

即時通訊保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 何謂即時通訊?.....	3
即時通訊在商業上的應用趨勢	3
II. 潛在威脅	4
III. 企業選擇即時通訊解決方案之考慮	6
IV. 最佳作業實務	7
給企業用戶的貼士	7
給終端用戶的貼士	8

摘要

迅速增長的即時通訊（Instant Messaging, 以下簡稱 IM）是家庭和企業用戶皆認識的熱門通訊媒介，雖然 IM 是一種有效及容易使用的網絡通訊工具，但若沒有適當的保安措施，它也會帶來許多保安風險。本文介紹關於使用這流行通訊渠道時所面對的保安風險，以及商業機構推行及採用 IM 時的最佳作業實務。

I. 何謂即時通訊?

即時通訊 (IM) 是透過近乎是即時的傳送和接收網絡訊息，來進行臨時的 (ad hoc) 和現場實況播送 (live) 的電子通訊模式¹，隨著 ICQ²和 MSN Messenger³等通訊工具的出現，越來越多人享受即時通訊系統，為生活所帶來的便利和舒適。同時，IM 也使用於商業服務上，例如與顧客和合作夥伴溝通、提供客戶支援、接收實時警告訊息、以及計劃管理和協調等服務。IM 工具支援需要迅速回應和快速解決問題的流程，也提供比電子郵件和電話更快速的通訊方式。

一般而言，用戶需要下載和安裝 IM 客戶端 (client) 在其電子設備 (可以是桌上型電腦、智能手機或 PDA)，在進行通訊之前，用戶必須設定其帳戶。IM 伺服器存放着用以找出聯絡資料的數據庫。對如 ICQ 和 MSN Messenger 之類的公共 IM 服務而言，該伺服器是存放在互聯網上的。對企業 IM 系統而言，IM 伺服器也許是寄放在機構的內部網絡中。

即時通訊在商業上的應用趨勢

根據 2007 年進行的即時通訊趨勢調查⁴，IM 不單受到家庭用戶所歡迎，也漸漸在辦公室內普及使用，調查中指出超過 27% 的人表示他們在辦公時使用即時通訊，大約 19% 的 IM 用戶指出他們傳送即時訊息給同事或同僚多於傳送電子郵件，而 55% 的青少年透過 IM 來得到作業上的幫助。此外，一半在工作上使用 IM 的用戶表示他們相信 IM 讓他們在工作上更有效率。然而，將近 79% 在辦公室使用 IM 的用戶指出他們使用 IM 來處理個人事務。

¹ <http://www.tech-faq.com/instant-messaging.shtml>

² <http://www.icq.com/>

³ <http://www.msn.com/>

⁴ http://press.aol.com/article_display.cfm?article_id=1343

II. 潛在威脅

公共 IM 服務已迅速成為散播病毒和惡性程式碼的另類渠道，一般公共 IM 服務不但通常缺乏加密功能來保護傳輸中的訊息，而且還能繞過公司的內容偵測過濾器。再者，缺乏完整的審計記錄，也許無法達到機構特定的保安或法規的遵從要求。

以下是使用 IM 服務的潛在威脅：

1. 惡性程式碼的散播工具

企業使用 IM 的數量和重要性日益增加，IM 用戶指出他們能夠從中得到較快速的決策過程、較高的生產力和較低的電訊服務成本等好處，但同時 IM 威脅（一般是病毒）亦快速地增加，因攻擊者開始把他們的注意力從漸漸得到更佳保護的電郵系統轉移到 IM 網絡上。濫發訊息也會透過 IM 散播，用戶透過 IM 服務接收的濫發訊息稱為 SPIM⁵。

2. IM 軟件漏洞

如同其它軟件應用程式，熱門的 IM 客戶端亦有其存在的保安漏洞，安裝 IM 客戶端可能會在電腦系統中引進新的保安漏洞。

3. 敏感資料外洩

當使用公共 IM 服務作為通訊方式時，保密性是一項重要的考慮。在公共 IM 網絡中，用戶間之訊息交換是透過 IM 伺服器中心所發送的，IM 伺服器中心是由服務提供者控制的，假如客戶端 IM 軟件有對等式（peer-to-peer）能力，用戶不需透過 IM 伺服器便可以彼此通訊了，無論使用哪一種模式，IM 傳輸都有被竊聽的弱點，因為大部份公共 IM 客戶端不具有任何加密能力，因此，未經授權用戶可能經此渠道讀取到敏感的資料。當公共 IM 服務使用於與機構外的人溝通時，情況則會愈加嚴重。

公共 IM 服務使用的規約通常被人認看為有欺詐的成份，因為這些規約是特地設計來迴避標準保安控制的，IM 客戶端不僅可透過 SOCKS 或是網上代理伺服器來安裝連接，規約也可穿越防火牆來尋找如 TCP 埠 80 等開放埠，或在

⁵ <http://www.quickonlinetips.com/archives/2005/10/spim-instant-messaging-spam/>

HTTP 要求中打開傳輸渠道，使其無法與標準網上傳輸分辨，IM 系統的手稿程式能力和檔案傳送能力也可能使機構處於敏感資料外洩的危險，因此機構應該在 IM 使用上訂立合適的保安政策和控制措施。

4. 監察和保留的難題

監察 IM 訊息和保留訊息作為商業紀錄用途並不是一項簡單的任務，在 IM 環境中決定需要記錄哪些即時訊息似乎顯得更加困難，因為要記錄一連串的訊息才可對特定訊息提供有意義的內容。

5. 職責 (Accountability)

在公共 IM 網絡中，IM 寄送者和接收者的身份是無法證實的，公共 IM 帳戶有著被竊持 (hijacking) 和仿冒 (spoofing) 的弱點，可讓入侵者與合法的用戶進行對話。

III. 企業選擇即時通訊解決方案之考慮

市場上出現了許多為企業而設的 IM 解決的方案，這些方案給予機構建立和管理其內部 IM 服務的能力，當選擇企業 IM (EIM) 解決方案時，該考慮的保安要求有⁶：

1. 認證控制：任何企業的 IM 解決方案應與公司現有的認證機制整合，例如：與微軟 Active Directory 接合。
2. 保密性控制：EIM 產品應該提供強大的加密功能，以保護企業網絡中的所有傳輸訊息，因為預算或銷售量數據等敏感資料也許會在企業的 IM 系統中傳輸。
3. 抗電腦病毒控制：EIM 應該與抗電腦病毒解決方案進行封閉整合，以確保所有透過 EIM 渠道傳送的檔案沒有受病毒感染。
4. 記錄/審計控制：為了確保員工沒有濫用該服務或滿足特定的法規要求，機構內所有即時通訊也需要記錄下來。選定的 EIM 產品也應達到機構的記錄要求。

此外，機構需要定義可接受的 IM 使用方式和私隱政策，並對所有員工簡介在商業上使用 IM 的風險。假如公司記錄及監察 IM 訊息，該政策也應清楚地告知所有員工。

⁶ http://www.instantmessagingplanet.com/enterprise/article.php/11208_2236051_1

IV. 最佳作業實務

給企業用戶的貼士

當明白到 IM 系統有著許多潛在的保安風險，IM 的使用應僅限定於商業用途上，在推行任何系統（公共或私人）時，也應取得事先的核准。假如機構決定使用 IM 系統，應推行以下保安措施：

1. 遵守所有保安程序

基本原則是當使用 IM 時，應遵守所有相關保安要求。

2. 開發 IM 使用政策和清楚地向所有 IM 用戶發布

無論機構是否接受使用 IM，皆應清楚說明 IM 使用政策。假如機構接受使用 IM，也應清楚說明有哪一些限制。IM 使用政策對科技和產品應是中立的。無論 IM 訊息是由公共系統或企業內部系統發放，該訊息應認為是商業記錄。假如 IM 使用於商業用途上，應遵守及執行內部保留政策或外部規例。

3. 推行 IM 衛生（Hygiene）解決方案

IM 衛生解決方案是一個服務集合體，准許機構強制執行 IM 使用政策，透過監察使用、管理 IM 傳輸和過濾內容來阻擋不想要的訊息、電腦病毒和冒犯內容，並記錄所有 IM 訊息作為審計用途。

4. 教育用戶 IM 的最佳使用方法和加強桌上（Desktop）保護

企業網絡內受到 IM 的其中一個主要威脅，便是基於 IM 的惡性程式碼攻擊，IM 病毒通常以可執行附加檔（executable file attachment）或是以 IM 文本超連結形式傳輸，引導受害者連結到惡性程式碼伺服器，在大部份的例子當中，這些病毒並不會自動執行，反之，它們利用社會工程（social engineering）策略來說服受害者開啟未知檔案或按下可疑連結。

專用的 IM 衛生產品可作為保護和管理使用 IM 的解決方案，透過過濾活動中

的超連結和所有附加檔案，這些產品有效地刪除大部份 IM 病毒所帶來的攻擊方法。桌上抗電腦病毒產品也有助偵測大部份的威脅。

訓練終端用戶對於傳入的即時訊息保持警覺也是整體策略的一部份，縱使是他們的朋友所傳來的訊息，也應保持懷疑態度。快速修補軟件漏洞、執行抗電腦病毒軟件和個人防火牆等經常性預防措施，皆是有效防範 IM 威脅的措施。

基於以上內容，當在企業內計畫推行 IM 時，用戶培訓和桌上保護都應考慮。

5. 執行企業 IM (EIM) 解決方案，而非使用公共 IM 客戶端

當 IM 服務用於商業用途，機構應探索所有部署企業 IM 架構在網絡環境中的各種可行性，此舉將導致廣泛的監察和數據儲存，並對有關內部用戶的身份加以保證。此外，一個封閉的系統對主要顧客和外部供應商仍是可行的，但所有外來的 IM 應透過監察和管理的通訊閘進入。企業 IM 解決方案為機構提供客戶端和伺服器端內建的企業保安功能，包含阻擋、記錄、審計、監察、路徑規劃和加密。

6. IM 客戶端保護

用戶應移除使用 IM 服務所提供的所有網絡服務功能，當接收進入的訊息/通話/檔案時，用戶應啟動所有通知訊息功能，用戶也需移除分享資源功能，並移除遠端執行麥克風和網路攝影機功能。

給終端用戶的貼士

以下是給終端用戶使用 IM 作為一般通訊工具的貼士⁷：

1. 不要設定 IM 客戶端自動接受檔案傳輸，假如你設定此功能，你將會處於自動接受電腦病毒感染檔案的高度風險中。
2. 在開啟從 IM 接收來的任何檔案時，你應要查證寄送者確實寄送檔案給你，此外，在開啟檔案之前，確定檔案已被抗電腦病毒軟件掃描過。
3. 絕不可按下從不被信任/不知名的 IM 用戶寄來的 URL 連結。有許多報告指出，病毒是透過用戶按下 IM URL⁸所傳播的。
4. 絕不在 IM 上寄送個人或敏感資料，即使有不得已的理由，也要確保敏感資料已加密。

⁷ <http://chris.pirillo.com/2007/11/17/instant-messenger-virus/>

⁸ <http://antivirus.about.com/od/virusdescriptions/a/kelvir.htm>

5. 保持 IM 軟件(和其它系統零件)更新至最新修補程式、開啟個人防火牆保護、安裝具有最新病毒識別碼和最新惡性程式碼定義的抗電腦病毒軟件、以及安裝偵測和修補引擎。