第一章　匿名電子文件的起源與防制

1.1 概述

匿名電子文件的防制之目的，簡單的說，就是要確保電子文件的發函人能夠被正確地記錄在其所發送的電子文件之內。亦即在電子文件的稿頭(header)中有關From欄位的資料，足以正確地描述出原始發函人。但以現今TCP/IP或UUCP的技術而言，這項工程似乎是不精確的、消極的。原因有二：

- 當電子文件以區段(segment)的格式在網路上傳送時，發函人的資料並沒有像區段的起、迄地址一樣，被記錄在區段標頭(segment header)中。而原電子文件的檔案屬性(attributes)如檔案擁有者，也不會被記錄在區段中。有關發函人的資料必須從區段的資料區(data field)去尋找才能獲得。因此，對於已經離開收、送站並向外流傳的匿名電子文件而言，此時所做的任何挽救都已經是於事無補。
- 幾乎所有TCP/IP與UUCP上的應用程式都提供了彈性空間，讓發函人不受拘束地在電子文件中改變預設的發函人資料。具體的用法是使用者可以在Mail或News的應用程式中改寫From或Sender的資料。雖然在許多RFC文獻中對信函格式(message format)與發函人資料皆有嚴格的規定[1]，但鮮少有應用程式在確實遵循。

然而在網路被濫用的情況下，爲繫網路正義與網路道德於不墜，任何防範與補救的措施仍然有其必需性。附錄二所附的文章足以顯示出匿名電子文件對網路使用者與管理者的威脅性。[2]

1.2 防制工程

---

[1]如RFC822、RFC976與RFC1036。

[2]附錄二所附的黑函出現於News中的alt.hackers，時間爲1993年5月。當時幸虧數名國外的網友好心來函相告，因此免去了不少困擾。

由於目前匿名電子文件的來源有二：電子郵件與電子新聞。而電子文件的傳送，可以在即時傳送(real-time transmitting)系統如TCP/IP的架構下進行，亦可在批次傳送(batch mode transmitting)系統如UUCP的架構下爲之[1]。本文將就下列的次序，分別來探討匿名電子文件的防制之道：

- 即時傳送架構下News的防匿方法
- 即時傳送架構下Mail的防匿方法
- 批次傳送架構下News與Mail的防匿方法

此外，不論是在即時傳送或批次傳送架構下，在對News或Mail進行防匿工作前，我們應有下列三點認知：

- 實行防匿措施的最佳時機，是在匿名者完成電子文件的傳送前。因爲當匿名電子文件離開收、送站並向外流傳後，我們已經無法從文件的內容或檔案的屬性來追查原始發函人的資料。
- 實行防匿措施的最佳地點，是在收送匿名電子文件的主、客站上。
- 實行防匿措施所需的各項資訊(如匿名者的帳號、匿名的地點、時間)，必須從匿名者所在之系統的主記憶體中直接擷取。任何間接的、非即時的資訊(如系統的各項記錄檔pacct、syslog、wtmp等)，不但在應用上的效率(performance)不好，且其正確性亦無法掌握。

在本計劃中所提及相關應用程式的修正方法，我們將以NNTP、INN、TIN與sendmail[2]來作輔助說明[3]。

---

[1]在TCP/IP的架構下亦可進行批次傳送。
[2]本計劃所用之sendmail以V8版本爲主，IDA版本爲輔。
[3]這些軟體的原始程式可以在任一FTP站(如nctuccca.edu.tw)取得。