

以亂數與虛擬技術為基礎的電腦課程實習環境

蔡哲民	王建仁	張靜芬
崑山科技大學資訊 傳播系	崑山科技大學電腦與 通訊系	高雄醫學大學通識 教育中心
tjm@mail.ksu.edu.tw	cjw@mail.ksu.edu.tw	chcfen@kmu.edu.tw

摘要

傳統電腦教室通常使用硬體還原卡、軟體還原或 thin-client 的架構建置，且網路結構固定，這種建置方式造成一些需要重新開機或修改架構的電腦課程無法實際操作。另外，實體電腦教室也無法支援遠距教學課程實習的需求。為了解決此一問題，我們引進虛擬化技術，透過亂數動態分配使用者利用 RDP (Remote Desktop Protocol) 協定連接的伺服器與 TCP port，使得使用者可以透過網路安全的使用虛擬機器。此一架構提昇了電腦實習環境的彈性，並可支援遠距教學的實習需求。Client 端的程式除了可安裝在既有的電腦教室中，強化原有教室使用的彈性，並提供學生下載安裝在自己的電腦上使用，同時我們也製作了 LiveCD，可以用於新建的電腦教室，以節省硬碟與還原卡的成本。

本系統已經在一個五十人上課的環境中順利使用過，結果證明本環境可強化電腦教室的彈性。除了上課環境之外，本系統也可以應用於企業電腦化等環境之中。

關鍵詞：虛擬化、亂數、電腦教室

壹、前言

隨著社會資訊化的程度日漸加深，資訊相關課程佔據學生課程比重與其他課程倚重資訊技術的程度也日漸加深，電腦、網路的操作與使用成了每個人工作、學習必備的基本工具。為了因應這個趨勢，各級學校無不廣泛設立電腦教室，以利電腦相關課程進行講授、實習。此外，隨著遠距教學的普及，如何提供學生電腦實習也成了遠距教學成功與否的重要因素。

目前一般電腦教室的管理工作，單單是維護軟硬體的正常運作就是一項相當耗費人力的業務[10]。為了簡化這些管理工作，避免沒有經驗的使用者任意或錯誤使用導致的問題，通常管理者會利用硬體還原卡、軟體還原或 thin-client 方式[10][11]來建構電腦教室。

其中軟體還原和 thin-client 的架構成本較低，但是需要依賴伺服器與網路系統的輔助，且對於惡意破壞的免疫力較低，通常用在圖書館等環境較單純的地方。硬體還原卡的成本較高，且需花費額外的硬碟空間，但具有還原速度快，無須額外的伺服器、網路系統輔助等優點；且因為硬體還原卡還原完整，對於 fdisk 一類的惡意破壞具有較大的免疫力，更能一併解決病毒、木馬感染等系統安全問題，進一步降低管理者的負擔，因此成為大部分電腦教室使用的解決方案。

上述這些解決方案都有其特定的適用範圍，但今日的電腦課程較以往多樣化，且電腦的價格高昂，學校無不希望盡力提昇電腦教室的使用率，因此電腦教室就更必須滿足各種不同教學型態的需求。不論是硬體還原卡、軟體還原或 thin-client 的架構，多半都只能適用於比較單純的電腦教學環境，僅支援一種或少數幾種作業系統與一種網路結構。如果遇到要教授需要重新開機的軟體安裝、作業系統安裝等主題，或需要修改網路結構的資訊課程，常常會遭遇問題。實體課程都已經受到上述的各種問題的困擾，而目前盛行的遠距教學課程，更不用說是難以使用目前的實體電腦教室進行講授與實習。

如果希望透過電腦教室來進行線上評量，則會面臨更大的挑戰。因為學生可以透過網際網路、USB、藍芽、無線網路等等通訊設備進行舞弊。而無論是硬體還原卡、軟體還原或 thin-client，都很難滿足平時維護方便與考試防堵電子舞弊的要求。

過去已經有不少人嘗試建置虛擬實驗室[12][16]，不過這些系統多半僅用於特定的科目與特定的實驗，無法支援一般性的電腦教室課程，也比較少考慮大部份使用者其實為不具備專業資訊素養的一般學生，

近年來虛擬化已經成為企業節能省碳、降低營運成本[13]的重要手段。虛擬化是透過將許多台伺服器虛擬執行在一台伺服器上，因此可以獲得節省成本、配置靈活的好處。本論文透過虛擬化技術結合亂數配置伺服器與通訊埠號，讓使用者透過 Remote Desktop Protocol (RDP)協定連接進入虛擬機器，期望以少量的成本解決目前電腦教室靈活度不足的問題，並可支援遠距課程進行實習。另透過管制虛擬機器的網路與週邊設備運作，建置一個可以防堵常見電子舞弊的線上考試環境。本系統除了可以搭配已經使用硬體還原卡、軟體還原與 thin-client 建置完成的電腦教室，強化其靈活度外，也可以透過 LiveCD 一類的方式直接建立無硬碟的新電腦教室，遠距課程的學生也可以透過下載一套跨平台的 Java Client 端程式，直接連上虛擬電腦教室進行實習。

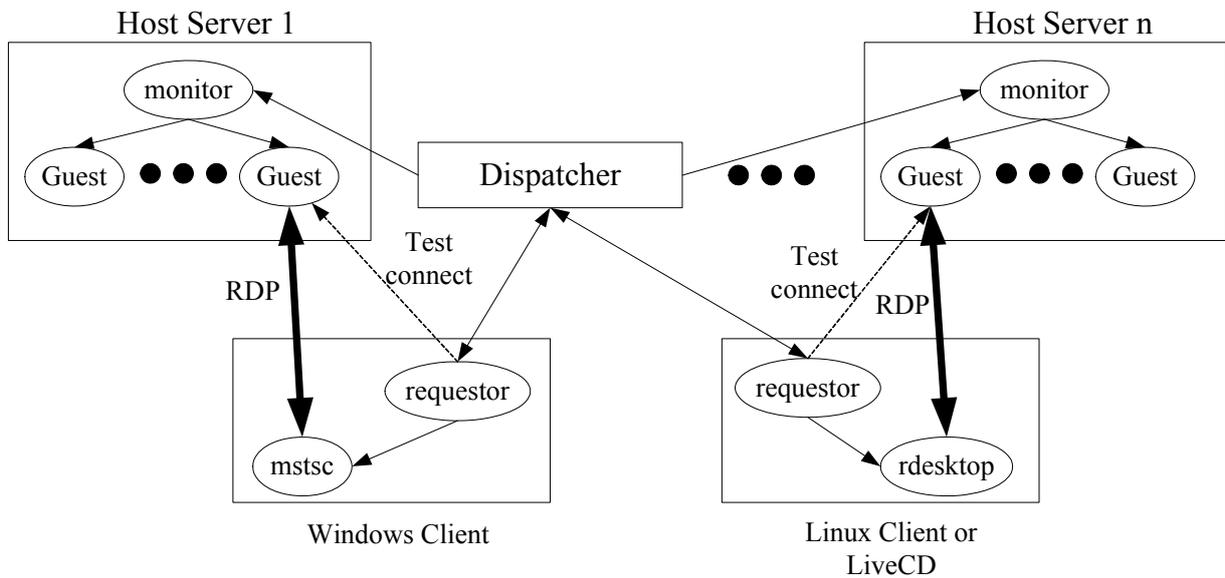
本系統已經實際用在某科技大學進修部一年級的課程中，學生人數是 50 人，進行 Windows XP 的安裝實習，大部分學生都可在課程中完成安裝。

貳、系統結構與運作

一、系統架構

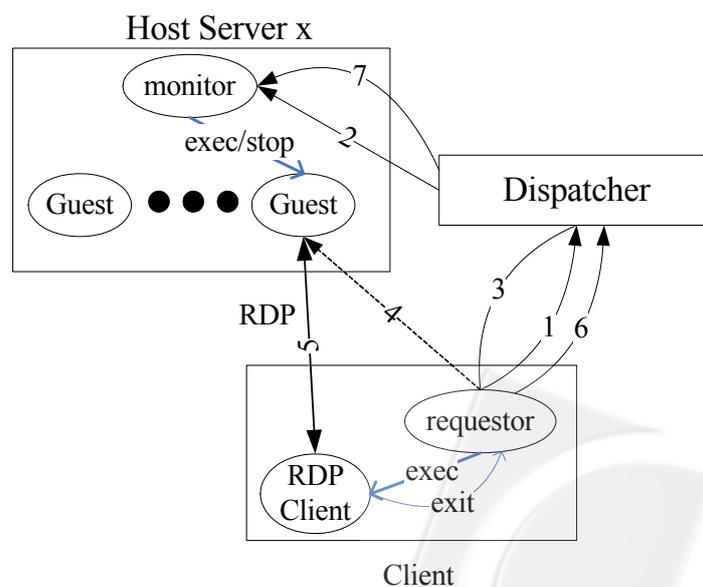
由於電腦課程修習人數可能很多，以目前的虛擬化系統的效能，不一定能在單一伺服器上承載提供修習學生一人一機的虛擬機器數量，因此我們提出的系統包括數台實際

承載虛擬機器的 Host Server，與一台負責配置所有使用者 request 到 Host Server 的 Dispatcher，使用者端〔Client〕則使用 RDP 協定透過 Linux 或 Windows 上各自的 client 連接進入 Host Server 中的虛擬機器(Guest)使用，系統架構如圖一。



圖一：系統架構圖。

選用 RDP 作為連線協定的主要原因，是因為目前主要的作業系統都提供 RDP Client 程式，我們不須重複開發專屬的通信協定。而且 RDP 已經使用多年，成熟穩定也具備一定的安全性，因此我們只要控制主要作業系統的 RDP Client 連接虛擬機器，即可降低整個系統的開發時間與使用者端安裝檔案的大小。



圖二：系統運作流程圖。

系統運作流程如下：Client 端必須先透過一個 Java based requestor 程式對 Dispatcher 發出要求，Dispatcher 查詢內部尚未被使用的 Host Server，然後其中一未被使用的 Host Server 送出一個包含啟動信號、Client 端的 IP address 與對應的亂數 TCP 埠號的封包給該 Host Server 上的 monitor，由該 monitor 啟動虛擬機器並開啟連接埠到指定的埠號上。同時 Dispatcher 也回應 Client 端上的 requestor 對應的 Host Server 與埠號。Requestor 測試該 RDP 連線已經暢通之後，就啟動 Client 端的 RDP client 程式進行連接，完成整個連接流程。當 Client 端的 RDP client 程式停止運作後，requestor 會判斷 RDP client 的回傳信息，重新執行 RDP client 或傳送完成信號給 Dispatcher，轉通知對應的 monitor 停止對應的虛擬機器運行。運作流程如圖二所示。

二、虛擬機器

目前市面上常看見的虛擬機器有 vmware[7]、VirtualPC[3]、Xen[8]與 VirtualBox[5]等，為了降低系統成本、提高系統靈活性，我們選用 VirtualBox 作為虛擬機器解決方案，該系統以效率良好聞名[1][9]；且使用 VBoxHeadless 來啟動虛擬機器，不必等到 Guest OS 啟動完成（虛擬機器啟動完成即可提供）就可以提供 RDP 連接，使得學生能看到整個作業系統的完整啟動過程，非常適合教學使用。更重要的是 VirtualBox 可以安裝在多種作業系統上，且可以免費用在教育用途上[6]，使得我們可以將 Host Server 建置在現有的伺服器上，無須額外購置新的軟硬體設備。

三、認證與安全機制

為了有效降低入侵者劫奪或干擾使用者被分配之虛擬機器，我們在 Client 端的 requestor 向 Dispatcher 發出 request 時（圖二中的流程 1），即紀錄 Client 端電腦的 IP address，然後 Dispatcher 分配好 Host Server 時，也將 Client 端的 IP address 傳遞到對應 Host Server 的 monitor（圖二中的流程 2）。Monitor 除了啟動虛擬機器，並將其連結到 Dispatcher 指定的埠號；同時也設定防火牆，僅允許 Dispatcher 提供的 Client 端 IP 連入對應的埠號。由於埠號是用亂數指定的，而且一般可用的 TCP 埠號範圍是 1001 到 65535，入侵者除非能完全掌握分析網路封包，否則是難以在有限時間內，透過嘗試錯誤劫奪使用者與被分配之虛擬機器中間之 RDP 連線。VirtualBox 的另一優點為 VirtualBox 2.0.x 版支援 RDP 5.2 的認證與 RC4 加密功能，可以配合 Windows 的 mstsc 與 Linux 上的 rdesktop[4]的能力進行連線加密。

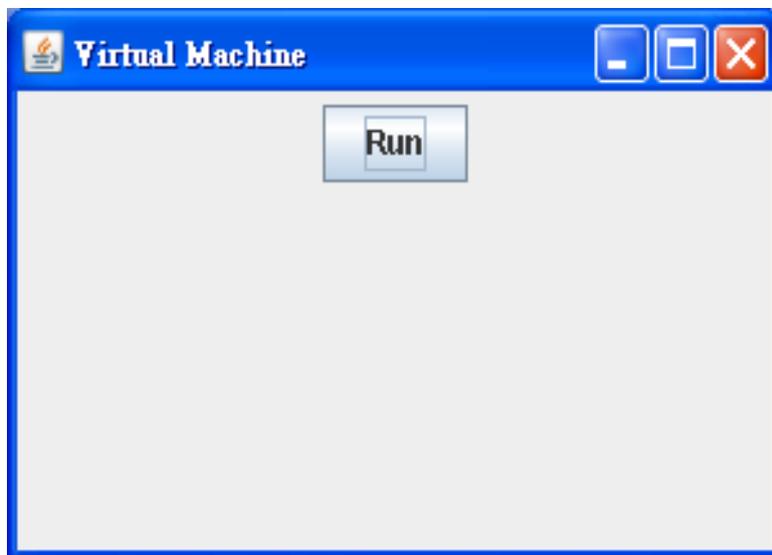
目前常用的認證機制有傳統的帳號密碼認證、public key 等機制；但考慮到此系統為教學環境，使用本系統進行實習的學生不一定擁有足夠的資訊素養，因而本系統不宜採用太過複雜的認證機制。且由於 Windows 上的 RDP client 程式 mstsc 只能連接上運作中的 Windows 系統再進行認證，無法像 Linux 系統上常見 Open Source 的 RDP client 程式 rdesktop，可支援直接對 RDP 連線認證；因此如果在執行一般 Windows 作業系統下的電腦教室使用本系統，則甚至無法使用傳統的帳號密碼方式進行 RDP 連線身份認證。

由於上述原因，且加上標準的 Windows XP 或 Vista 作業系統提供多樣的電子通訊管道，因此我們並不建議直接在一般的 Windows 作業系統電腦下，使用本系統作為線上考試等需要比較嚴謹身份認證的環境。為解決上述問題，我們開發 LiveCD 作為 Client 端的環境，相關建置方式將於下文中介紹。

雖然因為上述種種原因，我們無法對 Client 端的 RDP 連線作嚴謹的認證，但我們在伺服器端還是可以透過記錄連線使用者 IP 的資訊，作為基本的防弊措施。並且以透過亂數指定 Client 連線的 Host Server 與對應的 TCP port，配合 Host Server 端防火牆的設定，避免入侵者劫奪使用者分配到的虛擬機器，或者有學生偽裝其他學生身份登入虛擬機器。事實上，帳號密碼認證也無法有效遏止意圖作弊的使用者，因為如果有人要代考，一定早就已經擁有對方的帳號與密碼，所以我們還是要依賴防火牆、log 分析等方式來進行防弊措施。

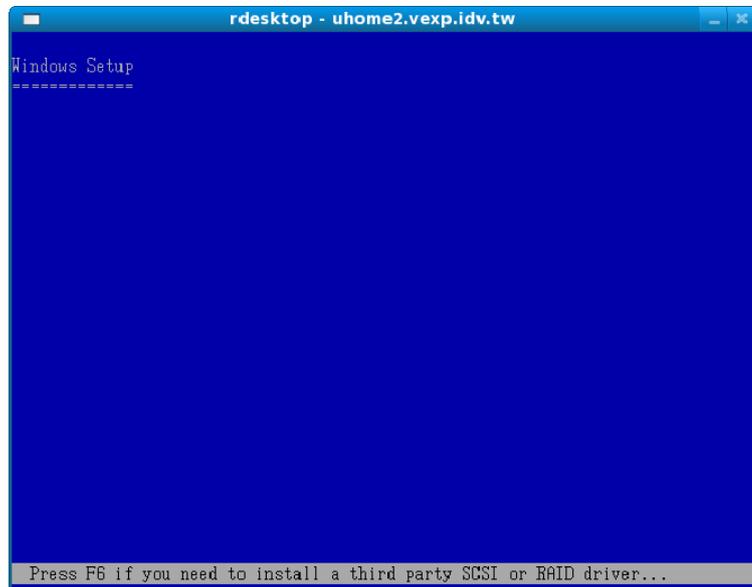
四、Client 端的 requestor

為了簡化軟體的發展與佈署過程，我們使用跨平台的 Java 作為 Client 端 requestor 程式的發展工具。為了簡化整個安裝與操作程序，使得對電腦不熟悉的使用者也能輕鬆上手，我們將整個 requestor 的操作介面簡化成一個按鈕，如圖三所示。



圖三：Client 端 requestor 程式的操作介面。

當使用者按了 RUN 鈕之後，系統就自動連接到 Dispatcher 去取得相關的資訊，並自動連接到對應的虛擬機器。為了避免 Host Server 負載沈重時，回應時間太慢，requestor 在啟動 RDP client 程式前，會每秒檢測一次 Host Server 上對應的 port 是否已經可以連接上，當確認虛擬機器已經可以被連接，才啟動 RDP client，圖四是 requestor 啟動 Linux Client 連接虛擬機器的畫面。



圖四：Linux Client 連接虛擬機器的畫面。

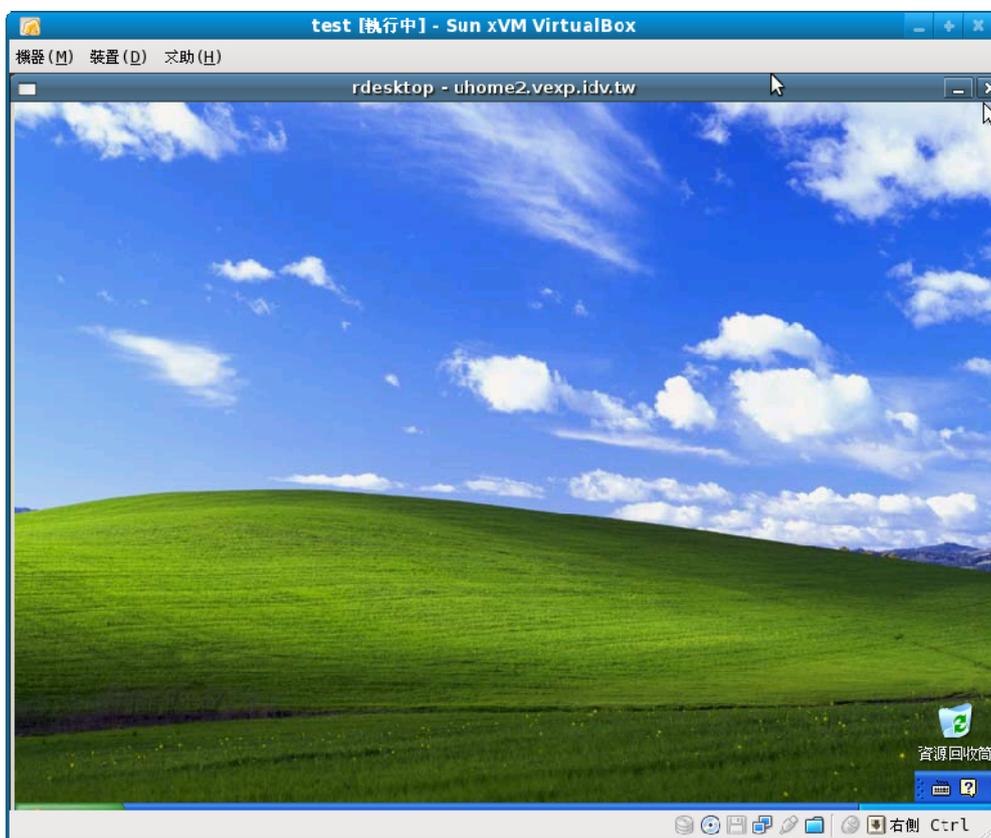
當 Client 當機或是網路故障期間，伺服器上的虛擬機器仍然會繼續運作，並不受 Client 當機或是網路故障影響，因此 requestor 是可以嘗試復原當機或網路故障前的作業。因此，Requestor 先將 Dispatcher 傳送過來的資料寫入一個檔案，此檔案直到整個作業正常完成後才刪除；而 requestor 開始執行時，就先檢查該控制檔案是否存在，而決定是否先連接上一次的虛擬機器。藉著這樣的機制，使得 Client 端設備及網路的穩定度不至於太過影響整個學習的進度。

五、LiveCD Client

雖然在現有的電腦教室系統中加裝 requestor 程式，就可以直接使用本系統，增加上課彈性；且透過亂數產生 port、分配 Host Server、配合 Host Server 上防火牆設定，可以解決一部分防弊的問題。但是如果真正想利用電腦教室進行線上考試，或者想要進一步節省掉再生卡與硬碟的成本，就必須使用 LiveCD 或 LiveUSB 這類的解決方案。

使用 LiveCD 作為線上考試[14][15]或教學環境並不罕見，因為價格便宜、可開機，且 LiveCD 的唯讀特性可以使得學生無法任意修改系統配置；如果加上建置於 LiveCD 上的防火牆，對網路連接都可以嚴格限制。目前拿來作為 LiveCD 的作業系統主要是 Linux，這是由於 Windows 作業系統限制不得任意更換執行硬體，使得這個學生最熟悉的作業系統很難廣泛的作為 LiveCD 的平台；為解決此問題，需要透過虛擬技術[15]等等技巧才能勉強提供學生熟悉的環境。

我們利用 Linux 上的 RDP client 可以連接上執行 Windows 的虛擬機器，使用 Ubuntu Linux 上的 reconstructor[2]，建置一套 LiveCD。將 RDP client 與 requestor 程式都放在開機自動執行命令中，且啟動 LiveCD 上的防火牆，限定該系統僅能連上 Dispatcher 與 Host Server，就能有效限制使用者的電子通訊途徑。此外，必要時可以抓取電腦上的 MAC address 等可以用來確認使用者電腦的資料，於 requestor 要求虛擬機器時一併送至 Dispatcher 上記錄下來，如此就可以更進一步掌握學生的資訊。透過這樣的機制，更可以直接節省下電腦教室電腦上的硬碟與還原卡等硬體，進一步降低成本。為了進一步簡化使用者的操作，我們修改了 requestor 程式，讓 LiveCD 一開機就直接自動去 request 一個虛擬機器，省去了使用者按「Run」鈕的步驟。LiveCD 透過虛擬機器執行的開機運作畫面如圖五所示。



圖五：LiveCD 的運作畫面。

參、實驗結果與討論

我們將此系統應用在某科技大學進修部一年級的課程中，學生人數是 50 人，進行 Windows XP 的安裝實習。我們採用兩台 Host Server，一台是 Dual-Core AMD Opteron

Processor 2.2G Hz 2G RAM，這台機器另外還扮演 Dispatcher 的角色；另一台是 Dual-Core AMD Opteron Processor 2.8G Hz 16G RAM。兩台機器都有配置有 12 個 SATA 硬碟的磁碟陣列，並安裝 Fedora 9 Linux 64bit 版本與 VirtualBox 2.0.4 虛擬機器。我們將大部分的負載都配置到擁有 16G RAM 的 Host Server 上，每台虛擬機器配置 256M RAM 與 10G 硬碟。

學生都透過安裝 Windows XP 與還原卡的同一間電腦教室電腦連上虛擬機器。該電腦教室與 Host Server 在同一個校園的不同網段上。Client 端的 requestor 程式則由學生自行透過網頁下載、解壓縮並執行。由於學生並不熟悉 Windows XP 的安裝，因此安裝的過程是先由老師示範後，交由學生進行安裝。

結果絕大部分學生都在三小時的課程中完成安裝，但在學生實習的高峰期則發生過幾次因為 Host Server 負載太高 (Linux 系統 loading 回報高達 30 左右)，導致學生反應系統回應遲鈍。由於每一台虛擬機器都需要配置一定的記憶體才能正常運作，因此即使擁有 16G 的主記憶體，也至多能讓大約 50 個左右使用者同時上線。如果考慮 Windows 作業系統的安裝是 I/O Bound 的作業，則硬碟系統的負荷恐怕也將限制同時上線使用者的人數。如果考慮一般電腦作業，至少要配置 512M RAM 才夠用，那一個 50-60 人的班級應該要配置兩台具備 16G RAM 與磁碟陣列的 Host Server 才能夠順暢的執行比較複雜的電腦實習課程。以目前電腦硬體價格滑落的速度來看，這樣的設備價格應將遠低於一間 60 個人的電腦教室。

由於本系統發展之初就已經考慮到不熟悉電腦操作的使用者的需求，大幅降低操作界面的複雜度，因此進行實作時，並沒有學生反應不會使用。不過目前虛擬機器的配置仍要依賴人工撰寫 Script，未來如果要推廣到更多電腦課程使用，則仍需要開發讓授課老師或管理者容易配置虛擬機器的伺服器端系統。

因考量使用者的方便性而與通用的 Windows RDP Client 程式功能妥協，本系統僅用亂數來建構安全體系，因而缺乏進一步的使用者認證機制。且因為教學的需要，系統 Client 端的 requestor 程式也難以保密，因此本系統非常需要仰賴防火牆的協助，以阻擋不合法的連線嘗試及阻止可能的 DoS 攻擊。未來我們也考慮在 Dispatcher 處進行身份認證，通過認證的 IP，則由防火牆放行，以兼顧安全及增加使用者的連線彈性。

由於本系統發展完成時日尚短，僅初步用來進行作業系統安裝課程的實習，尚未完全發揮虛擬化的彈性與特點。未來將進一步應用在「資訊安全」或者其他需要多台電腦互動的課程環境中，並對於學生學習成效進行更精確的評估分析，以期獲致更大的成效。

肆、結論

我們發展出一套以亂數與虛擬技術為基礎的電腦課程實習環境，Client 端系統可以附加在現有的電腦教室架構上，或者以 LiveCD、LiveUSB 的形式用於新建立的電腦教室，

也可以由學生自行下載安裝在自己的電腦上。

本系統的 Client 端透過 requestor 對伺服器端的 Dispatcher 提出要求，Dispatcher 利用亂數分配 Host Server 與虛擬機器 Listen 的 TCP port number，配合 Host Server 端的防火牆設定來提供安全機制。Client 端的 requestor 程式提供簡易操作的介面，並提供一定的錯誤回復能力。該系統曾經在一個五十個人上課的課程中實際使用過，證明確實可行。

本系統除了可用於電腦實習環境之外，也可用於一般企業電腦化環境中，供員工以運算能力較低的電腦連接至虛擬機器中。未來我們除持續將此環境應用在各樣的課程與線上考試之外，也將持續發展伺服器端的虛擬機器配置系統，以強化此系統的可用度。

參考文獻

- [1] "Benchmarks: VPC 2007 SP1 vs. VirtualBox 1.6",
<http://www.wilderssecurity.com/showthread.php?p=1252392> (2008/5/29)
- [2] <http://reconstructor.aperantis.com> (2008/11/26).
- [3] <http://www.microsoft.com/windows/products/winfamily/virtualpc/default.msp>
(2008/11/26)
- [4] <http://www.rdesktop.org> (2008/7/09)
- [5] <http://www.virtualbox.org> (2008/11/26)
- [6] http://www.virtualbox.org/wiki/VirtualBox_PUEL (2008/11/26)
- [7] <http://www.vmware.com> (2008/11/26)
- [8] <http://www.xen.org> (2008/11/26)
- [9] P. Feuerer," VirtualBox vs. Qemu vs. VMware-player (updated) ",
<http://www.linux-gamers.net/modules/smartsection/item.php?itemid=56> (2007/1/21)
- [10] 王光山，“以自由軟體協助電腦教室管理”，碩士論文，朝陽科技大學資訊管理系，2003。
- [11] 吳素芬，“以軟體為基礎之有碟 PC 教室管理系統—以中央大學電算中心為例”，碩士論文，國立中央大學資訊管理學系碩士在職專班，2004。
- [12] 陳俊廷，“虛擬化網路安全實習實驗室之規劃與建置”，碩士論文，淡江大學資訊管理學系，2007。
- [13] 蔡佳帆，“虛擬化技術之績效測試比較”，碩士論文，淡江大學資訊管理學系，2006。
- [14] 蔡哲民、王麒讚、吳明昆，“大學校園資訊基本能力檢定平台之建置與運作”，2008 年中華商管科技學會年會暨學術研討會，2008。
- [15] 蔡哲民、楊家龍、許芳斌、賴滢羽、林承融、謝宗廷、陳明唐，“以 Live-CD 為基礎的程式上機考試環境”，2006「開放原始碼」技術與應用研討會，2006。
- [16] 劉維竣，“虛擬實驗室之建立”，碩士論文，國立台灣科技大學機械工程系，2002。