

# 初探即時傳訊安全

游啟勝 (csyu@icst.org.tw)

國家資通安全會報 技術服務中心

最後更新：2004.8

## 【摘要】

「您永遠不知道誰對您的通訊內容有興趣，或是正在欣賞您的對話。」即時傳訊帶來了機密資料洩露、惡意程式引入及軟體本身漏洞可能遭受攻擊三個主要的資安威脅。本文主要針對使用即時傳訊傳輸機密資料時可能被第三者截取的問題加以探討，並提出當前的解決方案。

## 【前言】

即時傳訊(IM, Instant Messaging)在這幾年來的興起，使得它成為繼全球資訊網、電子郵件、檔案交換之後最熱門的網路應用。即時傳訊提供企業一個比電子郵件有效率的溝通方式。只需有一台上網的電腦，利用它就可與其他同時線上的人進行即時溝通，而且成本極度低廉。因此已有部份公司甚至利用即時傳訊來進行跨地區的會議及進行公司內部的各項討論。

## 【即時傳訊的資訊安全威脅】

不過新的應用總是會對企業安全帶來新的威脅。即時傳訊主要的資安威脅與電子郵件雷同，主要包含：機密資料的洩露、可能引入惡意程式及傳訊軟體本身可能遭受攻擊。

機密資料的洩露主要是傳輸不適合的檔案或傳訊內容，或是通訊內容遭到第三者截取所造成。檔案接收功能則可能將惡意程式（病毒、木馬程式等）帶入企業內部網路。最後，有心人士可能利用攻擊傳訊軟體本身的

弱點藉此入侵系統。

傳輸不適當的內容應靠管理政策來解決。首先，企業應視使用即時傳訊的效益來取捨是否開放即時傳訊及開放的範圍，例如：是否可允許傳送檔案或進行語音對談及視訊傳輸。若是打算開放則應制定與電子郵件類似的管理政策來防止機密洩露的問題，並利用防火牆限制未開放的檔案及語音傳輸功能。惡意程式引入的問題不大，現有的防毒程式多會檢查下載的檔案是否為惡意程式，所以只要注意定時更新最新的病毒碼。軟體的弱點問題則應經常注意軟體是否有安全通報並勤於修補漏洞，同時利用防火牆及代理伺服器來避免安裝有即時傳訊軟體的主機直接曝露在網際網路上，以免遭受攻擊。

最後是傳輸的資料是否會被中途的第三者所截取及傳輸對象的認證問題。企業級的傳訊軟體都會特別註明傳送訊息會經過加密，如：IBM Lotus Instant Messaging Everywhere 及微軟的 Live Communications Server 都具有訊息加密功能。

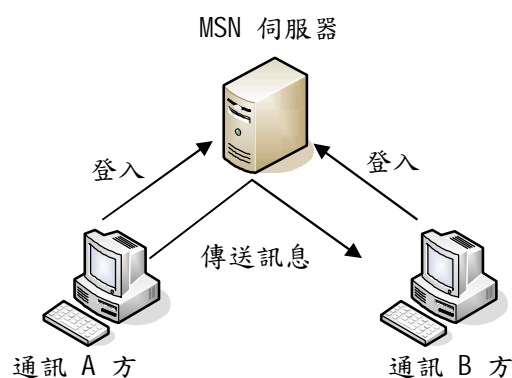
不過可惜的是目前大家常使用的傳訊軟體，如：yahoo messenger、MSN messenger，都未能對訊息加密，有心人士可以利用 ethereal 之類的網路竊聽工具，或是專門針對 MSN 的 MSN Sniffer 的特殊竊聽工具來截取通訊內容。此外，目前的即時傳訊協定也無法確保傳訊對象的身分，攻擊者可假造訊息，或是利用 session hijacking 的技術偽裝成您所認為的通訊對象與您進行交談。

#### 【即時傳訊的加密認證防護策略】

圖一是 MSN 傳送訊息的示意圖，首先通訊雙方都必須要以帳號密碼登入 MSN 伺服器才能進行之後的訊息傳送動作。而所有傳送的訊息也會先傳送到 MSN 伺服器再傳給通訊對方。舉例來說，通訊 A 方要傳送訊息給通訊 B 方，首先要先登入 MSN 伺服器，如果 B 方也有登入，A 方會看 B 方在線上，接下來便可以傳送訊息，所有訊息會先傳送到 MSN 伺服器再由伺服器轉送至 B 方。因此訊息很容易在傳送的途中被竊聽。而防止被竊聽的最好方法就是點對點的通訊加密，也就是 A 方到 B 方在通訊時由 A 方先將訊息加密，待訊息到 B 方後再進行解密。

但受限於目前的即時傳訊的架構多設計有集中的伺服器來轉送訊息，而非通訊雙方直接交換訊息。因此無法對整個封包內容(payload)進行加密，只能針對個別的即時傳訊協定(如：MSN 協定)的交談內容進行加密，至於協定中的其他欄位因轉送伺服器不支援加密，所以並無法加密。

所以就 MSN 來說，即使使用了文後的加密方法，攻擊者還是可以獲取部份通訊資訊，例如：傳訊的對象、好友名單等資料，但已無法看到傳訊的內容。



圖一：MSN 的運作模式

#### 【即時傳訊的加密解決方案】

根據統計，MSN Messenger、Yahoo Messenger 和 ICQ 是臺灣最普遍的三大即時傳訊軟體，其中又以 MSN 和 Yahoo Messenger 最為普遍，因此下面介紹的加密解決方案，至少能用在會 MSN 和 Yahoo Messenger 其中一種傳訊協定上。而現有的加密解決方案可以分為使用替代的傳訊軟體、使用代理伺服器、及使用附加程式達到加解密功能三類。

##### 一、使用替代的傳訊軟體

第一種方案主要是利用與 MSN 和 Yahoo Messenger 傳訊協定相容且具有加密功能的替代軟體來取代原有微軟及 yahoo 提供的傳訊軟體。

目前的幾個選擇方案如下：

- I gaim + gaim-encryption plug-in  
gaim (<http://gaim.sf.net/>) 是 windows 及 UNIX-like 平面上最佳的傳訊替代軟體，若需要在

UNIX-like 系統上進行即時傳軟，gaim 是目前最好的選擇，加上 gaim-ecryption 後，gaim 也能對訊息進行加密，文後會對 gaim 作一個詳細介紹及說明。

- I Miranda + SecureIM plug-in  
Miranda(<http://www.miranda-im.org>)是在 windows 及 alpha NT 上的傳訊替代軟體，加上 SecureIM 後能夠對 ICQ, MSN, YAHOO、AIM 等傳訊協定進行加密。
- I Trillion + SecureIM plug-in  
Trillion(<http://www.trillian.cc>)是另一個 windows 平台上的傳訊替代軟體，不過目前只支援 AIM、ICQ、IRC 加密。

## 二、使用代理伺服器加入加解密功能

在此方案中，則是利用代理伺服器 (proxy) 來加入加密功能。使用者還是使用原來微軟的 MSN Messenger 或 Yahoo Messgner，利用在傳訊軟體中設定代理伺服器，傳送時先將訊息送到代理伺服器進行訊息內容加密，到了目的主機後再進行解密。屬於此種類型的有：

- I SimpLite-MSN、SimpLite-Yahoo (<http://www.secway.fr/>) 安裝後會設定代理伺服器，由其對訊息加密。

## 三、以附加程式加入加解密功能

- I IM Secure (<http://www.zonelabs.com>) 安裝後只需輸入傳訊軟體帳號就能進行加密，不過免費版本只能支援一個帳號。

- I SpyShield(<http://www.commandcode.com>) 使用 GPG 來加密，不過現在只支援 MSN 5.0，似乎已停止發展。

經過實測上面數種現有的方案後，gaim 是筆者認為最佳的替代即時傳訊軟體。而 SimpLite-MSN 及 IMSecure 可以在不改變使用者習慣的條件下加強通訊的安全，適合應用在使用者沒有基礎電腦能力的環境，不過使用 SimpLite-MSN 為代理伺服器進行加密時，有時會有傳送訊息遺失的狀況，因此若是要使用原來的傳訊軟體，筆者建議使用 IMSecure。

## 【gaim 簡介】

gaim (<http://gaim.sf.net/>) 是一個可在多種作業系統平台上執行的即時傳訊軟體，也一直是 sourceforge 上最活躍 (most active) 專案的榜上常客。gaim 最初發展的原因有兩個：

第一是為開發出類似 Trillian、Miranda 可在同一介面上使用多種即時傳訊協定的傳訊軟體來避免需要安裝多套即時傳訊軟體的困擾。第二是想在 UNIX-like 系統開發出可與 windows 系統上的即時傳訊互通的軟體，因為 Yahoo messenger、MSN messenger 並沒有釋出可在 UNIX-like 系統上使用的版本，這些平台的使用者只好自行開發與其相容的傳訊軟體。

也因如此，現在 gaim 能同時支援 AIM、ICQ、MSN Messenger、Yahoo!、IRC、Jabber、GroupWise、Gadu-Gadu 多種即時傳訊協定，並能

在 Linux、FreeBSD、Windows、Solaris、MacOS X，甚至 iPAQ (qpe-gaim) 上運作。

不過 gaim 畢竟不像 MSN 或 Yahoo Messenger 擁有如此高的知名度，以下列出了用與不用 gaim 的幾個理由：

#### I 用 gaim 的理由

- n 高強度的訊息加密功能
- n 支援更多即時傳訊協定，並可同時登入，同種傳訊協定亦能允許多個帳號同時登入
- n 為開放原始碼軟體，且發展快速
- n 沒有煩人的廣告
- n 可以為好友自訂別名

#### I 不用 gaim 的理由

- n 無語音及視訊功能
- n 目前仍無法接收檔案傳輸
- n 沒有各種傳訊軟體花俏的介面及專屬的功能
- n 使用者介面較不為人熟悉

安裝完 gaim 和 gaim-encryption 套件之後，至「偏好設定」中的「模組清單」選單中勾取 gaim-encryption 套件就會產生 1024 bits 的金鑰。如果需要更高的加密等級，可以到圖二所示的 gaim-encryption 選單中重新產生各個帳號所要使用的加解密金鑰，最高支援到長度為 4096 bits 的金鑰。接下來只要傳訊對象也有使用 gaim 與 gaim-encryption，傳送的交談內容即會使用金鑰進行加密。因為使用公開金鑰加密法，因此也能對通訊對象進行認證。不過要注意的是，如果在多台主機使用相同帳號來登入

即時傳訊系統，也應將各台主機上的金鑰同步，以免通訊對象無法由金鑰做身份認證的動作。gaim 預設將設定檔和金鑰檔放置在 C:\Documents and Settings\Administrator\Application Data\gaim。若需要同步設定及金鑰只需複製此目錄即可。另外一點值得注意的是：gaim 並沒有對帳號密碼進行加密，故建議不要勾選「記住密碼」的選項，以免帳號密碼外洩。表一則是列出了一些選項設定，能讓 gaim 使用起來更加順手。



圖二：gaim-encryption 選單

#### 【結論】

目前大眾常使用的即時傳訊軟體，可以很容易地被第三者取得通訊內容。若您常用即時傳訊軟體傳送敏感的資訊，強烈建議使用專供企業使用的加密傳訊軟體、IMSecure、或類似 gaim 提供加密功能的替代即時傳訊軟體。您永遠無法預測誰正在截取您的通話內容，唯有做好最壞打算對通訊內容做高強度的加密才是根本防禦之道。

表一：gaim 設定列表

選 單	功 能	設 定 值
介面、好友清單	排序方式	依照狀態
	顯示好友圖示	取消勾選
模組清單	「WinGaim 選項」 「新版本通知」 「系統工作匣圖示」 「自動重新連線」	勾選
模組清單、WinGaim 選項	當 windows 啟動時同時啟動 gaim	勾選

【參考網址】

[1] IMSecure :

[http://www.zonelabs.com/store/content/catalog/products/sku\\_list\\_ims.jsp](http://www.zonelabs.com/store/content/catalog/products/sku_list_ims.jsp)。

[2] gaim : <http://gaim.sf.net/>。

[3] gaim-encryption : <http://gaim-encryption.sourceforge.net/>。