電子郵件退信攻擊之因應措施

范修維
世新大學資訊管理學系
fan@cc.shu.edu.tw

摘要

電子郵件系統的回函機制是網際網路運作的標準之一，幾乎所有的電子郵件伺服器都支援這項機制。但是這項機制卻可能被惡意人士利用來作為電子郵件攻擊的跳板。利用大量電子郵件所產生之退信作為攻擊的工具，至今時有所聞。如何避免自己的郵件伺服器成為攻擊者利用的工具，此乃本文之目的。電子郵件的回函機制除了可能成為郵件攻擊的工具外，亦可用來驗証或探測郵件名單之有效性，垃圾郵件發送者可利用回函機制進行電子郵件名單的收集。本文除了探討如何避免成為郵件退信攻擊之工具之外，亦同時探討如何避免被惡意人士進行電子郵件名單之探測。除了在理論上的探討，本文亦輔以實務設定作參考，使得相關建置可以更容易地完成。

關鍵詞：回函、退信、郵件炸彈、透通式郵件閘道器

Abstract

The DSN mechanism of e-mail system is the standard of the Internet operation. Today, all the e-mail servers have supported this mechanism. This mechanism has been used to attack the e-mail system by attackers. Besides, the huge bounce mail has become an attack tool. How to avoid becoming the attack tool of used e-mail server is the purpose of this paper. Furthermore, DSN mechanism of e-mail also has been used to verify or test the validity, spammer uses DSN mechanism to access the collection of e-mail list. In this paper, we propose a tool to audit the attack of bounce mail and the probing of e-mail list by attackers. The purpose of this paper shall obtain the theoretical research and practical setting in order to get the ideal implementation.

Keywords: DSN, bounce mail, email bomb, transparent mail gateway

1. 前言

利用電子郵件作為攻擊的工具是現今常見的資安事件之一，攻擊者利用大量電子郵件來灌爆收信人信箱或是癱瘓電子郵件主機。利用電子郵件退信的特性，攻擊者可以故意製造大量退信，並將退信的目的地指向被攻擊者，這些退信就會送往所指定的目標。藉由同時讓多個郵件伺服器產生退信，攻擊者可以輕易達成 DDoS 的攻擊效果。

雖然退信機制是電子郵件正常運作下的產物，但是被攻擊者利用而成為攻擊之跳板，仍會被視為攻擊的來源。因此，如果沒有對這些退信加以控制，產生大量退信的郵件伺服器很容易就被列入 DNSBL[2] 黑名單。

除了攻擊者故意製造大量退信以攻擊特定目標之外，當郵件伺服器收到垃圾郵件時亦可能產生大量的退信。部分垃圾郵件發送者採用暴力方式 (Brute Force) 瞎拚亂湊地指定收信人地址以寄發大量垃圾郵件，其目的雖不在於攻擊某個電子郵件信箱或郵件伺服器，但是其所產生之退信效應仍不亞於郵件炸彈所產生之效果。

除了暴力猜測寄發大量垃圾郵件之外，學生帳號亦可能導致大量退信之產生。每當學生畢業，大量畢業生帳號從郵件伺服器刪除後，垃圾郵件寄到這些已畢業學生之帳號就會產生退信。

雖然退信機制是電子郵件運作的標準之一，但是因為它已經被不當利用作為攻擊之工具，因此產生大量退信之郵件伺服器往往被視同為攻擊來源而被列入黑名單。

產生大量退信的原因，大部分都是因為查無相對應之收信人帳號而引發的 User Unknown 退信，如果我們可以針對這類的退信進行特別處理，就可以避免許多退信的問題。當然，除了 User Unknown 所引發的退信之外，其它如 Host Unknown、Quota Exceeded、……等原因亦可能產生退信，只是要發生這樣的退信並爆發巨量郵件需要相關外在因素地配合才會產生，因此鮮少被用來作為攻擊的工具。

對於 User Unknown 所產生之退信，其與郵件系統之架構有關。當郵件系統規模很小時，僅具有一台郵件伺服器，User Unknown 之退信幾乎不會造成任何困擾。但是如果郵件系統規模擴大，增加了郵件的代收與備援，這些退信的問題就會隨之產生。

電子郵件之退信機制已於 RFC 1891[3] 列入標準，並加以擴充而成為回函通知 (Delivery Status Notification，簡稱 DSN)，除了明定郵件傳送失敗與延遲傳送所產生之回函通知之外，另新增了成功寄達通知。部分郵件名單收集者可利用這項郵件寄達通知來探測電子郵件名單之有效性，藉以驗証並

更新所收集的郵件名單，進而寄發更多有效的垃圾郵件。

因此，本文的主要目的就是探討在郵件系統之架構與產生回函通知之關聯性，以及如何因應大量 User Unknown 所引發之退信。不同的架構、不同的因應措施會有不同的效果，當然也會有不同的建置成本以及所產生的伴隨效應。

在接下來的章節裡，我們先針對 RFC 1891 所制訂的郵件回函機制作扼要的描述，接著於第三節中討論郵件系統架構與退信產生之關聯性。在實作方面，我們提出了四種不同的因應之道，以應付不同場合之需求；此外，對於電子郵件帳號之探測，我們也提出了因應對策，這兩部分將於第四、五節作詳細地說明。最後，我們亦以本校的建置經費作為實測說明，並作簡單的結論。

2. 電子郵件系統的回函機制

在電子郵件系統的運作中，當郵件傳送失敗或產生延遲時，會由 SMTP 伺服器產生 Bounce Mail 通知原寄信人，這個 Bounce Mail 即一般所稱的「退信」。

在 RFC 1891 標準制訂之前，這些 Bounce Mail 並沒有統一的標準。而在 RFC 1891 的規範中，除了將郵件傳送「失敗」與「延遲」所產生的 Bounce Mail 納入「回函通知」之外，亦新增傳送「成功」回函通知，並且允許寄信人明確指定是否要產生上述三種回函。

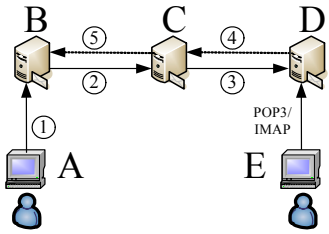

圖 1 電子郵件傳送示意圖

在圖 1 的電子郵件傳送示意圖中，寄信人從個人電腦 A 寄發電子郵件，其 SMTP 伺服器設定為 B 主機。B 主機在收到電子郵件之後，將信件寄往郵件閘道器 (或郵件中繼站) C 主機，最後再轉送到目的 D 主機。收信人由個人電腦 E 透過 POP3 或 IMAP 協定到 D 主機將信件取回。

按照 RFC 1891 之規範，個人電腦 A 將信件寄出時，可以在 SMTP 協定的 RCPT 指令加入 NOTIFY 參數，並給予 SUCCESS、FAILURE、DELAY 或 NEVER 參數值。這些參數的設定會使得 SMTP 伺服器產生不同的回函運作：

1. SUCCESS
   當信件成功寄達目的地主機時，目的地主機 (亦即 D 主機) 必須給予回函通知，此即為「信件寄達通知」。
2. FAILURE
   當信件寄送失敗時 (如 User Unknown、Host Unknown、Quota Exceed…)，無法成功地將郵件傳遞給下一級 SMTP 伺服器或 MDA 郵件派發程式時，該 SMTP 伺服程式就必須給予回函通知，此即為「送信失敗通知」。一般常見的 Bounce Mail 或退信，即屬於此類回函通知。
3. DELAY
   當信件無法在正常時限傳送給下一級 SMTP 伺服器或 MDA 程式時，發生延遲的 SMTP 伺服程式必須給予回函通知，此即為「送信延遲通知」。
4. NEVER
   不管信件是否成功寄達目的主機，或是產生延遲與失敗，均不給予回函通知。

除了 NEVER 參數值之外，其餘三項可合併使用。如果不指定 NOTIFY 參數，則 SMTP 伺服器可視為 FAILURE 或 FAILURE + DELAY。

產生回函通知有諸多原因，茲將常見的原因列舉如下：

1. User Unknown
   此為收信主機無相對應的收信人帳號。通常這個回函是由收信主機的前一級 SMTP 伺服器所產生 (如 C 主機)，但部分經過特別設定的情形下，亦可能由收信主機所發出 (如 D 主機)。幾乎所有的退信攻擊或垃圾郵件所產生的大量退信都源自於此。
2. Host Unknown
   當 SMTP 伺服器代收信件之後，卻無法解析下一級收信主機的位址時，就會產生 Host Unknown 的回函。通常這個回函是由郵件中繼器所產生 (如 B、C 主機)，但是當收信主機設定錯誤時，亦有可能由收信主機 (如 D 主機) 所產生。
3. Quota Exceeded
   當收信主機收到信件後欲寫入收信人信箱時，卻發覺磁碟空間配額不足，此時即可能產生這個回函。通常這個回函是由目的主機 (如圖 1 的 D 主機) 所產生。
4. Successfully Delivered
   當收信主機成功地將所收到的信件寫入收信人信箱時，且原寄信人指定了 NOTIFY=SUCCESS 之回函要求，收信主機就會產生回函通知 (如 D 主機)。

根據 RFC 1891 的規定，NOTIFY 參數之設定只能在信件寄出時作指派，中間轉運郵件的伺服器

都必須保留該信件之原始設定。如果中途遇到不支援 DSN 機制的郵件伺服器，則前一級支援 DSN 機制的 SMTP 伺服器必須進行必要的處理或回應。當郵件伺服器不支援 DSN 運作時，此時 RFC 1891 規定之前的運作模式，亦即將視為 FAILURE 或 FAILURE + DELAY。

須瞭解的是，NOTIFY=SUCCESS 與一般常見的「讀信回條」通知是不同的。當我們開啟一封電子郵件時，MUA (如 Outlook 或 Openwebmail) 會詢問使用者是否要產生讀信回條，這個讀信回條是紀錄在電子郵件的標頭 (Disposition-Notification-To 欄位)[4]，並且允許讀信者決定是否產生該回條。而 NOTIFY=SUCCESS 的 DSN 回函則完全不同，它是在信件成功寫入收信人信箱時就自動產生回函，不是在閱讀信件時才產生；而且該回函不能由收信人決定是否產生，而是由寄信人所指定；並且這個 DSN 回函要求不會出現在電子郵件的標頭欄位，而是出現在 SMTP 傳輸協定的 RCPT 參數中。

3. 郵件系統架構與產生退信之關聯性

郵件系統架構與退信的產生具有很大的關聯性，在不同的架構下，外界所視為的大量退信來源可能會有所不同。我們必須先瞭解退信產生之源頭，才可能採取相對應的防治之道。

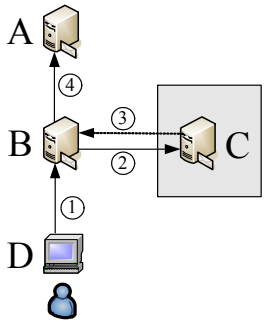

圖 2 最小規模的郵件系統架構

如果電子郵件系統僅具有單一的郵件伺服器，沒有其它的郵件中繼器或閘道器、也沒有其它的郵件備援主機或郵件代收主機時，即為最小規模的郵件系統架構，如圖 2 的 C 主機。如果垃圾郵件發送者對 C 主機發出大量垃圾郵件而產生 User Unknown 之退信時，其情形如下：

1. 垃圾郵件發送者在個人電腦 D 操作，將 SMTP 主機指向 Internet 上的 Open Relay 伺服器 B，將大量垃圾郵件寄出。
2. 當垃圾郵件的收信人地址為 C 主機時，Open Relay 主機會將垃圾郵件傳送到 C 主機。
3. 如果收信主機 C 查無收信人帳號，則會拒收該信件。
4. Open Relay 主機送信失敗，此時會按照 DSN 運作機制，將信件退回原寄件人。如果寄件人地址填入 A 主機之帳號，則此退信會被傳送到 A 主機。

在上述的過程中，雖然會有大量的 User Unknown 退信產生，但產生退信的主機是 Open Relay 伺服器 B，而非我們的郵件伺服器 C，因此我們無需對這些退信作理會。

對於某些自帶 SMTP 引擎的垃圾郵件發送軟體，它可能直接與收信主機的 SMTP 服務程式作連線而不依賴外部的 Open Relay 主機時，個人電腦 D 將會直接向郵件主機 C 發出 SMTP 連線請求。一旦連線建立，郵件主機 C 會查詢是否有收信人帳號，如果該帳號不存在，則拒收該信件。此時個人電腦 D 會得知寄信失敗，但不會產生任何退信。

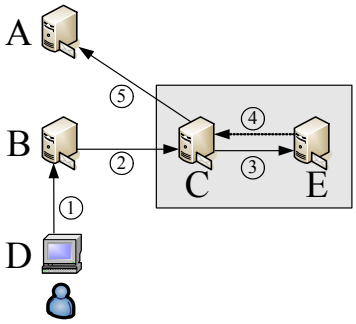

圖 3 具有郵件中繼功能的系統架構

在圖 3 的架構中，主機 C 是電子郵件閘道器，使用者帳號與 POP3/IMAP 服務則在後端的主機 E 中。郵件閘道器 C 負責對外界進行 SMTP 的溝通，可執行郵件代收、郵件備分、郵件過濾…等各項功能，而後端的電子郵件伺服器 E 則隱身於 Intranet，不直接對外作通訊。這種架構擁有較高的安全性以及備援能力，常見於企業網路及校園網路。在此架構下，垃圾郵件的發送以及退信的產生流程如下：

1. 垃圾郵件發送者在個人電腦 D 操作，將 SMTP 主機指向 Internet 上的 Open Relay 伺服器 B，將大量垃圾郵件寄出。
2. 當垃圾郵件的收信人地址為 C 主機時，Open Relay 主機就會將垃圾郵件傳送到 C 主機。
3. C 主機只是一個郵件中繼主機，不具有使用者的帳號，因此當 Open Relay 將信件傳送過來時，它無法進行收信人帳號是否存在的檢核。只要收信人地址符合郵件代收之條件，C 主機就會將信件收下。
4. 當 C 主機將所代收之信件送往後端電子郵件主機 E 時，E 主機會檢查是否有相對應的收信帳號，如果沒有則拒收信件。

5. 當 C 主機送信給 E 主機並遭拒收時,就會按照 DSN 之機制傳送出退信通知給原寄信人。如果寄信人地址之主機為 A 主機，則該退信就會送往 A 主機。

在此情形下，雖然 B 主機是 Open Relay 伺服器，但是 C 主機會成為大量退信的來源主機，同樣會被視為郵件攻擊來源之一。由於 C 主機屬於我們所管轄之範圍，因此我們必須對其所產生之退信進行管制措施。

對於自帶 SMTP 引擎之垃圾郵件發送程式而言，個人電腦 D 會直接與 C 主機作 SMTP 連線，C 主機也會因為收信人地址符合郵件代收之條件而收下，最後也會因為 E 主機查無相對應的收信帳號而產生退信給 A 主機。

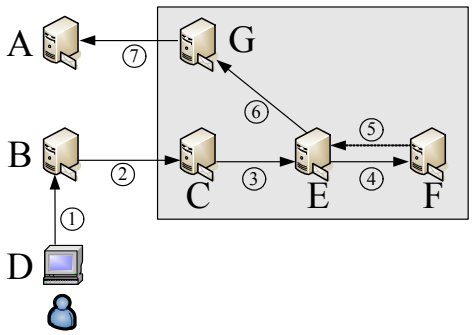

圖 4 具有內收與外寄郵件閘道器之架構

如果電子郵件系統規模變得更大 (如圖 4 所示)，單位內部可能具有內收郵件閘道器 (C 主機) 與外寄郵件閘道器 (G 主機)，並且於 POP3/IMAP 郵件伺服器 (F 主機) 之前另外增加郵件中繼器 (E 主機) 進行各項郵件作業，諸如：郵件備分、郵件過濾…，則此時垃圾郵件的退信會由 E 主機所發出，並透過 G 主機傳送到 A 主機。在此情形下，G 主機與 E 主機均可能被列入垃圾郵件的黑名單 (如果 E 主機屬於 Intranet 之主機，則 G 主機會被視為退信之責任來源主機，如果 E 主機屬於 Internet 之主機，則 E 主機會被視為退信之責任來源主機)。

4. 防止大量退信之對策

為了防止垃圾郵件所產生的大量退信，我們提出了下列四種因應之道：

1. 於終端電子郵件伺服主機 (圖 3 的 E 主機與圖 4 的 F 主機) 作設定，使其不會拒收任何郵件。既然郵件主機不會拒收任何郵件，當然也就不會產生 User Unknown 之退信。
2. 於內收郵件閘道器 (圖 3 的 C 主機與圖 4 的 C 或 E 主機) 作設定，使其所轉運之信件禁止產生任何 DSN 通知。只要將 DSN 機制的 NOTIFY 參數設定為 NEVER，不管信件派送成功與否，都不會有任何的回函通知。
3. 於外寄郵件閘道器 (圖 3 的 C 主機與圖 4 的 E 或 G 主機) 作設定，過濾任何來自於內部的 DSN 通知信件。既然所有 DSN 回函通知信件全部都被過濾，外部自然也就收不到退信。
4. 於最外層的內收郵件閘道器 (圖 3 與圖 4 的 C 主機) 作設定，對內收信件先作帳號檢查，如果查無相對應之帳號則直接拒收郵件。既然在最外部的郵信閘道器可檢查收信人地址是否正確，此時郵件系統架構就如同回歸於圖 2 之架構，當然不會有 User Unkown 的退信問題。

上述方法只要任選一種，即可避免 User Unknown 所產生的退信困擾。然而，不同的方法會有不同的伴隨效應，也會用不同的適用場合與時機，以下將針對上述四種方法作進一步的探討與說明。

4.1 接收所有信件

之所以會產生 User Unknown 退信，就是因為最後端的郵件伺服器拒絕接受無收信帳號的信件。如果我們能在該郵件伺服器作設定，不管收信帳號是否存在，一律接受所寄來之郵件，這樣就不會導致前一級的郵件轉運站產生 User Unknown 的退信。至於無收信帳號之郵件，我們可以直接丟棄，不予理會。

在 sendmail[7] 的實作並不困難，只要將 sendmail.mc 加入下列的設定即可：

```
define(`LUSER_RELAY',`local:/dev/null')dnl
```

使用這種方法來防止垃圾郵件的退信通知可說是最簡單的方式，但它會產生下列的伴隨效應與限制：

1. 它會增加郵件伺服器些許的負擔 (必須接收所有無收信帳號的信件)，不過這些負擔應該不致於產生困擾。
2. 當正常郵件的寄信人誤植收信人地址時，該寄信人將收不到退信通知 (包含 Internet 與 Intranet 的寄信者)。
3. 它僅能防止「User Unknown」的退信通知，但無法防止「Quota Exceeded」的退信通知。亦即，一旦攻擊者發現某個電子郵件帳號的磁碟配額已經超過時，即可改用這個收信人帳號作為攻擊的跳板 (雖然這種方式並非很常見)。
4. 它必須在郵件中繼器後端所有的郵件伺服器都啟用同樣的設定，只要有所遺漏，都可能導

致前端郵件中繼器產生 User Unknown 退信。

5. 如果郵件中繼器屬於透通式郵件閘道器 (Transparent Mail Gateway)[1]，則這個方法將不適用，因為所有寄往非電子郵件主機之信件 (如寄往 FTP 主機之信件，但該主機未開啟 SMTP 服務) 仍會被透通式郵件閘道器所代收，仍會發生退信通知的問題 (信件延遲通知與送信失敗通知)。

4.2 禁止產生 DSN 信件通知

按照 RFC 1891 的規定，是否要產生退信通知是由寄信端的程式所指定，中間的郵件轉運站不得修改 DSN 之參數。如果寄信端的程式未指定 DSN 之參數，或是郵件伺服器不支援 DSN 之運作，則視為 FAILURE 或 FAILURE + DELAY。

由於 RFC 的規定非常明確，因此 sendmail 並不提供中途修改 DSN 參數的功能，只有在寄出信件的時候才能指定 DSN 參數。為了達到抑制 DSN 的回函通知，我們將利用 Procmail[5] 信件處理的能力來攔截信件，並將信件重新寄出，以指派新的 DSN 設定值 (設為 NEVER)，即可避免退信的產生。這部分的實作共有二部分，首先必須更改 sendmail.mc 設定：

```
LOCAL_CONFIG
CPprocmail

LOCAL_RULE_0
R$*<@$+.procmail>$*     $@ $1<@$2.>$3
R$*<@$+.procmail.>$*    $@ $1<@$2.>$3
R$*<@$+.>$*             $#procmail      $@/etc/mail/filter.rc
$:$1<@$2.procmail>$3
R$*<@$+>$*              $#procmail      $@/etc/mail/filter.rc
$:$1<@$2.procmail>$3
```

接著必須建立 filter.rc 郵件處理腳本：

```
SENDER  = $1
SHIFT   = 1

:0 w
! -C /etc/mail/sendmail.cf -N never -f "<$SENDER>" "$@"
```

在上述腳本中，我們使用了「-N never」來指定 DSN 之參數，使得任何回函通知全部都被抑制，包含送信失敗或信件延遲通知等退信。

使用這種機制來防止垃圾郵件的退信具有下列優點：

1. 僅需在最外層的郵件閘道器作設定，之後的郵件轉運站或後端的郵件伺服器全部不必更改任何設定。
2. 如果架設了內收郵件的透通式郵件閘道器，則只需要在該閘道器作設定就可保護整個單位內部的郵件伺服器不會受到垃圾郵件退信的困擾。
3. 除了防止 User Unknown 的退信通知之外，亦可避免 Quota Exceeded、Host Unknown、… 的退信。
4. 如果來自於 Intranet 的寄信人誤植收信人地址，該 Intranet 的寄信人仍可收到退信通知。

當然，這個機制也有其缺點：

1. 所有的垃圾郵件都會被接收，不管該垃圾郵件的收信人是否存在。
2. 所有郵件會多出一級的郵件轉寄數 (Mail Hop Count)。

在實務上，這二項缺點幾乎不會造成任何影響，因此在內收郵件閘道器上停用 DSN 信件通知之功能可說是最徹底的解決方案。

4.3 過濾 DSN 信件

如果因為某些因素無法在內收郵件閘道器修改設定 (例如：內收郵件閘道器是制式商品無法修改)，亦可改由外寄郵件閘道器作 DSN 的信件攔截。

這部分的設定與先前的作法非常類似，同樣必須修改 sendmail.mc，同樣必須設定 filter.rc 腳本，但只有 filter.rc 稍微不同：

```
SENDER  = $1
SHIFT   = 1

:0
* $SENDER ?? .+MAILER-DAEMON.+
/dev/null

:0 w
! -C /etc/mail/sendmail.cf -f "<$SENDER>" "$@"
```

上述方法會將所有來自於 MAILER-DAEMON 的信件全部濾除，包含 DSN 退信通知。

使用這種機制的好處是可以確保所寄出的信件都受到控制，缺點則是大量垃圾郵件與其退信會在單位內部傳送，直到最後郵件送出時才被濾掉。

4.4 拒絕轉寄不存在收信人帳號之信件

如果可以在內收郵件閘道器作設定，當外部郵件主機提出郵件寄送的請求時，可以先檢查該郵件之收信人地址是否存在，再決定是否接受郵件的轉寄，則這些 User Unknown 的退信問題就可避免。

不過，這些郵件帳號是建立於後端的郵件伺服器，並不存在於前端的郵件閘道器，如何讓前端郵件閘道器得以查詢後端的郵件帳號就是個問題。

所幸，sendmail 提供了 LDAP Mail Route 功能，只要搭配 LDAP 伺服器之使用，就可以完成此目標。

在 sendmail.mc 檔案中，我們必須進行下列的設定：

```
FEATURE(`ldap_routing', `', `', `sendertoo')dnl
LDAPROUTE_DOMAIN(`example.com')dnl
define(`confLDAP_DEFAULT_SPEC', `-h ldap.example.com
-b dc=example,dc=com')dnl
```

而在 LDAP 的資料庫中，我們也必須為每一位使用者增加相關的欄位，例如：

```
dn: uid=alex,ou=People,dc=example,dc=com
.....
mailLocalAddress: alex@example.com
mailHost: mail.example.com
```

使用這種解決方案的最大好處是不必接收大量不存在帳號的垃圾郵件，直接將該郵件阻擋於單位之外；並且，它不違背 RFC 1891 之規範，所有 DSN 之運作仍可照常運行。但相對地，其最大缺點在於施行門檻較高，除非該單位已啟用 LDAP 服務，否則將電子郵件帳號移轉到 LDAP 伺服器並保持帳號的同步就是個大問題。此外，這個方案也僅能解決 User Unknown 的退信問題，對於 Quota Exceeded 的退信仍然無法解決。

5. 避免電子郵件帳號探測之因應對策

在 RFC 1891 的規範中，DSN 除了送信失敗或延遲而產生回函通知之外，亦可指定成功寄達之回函通知。這個成功寄達之回函通知並不需要使用者閱讀信件，只要信件成功地寫入使用者信箱，終端郵件伺服器就會主動發出回函。對於電子郵件名單的收集者而言，可以利用這個機制以字典攻擊法寄發大量電子郵件，並指定 DSN 為 SUCCESS，就可得知哪些電子郵件帳號為有效的帳號。

欲避免自己的郵件伺服器被探測出有效的電子郵件名單，我們可以在終端郵件伺服器的 sendmail.mc 檔案加入下列設定：

```
define(`confPRIVACY_FLAGS', `noreceipts')dnl
```

這個設定可以關閉 DSN 的 SUCCESS 成功寄達通知，但是無法關閉 FAILURE 與 DELAY 的退信或延遲傳送之通知。

除了在終端伺服器設定取消信件寄達通知之外，於 4.2 節與 4.3 節所提出之方法亦可用於抑制信件寄達之通知。

6. 實測經驗

本校電子郵件系統亦曾經因為大量垃圾郵件的退信而一度列入 SpamCop[6] 的黑名單，在啟用 4.2 所描述的機制之後，就再也沒有遇到類似的問題。因此，此方法是經過長時期上線運轉的驗証，為確實可行之方案。

7. 結論

利用電子郵件的退信作為攻擊的工具已非難事，雖然無法有效地避免大量信件的湧入，但是我們卻可避免大量退信的產生，以免成為攻擊者之幫兇，並讓自身陷入黑名單之列。本文中，我們提供了四種 User Unknown 退信的因應之道，在不同的郵件系統架構與不同的條件限制與需求的前題下，可採用不同的解決方案。此外，亦可衡量實際需求來考慮是否關閉信件寄達通知，以避免惡意人士進行電子郵件名單之探測。

參考文獻

1. 范修維，透通式外寄郵件閘道器之建置與應用，TANet 2006 台灣網際網路研討會。
2. http://forum.spamcop.net/dict/DNSbl.html
3. http://www.ietf.org/rfc/rfc1891.txt
4. http://www.ietf.org/rfc/rfc3798.txt
5. http://www.procmail.org/
6. http://www.spamcop.net/
7. http://www.sendmail.org/