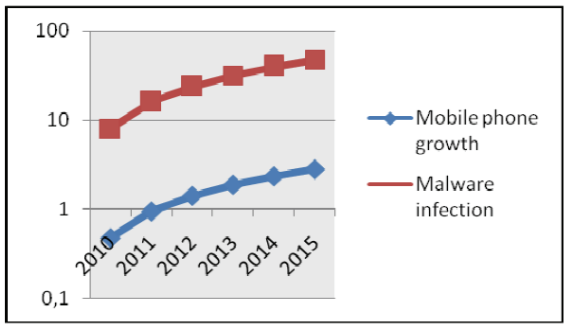

圖 3 近年來行動裝置的成長與惡意程式的增長趨勢圖

資料來源：趨勢科技新聞[21]

Cryptography Research 的專家表示，被側錄的手機並沒有經過特殊設定，純粹就是一般正常使用狀況。另外，手機被側錄時，使用者也不會發覺手機傳輸有任何異狀。McAfee 研究結果則是針對 Apple iOS，展示數種能由遠端入侵使用 Apple iOS 作業系統的 iPad 與 iPhone 之方法。

McAfee 專家展由遠端取得裝置控制權後，可啟動裝置麥克風錄下裝置附近的對話、竊取裝置金鑰、帳號密碼及裝置上機敏資訊如通訊錄、通話紀錄、電子郵件及簡訊內容等[35]。McAfee 專家同樣也表示，裝置被入侵後，使用者不會發覺裝置有任何異狀。雖然專家們均表示，目前尚未聽聞有駭客利用所展示的手法實際入侵行動裝置，但只是時間遲早的問題。

行動裝置已成為目前駭客研究下手的頭號目標[4]。根據國際數據資訊有限公司(International Data Corporation , IDC)的估計，可存取網際網路之行動裝置將於 2013 年突破十億。除了各路業者積極爭取商機外，駭客更是覬覦這塊大餅，欲從中獲取龐大不法利益。

行動裝置作業系統廠商應儘速修改及強化作業系統安全，讓全球未來能有安全的行動裝置使用空間。儘管大部分的行動裝置之持有與使用係歸私人所擁有，很少有多人共用一台行動裝置之情形，但這也未必表示行動裝置是可信任的。另外，部分使用者會進行行動裝置的越獄(Jailbreaking)這行為會繞過行動裝置內建的安全防護機制，而給了惡意軟體很好的機會。

而根據 IDC 調查報告顯示，2012 年全球手機出貨總量將達到近 18 億支，高於 2011 年的 17 億支，且預計在 2016 年之前，出貨至通路的手機數量將達到 23 億[21]。IDC 亦預測未來五年中，Android 仍將是出貨量最高的智慧手機作業系統，而其市占率會在今年達到頂峰。

趨勢科技行銷總監 Myla Pilao 表示：「隨著 Android 裝置越來越普及，Android 平台也就常成為歹徒的犯罪工具。Android 應用程式流通模式的開放性讓該平台成為最熱門的攻擊目標，我們相信這類攻擊事件的數量今年仍會攀升。事實上，我們偵測到針對行動裝置的惡意程式已在短短一個月中增加一倍，比我們之前所預估的還要多。RuFraud9 和 DroidDreamLight10 這兩個惡名昭彰的 Android 變種惡意程式，讓數百萬名用戶的資料外洩和金錢損失。」詳如圖 3。

此外，趨勢科技也公布十大惡意程式排行，其中近年來大行其道的偽應用程式以 30%

榮登第一；接著依序為資料竊取軟體(21%)、廣告軟體(18%)、高價服務濫用(14%)、遠端控制木馬程式 Rooter/RAT (13%) 和惡意下載軟體(4%) [21]。

除了前述這些大行其道的惡意程式當中，有些合法的應用程式竟然是因為使用了不安全有漏洞的開發工具、開發函式庫，以致於開發的產品全部都成為了駭客下手的目標，在 2015 年 11 月的一份報導指出，使用百度 SDK Moplus 所開發的 1 萬 4 千款應用程式，全部都因為 SDK 當中存在了不該有且無需身分認證的後門，讓駭客只需要掃描網路上的 IP 就能輕易的選定目標進行攻擊[29]。此外，在 Apple iOS 上，因為中國開發者在不知情下使用遭駭客竄改含有 XcodeGhost 惡意程式的蘋果開發工具 Xcode，導致許多知名且合法經過審核的 app 受到感染，使用者的資料很可能已經經過此管道外洩[39]，估計有上億的裝置受到影響。

依照此研究成果，使用官方認可且經過審核機制上架的 APP 應用程式，都可能存在著資訊安全的風險，若使用者安裝各種行動即時通訊軟體，卻沒有從官方認證、認可的平台下載安裝，其所帶來的風險相對來說是非常高的，一時的疏忽，卻可能讓個人的機密資料外洩。

此外，利用個人裝置存取公司資料的情況越來越普遍，但 IT 管理單位卻無法有效控管這些裝置，在沒有安全機制的防護下，若隨意安裝了來路不明的應用程式，很可能會造成個人資料的外洩，更嚴重的，還可能導致整個組織的重要、機密資訊曝光，此類事件更是每天不斷的在發生當中。

在這當中，對行動裝置的威脅主要是來自於木馬程式和蠕蟲，這類型的程式主要目的就是希望透過用戶作為散佈自身的媒介。有些間諜程式，可以暗自記錄電話號碼和對話，如此一來，隱私不但受到侵犯，還會面臨身分可能被盜竊的風險，更有可能因此造成公司機密資料外洩，危及組織的智慧財產權與利益。

在外部的資安風險不斷升高的同時，行動裝置作業系統實在有需要建立一套更加安全的機制以保障各項需要保護的內容能夠維持裝置的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)：

- 機密性－確保傳輸與儲存之資料無法被未授權人士存取。
- 完整性－偵測傳輸與儲存之資料是否有任何有意或無意的變更。
- 可用性－確保使用者可透過行動裝置存取所需的資源。

為了滿足以上的資安要求，除了裝置平台與即時通訊軟體所內建的防護機制，使用者需要更多的資安保護措施與安全教育訓練，一部分資安防護功能是行動裝置本身內建，另一部分是需要透過額外附加的控制措施，兩者互相搭配，輔以實施不斷加強改進的安全教育訓練，才能有效降低資訊安全事件所可能造成危害的風險。

3.6 即時通訊軟體 LINE 各版本的安全改進措施

面對前述日益升高的資安風險，LINE 也持續的做出許多攸關安全性議題的改進，就過去一個年度的版本異動來說，與安全性有關的改進主要有以下幾個項目(資料來源：LINE 官方部落格版本更新訊息[28])：

表 1 LINE 各版本安全性更新表

日期	版本	更新項目
2014.05.02	4.3.0	➢ 提供用戶更加嚴密的身分認證步驟 ➢ 日後在更換智慧手機、重新安裝 LINE 等情況下，除了原本的「電子郵件帳號密碼」外，用戶可以透過「換機密碼」讓您的帳戶更安全
2014.07.01	4.5.0	➢ 特別針對完成 Facebook 帳號認證的用戶，追加了必要的使用設定項目，以強化用戶使用安全 ➢ 已設定完電話號碼或換機密碼的用戶，則無需進行本追加設定

		➢ 新增傳送限時訊息的「限時聊天」功能
2014.10.10	4.7.1	➢ 改善多人聊天室「聊天群組」的安全隱私相關功能，加強檢舉功能
2014.12.17	4.8.0	➢ 新增了交易服務「LINE Pay」，以及裝置儲存空間不足時顯示提醒
2015.01.06	4.9.0	➢ 聊天室的功能內新增「對話紀錄」的搜尋項目
2015.03.10	5.0.3	➢ 針對 2015 年 2 月日本 JPCERT/CCJPCERT Coordination Center(JPCERT/CC) 及情報處理推進機構(IPA) 所提出的安全疑慮，本版本防止惡意的攻擊者，設置無線網路並開放給他人使用，以中間人攻擊 (man-in-the-middle attack)，造成用戶連線至該網路時可能發生的聊天內容或好友名單等資料就有可能被惡意攻擊者取得或更改。
2015.08.25	5.3.0	➢ Letter Sealing 進階加密功能，採用 End-To-End encryption(E2EE) 技術保護對話隱私 ➢ 完整刪除 (True Delete)，用戶所刪除的訊息，將無法再透過本人、任何手機使用者或第三方還原，這項功能將徹底避免手機上已被刪除的對話紀錄被他人還原、使用，此功能也可以跨平台使用。

資料來源：LINE 官方部落格，版本更新公告訊息[28]

由表 1 可知，LINE 在最近一年的版本異動中，大幅的加入安全性改善的相關設定與控制措施，雖然過去也曾有過安全即時通訊系統之設計與實作方面的研究，研究主要提到訊息交換應該透過加密保護機制進行，並透過三方驗證金鑰為基礎，設計一套安全的即時通訊協定，並且研究也分析了相關的網路攻擊手法[13]，但是在這一年即時通訊軟體大幅改善安全控管措施以後，卻沒有更多的研究來探討這樣的改變，因此，本文嘗試探討當外部的資安風險不斷的提昇與即時通訊軟體也做出新增相對應的安全控管措施時，透過將這些安全控制的措施進行分類與研究，並將安全措施的分類結果作為使用者在使用行動即時通訊軟體時對自身安全防護的實質參考。

4. 即時通訊軟體 LINE 的安全控制分類整理與防護目的

依照安全設定的性質，經過分類與整理，LINE 的相關安全控制措施可以分為以下幾個大類，包含登入設定、換機密碼與帳號綁定、隱私設定、訊息管理與版本更新，各項控管措施均可由 LINE 設定中的相對應位置進行設定，詳細功能描述與建議事項分述如下：

4.1 登入設定

■ **不允許自其他裝置登入：**

減少因為安裝即時通訊軟體於其他裝置，如電腦、平板等等，因為其他裝置相對較為容易遭到惡意攻擊或入侵、被植入鍵盤輸入側錄程式、中毒等，以致帳號密碼外流。可自：其他→設定→我的帳號→允許自其他裝置登入進行功能的開啟或關閉。

本設定可以針對手機以外的裝置，做出登入限制與控管，使用者可以設定關閉除了手機以外裝置的登入權限，讓其他裝置，如電腦、平板等，即使掌握了使用者的帳號與密碼，也無法進行登入，目的是希望減少與降低因為其他裝置遭受到惡意程式的攻擊、注入、或是側錄輸入指令的方式以致於帳號密碼外洩的風險，再者，也能在使用者察覺帳號密碼遭到外洩時，設定關閉此項功能，讓資訊被竊取的可能性大幅降低。

■ **使用行動條碼登入：**

電腦或平板登入時，需要使用手機掃描電腦端畫面顯示的行動條碼 QRCode 進行登入，設定此一措施，可以防止電腦或平板端遭到植入鍵盤側錄程式導致輸入密碼被側錄的可能性。設定方式為，電腦端：登入時選擇使用行動條碼登入，手機端：其他→加入好友→掃描行動條碼後登入。

若因為各種原因，而必須開啟其他裝置，如電腦、平板的登入權限時，可以設定必須使用行動條碼進行登入，如此一來，當在其他裝置登入時，電腦或平板會顯示一組行動條碼，使用者需使用手機開啟 LINE 後，選擇其他→個人資料→行動條碼→掃描行動條碼，成功掃描後方可登入。讓在其他裝置的登入時，減少被側錄帳號密碼的風險以及確認操作登入行為的使用者就是手機的持有者。

■ **變更密碼：**

重新設定 LINE 的登入密碼，定時或週期性的更新 LINE 的登入密碼，可防止有心人士，透過各種方式破解密碼對於安全造成的危害。設定變更密碼的方式為：其他→設定→我的帳號→設定電子郵件→帳號變更密碼 。

透過重新設定密碼，更換登入時使用的驗證密碼，若採取定時更新密碼，更可以降低因為密碼遭到側錄、窺視或被猜測而導致個人隱私外洩的可能性。此外，若因故忘記了登入密碼，也需要透過此功能當中的忘記密碼功能，讓系統傳送變更密碼的連結至所綁定的電子郵件帳號中，以進行密碼的回復。

■ **登入裝置管理：**

對目前登入的本人帳號進行控管，對於可能已經遭到盜用的帳號來說，本設定可於帳號密碼外洩或被盜用時，強制登出不被認可的裝置，並即時更改密碼，防止資料進一步的外洩。設定的方式為：其他→設定→我的帳號→登入中的裝置→強制登出不被認可的裝置。

由於 LINE 支援了各種平台，所以為了有效管理登入中的裝置，需要有一定的策略，目前 LINE 已經可以運作在屬於行動裝置的多數平台上，包含了 Android、iPhone、BlackBerry、Windows Phone、Nokia Asha、以及 Firefox OS，此外，也支援了 PC 平台的 Windows 7/8/10、OSX、iPad 上，更支援了 Chrome OS 或以 Chorme 瀏覽器的應用程式型式開啟，在這麼多的平台、系統、架構支援下[26]，LINE 很明確的限制了，除了行動裝置外，其他的裝置同時只能有一個進行登入，使用 Chrome 應用程式登入者，則不在此限。於是有效控管登入中的裝置就變得非常重要，透過本設定，可以讓使用者掌握目前登入的裝置是否為自己認可的裝置，若為非認可的裝置，也能即時將其登出，並且修改密碼，重新取回帳號的主控權。

4.2 換機密碼

■ **設定換機密碼：**

換機密碼主要是用來設定驗證身分的一組密碼，為防止 LINE 帳號遭到盜用，用戶可設定四位數換機密碼，換機密碼預設為電話號碼的末四碼，在手機更換之後，登入 LINE 需輸入所設定之換機密碼，可有效防止帳號密碼遭竊時所可能造成的損失，延緩對方取得帳號主控權的時間，讓使用者得以藉由前述的裝置管理進行相關的措施，取回自己的帳號，避免隱私資料進一步的外流。本設定可於：其他→設定→換機密碼 進行設定。

設定換機密碼，在原本的帳號密碼之外，加上的第二層密碼，以保障及確認使用者使用不同手機登入時，為使用者本人，減少因為帳號密碼因為各種原因被竊取時，竊取者冒用使用者帳號密碼登入所發生的隱私危害，研究顯示，正確設定換機密碼，將可減少 90%因為帳號密碼外洩所帶來的風險[32]。此外，若將

LINE 帳號同時綁定 e-mail 與手機號碼，並設定「換機密碼」，就能在更換手機或重新安裝 LINE 的 app 時，無痛轉移好友名單以及付費購買之貼圖與代幣(不包括訊息紀錄)[3]。

4.3 隱私設定

■ **不允許利用 ID 加入好友：**

開啟或取消透過 ID 搜尋被加入好友，改採行動條碼或近距離搖一搖方式進行好友加入。或於加入好友時才開啟本設定，加入後取消本設定，避免被機器人程式或是有心人士鎖定，搜索 ID 後加入好友進行攻擊。本設定可於：其他→設定→隱私設定→允許利用 ID 加入好友 或 其他→設定→我的帳號→允許利用 ID 加入好友 進行設定。

設定開啟或關閉其他使用者，使用 ID 搜尋方式，搜尋並將您加入好友的功能，由於許多人的 ID 無論是 eMail、Facebook 或是 Blog 都會習慣使用一樣的帳號，所以當有心人士想要針對您作為目標進行攻擊或詐騙時，往往都透過這種方式，由網站資訊中得知您的 ID 後，在至 LINE 中搜尋 ID 後加您為好友。若設定為不允許，將可避免 ID 透過此方式被搜尋並加入好友，帶來無謂的困擾。

建議需要新增好友時，改採行動條碼或雙方面對面近距離搖一搖方式進行好友加入。或於加入好友時才開啟本設定，加入後取消本設定。

■ **不自動加入好友：**

開啟或取消自動透過通訊錄上的聯絡人加入其他人為好友，防止加入未預期的聯絡人為好友，造成不必要的困擾或危害，本設定可於：加入好友→右上方設定→自動加入好友進行設定。

建議取消自動將手機通訊錄的好友加入 LINE 的好友名單，防止未預期的新增不該新增的聯絡人為好友。

■ **不允許被加入好友：**

若其他用戶的通訊錄有您的電話號碼，您會被自動加入該用戶的 LINE 好友名單內，開啟本設定後，將不允許其他用戶透過新增手機聯絡名單方式自動將自己加入對方好友名單中，設定方式為：加入好友→右上方設定→允許被加入好友。

若開啟本設定，則若其他用戶的通訊錄有您的電話號碼，您可能會被自動加入該用戶的 LINE 好友名單內。建議不允許其他用戶透過新增手機聯絡名單方式自動將自己加入對方好友名單中。

■ **密碼鎖定：**

設定後，於手機端設定開啟 LINE 必須輸入密碼，若忘記密碼，需重新安裝 LINE，但所有對話紀錄將被刪除，可有效防止手機在未鎖定或遭到未經授權的使用時，對方可隨意瀏覽對話紀錄、調整各項設定的風險，本設定可於：其他→設定→隱私設定→密碼鎖定(選取後，設定四位數鎖定密碼)後生效。

若開啟本設定，則若其他用戶的通訊錄有您的電話號碼，您可能會被自動加入該用戶的 LINE 好友名單內。建議不允許其他用戶透過新增手機聯絡名單方式自動將自己加入對方好友名單中。

4.4 訊息管理

■ **阻擋訊息：**

設定阻擋非好友傳遞來的訊息，可防止陌生人隨意傳送有害的連結、圖片、詐騙訊息等。本設定可於：其他→設定→隱私設定→阻擋訊息 中設定。

建議設定為自動阻擋非好友所傳遞的訊息，防止有心人士嘗試傳送有害的、釣魚的連結、圖片、詐騙訊息，降低誤點、誤觸、上當或被詐騙的可能性。

■ **封鎖好友**

對於疑似被盜用帳號亂發有害連結、圖片或其他原因需要暫時停止互動的好友，可先行封鎖，至好友帳號回復，不再亂發有害訊息為止。可於：其他→設定→好友→封鎖名單中進行管理。

對於可能遭到帳號冒用、盜用而傳送有害連結、圖片、詐騙訊息的好友，建議將其進行暫時性的封鎖，至好友狀態正常或取回帳號主控權為止。降低誤點、誤觸、上當或被詐騙的可能性。

■ **定期清理：**

定期清理轉存於 Keep 的暫存訊息，透過定期清理可能存放機密資訊的 Keep 內容，減

少機密資訊外流的可能性。本操作可於：其他→設定→Keep→全部刪除 進行之。

建議應該定期清理轉存於 Keep 的機密訊息、暫存訊息、及相關資訊。降低手機遺失或帳號密碼遭竊或是冒用，機密訊息外流的風險。

■ **訊息保護：**

開啟訊息保護(Letter Sealing)，使用點對點加密技術(End-to-End Encryption, E2EE)來增強文字訊息與所在位置資訊的保護，讓除了對話雙方外的第三方無法解密。但此功能僅限同時開啟此功能的好友有效。設定的方式為：其他→設定→聊天。語音通話→Letter Sealing

建議每位使用者都應該開啟使用點對點加密技術(End-to-End Encryption, E2EE)來增強文字訊息與所在位置資訊的保護，透過只存放於交談雙方而非伺服器端的金鑰對往來的訊息加解密，讓除了對話的第三方無法解密，但此功能僅限同時開啟此功能的好友有效。本設定目前支援平台包含了 Android、iOS、Windows、Mac OSX 等等。

■ **刪除訊息：**

完全刪除訊息，無法回復(True Delete)，設定完全刪除以後，任何方式的回復作為，將無法將已經刪除的對話訊息回復。設定的方式為：其他→設定→語音通話→刪除聊天內容

使用 True Delete 完全刪除訊息，無法使用任何方法回復。相較於以往的對話資料刪除只是註記 SQLite 資料庫中存放的對話資訊為已刪除，而並未真正刪除資料，若需要真正刪除資料有三種作法，覆寫、加密、或是消磁[28]。

True Delete 刪除資料時，除了刪除紀錄外，還會將原先存放資訊的實體，本項防護措施，自更新版本後，預設即是使用 True Delete 進行刪除，建議每位使用者都應該將程式版本更新，以避免紀錄遭到竊取並衍生相關資訊安全的風險。

■ **限時聊天：**

限時自動刪除聊天對話的內容，限制所傳遞訊息的顯現時間，時間終了，訊息自動消失。設定的方式為：聊天室窗中，點左上角對方使用者的名稱後，選擇限時聊天。

傳送交談訊息時，指定閱讀訊息的時間限制，限時訊息的接收方點選限時訊息後，開始計時，可成為原先需要手動刪除敏感或機密訊息的替代方案。但本設定仍然無法限制對方透過截圖、拍照方式保留限時聊天的對話內容，只能確保欲於事後進行刪除的對話資料，能正確的被刪除，建議使用此功能時，應適當評估可能的風險，謹慎使用。

4.5 版本更新

■ **檢查版本與設定自動更新：**

設定自動在 LINE 有最新版本發表時進行更新，為避免舊版本的 LINE 可能包含了潛在的危機，需設定自動更新至最新版本或時常檢查目前版本是否為最新。設定自動更新的方式為：Play Store→設定→自動更新應用程式，版本檢查： 其他→設定→關於 LINE(使用版本、最新版本)

透過應用程式更新，解決程式當中已知的漏洞、缺陷。或加強對已知攻擊的手法做出防護作為，例如，2015 年 2 月，日本電腦緊急應變中心 (JPCERT/CC, Japan Computer Emergency Response Team Coordination Center)及情報處理推進機構 IPA 通報：舊版 LINE 有安全疑慮，當用戶使用非可信賴業者提供的 Wi-Fi 網路，隨意連線惡意第三者設立的 Wi-Fi 服務，可能受到中間人攻擊(man-in-the-middle attack)，曝露資安風險。LINE 於接到通報後，立即著手相關程式加強、更新、反制的作為，並於 3 月針對兩大行動裝置平台，分別釋出了更新的修正程式，目前尚未傳出任何災情。

建議所有使用者都應該透過官方認可的應用程式下載渠道，設定應用程式為自動更新，以降低外在資安風險可能的影響。

5. 結論與未來展望

本研究透過將研究標的行動即時通訊軟體 LINE 的安全控制措施依照性質進行分類整理，並提出實際設定時的建議，希望能在詐騙手法層出不窮、帳號冒用盜用時有所聞、外部資安風險急遽升高的同時，能對使用者在使用行動即時通訊軟體，在安全性的設定上提供更進一步的參考，以增加個人資訊的防護，降低可能的風險。

展望未來，研究或可近一步透過問卷調查，將目前的分類項目結合問卷題項，評估使用者的安全意識與認知或是對行動即時通訊安全設定的熟悉程度，了解一般使用者在各個系統平台上使用即時通訊軟體時，是否會注意到資安風險的相關議題，探討外部持續升高的

資安風險對使用者使用即時通訊軟體影響，並希望藉以找到適當的方式能有效降低經由即時通訊軟體所造成的資安事件的風險。

參考文獻

[1] 王志斌，“結合層級分析法與德菲法發展資訊安全認知評量表之研究”，***世新大學資訊管理研究所碩士論文***，2009。

[2] 王可婷，“探討行動即時通訊貼圖對持續使用意圖之研究-以LINE為例”，***國立高雄第一科技大學-國際管理碩士學位學程碩士論文***，2014。

[3] 正確認識LINE「換機密碼」http://www.appledaily.com.tw/appledaily/article/headline/20140729/35986340/

[4] 行政院國家資通安全會報：行動裝置是否安全引發疑慮 http://www.icst.org.tw/NewsRSSDetail.aspx?seq=13989

[5] 邱顯貴，“影響使用即時通訊軟體行為意圖之研究”，***中央警察大學『資訊、科技與社會』學報***，**第 1 冊**，頁 2-3，2008。

[6] 何哲勳、陳俊忞、邱基峰，“即時訊息與現狀資訊相關技術-SIMPLE 與XMPP 之研究”，***電腦與通訊***，第 109 期，頁 41-54，2004。

[7] 宋曉玫，“以科技接受模式探討中高齡者使用網路即時通訊軟體之意圖與行為”，***國立台灣師範大學社會教育學系碩士論文***，2012。

[8] 何全德，“淺論國家資通安全工作推動方向”，***《網際空間：資訊、法律與社會》學術研究暨實務研討會***，2004。

[9] 吳丞璵，“行動通訊應用程式的使用行為意圖、滿意度對品牌偏好的影響”，***成功大學企業管理學系碩士論文***，2011。

[10] 洪唯軒，“消費者持續使用行動即時通訊軟體之研究”，***國立暨南國際大學，資訊管理學系碩士論文***，2013。

[11] 林素蓮，“結合科技接受模式及社會資本理論探討即時通訊App之持續使用意圖”，***中原大學資訊管理研究所碩士論文***，2013。

[12] 林杰彬，“社會互動超載： 探討影響行動即時通訊服務的社會與情感因素”，***國立中正大學資訊管理學系暨研究所碩士論文***，2014。

[13] 林德政，“安全即時通訊系統之設計與實作”，***國立交通大學理學院科技與數位學習學程碩士論文***，2011。

[14] 許孟祥、郭峰淵，“電腦倫理效能對電腦偏差行為之影響：以盜版軟體為例”，***管理學報，***第 18 期第 1 冊，頁 23-47，2001。

[15] 薛雅惠，“行動通訊軟體用戶持續使用之意圖研究-以 LINE 為例”，***國立臺灣大學商學研究所碩士論文***，2014。

[16] 馮千晏，“消費者採用即時通訊應用程式 之決策因素”，***國立政治大學企業管理研究所碩士論文***，2012。

[17] 張瓊怡，“即時通訊App貼圖訊息之持續使用意圖”，***中央大學資訊管理研究所碩士論文***，2014。

[18] 創市際ARO公佈台灣首份智慧型手機使用行為測量報告 http://www.insightxplorer.com/news/news_03_23_13.html

[19] 蔡燕平，“組織採用即時通訊軟體與組織溝通之研究”，***銘傳傳播學資訊管理所碩士論文***，2004。

[20] 趨勢科技新聞：台灣詐騙簡訊 五月份成功騙到近 89 萬次！ http://www.trendmicro.tw/tw/about-us/newsroom/releases/articles/20140602044903.html

[21] 趨勢科技新聞：資料安全威脅是行動世代的最大隱憂 針對 android 行動惡意程式數量持續飆升 擁抱BYOD 資安防護不可少 http://www.trendmicro.tw/tw/about-us/newsroom/releases/articles/20121030014735.html

[22] 趨勢科技新聞：百度SDK亂開後門，「蟲洞」影響1.4萬款程式上億Android裝置 http://www.ithome.com.tw/news/99696

[23] 蘋果日報：調查局語出驚人，LINE、WhatsApp 、WeChat 都能監聽 http://www.appledaily.com.tw/appledaily/article/headline/20131010/35353427/

[24] 舊版LINE有個資外洩風險，用戶儘快升級更新 http://www.ithome.com.tw/news/94623

[25] ETtoday 新聞：台灣學生駭客入侵，偷 NAVER 伺服器 169 萬筆個資 http://www.ettoday.net/news/20131115/296469.htm

[26] LINE 周邊程式列表 http://line.me/zh-hant/family-apps

[27] LINE 各平台程式下載 http://line.me/zh-hant/download

[28] LINE 版本更新訊息 http://official-blog.line.me/tw/archives/cat_567895.html

[29] LINE: True Delete http://developers.linecorp.com/blog/?p=3660

[30] LINE 在台好夯逾九成五民眾使用 http://www.bcc.com.tw/newsView.2639571

[31] LINE加入端到端加密功能確保用戶通訊隱私安全 http://www.ithome.com.tw/news/99268

[32] LINE 強化資安 徵才無上限 https://tw.news.yahoo.com/line強化資安徵才無上限-215007180--finance.html

[33] LINE 免費貼圖詐騙中，請保護好你的 LINE ID http://www.techbang.com/posts/12286-line-id

[34] Furnell, S. M., Bryant, P., Phippen, A. D., "Assessing the security perceptions of personal Internet users," 2007.

[35] Stafford, T. F., Belton, M., Nelson, T., Peevyhouse, A., "Exploring dimensions of mobile information technology dependence. Proceedings of the International Conference on Information Systems," 2010.

[36] TechCrunch: Thailand's Government Claims It Can Monitor The Country's 30M Line Users http://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/?ncid=rss

[37] The News Len: 南韓監控 LINE 等通訊軟體箝制反朴槿惠言論 http://www.thenewslens.com/post/82740/

[38] WikiPedia:LINE http://zh.wikipedia.org/wiki/LINE_%28%E6%87%89%E7%94%A8%E7%A8%8B%E5%BC%8F%29

[39] XcodeGhost災情比原先預期嚴重：可能有上千款app受感染，數量持續增加 http://www.ithome.com.tw/news/98950

[40] Tao, Z., Yaobin, L., "Examining mobile instant messaging user loyalty from the perspectives of network externalities and flow experience," ***Computers in Human Behavior***, Vol. 27, No. 2, pp. 883-889, 2011.