電子郵件日誌偵測分析系統

作者/李武耀 上尉

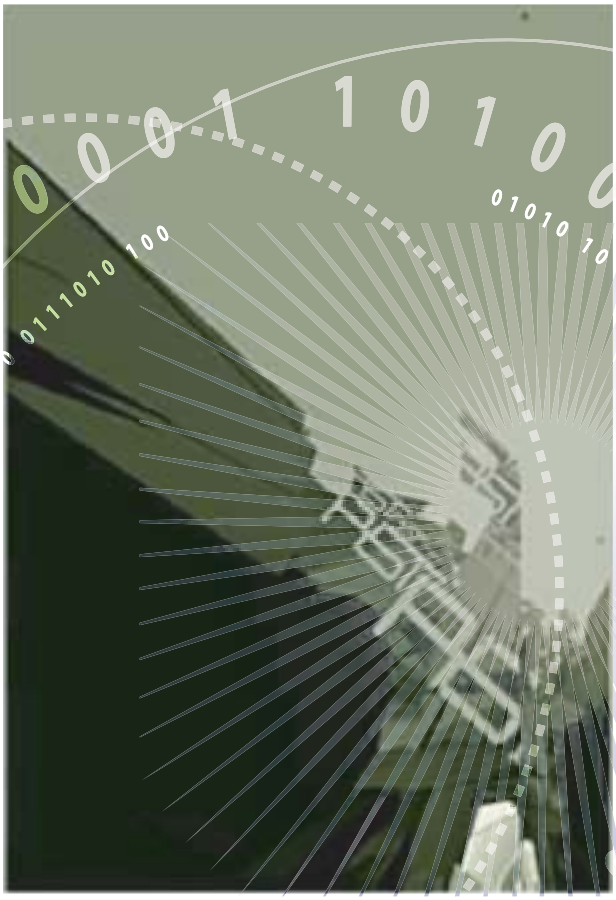
提要

垃圾郵件、病毒郵件皆是現今電子郵件所面臨最嚴重的問題。現今郵件過濾偵測機制大多針對伺服器端來設計，對不安全的郵件予以阻隔，可大幅降低垃圾、病毒郵件對單位所帶來的災害，但缺點是造成郵件系統本身負擔，影響系統效能。本篇論文利用離線式(off-line)郵件日誌系統架構與自動機原理兩個核心技術進行系統設計與實作。離線式郵件日誌系統將郵件日誌傳送至遠端電腦進行分析偵測，不對郵件本身實施過濾偵測，優點是日誌處理不佔用系統資源與空間，即時分析與不易受攻擊，適用高網路使用量的單位。

自動機具備易描述、記錄與實作的特性。根據異常日誌來設計自動機，可歸納日誌特徵與日誌行為的異常偵測。日誌偵測分析系統是以兩階段分析流程來進行日誌收集、分類、分析與異常偵測，提供現今嚴重郵件問題一個解決方法。

前言

垃圾郵件與病毒郵件皆是目前電子郵件最嚴重的問題。



根據IDC於2002年9月發表的研究報告指出業者大量利用電子郵件作爲行銷管道，使垃圾郵件日益氾濫。預估全球電子郵件使用量將由2002年的310億封，大幅增加至2006年600億封。因此，未來過濾電子郵件的技術將逐漸受到重視。

趨勢科技2003年病毒預報中指出，未來利用郵件軟體作爲網路行銷的手法與作法，將成爲散播大量病毒的趨勢，且病毒製作者將自行編寫SMTP引擎，不再使用微軟Outlook或Outlook Express來散播染毒郵件。

爲了解決以上的問題，常見的網路安全防護機制有：資料編碼加密來保護資料安全及完整性、資料隱藏來保護資料機密及專利權、主機系統安全防護以修補系統漏洞爲主、防火牆系統以訂定進出規則及權限表、頻寬管理系統爲防止網路頻寬遭濫用與網路入侵偵測系統對進出資料封包進行比對與分析。然而，以上之網路安全防護機制設置成本高，降低整體網路系統效能，且若干機制易遭攻擊。

圖一　日誌型分析系統架構圖 (作者繪製)

因此，本論文郵件日誌分析系統的核心技術以日誌型分析系統(Log-based Analysis System)與自動機(automata)爲主。

日誌型分析系統即是將伺服軟體在運作過程所發出警告訊息，透過syslog協定轉送到分析系統。在Unix系統中，syslog根據/etc/syslog.conf檔中所指示的郵件訊息處理設定值來處理警告訊息，可設定警告訊息利用UDP格式轉送到另一部主機或存在本機目錄檔案中。以圖一爲例，Sendmail郵件伺服器所產生的一般等級警告訊息透過syslog以UDP格式傳送到另一台主機Logging Server中的514埠。若在本機存成檔案，檔案日積月累，會佔用大量空間，而且若想從日誌檔案分析偵測異常既費時、消耗系統資源又不即時。所以日誌型分析系統的優點是日誌處理不佔用伺服器系統資源與空間，可即時分析郵件日誌且不易受駭客攻擊。

自動機來作異常偵測的優點有容易描述、記錄狀態與容易實作。根據目前資料及狀況來決定切換到下一個狀態，對映到異常偵測是當收到一個日誌記錄(目前資料)和目前此類日誌所在的狀況(目前狀況)我們可以知道是否此筆日誌構成了異常的條件。有限狀態機轉換成表格(table)，也就是陣列(Array)的資料結構即可表達異常偵測。以圖二爲例，起始狀況開始接收與記錄日誌，當日誌到達一定門檻值(異常條件)時，切換至下一個狀況並觀察之，一直至結束狀況爲止，來判斷其最後該屬之結果(垃圾郵件或病毒郵件)。

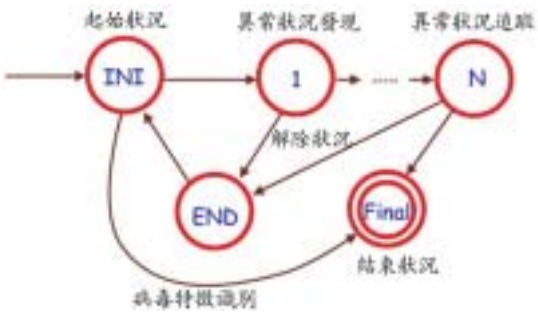
惡意郵件之研究與討論

垃圾郵件定義：所謂垃圾郵件SPAM (Send Phenomenal Amounts of Mail)即是巨量廣告信或網路行銷郵件，藉由郵件伺服器所提供的轉寄服務、免費信箱或是發信軟體，寄給未經收件者授權同意的電子郵件地址。

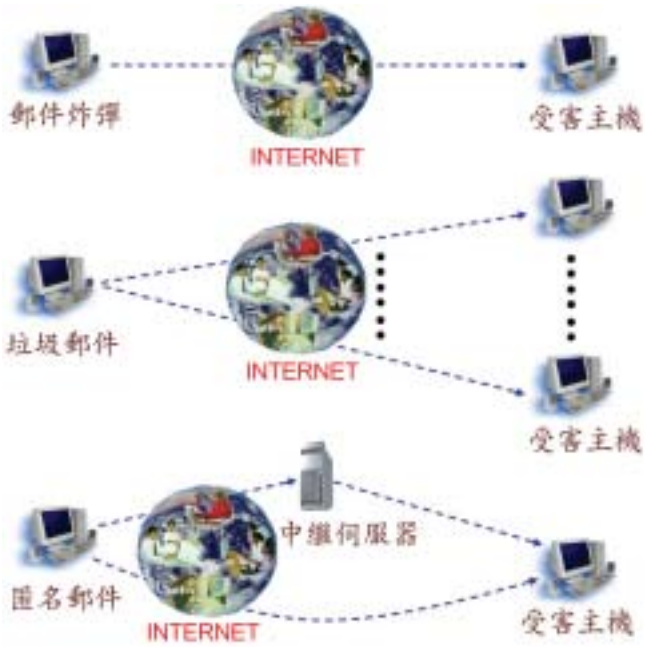
郵件炸彈(Email Bomb)是以寄送大量郵件塞爆個人信箱，使信箱容量被佔滿以致無法收信。

匿名郵件(Anonymous Email)的原意是針對集權專制國家，爲保障人權言論自由，所留給政治異議者一個評論的空間，但被濫用的結果造成誣告和詆毀。

結合郵件炸彈、垃圾郵件和匿名郵件的特點可以成爲僞造郵件(Spoofed/Forged



圖二　自動機範例 (作者繪製)



圖三　垃圾郵件、郵件炸彈與匿名郵件圖(作者繪製)

Email)如圖三所示。讓管理者無法追查大量郵件的來源處，進而超出網路連線負荷，消耗過量系統資源，導致郵件無法正常收送或系統當機，這是一種阻斷攻擊或分散式阻斷攻擊DOS/DDOS(Denial of Service/ Distributed Denial of Service)。

垃圾郵件過濾機制探討

針對垃圾郵件與匿名郵件、病毒郵件等惡意郵件之偵測過濾機制研究與作法加以討論。

散發垃圾信的方式大致上有兩種：第一種是透過郵件伺服器提供的轉寄(Mail Relay)服務或是免費的信箱代爲發信；第二種是申請ADSL或專線利用發信軟體來發信。

在垃圾郵件過濾機制目前的方式有下列幾種：

一資料探勘(Data Mining)演算法

利用資料探勘的技術從電子郵件日誌檔中發掘其蘊含之郵件傳送行爲模式，進行關聯組合屬性分析，再配合探索式規則將其行爲模式作屬性歸納，針對大量異常與出現頻率高的關聯組合進行對照分析。然而，以資料探勘方法作異常郵件分析，其異常歸納規則是否適合多變的現況，仍需驗證。

二異常連線數目判斷法

在一定時間內，例如：五分鐘，當其它郵件伺服器以相同的郵件主旨、寄件人或是主機IP位址，發送超過一定數量的郵件時，例如發送超過100封郵件，可判斷其郵寄行爲不屬於正常郵寄模式。若收信郵件地址是屬內部區網，系統會延遲收信的速度，若收信郵件地址不屬內部區網，系統應採取反制轉寄(anti-relay)作爲，這時可判斷是郵件炸彈或垃圾郵件。

三IP位址反查法

垃圾郵件多利用ADSL的環境和網路行銷軟體來作垃圾郵件的傳送。假若郵件伺服器在收信的同時，反查對方郵件伺服器的IP位址是否在網路名稱伺服器DNS(Domain Name System)中有註冊，並與寄件者的網域名稱相同，若不是的話，它會認爲這是經由ADSL的發信軟體所發出而予以拒收，也可判斷是垃圾郵件。

四SMTP中繼控制

內部郵件伺服器應採取SMTP反制垃圾郵件轉寄(Anti-spaming Relay)的作爲，有兩種方法：

㈠限制IP

只針對內部區網的用戶方可使用郵件主機進行中繼服務。限定只有單位網內用戶才能使用郵件伺服器，避免郵件伺服器成爲垃圾郵件中繼站。但若有外人在單位內上網，仍無法避免亂寄發信件的可能。

㈡用戶認證

用戶驗證方式可以避免非單位內的使用者，進入單位內實施散播大量郵件的可能。在透過SMTP主機發送郵件的時候，系統需要用戶輸入用戶名和密碼來檢驗身份，當通過驗證之後，系統將接受用戶的發信請求。

五文件分類演算法

要達到樣本空間的分類集合，無論是以人工的方式篩選或是類神經網路的方式篩選，藉此分類集合母體作垃圾郵件和非垃圾郵件的判斷樣本，而非只單純依據關鍵字來判斷。以IEEE中的一篇論文「Support Vector Machines for SPAM Categorization」爲例，利用四個演算法將資料分成彼此對照的群組，從中找到垃圾郵件1,000個最佳特徵，另一組則是將每封信件轉換成向量，建置超過7,000個向量值。讓每封信件檢驗時，依據所顯示的向量值與樣本空間所出現頻率對照，藉此比較在誤差值容許範圍內的樣本相似度。若相似度在垃圾信的範圍內，則歸類至垃圾郵件中。這方法具有自動分析、分類和智慧型過濾機制，但是未經長時間的樣本收集和資料分類，事實上，樣本空間仍會無法過濾最新的垃圾郵件多變型式。而且，單一語言的訓練不足以完全過濾所有垃圾郵件，而多國語言的訓練也有其執行困難度，再加上多媒體的本文和附件檔，文件分類演算法無法完全適用。

六黑名單比對法

站台黑名單是透過集中式網路資料庫來蒐集全世界的Open Relay站台。所謂的Open Relay就是無條件作轉接/轉送服務(Relay Service)的郵件主機。

根據郵件傳送協定SMTP(Simple Mail Transfer Protocol)RFC821的內容原意是Sendmail在TCP/IP網路上將郵件從一台機器傳到另一台機器，不論機器的網路型態或作業系統，不需帳號和密碼查驗，盡其所能地將郵件傳送出去。因此，垃圾郵件的寄發藉由這個郵件服務的漏洞，作大量的散播動作。所以，蒐集黑名單是爲了提供系統管理者在設定郵件伺服器時可拒收來自黑名單主機所傳送過來的信件。蒐集黑名單的站台很多，例如：SPAMCOP、ORBZ、MAPS、CAUCE等國外網站，蒐集像RBL、DUL、RSS等黑名單。雖然，國外網站提供了許多Open Relay主機的黑名單，但是，還有許多郵件主機提供Relay Service而未被列入黑名單中，更何況最新的網路行銷軟體可以作到自動更換IP位址、自動更換發信主機、自動變換寄件人、自動指定收件人、自動更換退信信箱、斷線保留、接續發送、在代理主機及防火牆內發送，甚至支援隱藏IP發信，因此，針對垃圾郵件過濾仍有缺口，無法完全阻擋。

七TMDA驗證法

TMDA(Tagged Message Deliver Agent)是維護一組白名單(White List)，使單位郵件伺服器依其記錄來提供轉寄服務的，其作法是比較簡單的，系統管理員可以隨時增加服務的成員和主機。

假設一狀況爲寄信者Host A寄信至單位內部Host C，中間透過郵件伺服器Host B進

行轉送，則其運作流程可假設爲兩種狀況：

㈠郵件伺服器中的白名單比對中有Host A的記錄。

㈡郵件伺服器中的白名單比對中沒有Host A的記錄。

在第一個狀況中，郵件伺服器Host B是透過TMDA的機制查詢得知Host A在其記錄內，利用自動回覆郵件的功能，將信件傳送給Host C。

在第二個狀況中(如圖四)，可分以下步驟：

㈠寄件者Host A寄信到郵件伺服器Host B。

㈡郵件伺服器Host B透過TMDA的機制比對寄件者。

㈢比對結果告知郵件伺服器Host B，得知寄件者Host A未在白名單中。

㈣自動回覆郵件機制回送一封確認信給Host A寄件者，請求查驗郵件主機或寄件者是否僞冒。

㈤寄件者回信確認。

㈥郵件伺服器Host B轉發至收件主機Host C，確認並詢問是否要將Host A寄件地址增至白名單中，以利往後節省再驗證的動作，可有效阻擋未經授權的垃圾郵件。

然而，在病毒郵件防護機制上，容易產生極大的漏洞。近年來的病毒郵件是以通訊錄中的郵件地址進行大量的病毒散播，而透過TMDA已認證機制，使得病毒信件毫無困難地傳送到收信者。因此，TMDA機制對病毒郵件無法作到有效防護。除前述方法外，另有郵件主旨和表頭檢驗法等。

病毒郵件之研究與討論

所謂病毒係指能藉本身程式碼進行感染、潛伏、隱藏及發作的程式碼。現今病毒所具備的散播能力及變形(polymorphic)能力，已非昔日電腦病毒所能比擬，例如：利用多型引擎(Polymorphic Engine)使電腦病毒具有自我編碼的能力，增加掃描病毒特徵(signatures)的困難。而且，藉由網際網路之便，病毒可以瞬間感染至全世界電腦，因此有蠕蟲(Worm)的產生，所造成的損失通常是難以估計。

病毒原理從早期的MS-DOS作業系統，病毒多以攔截修改中斷向量(13h)對硬碟進行格式化、BIOS的flash ROM清除等，然而，到了MS-Windows9x Win32架構時，病毒在Ring 0(系統最高權限的執行模式)模式下對檔案進行感染。

病毒結合郵件，使病毒透過郵件提供多傳播管道，利用社交工程技巧(Social Engineering Techniques)來誘騙人們去開啓病毒檔或下載蠕蟲，取得系統root的權限，進行系統入侵和破壞，造成系統當機或網路品質不佳的狀況。以微軟的Outlook和Out-

圖四　TMDA驗證過程圖

look Express 5.5爲例，其軟體自動執行附件檔的機制造成Nimda和CodeRed等病毒入侵系統，造成大量帶有病毒郵件的散播，影響網路頻寬和郵件伺服器過重負荷。

病毒郵件過濾機制探討

所有的病毒郵件過濾機制都面臨了一個重大挑戰—「如何自動偵測新病毒」。

一般而言，現今病毒掃描技術可分爲兩部分：一是利用病毒特徵的掃描機制(Signature-based Detector)，一是探索式的病毒分類機制(Heuristic Classifier)。

就病毒特徵的掃描機制而言，典型的病毒偵測演算法是使用所謂的病毒特徵(signatures)，即病毒碼(Unique Telltale Strings)來產生病毒偵測模組，而由於病毒特徵對病毒的單一性，使得其郵件過濾機制具有高度病毒攔截率。但也由於其對病毒的單一性，使得針對大多數的病毒無法作一般化的病毒偵測模組。

而以探索式的病毒分類機制來說，這類的分析機制大多是費時的(time-consuming)，且大多無法即時偵測到新式病毒。而有人提出了用資料探勘(Data Mining)演算法來偵測新病毒。有人以人工智慧爲基礎，發展一套階層架構的分散式代理機制防禦系統來保護網路安全。

郵件日誌分析系統設計

本系統架構區分爲軟體架構及硬體架構說明。

一、系統軟體架構

軟體架構區分爲六個子系統模組(如圖五)；分別爲日誌接收模組、日誌分析模組、資料庫查詢模組、異常分析自動機模組、異常流量監視模組以及系統工具模組等六個子系統模組。

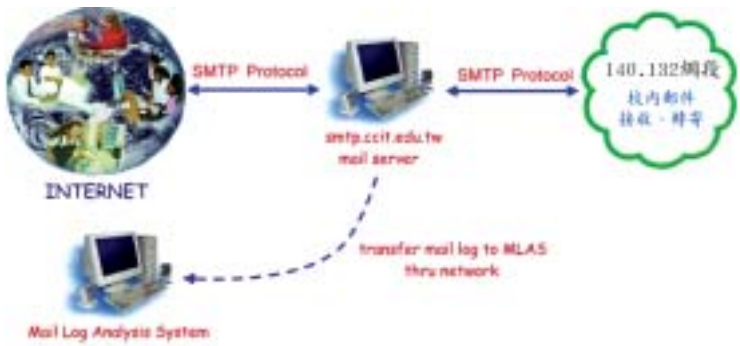
圖五　系統軟體架構圖 (作者繪製)

二、系統硬體架構

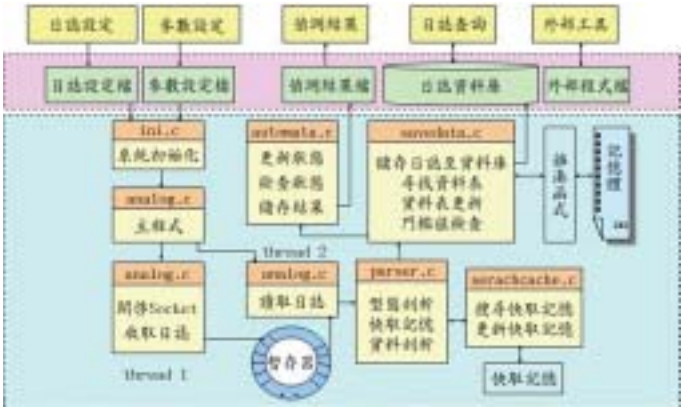
系統硬體架構(如圖六)主要由郵件伺服器及一般電腦所組成，郵件伺服器藉由系統日誌(syslog)上的郵件日誌設定，將郵件封包傳送至郵件日誌分析伺服器(Mail log Analysis Server, MLAS)，其上安裝網頁伺服器、圖形函式庫、資料庫系統及本系統的網路程式模組。

郵件日誌分析伺服器爲一般電腦，中央處理單元爲Pentium IV，主記憶體爲512MB。作業平台爲Red Hat Linux 8.0，網頁伺服器採用在UNIX平台中廣泛使用的阿帕契(apache)。(如圖七)

網路程式是用C語言寫成的，運用multi-thread的觀念，一個thread收集日誌存



圖六　系統硬體架構圖 (作者繪製)



圖七　網路程式架構圖 (作者繪製)

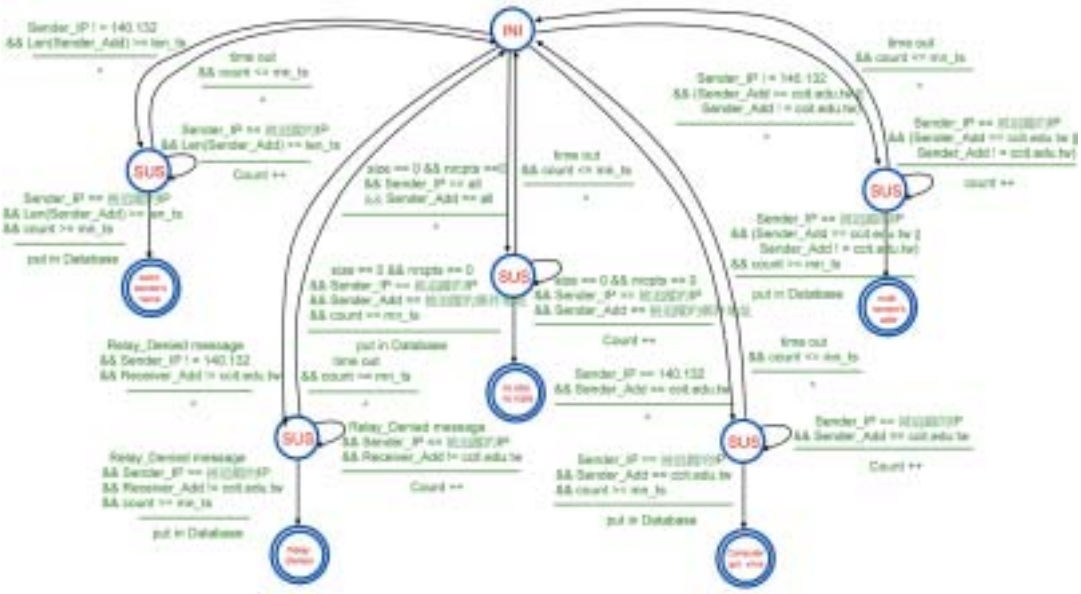
入暫存器，另一個thread讀取日誌，進行日誌擷取，經日誌欄位分類後進入自動機狀態轉移，到達偵測門檻值後，儲存至資料庫。(如圖八)

郵件日誌格式分析

信件透過郵件伺服器收送或轉寄皆會留下許多列日誌記錄(如圖九)，若日誌不經處理或說明，對系

```
Mar 22 23:00:02 smtp sendmail[67632]: g8UF02067632: from=<s934512@ccit.edu.tw>, size=18606,
class=0, nrcpts=1, msgid=<014201c26892$0a7b1e70$9168848c@os>, proto=SMTP, daemon=MTA,
relay=h104-145.dpm3.ccit.edu.tw [140.132.104.145]
Mar 22 23:00:02 smtp sendmail[67630]: g8UF02067628: to=<net-maintain@ccit.edu.tw>, delay=00:00:00,
xdelay=00:00:00, mailer=smtp, pri=60705, relay=ms1.ccit.edu.tw. [140.132.3.210], dsn=2.0.0, stat=Sent
(g8UExup01035 Message accepted for delivery)
Mar 22 23:00:02 smtp sendmail[67623]: g8UF01067623: from=<s923229@ccit.edu.tw >, size=0, class=0,
nrcpts=0, proto=SMTP, daemon=MTA, relay=61-230-196-168.HINET-IP.hinet.net [61.230.196.168]
Mar 22 23:00:02 smtp sendmail[67630]: g8UF02067628: to=<s924511@ccit.edu.tw>, delay=00:00:00,
xdelay=00:00:00, mailer=smtp, pri=60705, relay=ms2.ccit.edu.tw. [140.132.3.209], dsn=2.0.0, stat=Sent
(g8UExuM17903 Message accepted for delivery)
Mar 22 23:00:05 smtp sendmail[67638]: g8UF04067638: ruleset=check_rcpt, arg1=<swchu@cyit.edu.tw>,
relay=61-226-68-192.HINET-IP.hinet.net [61.226.68.192], reject=550 5.7.1 <swchu@cyit.edu.tw>...
Relaying denied
Mar 22 23:00:05 smtp sendmail[67641]: g8UF05067641: ruleset=check_rcpt,
arg1=<web@pchome.com.tw>, relay=61-230-196-168.HINET-IP.hinet.net [61.230.196.168], reject=550
5.7.1 <web@pchome.com.tw>... Relaying denied
Mar 22 23:00:06 smtp sendmail[67638]: g8UF04067638: from=<s914504@ccit.edu.tw >, size=0, class=0,
nrcpts=0, proto=SMTP, daemon=MTA, relay=61-226-68-192.HINET-IP.hinet.net [61.226.68.192]
Mar 22 23:00:06 smtp sendmail[67641]: g8UF05067641: from=<s933904@ccit.edu.tw >, size=0, class=0,
nrcpts=0, proto=SMTP, daemon=MTA, relay=61-230-196-168.HINET-IP.hinet.net [61.230.196.168]
Mar 22 23:00:06 smtp sendmail[67642]: g8UF06067642: ruleset=check_rcpt,
arg1=<kerry630322@Yahoo.com.tw>, relay=h81.s243.ts31.hinet.net [163.31.243.81], reject=550 5.7.1
<kerry630322@Yahoo.com.tw>... Relaying denied
```

圖八　郵件伺服器日誌記錄 (作者繪製)



圖九　日誌行為異常偵測自動機總圖 (作者繪製)

表一　寄信訊息列欄位表 (作者繪製)

編號	欄位名稱	欄位說明
1	From	信封上的寄信者
2	Size	郵件大小
3	Class	佇列類型
4	Nrcpts	收信人數
5	Msgid	識別碼
6	Proto	傳輸協定
7	Daemon	代理程式
8	relay	寄信主機

表二　收信訊息列欄位表 (作者繪製)

編號	欄位名稱	欄位說明
1	to	收信者
2	delay	總傳遞時間
3	mailer	遞送代理程式
4	pri	優先權
5	relay	收信主機
6	stat	遞送狀態

表三　Ruleset規則集 (作者繪製)

編號	檢驗規則名稱	檢驗規則說明
1	Check_mail	驗證收件者電郵地址
2	Check_rcpt	驗證寄件者電郵地址
3	Check_relay	驗證提供SMTP連線主機
4	Check_compat	郵件遞送前，驗證寄件者與收件者電郵地址

表四　系統檢驗列欄位表 (作者繪製)

編號	欄位名稱	欄位說明
1	Ruleset	系統檢驗規則
2	Argl	收件者電郵地址
3	Relay	寄件主機與主機IP
4	Reject	系統拒絕轉寄訊息

統管理者而言，這些日誌列的各欄位難以判讀。以下針對三種日誌列的格式詳加說明。

一、寄信訊息列(From_Line)

寄信訊息列提供了寄信者電子郵件地址、信件大小、收信人數和寄信主機的名稱與IP位置等相關資訊。表一用來說明寄信訊息列所有欄位的名稱與說明。

二、收信訊息列(To_Line)

收信訊息列提供了收信者電子郵件地址、總遞送時間、遞送代理程式和收信主機的名稱與IP位置等相關資訊。表二則用來說明收信訊息列所有欄位的名稱與說明。

三、系統檢驗列(Ruleset_Line)

在目前電子郵件氾濫的情形下，sendmail版本8.8之後增加四組檢查電子郵件的檢驗規則集，說明如表三。

以ruleset=check_rcpt爲例，其目的是爲要驗證寄件者電子郵件地址。若有非屬單位區網的寄件主機欲透過中正校園的SMTP Server遞送信件，基於不提供轉寄、轉送的原則下，拒絕其轉寄請求，同時在日誌中也留下記錄。

在系統檢驗列中，我們可知有寄件主機企圖透過本校的郵件伺服器來達到轉寄的目的，假若在單位時間內有大量郵件寄發，這郵件異常行爲便可歸納爲垃圾郵件、廣告信或郵件炸彈的行爲模式。表四是針對系統檢驗列的欄位名稱進行說明。

郵件日誌分析系統功能

透過以上日誌格式與欄位的介紹，從各欄位取得鍵值進行日誌分析、郵件流量異常偵測、日誌特徵值異常偵測與日誌行爲異常偵測。

一、日誌分析

日誌分析的目的就是要從日誌中尋找異常現象，原始日誌是以時間爲順序，較雜亂無章，無法單從肉眼來觀察日誌異常，需要日誌分析介面將日誌淬取、整理、排序與歸

納，較易作異常分析。

二郵件流量異常偵測

過去流量偵測異常的作法是利用SNMP網管協定從路由器傳回流量資料，其中包含整個單位內部使用網路的狀況。若想單就郵件流量來觀察，就無法利用過去的方法。

本論文利用郵件日誌(From_Line)格式中的size欄位作單位時間(五分鐘)內郵件數與郵件檔案大小的累加。長時間的觀察每日的郵件進出量和郵件內容，可發現異常郵件數目增加或異常郵件檔案大小量的巨增等現象。

三日誌特徵值異常偵測

所謂日誌特徵值即是直接從日誌上取得其特徵值作爲異常判斷，可分爲弱點攻擊與延遲收信。弱點攻擊的定義是針對2003年3月3日在CERT網站發布的「Sendmail遠端緩衝區溢位漏洞」進行偵測。已修補的郵件系統，若遭攻擊時會留下日誌記錄(Dropped Invalid Comments From Header Address)。延遲收信的定義是電子郵件傳送過程中，因對方收件主機無法接收郵件時，延遲訊號持續發送。

四日誌行為異常偵測

郵件日誌異常行爲的偵測，需搜集連續相關的日誌封包加以分析判斷才可歸納爲異常行爲。不同於病毒郵件，這些郵件無法從防毒軟體的病毒碼、IDS的異常入侵特徵偵測或Firewall的服務埠規則設定來進行防堵與預判。而郵件日誌之異常行爲可區分爲異常轉寄、異常地址、動態地址、異常信件與異常電腦。

異常轉寄的定義爲在單位時間內，若校外寄件主機意圖經本校SMTP Server轉寄電子郵件當作跳板發信，而遭校園郵件主機拒絕，且拒絕次數超過所定的門檻值。

異常地址的定義爲若寄件者的電子郵件地址長度超過所定的字串門檻值，且在單位時間內的郵件發送量超過標準。

動態地址的定義爲在單位時間內，若單一寄件主機發送多個電子郵件地址，且發送次數超過所定的門檻值。

異常信件的定義爲在單位時間內，若寄件者的電子郵件內容爲零，或是其收件者人數也爲零，且發送次數超過所定的門檻值。

異常電腦的定義爲單位時間內，若寄件者發送的電子郵件數量超過所定門檻值，可視爲異常。例如：一分鐘內發送十封信件以上。

圖九爲日誌行爲異常偵測自動機總圖，圖中每個自動機是獨立的，從日誌欄位取得所需鍵值來記錄，等下一筆日誌輸入進行狀態轉移，若單位時間內達到門檻值即存入資料庫；反之，解除狀況。

異常日誌分析實驗結果

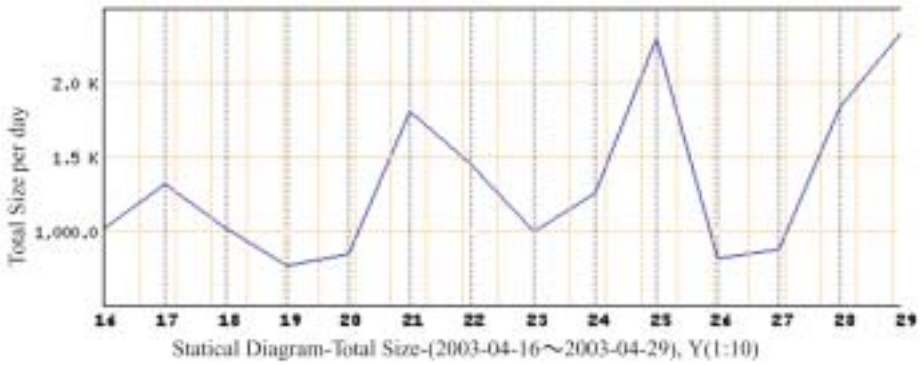
透過長時間日誌收集、分析與異常判斷，在民國92年4月16日至4月29日共十四天的時間裡，異常電腦分析自動機所偵測筆數如圖十。

結論

在本篇論文中，我們認爲從郵件日誌來作異常分析有以下幾項優點：

一對郵件系統本身不增加任何負擔，且能反應郵件異常現象。

二針對病毒的行爲模式來進行防堵病毒郵件，可適用未來病毒的偵測。



圖十　異常電腦分析系統之分析數據(92/4/16~92/4/29) (作者繪製)

三不受不同語言的限制，單純就郵件日誌的記錄來分析。

四能同時偵測垃圾郵件與病毒信件。

五將郵件異常特徵一般化，歸納異常郵件行爲模式。

六長期郵件日誌收集可爲法律證據，若有任何洩密行爲或散發匿名信行爲，可由日誌分析系統提出相關證明。

參考資料

一Brian Bangnall, Chris O. Broomes, Ryan Russell著，賴冠州、葉育如編譯，E-MAIL病毒防護技術手冊，台北，旗標，2002年。

二台灣電腦網路危機處理/協調中心，Remote Buffer Overflow in Sendmail，2003年。

三游適彰，曾憲雄，「兩階段演算法應用於電子郵件近似性關連規則之探勘研究」，新竹，國立交通大學電資學院，2001年。

四滕儒恩，匿名電子郵件大解析，網路通訊，2002年。

五嚴大中，江清泉，「網路防火牆系統安全之設計與分析」，中和，國防大學管理學院，2002年。

六劉芳梅，「電子郵件使用量仍將大幅增加」，台北，資策會，2002年。

七趨勢科技，「趨勢科技2002年病毒總結及2003年病毒預報」，2002年，http:// www.trend.com. hk/tml-pccillin/ news/news_ a20021213. htm。

八Bryan Costales and Eric Allman, "Sendmail: The Fundamentals", O'REILLY, 2000.

九Bryan Costales and Eric Allman, "Sendmail: The Setup and Management", O'REILLY, 2000.

十C. Lonvick, "RFC 3164: The BSD syslog protocol", 2001.

十一Matthew G. Schultz, Eleazar Eskin, Erez Zadok, Salvatore J. Stolfo, "Data Mining Method forDetection of New Malicious Executables", IEEE Symposium, 2001.

十二Steve R. White, "Open Problems in Computer Virus Research", Virus Bulletin Conference, 1998.

作者簡介

李武耀上尉，中正理工學院資訊科學系86年班、國防大學中正理工學院電子研究所碩士92年班。曾任排長資訊安全官。現任陸軍通信電子資訊學校系統資訊組教官。