以串流為基礎具有硬體加速內容檢查的郵件病毒掃描系統

A Stream-based Mail Virus Scanner System with Hardware-Accelerated Content Inspection

游坤明
中華大學資訊工程學系
yu@pdlab.csie.chu.edt.tw

吳東名
中華大學資訊工程學系
e09402019@chu.edu.tw

摘要

在資訊科技發達的今日，資訊系統除了便利的功能外，現在更須注意安全的問題。其中電腦病毒更是一般我們使用電腦時所常見的問題。現有市場上可以看到支援郵件防毒閘道器有中央控管與提早防禦病毒入侵到內部網路等優勢，但這些傳統郵件防毒閘道器都是以先存檔後掃瞄的方式來做病毒的掃描，也由於這樣的防毒閘道器所需要的系統資源與暫存檔案空間都需要極大的需求才可以符合系統本身的功能，亦即越大的系統資源就可以有更好的系統效能，越大的暫存檔案空間所能掃描的檔案就越大。

因此我們提出一個以串流為基礎具有硬體加速內容檢查的郵件病毒掃描系統的概念來讓網路電子郵件做病毒掃瞄檢查時，完全不需使用到暫存檔的空間以及最少量的系統記憶體就可以執行防禦的功能，串流式硬體加速內容檢查的郵件病毒掃描系統另外一個特色是降低系統處理器使用率，當郵件系統需要做檢測病毒功能時，只需將檢測病毒的工作交由硬體去執行，此時系統處理器便有多餘的執行空間去處理系統上其他的工作。

在實驗結果後發現我們的郵件病毒掃描系統在網路效能上比儲存式郵件病毒掃描系統快六倍也比串流式郵件病毒掃描系統快二倍，而當郵件檔案是壓縮格式時，我們的病毒掃描系統也有六倍與三倍的差距。在系統記憶體使用上，不論病毒掃描系統所傳送的資料大小，對單一連線都維持一個定值。而在系統處理器使用率方面，我們的病毒掃描系統比另外兩種病毒掃描系統有更少的系統處理器使用率。

關鍵詞：串流、病毒掃描、網路安全、解壓縮、硬體加速

1.緒論

現今網際網路通行全球，提供各種方便的服務供民眾使用，諸如全球資訊網(World Wide Web, WWW)、電子郵件(E-mail)以及檔案傳輸協定(File Transfer Protocol, FTP)等各項協定基礎，然而在這眾多便民的服務中卻存在著各式各樣潛在性危機，其中病毒入侵便是現今網際網路安全上一個值得討論的問題。現有個人消費者都會習慣的在個人電腦上安裝一個防禦病毒郵件的偵測軟體；舉如趨勢科技[18]的PC-Cillin 2006或賽門鐵克[15]的Norton AntiVirus 2006等，這些防毒軟體也確實的能將網路上具有威脅性的病毒郵件阻擋下

來以保護個人電腦資料的安全，但是針對企業用戶而言，企業內部的電腦更是需要郵件防毒系統的保護，因為只要病毒郵件入侵到企業裡的工作站或個人電腦時，這對企業而言將是一個很大的損失。

現今市面上除了我們可以看到的防毒軟體外，郵件防毒閘道器也因為網路安全議題慢慢的被企業用戶所重視。這對企業用戶而言這確實是一項不錯的應用，企業用戶安裝郵件防毒閘道器作為網路入口的第一層保護，內部的工作站以及個人電腦所安裝的防毒軟體便是第二層保護，藉由這樣的雙層保護機制來讓整個公司內部的網路安全與電腦避免受到病毒郵件的入侵與破壞，確實是越來越可行的辦法。

現有市面上的郵件防毒閘道器都是以先存檔後掃瞄的方式來做病毒的掃描，當傳輸的網路郵件有附帶檔案時會先將檔案暫存起來，等到檔案資料再硬碟上收集完畢時再針對郵件檔案內容做解壓縮或掃描郵件檔案是否有病毒的存在，如此的架構卻是需要花費比較多的硬體成本以及當企業的入口郵件防毒閘道器流量很大時，網路頻寬不足的問題也會一併發生。

隨著硬體技術的增進，使用硬體加速掃描更可以減輕系統處理器因為掃描郵件封包內容時所需耗損的處理器資源外，如何使用具有硬體加速內容檢查的郵件病毒掃描系統來保護企業內部網路與電腦避免受病毒郵件的破壞外，有效地降低郵件防毒閘道器因為掃描病毒時耗損大量的處理器資源，這將是本篇論文所要研究與探討的方向。

2.背景與相關研究

2.1 儲存式郵件病毒掃描系統

儲存式的郵件病毒掃描閘道器是現今市場上最能讓企業界用戶所使用的網路入口閘道器，閘道器本身除了有郵件病毒掃描功能外，Firewall、IPS、Anti-Spam、Content Filter 等針對網路安全的功能也都具備在裡面。舉如 Fortinet[6]的 Fortigate 系列，CP Secure[3]的 Content Security Gateway 系列以及 Symantec[15] 的 Symantec Gateway Security 系列等，這些防毒閘道器都具備了防毒、防駭甚至阻擋垃圾郵件等多功能的網路安全功能。

在這些多功能的防毒閘道器裡都有一個共同的特色，就是放置一顆硬碟在防毒閘道器裡，當進出防毒閘道器的網路郵件有附帶檔案時，防毒閘道器必須先將傳輸的郵件檔案完整的儲存下來，等儲存完畢後，郵件系統會先解析郵件檔案格式是一般檔案或者是壓縮檔案，然後再進行後續的病毒掃瞄與解壓縮掃瞄動作。

隨著企業網路流量的增加，儲存式郵件病毒掃描閘道器便需要更多的硬碟空間來存放資料，這將導致企業在硬體購置成本的增加，而硬碟的轉速也是影響儲存式郵件病毒掃描閘道器效能的關鍵。另一點則是網路的流量受限於儲存式郵件病毒掃描閘道器要先儲存網路郵件資料再檢查郵件傳輸檔案是否有夾帶病毒的行為模式而讓整體網路頻寬變慢，相信這是企業對於現有儲存式郵件病毒掃描閘道器所困擾的地方。

2.2串流式郵件病毒掃描系統

串流式郵件病毒掃描技術是用來改進儲存式郵件病毒掃描閘道器上的缺失所衍生出來的一種技術，[17]以及CP Secure[3]的CSG系列很清楚的描述出串流式郵件掃描的技術比傳統的儲存式郵件掃描技術不

管是在網路的頻寬或同時間處理的網路連線數上都較傳統的儲存式郵件病毒掃描閘道器來的好。

串流式郵件掃描技術是掃描企業網路上流經郵件防毒閘道器的網路郵件有夾帶郵件檔案的封包為主，當流經郵件防毒閘道器的連線傳輸附帶有檔案時，會在掃描檔案之前將必要的網路封包資料記錄起來，舉如網路郵件的連線是否有夾帶檔案或夾帶的郵件檔案是否有可能會是感染的病毒檔等，在前置處理完成後就可以將原始的封包夾帶檔做及時的病毒掃描檢查，無需像儲存式郵件防毒閘道器需要存放大量的資料。

串流式病毒掃描技術可以節省大量的掃描時間以及降低系統的記憶體使用量，每一條網路連線在做檢查時只需要少量的系統記憶體空間，等到網路連線傳輸完畢時就可以將使用的系統記憶體回收繼續使用，藉由這樣的機制可以讓網路的使用率大大的提高，並且讓企業的硬體架設成本降低很多。

2.3病毒掃描搜尋引擎

現有個人電腦、工作伺服器或郵件防毒閘道器等所架設的防毒系統裡。病毒搜尋引擎是整個病毒掃描系統的核心部份，其原理便是字串的比對。當郵件防毒閘道器做完前置處理且取得要傳輸的原始檔案資料後，此時必須與郵件防毒閘道器內部系統上存在的病毒資料庫做字串的比對，我們由ClamAV 使用手冊[2]可以得知，郵件防毒系統做病毒掃描時都是以字串比對的方式來做病毒特徵的搜尋，舉如Aho-Corasick [1]以及Boyer-Moore[12]的pattern matching algorithm等演算法。更由[4]可以得知，使用字串搜尋比對做資料庫特徵碼的搜尋是最耗損系統處理器的資源，因為所有流經郵件防毒閘道器的網路封包由最原始的封包表頭拆解分析到封包內容的病毒掃描比對，再到封包掃描完畢的後續處理工作，這些的繁瑣的工作都是由系統處理器來做處理的，假如系統處理器一直在做病毒特徵碼的比對檢查，那整體的網路傳輸效能還是會因為系統處理器太過於繁忙而對整個網路傳輸效能提升有限。

2.4硬體加速

隨著硬體技術的增進，在郵件病毒掃描閘道器上使用硬體內容加速掃描技術較傳統的儲存式郵件病毒掃描技術來做比較的話。硬體加速的郵件病毒掃描系統不會有系統資源大量耗損的問題以及網路郵件檔案必須先儲存完整檔案後再掃描病毒的問題，[16][7][8]已經很成功的使用硬體加速技術來增加入侵偵測防禦系統(IPS or IDP)的整體網路傳輸效能，所以藉由使用Hardware-Accelerated Content Inspection Co-Processor 來取代郵件防毒閘道器內系統處理器的病毒特徵碼比對的工作將是一個不錯的選擇。

對於串流式郵件病毒掃描系統而言，當郵件病毒掃瞄系統做病毒特徵碼比對時，由於所有的系統處理器資源都讓病毒特徵碼比對所佔用去，此時的系統處理器很難再去執行系統上其他的工作。使用硬體加速病毒掃描可以將系統的病毒特徵碼比對工作交由硬體加速處理器去執行，當硬體加速理器在做病毒特徵碼比對的同時，系統處理器可以去處理其他系統上的工作，這樣的硬體平行處理架構，可以減輕系統處理器因為檢查封包內容時所需耗損的資源。

3.串流式硬體郵件病毒掃描系統

3.1 系統架構

由於現今硬體技術的發展快速與成熟，將最耗損系統處理器資源的病毒特徵碼比對使用硬體的方式取代，可以讓郵件病毒掃描閘道器做到最節省系統耗損率以及提升網路頻寬上的整體吞吐量。串流式硬體郵件病毒掃描系統可以讓系統在執行郵件掃瞄病毒工作時完全不需使用到硬碟的暫存檔空間以及使用最少量的系統記憶體就可以執行病毒的偵測防禦功能。具有硬體加速內容檢查的郵件病毒掃描系統另外一個特色是可以減少系統處理係在系統運作上的使用率，當系統需要做偵測病毒功能時，只需將偵測病毒的工作交由硬體去執行，此時的系統處理器便可去做其他的工作。藉由這樣的非同步處理設計更能讓串流式硬體加速郵件病毒掃描系統發揮比傳統郵件病毒掃描系統有更快速的網路傳輸頻寬以及更少的系統資源使用率。

硬體加速處理器是一個 Co-Processor 的架構，使用標準的 PCI 介面以及配合一個 DDR SDRAM 來存放病毒碼，整個作業系統是以 Linux 的 Fedora Core 3 [5]為主要系統，Linux kernel 版本為 2.6.12，串流式硬體加速郵件病毒掃描系統的架設硬體設備是 Intel PentiumIII 1.0GHz，記憶體為 SDRAM 512MB，硬碟為 80GB 的 IDE 界面，郵件病毒掃描系統會以網路上傳輸電子郵件的通訊協定 SMTP[14]、POP3[11]來做檔案病毒的檢查。

圖 1 繪出整體的系統架構圖。其中本篇論文所要研究的方向就 HW-Accelerated Solution 對於系統加速郵件病毒掃描的部份。

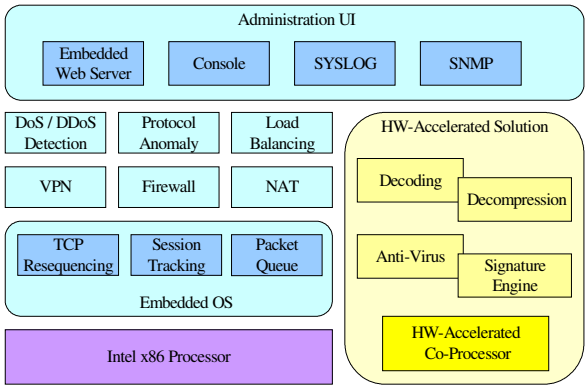

圖 1：系統架構圖

硬體加速處理器另一個特色是 off-load 系統處理器做病毒特徵碼比對的工作，當硬體加速處理器在做病毒特徵碼比對的同時，此時的系統處理器可以去處理其他的系統上的工作，等到硬體加速處理器將封包資料與病毒資料庫做病毒特徵碼比對完畢後，系統處理器再藉由讀取硬體加速處理器裡的檢查結果來判斷剛剛進行的網路郵件檔案掃描和現行的系統內病毒資料庫是否符合。符合的話就代表著硬體加速處理器有找到在網路郵件夾帶檔裡的病毒，不符合的話就表示傳輸的網路郵件檔案是一個乾淨的檔案，此時系統管理者可以針對檢查到的病毒郵件檔案做後置處理。

硬體加速處理器和系統處理器之間可以做平行處理的工作，讓最繁瑣也最消耗系統處理器資源的病毒特徵碼比對工作藉由硬體加速處理器來 off-load。這樣的架構讓串流式硬體加速郵件病毒掃描系統只需增加一點點的硬體成本就可以得到比傳統儲存式郵件防毒系統有更好的系統效能和系統處理器使用率，更可以避免無硬體內容加速的串流式郵件病毒掃描因為系統處理器過於繁忙而降低整體系統的效能。

整個串流式硬體加速郵件病毒掃描系統規劃與硬體加速之間的關係圖如 2 所

示。

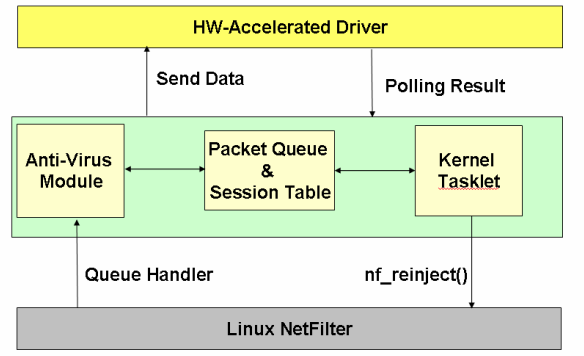

圖 2：模組架構圖

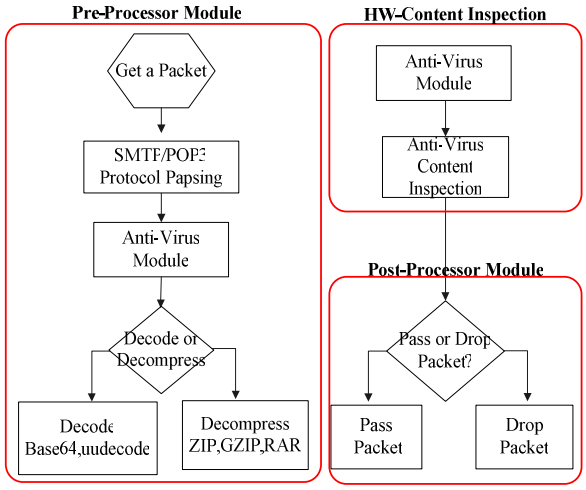

圖3：系統處理流程

3.2系統處理流程

圖3為我們提出的系統處理流程。當串流式硬體加速郵件病毒掃描系統接收到封包時，會先處理封包內容的解析來得到封包資訊。處理完基本的封包內容解析動作後，再將要檢查網路封包內容傳遞到硬體加速郵件病毒掃描系統的模組裡作病毒特徵碼的比對。但在做病毒特徵碼比對之前，需要針對電子郵件的SMTP以及POP3這兩種通訊協定做Base64 和 uudecode的解碼分析。

另一點需要做前置處理的便是郵件解壓縮的處理。當郵件的附帶檔是有一個壓縮的檔案格式時，串流式硬體加速郵件病毒掃描系統的模組需要能提供即時的郵件檔案解壓縮動作，當郵件檔案內容做解壓縮後才能將最原始的郵件檔案內容傳遞到硬體加速處理器做特徵碼比對的動作。所以系統處理流程有前置處理模組負責封包內容的解析，而硬體掃瞄偵測模組主要的執行項目為特徵碼比對的工作以及後置處理模組負責偵測到病毒檔案的處理。

4.系統實作

4.1系統架構

在串流式硬體加速郵件病毒掃描系統裡，我們使用 SMTP 以及 POP3 這兩種通訊協定做郵件病毒的偵測。由於硬體加速處理器是架構於標準 PCI 介面上，所以整個解決方案的前置處理、後置處理以及網路封包內容的檢查將會在 Linux Kernel Space 上來進行，舉如網路封包類型與長度的判斷、網路封包表頭的拆解、網路郵件夾帶檔案內容的病毒掃描等。

在Linux 核心裡，“Netfilter” [10]為負責處理網路封包的子系統， iptables[9]乃是用於設定這個子系統的命令。iptables 以「表 (table)」組織網路封包的處理「規則 (rule)」，不同用途的規則分別獨立為各自不同的表(計有filter、NAT、Mangle表)；每一條規則由「篩選條件」及「處理目標」所組成，篩選條件是用來比對封包，而處理目標是用於處置經比對符合的封包。iptables 為 OSI model 第三層(網路層)的工具，但加上擴充模組之後也可以處理第四層(傳輸層)的資料。在Linux 核心

封包處理流程中，共有五個攔截點(hook points)，分別是 INPUT、OUTPUT、FORWARD、PREROUTING 及 POSTROUTING，架構如圖4所示。

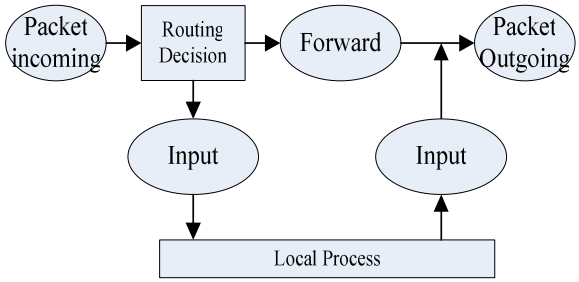

圖4：核心封包處理流程

首先，我們運用Linux Netfilter來做系統封包的進入點。當系統在初始化過程時，藉由tasklets[19]來掛載一個程式的進入點。另一方面，系統上會掛載一個Queue Policy於iptables的FORWARD chain上，詳細的示意圖如圖5所示。

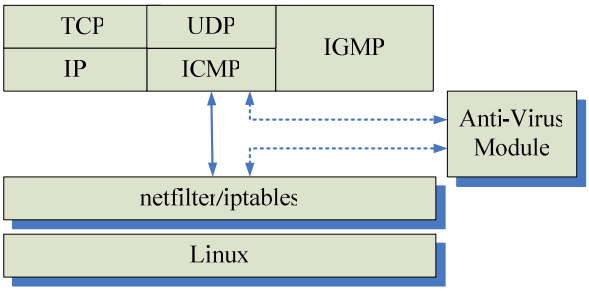

圖 5：系統模組

4.2系統前置處理模組

當系統模組接收到 Linux Netfilter 所傳遞過來的封包時，此時的封包內容是最原始的，系統模組需要從最底層的通訊協定開始做分類。當客戶端在傳送與接收郵件時，系統模組需要由郵件伺服器和客戶端兩邊溝通的過程來做判斷，系統模組要能判斷此次的郵件傳送與接收是否有夾帶檔案，假如郵件的傳送與接收只是一般的網路溝通封包或者郵件內並沒有夾帶檔案的話，則系統模組並不需要做封包內容的病毒特徵碼比對動作，直接讓封包回到 Linux Netfilter 裡讓封包繼續下面的行程，假如系統模組檢查到郵件傳輸有附帶夾帶檔案的話，則系統模組需要判斷郵件掃描的長度，然後在交由硬體加速處理器做郵件內容做檢查。

在 SMTP 以及 POP3 這兩種通訊協定裡，串流式硬體加速病毒掃描系統必須先做 MIME[13]的 header&body 的判斷以及 MIME body encoding，而 MIME encoding 包含 UUE、Base64 quoted-printalbe 等，當系統模組的前置處理完成後，就可以將郵件傳送封包交由硬體加速處理器做封包內容的檢查了。

4.3系統硬體掃描偵測模組

系統模組前置處理完成時，所有需要做病毒特徵碼比對的封包會交由硬體偵測模組來做處理，此時硬體掃描偵測模組如圖6所示，當硬體加速處理器需要做字串比對的時候，會藉由DMA(Direct Memory Access)做資料的存取，此時的系統處理器還是可以繼續工作無須理會硬體加速處理器，當系統處理器完成目前的工作時，只需檢查硬體加速處理器是否有檢查結果，有的話就將資料搬移出來交給後置處理模組，沒有的話就繼續系統處理器下一個工作。

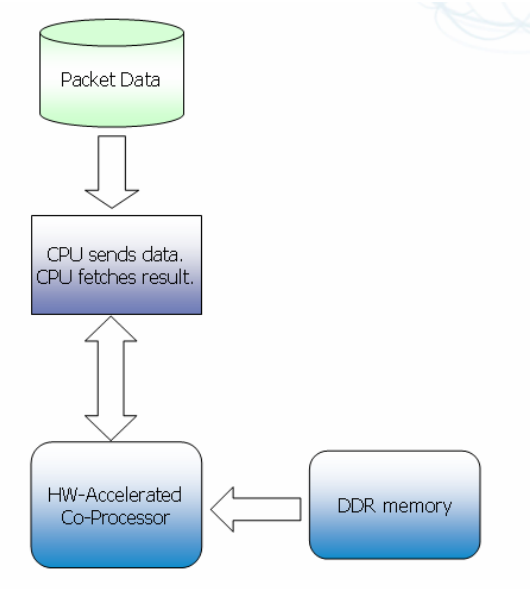

圖 6：硬體掃描偵測模組

4.4 系統後置處理模組

系統的後置處理模組主要的目的是當硬體掃描偵測模組有比對到封包內容與病毒特徵碼吻合時，代表此次的郵件接收與傳送的檔案內容是有夾帶病毒的郵件檔案，後置處理模組可以依據管理者的設定將連線強迫中斷，讓後續的網路連線無法繼續傳輸並且用紀錄的方式通知管理者或清除感染的資料內容等，所以在後置處理模組裡可以依據不同的條件需求做不同的設計。

5. 系統實驗結果

5.1 系統建置

針對本篇論文所提出的研究，我們架設系統實驗的基本建置如表一所示，我們使用一個 Intel PentiumIII 1.0GHz 的 CPU，512MB SDRAM，80GB 的硬碟與 Intel 100Mbps 的網路介面來安裝 Linux 2.6.12 的作業系統。在實驗測試檔案方面，我們使用一個檔案大小為 1MB 的可執行檔案作為郵件夾帶檔案的附件夾帶檔，在測試壓縮檔案方面，我們使用一樣的 1MB 可執行檔案來製作壓縮測試檔。

針對本篇論文的研究，我們將會比對的系統包含儲存式郵件病毒掃描系統、串流式郵件病毒掃描系統以及串流式硬體加速郵件病毒掃描系統這三種不同的郵件病毒掃描系統裡，當郵件做網路傳遞且有夾帶附件檔時在網路效能上的差異外，還將比對郵件夾帶是壓縮檔案格式時的網路效能差異，以及郵件病毒掃描系統上的處理延遲、系統處理器使用率、記憶體使用率來做比較。

表一：硬體架構平台

CPU	Intel PentiumIII 1.0GHz
RAM	SDRAM 512MB
Hard Disk	80GB
Ethernet Network	Intel e100 NIC
Kernel Version	Linux 2.6.12

5.2 系統效能測試

我們架設如圖7 所示的實驗環境架構圖。

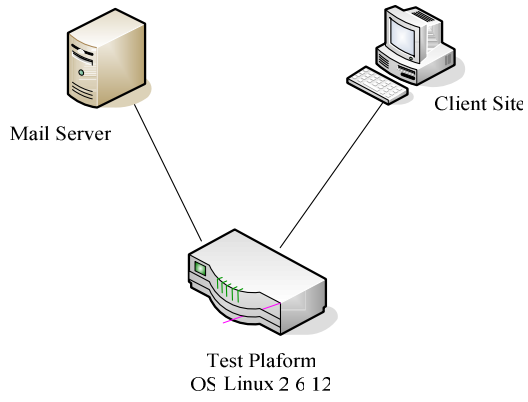

圖 7：實驗環境架構圖

首先，在測試實驗環境上我們安裝所要測試的三種模式，而在伺服端電腦上架設測試的Mail Server，而在客戶端電腦上安裝Microsoft Outlook收送信件軟體。郵件病毒掃描系統的功能測試主要目的是驗證上述三種郵件病毒掃描系統是否可以正確無誤地找到當網路傳輸郵件時所夾帶的病毒檔，所以功能測試實驗上我們模擬當使用客戶端電子郵件軟體作收信以及送信且夾帶的附件檔都是病毒檔案時，郵件病毒掃描系統是否可以正確無誤地檢查郵件的夾帶檔案是否是病毒所感染的檔案。

表二：功能比較表

Format	Program	File extent	HW-based
gzip	gzip	.gz	Yes
zip	Winzip	.zip	Yes
rar	WinRAR	.rar	Yes
bzip2	BWT	.bz2	No
7zip	7-zip	.7z	No
Self-extract	itself	.exe	Yes

在系統效能測試方面，我們將測量三種系統在夾帶郵件是執行檔案以及當夾帶的郵件檔是壓縮格式的檔案時，這三種郵件病毒掃描系統在網路傳輸效能上的差異，以驗證串流式硬體加速郵件病毒掃描系統與其他兩種郵件病毒掃描系統有更好的效能表現。

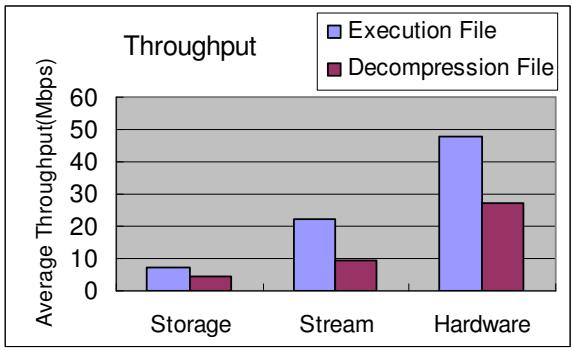

圖 8：效能比較表

圖 8 的效能比較表可以展現出使用串流式硬體加速郵件病毒掃描系統的網路效能可以較其他兩種系統有更好的網路效能，這是因為複雜的字串比對工作已經交由硬體加速來進行，串流式硬體加速郵件病毒掃描系統只需要做前置處理以及後置處理的工作即可。而在解壓縮郵件掃描的網路效能部份，串流式硬體加速郵件病毒掃描系統也是較其他兩種郵件掃描系統一樣有更好的網路效能表現。

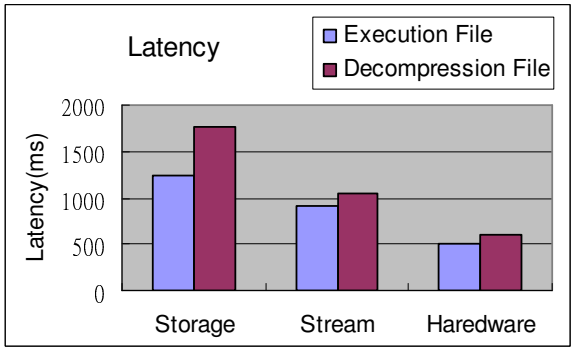

圖 9：延遲(Latency)比較表

再由圖9的延遲(Latency)比較表可以得知，由於系統上的CPU已經不需要做字串比對的複雜工作，所以串流式硬體加速郵件病毒掃描系統上所流經的封包要做內容檢查時，可以很快的通過郵件病毒掃描系統，讓整體的網路效能的瓶頸不會是在系統處理器處理字串比對上。

5.3 CPU使用率與記憶體使用率

在郵件病毒掃描系統內部資源的比較方面，當三種郵件病毒掃描系統在做網路效能比對時，我們觀察三種郵件病毒掃描系統上的處理器使用情況以及記憶體使用率。

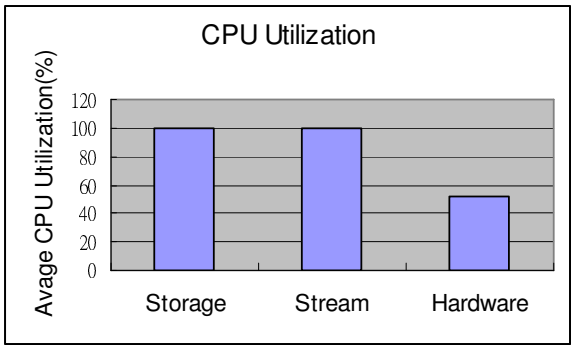

圖 10：CPU 使用率

圖10的CPU使用率可以展現出使用串流式硬體加速郵件病毒掃描系統的CPU使用率遠低於其他兩種郵件掃描系統，也由於這樣的表現，在串流式硬體加速郵件病毒掃描系統上的CPU可以去處理郵件病毒掃描系統上其他的工作，不會因為郵件病毒掃描系統需要檢查郵件夾帶檔的內容而佔用了所有的CPU資源。

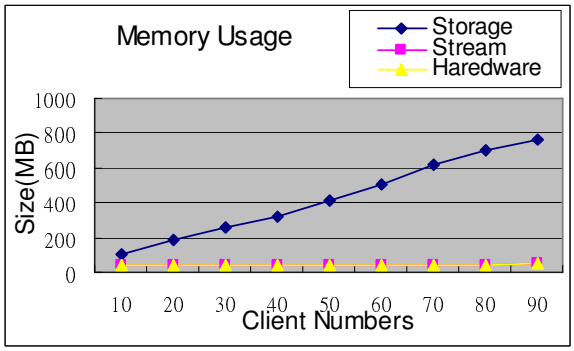

圖 11：記憶體使用率

圖11是三種郵件掃描系統記憶體使用率的比較表，串流式郵件病毒掃描系統由於不需要做先存檔後再掃描的動作，其記憶體的使用率不會像儲存式郵件病毒掃描系統一樣需要耗費很多郵件病毒掃描系統上的記憶體資源，也藉由這樣的表現，郵件病毒掃描系統上的記憶體資源也可以讓其他需要記憶體資源的系統工作來使用。

6.結論與未來工作

提升網路整體的安全性以及傳輸效率，將會協助管理者更有效率的進行網路管理的工作，本研究透過硬體加速內容掃描的方式，將原本郵件防毒閘道器的效能問題以及系統資源耗損問題解決。透過這次的研究來提供更快速的網路傳輸效能以及提供更安全的網路環境。未來工作不只在郵件防毒閘道器系統可以做硬體加速內容掃描的方式，相同的方法一樣可以運用在整合式威脅控管設備上，現在市售的整合式威脅控管設備都有入侵偵測與病毒掃瞄功能，讓病毒掃描系統以及入侵偵測系統都使用硬體加速內容掃描的方式來做整體性的安全防護措施，這將會有效的建立安全、高品質的網路使用環境。

參考文獻

[1] A. Aho and M. Corasick. Fast pattern matching: an aid to bibliographic search. *Commun. ACM*,18(6):333–340, June 1975.

[2] ClamAV User Manual https://sourceforge.net/docman/display_ doc.php?docid=18277&group_id=86638

[3] CP Secure, http://www.cpsecure.com/

[4] E. P. Markatos, S. Antonatos, M.Polychronakis,and K. G. Anagnostakis,"Exclusion-based signature matching for intrusion detection," in /IASTED International Conference on Communication and Computer Network(CCN'02)/, 2002.

[5] Fedora Core 3, http://fedora.redhat.com/

[6] Fortinet, http://www.fortinet.com

[7] H.-J. Jung, Z. K. Baker and V. K. Prasanna"Performance of FPGA Implementation for Bit-split Architecture for Intrusion Detection Systems" in Proceedings of the Reconfigurable Architectures Workshop at IPDPS, 2006.

[8] L.Tan and T. Sherwood, "A high Throughput String matching architecture for intrusion Detection and prevention," in Proceedings of the 32nd Annual International Symposium On Computer Architecture, 2005, pp. 112-122.

[9] Linux iptables http://www.netfilter.org/projects/ iptables/index.html

[10] Linux Netfilter, http://www.netfilter.org/

[11] POP3 Protocol – RFC1225 Post Office Protocol – Version3, TCP/IP protocol Suite, application layer email access protocol

[12] R.Boyer and J. Moore. A fast string Searching algorithm. *Commun. ACM*, 20(10):762–772, October 1977.

[13] RFC 2045 – Multipurpose Internet Mail Extensions (MIME) Part One : For mat of Internet Message Bodies, http://www.faqs.org/rfcs/rfc2045.htm

[14] SMTP Protocol – RFC788 Simple Mail Transfer Protocol. TCP/IP protocol Suite, application layer message transfer protocol

[15] Symantec, http://www.symantec.com

[16] "Systolic array for string matching in NIDS"

[17] Szu-Hao Chen, "A Stream-based Mail Proxy with Interleaved Decompression and Virus Scanning"

[18] Trend Micro, http://www.trendmicro.com

[19] Understanding the Linux Kernel, 2nd Edition Publisher: O'Reilly, Pub Date: December 2002, ISBN: 0–596–00213–0