應用 RFID 技術於電腦教室之滑鼠使用權限與網路存取控管

Access Control for Mouse and Network Functions in Computer Classroom Using RFID Technique

楊慶隆 邱志揚 林郁琪 陳穎凡 游雅棻 陳澤世 李宇峰
國立東華大學資訊工程系　國立東華大學計算機與網路中心
cnyang@mail.ndhu.edu.tw

摘要

校園電子化，不僅能讓行政管理作業更快速便捷提高整體效率，降低管理成本，也能增加安全性。在校園中，電腦教室的使用權限管理，以及紀錄使用狀況，是普遍需要面對的一個課題。電腦教室的控管目前仍多使用人工方式搭配識別身分條碼或晶片卡進行管理。因此，難免會遇到人為管理疏失、缺乏效率或者安全性不足等問題。無線射頻辨識標籤(RFID)技術扮演了條碼的腳色，但是又具備了無線、可讀寫、同時讀取、不易毀損等好處。本文中介紹了一套適用於電腦教室之教室控管系統。本系統採用 RFID 技術，並結合網路位址轉換協定(NAT)與滑鼠上層驅動程式(Filter Driver) 。實作出一個有效且完善的自動化電腦教室管理系統，解決校園電腦教室管理的困擾，達到節省人力資源、降低管理成本、增加安全性等好處。有合法 RFID 標籤證件的學生才能有權限使用網路與滑鼠功能。

關鍵詞：無線射頻辨識系統、網路位址轉換協定、校園電子化。

Abstract

For e-campus environment, to achieve the efficient management and security in computer classroom, we usually use bar code on the student card or IC card to secure the management of computer classroom. Recently, Radio Frequency Identification (RFID) technique had become popular for identifying not only objects but also persons. Actually, RFID works like bar code. Moreover it has the advantages: read and write; non-line-of sight; multiple read simultaneously; suited to kinds of surroundings; non-human interface. In this paper, we adopt the RFID technique and combine the NAT and the Filter driver for mouse to design and implement an access control system for the management of computer classroom. Our system successfully manages the networking and mouse functions via a legal RFID tag on a student card.

Keywords: RFID, NAT, e-campus.

1. 前言

目前電腦教室管理最常出現的問題，例如：非法竊取使用者密碼、破壞教室電腦的軟硬體設備等行為，通常很難在第一時間發現與處理。然而採用人工監控紀錄教室使用者的相關資料，無論以填寫或輸入資料的方式都不方便，因為資料越詳細則越耗費時間，而且也可能發生冒用別人身分的問題。因此，本文中我們設計使用 RFID 降低上述情形發生的頻率；由於 RFID 電子標籤能與學生證結合、大小適中攜帶方便，而且利用非接觸的掃描方式，加上快速讀取、準確性高與安全性佳的特性，很適合用在電腦教室這類出入頻繁又需控管的場所。

本文所提之電腦教室滑鼠使用權限與網路存取控管模組，是當使用者持 RFID 標籤(Tag)進入電腦教室時，電腦教室中之個人電腦上均配備有 RFID 讀取機(Reader)可讀取學生證上 RFID 標籤的識別碼達到辨識使用者的目的。待身分資料經辨識通過後，即可取得滑鼠的使用權限以及對外連接網際網路的連線功能，藉此達到電腦教室使用權限之監控與管理。本文之文章架構如下：第二章中簡述 RFID 相關技術，第三章為系統介紹與實作說明，第四章則為安全性與便利性分析，結論述於第五章。

2. RFID 技術簡介

RFID 系統包含：讀取機、標籤以及後端資訊系統。其原理是讀取機以有線或無線的方式與後端資訊系統相連，且讀取機可透過所發射的 RF 無線電波讀取標籤內資訊並傳回主資訊系統辨識。

RFID 的重要特徵之一為其標籤的電源供應模式可分為主動式(Active)與被動式(Passive)。被動式標籤是接收讀取機所傳送的能量，轉換成電子標籤內部電路操作電能，不需外加電池；可達到體積小、價格便宜、壽命長以及數位資料可攜性等優點，因此被廣泛應用於各領域，如：EAS 防竊系統等。主動式標籤則是內含電池，因此具備較長的通訊距離，但主動式標籤的壽命卻受限於電池壽命，此外，主動式標籤又可分為半主動與全主動，其中半主動式標籤之電源僅供內部電路使用，RF 訊號之回應則需仰賴讀取機的訊號充電;而全主動標籤則擁有較強之電力，可主動發出 RF 訊號給讀取機

處理。

此外，根據 RFID 操作頻帶，其頻率工作範圍可劃分為四個區段: 低頻(LF:125kHz~135kHz)、高頻 (HF:13.56MHz) 、 超 高 頻 (UHF:100MHz~960 MHz)、微波(1GHz 以上)。表 1 為各頻帶特性，其中，越高頻的標籤則越容易受到環境干擾，不適合用於金屬表面或是干擾較大的環境中。

而在 RFID 中，標準化的制定與推廣主要的單位有美國自動辨識中心(Auto-ID Center)，EPCglobal 和日本 Ubiquitous ID 中心[1][2]。其中 Auto-ID Center 成立於 1999 年，其主要進行產品電子編碼 EPC (Electronic Product Code)的研究與開發。EPC 簡單的說，是 RFID 的一種應用標準。其實際操作是將 EPC 碼存放在標籤中，隨著物品的移動，沿途讀取機發射無線電波感應物品上的標籤，後端系統便展開資料的查詢與存取。如此，不只可以調查物件外觀、重量、材質等資本資料，還可追溯至上游原料生產，下至終端的配送，詳細記錄物件活動路徑與生產過程。

表 1. RFID 各頻帶特性

頻率	優點	缺點
LF	佈署廣泛、金屬干擾低	讀取範圍小(1.5m 內)
HF	溼氣影響低、佈署廣泛	讀取範圍小(1.5m 內)、易受金屬干擾
UHF	佈署廣泛、通信範圍高於其他標準	溼氣影響高、標籤間隔太近會產生頻差(Detuning)
微波 (2.45GHz)	讀取範圍廣	普及率不高、實作複雜、未完全標準

Auto-ID Center 依標籤讀/寫等級的能力區分為 6 等級(如圖 1)，分別為 Class 0~5，其區分準則是根據各種標籤的運算能力以及儲存能力，比如說：Class 0 的 EPC 標籤為唯讀且為被動式標籤，Class 1 的 EPC 標籤則為被動式標籤但能擁有少許的運算能力或是外加少許記憶體。

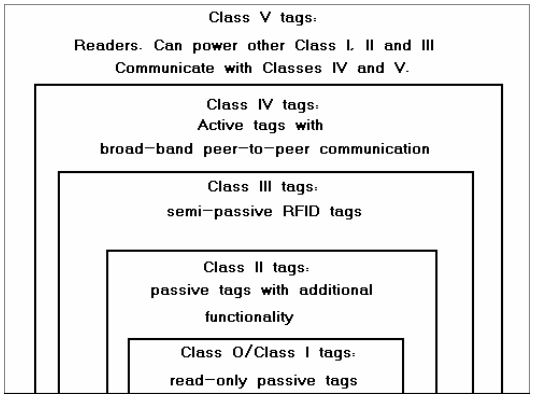

圖 1. EPC Class 0 – 5 及分項功能

EPC 碼的標示對象，包含使用傳統條碼的物品之外，小至硬幣、箱子，大至推車、貨櫃、貨車等，皆可採用 EPC 碼，其編碼有下列特色：號碼容量大;獨一無二的編碼;可擴充性。由目前已公佈的 EPC 標籤規格書得知，標籤容量有 96 位元與 64 位元的區別，未來也會有 256 位元的編碼出現，可視使用者需要選擇標籤容量，亦可隨容量大小調整編碼結構。EPC 依據基本編碼方式，可將 EPC 碼結構分為以下四個區塊：標頭、管理者代碼、物件類別碼、序號。

Auto-ID Center 已提議使用 64 位元、96 位元或是更多位元的 EPC，其中以 96 位元的 EPC 較符合業界需求。且早在 AUTO-ID 中心研發 EPC 時，亦已表明 EPC 的存在不是為了取代現有條碼系統，而是為了輔助各行各業在應用條碼時所遭遇到的困境，基於這樣的理念，EPC 編碼的設計也考慮到現行 EAN & UCC 條碼號碼之普遍性，而將條碼號碼轉換為 EPC 碼列為必要條件之一[2]。

目前大多數 RFID 所遵循的標準有二：一為上述所提為 EPC 所制定之規格;另一為 ISO 國際標準組織所定之標準。其中 RFID 使用頻率分配與無線通信條件(Air interface)如圖 2 所示(ISO/IEC 18000 系列)，ISO 對各個頻段均提供相關之設置規定，而 EPC 則只針對 13.56MHz 與 900MHz 提供標準。另外由於 RFID 的資料傳送透過空中介面，因此要考量較高之安全性。與 RFID 相關之安全性研究的論文也被陸續提出[3-7]。

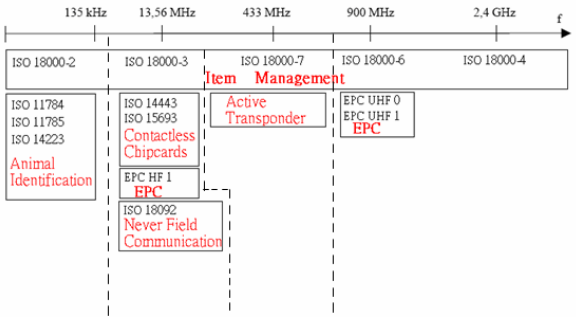

圖 2. RFID 頻段與相關標準

3. 系統介紹與實作說明

透過自動辨識技術管理電腦室的方法很多，目前多採用「條碼」、「磁卡」、「晶片卡」等，不過，這些方式和 RFID 相比，仍有顯著差異。前者在使用時，必需由人工將它置於讀取機前，才能一一進行讀取，由於必須使用人力來進行此項作業，運用範圍也自然變得狹隘。採用 RFID 則不需依序置於讀卡機前且卡片的使用也沒有方向性。此外，除了晶片卡，條碼對環境忍耐度較差，一旦汙損超過一定量就無法使用，而 RFID 則無此考量。

本論文所描述之電腦使用權限控管系統，其目的為電腦教室資源使用之控管，如：單機電腦使用、網際網路連接等。所提之系統架構圖如圖 3 所示，於校園電腦教室中，每部電腦單機均需部署 RFID 讀取機，用於讀取電腦使用者(如：學生、教員等)之 RFID 卡片(如：學生證、教職員證等)。此

外，為了與一般校園中電腦教室之網路部屬建置相同，因此，我們採用 NAT 來分配電腦教室內部電腦主機對外的連線資源。藉此達到與現有既存電腦教室部屬最接近之環境，降低實際運用之成本。此外，NAT/AUTH. Server 除了分配連線資源外，RFID 中 UID 的合法性驗證也同時在此部機器上完成，藉此節省驗證伺服器的額外建置成本，以及方便日後更新 UID 驗證準則，僅需更新此 NAT/AUTH. Server 即可。且由於 RFID 的非接觸性與無方向性特性，在使用上易於操作，其耐環境性強亦降低毀損機率，使得使用成本隨之下降；這個考量是基於學生證使用機會頻繁，受損機率較大的緣故。

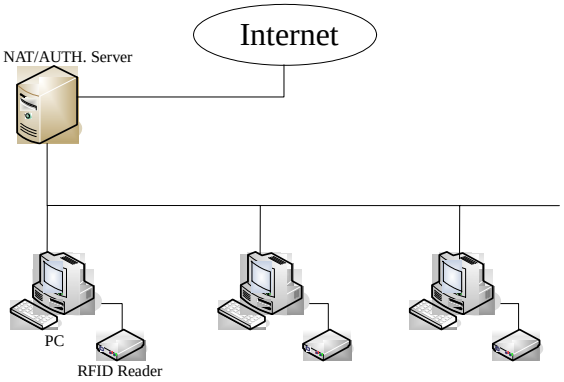

圖 3. 電腦教室之電腦部署架構

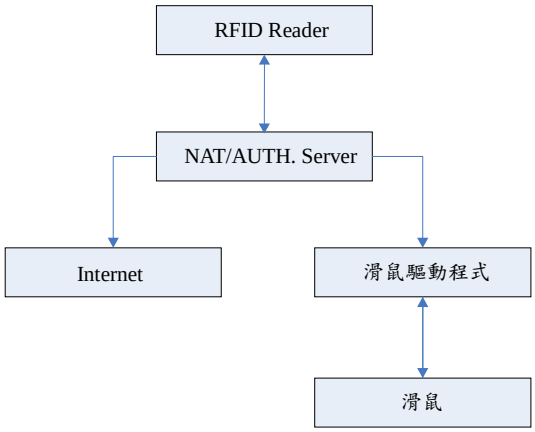

圖 4. 系統整體架構

在電腦教室控管部分，我們可分為兩方面討論，一方面為網際網路存取控管，這是由於電腦教室為開放式空間，任何人均可透過教室中電腦連接網路，因此，紀錄某部電腦於何時為何人所用是必須的。此外，在不連接網際網路時，單機電腦的使用由於現今作業系統多均採用圖形化介面，且使用者操作多使用滑鼠點選之緣故，因此，我們設計對滑鼠之使用權限控管，系統控管流程如圖 4 所示，其中，需開發跨平台程式擔負各程式間溝通與協調之任務，針對輸入設備（滑鼠）和網路連接兩部份進行控管。程式啟動後，將會不停監視 RFID 讀取機的狀態（如圖 5），偵測 RFID 讀取機是否被放上 RFID 卡片或者原有卡片被移除，藉此隨時監控網路或是單機的使用狀況。

當 RFID 讀取機未偵測到 RFID 卡片時，滑鼠會處於被鎖定狀態，不接受任何輸入而無動作，令使用者無法透過滑鼠進行電腦之操作，這個部份可靠開發滑鼠上層過濾式驅動程式來完成；同時，擔任網路連接守門員任務的 NAT/AURH. Server 也將此 PC 之對外連線切斷，使其無法對更上層之網路進行存取。而當使用者將具合法身份之 RFID 卡片放上 RFID 讀取機時，迄 NAT/AURH. Server 確認卡片身份合法後，會分別和滑鼠上層過濾式驅動程式解除滑鼠鎖定以及同步解除網路連線之鎖定，此判定流程如圖 6 所示。

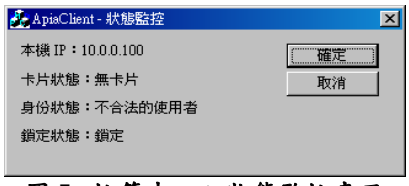

圖 5. 控管中心之狀態監控畫面

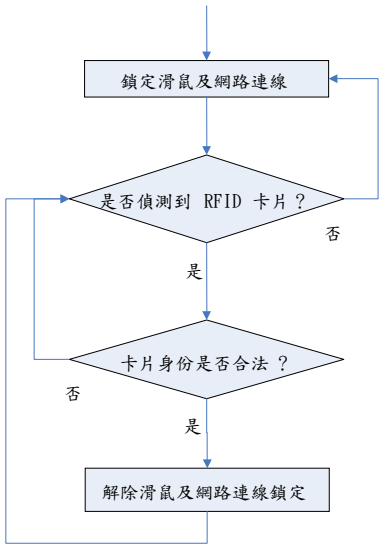

圖 6. 系統控管流程

3.1 控管系統開發平台

現有 RFID 頻段較為大眾廣泛採用的有 135kHz、13.56MHz、433MHz、900MHz 以及 2.4GHz(詳見圖 2)。這些不同的頻段配合不同的 Reader 發射功率，可以發展出不同讀取距離的 RFID 系統。其中，遠距與中距的 RFID 系統可用於航空、倉儲、工廠生產線等，需要讀取範圍較大的場合使用。而本系統所採用的 RFID 為近距系統，這是因為在啟用與認證身份時我們僅需要正確的使用者將卡片置於讀卡機上即可，過遠的讀取距離不適合運用於電腦教室中，這是因為電腦教室中單機電腦間的距離不大，若是採用距離過長的 RFID 讀取系統將會造成許多誤判的困擾。圖 7 為本系統採用之 Reader 與 RFID 卡片之外觀，其 Reader 為 13.56MHz 之 RFID 系統，並可讀取多種 RFID 卡片，如：ISO14443、ISO15693 等。此外，本系統採用之 RFID

卡片則以 ISO14443 為主，為 Mifare 公司所設計開發之 RFID 卡片，台北捷運悠遊卡也採用相同型式的卡片。

圖 7. RFID 讀取器與測試用卡片外觀

本系統所採用的 Mifare RFID 卡片，其內部資訊讀取與存放格式可分為四個部份：UID 區、記憶體存取控管區、數值累進區以及記憶體區。詳細記憶體區塊分佈圖，如圖 8 所示。其中前 9 個位元組為 UID 及其檢查碼，分別存放在記憶體中的第 0 頁、第 1 頁與第 2 頁的第一個位元組。其檢查碼的計算方式依據 ISO 14443 的規定，BCC0 為 CT⊕SN0⊕SN1⊕SN2，BCC1 為 SN3⊕SN4⊕ SN5⊕SN6，而 SN0 為廠商代碼，我們採用的 RFID 卡片中之晶片為 Philips 所生產，因此為 04h。

Byte Number	0	1	2	3	Page
SN	SN0	SN1	SN2	BCC0	0
SN	SN3	SN4	SN5	SN6	1
Internal/Lock	BCC1	I	Lock0	Lock1	2
OTP	OTP0	OTP1	OTP2	OTP3	3
DATA	Data0	Data1	Data2	Data3	4
…	…	…	…	…	…

圖 8. RFID 記憶體分配

緊接著第二頁中的第 2 與第 3 個位元組，則控管後段記憶體頁的寫入權限，倘若這兩個區域所有位元全設定為 1 則此 RFID 卡片中之記憶體將會全設定為唯讀。相對應的鎖定控管區塊如圖 9 所示。其中 Lock0 與 Lock1 下方八個位元位置所相對標示的數字，為所相對應的記憶體頁編號，而 BL 則表示可供鎖定一個區塊頁。此外，這個唯獨的設定是一個不可逆的機制，也就是說，當位元被設定為 1 後將不可被更改回 0，因此，在決定某些記憶體區塊頁是否為唯讀時，需要格外的注意。

MSB				Lock0			LSB
7	6	5	4	OTP	BL 15-10	BL 9-4	BL OTP
MSB				Lock1			LSB
15	14	13	12	11	10	9	8

圖 9. 記憶體存取模式控管區塊

OTP 數值累進區塊為記憶體第 3 頁所控制，這個區域可供使用者累進數值且不可遞減，是一個單向的計數器，可用來累計使用次數等，此區域共有 32 個位元可供累計記錄 2^{32} 次，已經足夠大部分的系統使用。而從第 4 頁之後的區域，就是所謂的記憶體區塊，使用者可依據所需，只要這個記憶體區塊沒有被標示為唯讀，使用者就可以任意的寫入與刪除資訊，作為系統開發應用所需。這個記憶體區塊，在 Mifare 一系列的卡片中可分為 1K,4K 以及 Light，其中 Light 僅提供 4 個位元組的資料區塊空間。而本系統採用的即為上述中之 Mifare Light 系統。

RFID 卡片讀取開發部分，我們配合採用 Mifare 卡片的開發用 SDK 以及 Visual C++程式開發平台，在每部單機安裝此 UID 讀取程式，並將讀取到之 UID 送至 NAT/AUTH. Server 驗證合法性。此合法性可採用列表記錄或是運算 UID 位元間關係來驗證，當驗證通過後，NAT/AUTH. Server 會回應訊息給單機中滑鼠使用權限控管介面並開啟網路連接介面。此 UID 讀取程式為一系統常駐程式，於電腦開機時即載入執行，此外，滑鼠以及網路使用權限於初始預設時均為關閉。

在滑鼠使用權限控管開發平台上，由於電腦教室單機多採用視窗 WINDOWS 作業系統，因此，我們採用 WINDOWS 所提供的 WINDOWS DRIVER MODEL(WDM)環境，開發滑鼠的上層過濾驅動程式。並結合使用 Numega 的 Driver Studio 作為發展驅動程式的整合開發環境(IDE)工具。

此外，在網路控管部分，基於一般電腦教室在建置內部網路時多採用 NAT 的方式，而 NAT 伺服器的作業系統多為 UNIX 或是 LINUX，因此，在網路控管的控制部分我們採用 JAVA 撰寫建立跨平台橋樑，藉此溝通與傳遞電腦教室中單機與網路伺服器間的控管命令，以此控制 NAT 軟體對於網路連接的設定。本系統中的 NAT 伺服器，採用 Iptables 架設，並透過所開發的 JAVA 跨平台控制介面傳送控制指令，藉此達到有效控管每部單機電腦存取網路之權限。本系統實作所採用之各項軟體工具以及作業系統平台詳列如下表 2。

表 2. 軟體工具與開發平台

	控管中心	滑鼠控管	網路控管
作業系統	WINDOWS XP	WINDOWS XP	WINDOWS XP
			LINUX Red hat 9
服務/開發平台	WINDOWS XP	WINDOWS XP HAL/WDM	IPTABLES 1.3.5
開發環境	Mifare SDK/VC++ 6.0	Driver Studio 2.7	JAVA2 SDK 2.14

緊接著，我們將詳細介紹本系統中所採用的 UID 讀取程式、滑鼠鎖定機制以及網路連線鎖定機制，並以此兩機制達到控管單機使用以及網路連接使用的管理目的。

3.2 UID 讀取程式

UID 讀取程式負責讀取 RFID 中所存放之 UID 並發送至 NAT/AUTH. Server 驗證是否為合法 ID，並於接受到 NAT/AUTH. Server 的通知後決定滑鼠

運作模式。Mifare 所提供的 RFID UID 讀取流程如圖 10 所示，首先，單機電腦要先建立與讀卡機之連線，並執行一獨立執行緒不斷讀取在 Reader 可讀取範圍內之 RFID 卡片。若有 RFID 可供讀取時，於取得 UID 後隨即送出 UID 至 NAT/AUTH. Server 驗證是否為合法使用者，若為合法使用者即開啟滑鼠使用權限而 NAT/AUTH. Server 也會同步開啟網路使用權限，若為非法使用者即回到讀取 RFID 程序，重新讀取驗證，藉此循環中止使用權限之開啟。

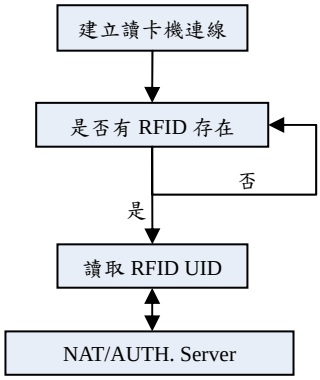

圖 10. RFID UID 讀取流程

RFID 中 UID 讀取以及建立讀卡機連線程式片段如圖 11 所示。讀卡機的連線建立透過函式 ScardEstablishContext 完成，而當有卡片接近讀卡機時，函式 ScardConnect 就會負責建立與 RFID 卡片的連線。而對卡片的讀取動作則透過函式 SCardCLMifareStdRead 達到讀取 RFID 卡片的目的。

```
dwErrorFlage = ScardEstablishContext (SCARD_SCOPE_USER,
  NULL,NULL,&hContext);
…
dwErrorFlage = ScardConnect(hContext, szReaderName,
SCARD_SHARE_SHARED, SCARD_PROTOCAL_T0,
&hSCARDHandle, &dwActiveProtocol);
…
okRead = SCardCLMifareStdRead( hSCARDHandle,
1, buffer, 12, &ulRead);
```

圖 11. 建立讀卡機連線與讀取 RFID 程式片段

3.3 滑鼠鎖定機制

滑鼠鎖定可以藉由過濾式驅動程式（Filter Driver）來達成[8]，將一上層過濾式驅動程式安插於原有之滑鼠驅動程式上層，負責攔截滑鼠的 I/O 請求封包（I/O Request Packet、IRP）。若該部電腦目前處於鎖定狀態，過濾式驅動程式會直接將攔截到之 IRP 丟棄、不予處理，使滑鼠移動訊息無法送入作業系統而使其無法動作；反之，若處於解除鎖定狀態，則此過濾式驅動程式會將 IRP 繼續往下層的滑鼠驅動程式遞送，使滑鼠得以正常工作，其流程如圖 12 所示，此部分要注意的是，為了防止使用者進入安全模式將過濾式驅動程式移除，破解滑鼠鎖定之限制，電腦可以安插還原卡等硬體設備，一旦系統重新開機後，系統設定可以自動回復至原先狀態，如此可免除滑鼠設定遭受使用者破解之風險。而在作業系統驅動程式的開發部分，則採用 Windows Driver Model (WDM) 的開發環境，適用於現今所有的 Windows 視窗作業平台，因此可以很快速方便的部屬建置所需要的控管機制。且透過 WDM 的採用，此滑鼠上層過濾驅動程式僅需透過簡單的 INF 安裝程序即可，以此降低管理人員設定時的技術門檻。

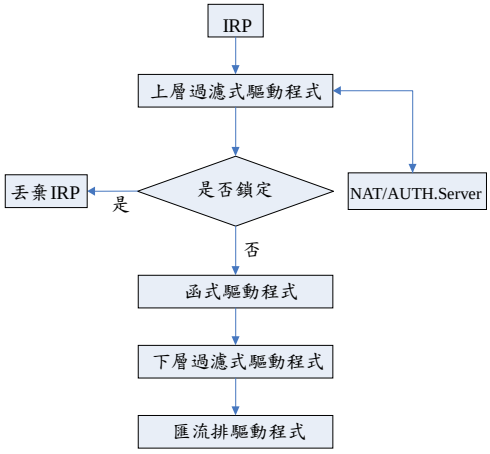

圖 12. 滑鼠鎖定處理流程

滑鼠上層過濾驅動程式片段，如圖 13 所示，此上層過濾驅動程式的部分命令會將滑鼠所有的動作行為之 IRP 傳遞給真正的滑鼠函式驅動程式，因此，我們僅需在此處檢查使用者認證狀態，即可控管滑鼠的所有動作。合法的使用者在通過驗證後，其滑鼠傳遞下來的 IRP 封包，將會被交遞給滑鼠驅動程式，而非法的使用者因未通過驗證，因此傳遞下來的 IRP 封包會被此上層驅動程式攔截並且不往下傳遞，達到鎖定滑鼠動作的目的。

```
…
PIO_STACK_LOCATION irpStack =
IoGetCurrentIrpStackLocation(Irp);
      // Pass the IRP to the target
      IoSkipCurrentIrpStackLocation(Irp);
return IoCallDriver(((PDEVICE_EXTENSION)
DeviceObject->DeviceExtension)->TopOfStack, Irp);
```

圖 13. 滑鼠上層過濾驅動程式片段

3.4 網路連線鎖定

本系統中網路連線鎖定是透過 NAT Server 統一控管，NAT Server 上則使用 Iptables 軟體針對每一 IP 指派特定封包處理規則，分別處理每個 IP 對外連線之鎖定及開放。因此，若要進入鎖定或解除狀態，每部電腦教室中單機上之 UID 讀取程式會透過 JAVA 建立 Socket 與 NAT Server 上之服務程式連線，送出所讀取到之 UID 並於 NAT/AUTH. Server 中驗證合法性，並由此服務程式呼叫 Iptables 修改封包處理規則，其流程如圖 14。

在 Server 與 Client 的連線上，我們採用 JAVA 作為建立連線的開發環境，這是因為一般電腦教室電腦多為 Windows 視窗作業系統，但是 NAT 網路控管主機則多採用 UNIX 或是 LINUX 的作業系統，因此，為了使我們所提之網路連線鎖定控管機制能適用於各種平台，我們透過 JAVA 的跨平台特性來達到無論電腦教室的建置方式為何，我們的控

管機制均可以採用的目的。

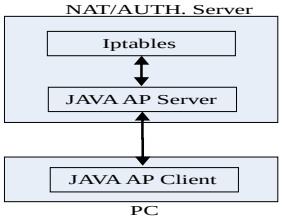

圖 14. 客戶端與 NAT/AUTH Server 架構

下圖 15 為 Client 與 Server 間傳遞之部分主要命令，在增加 Iptables 規則部分，我們可透過圖中所示之增加規則命令，將電腦 IP(以 10.0.0.100 為例)送至 NAT Server，並將其插入 Iptables 規則表即可完成該部電腦對網際網路連線之接通(採用參數 -A)。反之，若要停止某部電腦對網際網路之連接，只需採用類似相同的命令，但給予不同的參數(採用參數 -D)即可將該虛擬 IP 從 Iptables 規則表除去。

增加規則：
iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.100 -j MASQUERADE
刪除規則：
iptables -t nat -D POSTROUTING -o eth0 -s 10.0.0.100 -j MASQUERADE

圖 15. Iptables 命令

圖 16. Iptables 封包處理規則之列表

因此，一旦 IP 被加入 Iptables 規則表後，也就是說，使用者將 RFID 置於讀卡機上且通過認證後，使用者就可以透過 NAT Server 自由對外連線；反之，則無法對外連線，呈現鎖定狀態。圖 16 為 Iptables 目前已建立的封包處理規則，圖中顯示有三個客戶端 IP，分別為 10.0.0.200, 10.0.0.201 以及 10.0.0.100 可以自由對外連線，也就是放置了合法的 RFID 於該部單機電腦之 RFID 讀取機上。

4. 安全性與便利性分析

為了避免惡意的使用者擅自終止單機電腦中的 UID 讀取監控程式，單機中所安裝的 UID 讀取監控程式需採取監控機制，也就是在短暫的固定時間內連續且不間斷的向 NAT/AUTH. Server 送出獨立對應該部機器的認證訊息，一旦 NAT/AUTH. Server 發現認證訊息中斷超過設定的逾時時間，就會馬上中斷該部機器的所有權限，以此防止此類之惡意操作。在此要注意的是，NAT/AUTH. Server 對於所有控管之單機電腦於初始設置時均會將所有權限設定為無效，也就是網路中斷以及滑鼠失效的狀態，以此達到完整嚴密的管控。

此外，若是惡意的使用者將 WINDOWS 作業系統開啟至安全模式則會導致滑鼠上層過濾驅動程式失效，但此時使用者的其他功能也因為啟動於安全模式中，使得操作上產生許多不便，如：顯示介面不完整、影音無法播放等。這些操作上的不便與滑鼠上層過濾驅動程式造成的不便，其限制目的相同，均為不利使用者操作該部電腦。因此，惡意的使用者依舊無法十分順利的使用該部電腦以及網路功能。

5. 結論

目前校內電算中心開放的電腦教室，監管方式多是雇聘工讀生負責管理，管理部分包括：紀錄使用者所使用的電腦編號、進出入時間以及使用者學生證號的確認。然而，電腦教室開放時間較長，人力資源僅用於很簡單的重複性工作，十分不經濟，因此透過有效的系統設備取代是有必要的。

本系統採用RFID作為辨識裝置，來管理電腦教室的使用狀況，能有效控管對網際網路的連接控管以及單機電腦之使用，進而取代現行的人工登記方式，不僅僅減少人力資源浪費，對於電腦教室的管理，如：身分登記、使用電腦紀錄等，均有很大的效益可節省許多時間及資源。

參考文獻

[1] http://www.rfidjournal.com.

[2] http://www.epcglobalinc.org/standards_technology/specifications.html.

[3] A. Juels, “RFID Security and Privacy: A Research Survey,” IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 381-394 February 2006.

[4] A. Juels and J. Brainard, “Soft Blocking：Flexible Blocker Tags on the Cheap,” In Workshop on Privacy in the Electronic Society (WPES), 2004.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Efficient Hash-Chain Based RFID Privacy Protection Scheme,” In Ubiquitous Computing (UBICOMP), September 2004.

[6] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,” In Security in Pervasive Computing, Lecture Notes in Computer Science, Vol. 2802 , pp. 201–212, 2004.

[7] S. Kinoshita, Ohkubo, M., Hoshino, F., Morohashi, G., Shionoiri, O. and Kanai. A, “Privacy Enhanced Active RFID Tag,” In 1st International Workshop on exploiting context histories in smart environments, 2005.

[8] W. Oney, “Programming the Microsoft Windows Driver Model, 2/e”, Microsoft, 2002