建置以 802.1X 及 PEAP 為基礎的校園無線區域網路

周文正
國立清華大學
計算機與通訊中心
wjchou@cc.nthu.edu.tw

賴守全
銘傳大學
電腦與通訊工程學系
sclai@mcu.edu.tw

摘要

無線區域網路 (WLAN) 在新一代校園 e 化與資訊應用整合上扮演重要的角色，因此如何建置一個兼顧使用方便性與資訊安全性的無線區域網路實為一重要課題。在無線網路技術中，IEEE 802.1X 及 PEAP 係以安全為考量之設計，其內建於多數電腦作業系統且可於開機後自動連線之特性在使用上相當方便。因此，本文將探討如何以開放原始碼軟體為基礎，建構一個以 IEEE 802.1X 及 PEAP 為基礎的校園無線區網路，以提供校園師生一個便捷安全的無線網路環境。

關鍵字：無線網路、802.1X、EAP、PEAP、RADIUS。

Abstract

Wireless Local Area Network (WLAN) plays an important role in e-campus and integration of information systems; therefore, how to build a convenient and secure WLAN has become an essential topic. In WLAN technology, the IEEE 802.1X and PEAP mechanisms are designed for information security and are built-in in most modern computer operation systems which may automatically connect to WLAN after booting. Thus, the IEEE 802.1X and PEAP are adequate solutions to the campus WLAN. In this paper, we studied how to build an IEEE 802.1X and PEAP campus WLAN based on the open source software to provide campus members a convenient and secure wireless network environment.

Keywords: WLAN, 802.1X, EAP, PEAP, RADIUS.

1. 前言

無線區域網路(WLAN)在新一代校園 e 化與資訊應用整合上扮演著相當重要的角色，透過 WLAN 可將網際網路的觸角延展至校園的每個角落，讓校園網路實現於過去實體網路不易佈建之區域，因此如何建構一個適合學校師生的無線區域網路環境，已經成為校園 e 化的的重要課題。

校園無線區域網路的佈建首重使用的方便性與資訊傳輸的安全性。就使用的方便性來說，如果所佈建的無線網路並非透過電腦作業系統內建的程式即可連線，而是必須另行安裝特定的軟體方能連線，這對初次進入此一環境卻尚未安裝特定連線軟體的無線網路用戶來說，會是個極大的使用障礙。因為該使用者會需要連上網路來下載安裝該軟體，但卻因為沒有安裝該軟體而無法連上網路，如此一來就無法順利使用無線網路了，這也是有些無線區域網路會採用不須認證的開放架構或以網頁瀏覽器(web-based)進行網路連線認證的主要因素。

無線網路的傳輸訊號是散播於開放的空域之中，透過這樣的媒介來傳輸資訊，若不經過加密處理，無疑是將帳號密碼等機敏性資料變成是公開的祕密，這對所傳輸資訊的安全是相當有疑慮的。因此無線網路的建置應將網路傳輸的安全性納入考量，以避免用戶在不知情的情況下，因使用無線網路而讓其傳輸資訊遭竊。

在 2003 年，清華大學以 IEEE 802.1X 為基礎，採用 EAP-MD5 協定，配合無線網路帳號與密碼的認證，建置了校園無線區域網路[1]，期能提供用戶較安全的無線網路環境。然而，Windows XP 於升級成 SP1 後因安全性考量，在無線網路認證上取消了 EAP-MD5 選項，造成了校園師生使用上的不便與困擾，因此重新尋求同時兼顧連線方便性與網路安全性的解決方案，成為我們調整建置校園無線區域網路的主要努力方向。

以網路安全的認證機制來考量，不須用戶認證的開放網路架構，可能成為網路犯罪的溫床，因此不做考慮；若加上無線網卡之卡號(MAC address)作為過濾機制，則有管理不易、卡號可以造假以及不易開放訪客使用的問題；若採用 web-based 的認證方式，則有資訊傳輸過程並未加密的疑慮；至於其他非硬體管控的策略則需要用戶端軟體的配合方能順利連線。

從過往的經驗，我們得知要用戶另行安裝軟體方能進行連線會造成極大的使用困擾，因此我們將選擇多數用戶電腦作業系統所內建支援的協定作為我們的認證機制。考慮目前多數用戶可攜式電腦使用的作業系統，如：Windows 2000 SP4、Windows XP SP2、Window Mobile 2003 及 Mac OS X 10.4，

我們發現這些作業系統都內建有對 IEEE 802.1X [3] 的支援，且都支援 EAP-TLS [4]及 PEAP [7] (MS-CHAPv2 [9])的認證方式，即便是 Linux 用戶亦有開放原始碼的支援，加上現有校園無線網路之 AP (Access Point)及認證主機軟體 FreeRADIUS [5] 均支援 EAP-TLS 及 PEAP。然而 EAP-TLS 在實務上有憑證管理核發的困難，因此 PEAP 成為我們此次更新調整之最佳選擇。

配合 PEAP 的認證機制，我們選擇 FreeRADIUS 作為 WLAN 的認證主機，除了開放原始碼軟體之經濟考量外，其具有支援 PAP/CHAP、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP 與 EAP-SIM 等多功能認證方式，相當符合整合校內各單位帳號，達成單一帳號於校內自由無線上網之需求，亦能達成校際無線網路帳號漫遊認證之目的。

在確認所使用的無線網路認證技術、用戶端的設定、無線網路之 AP 設備、及所選用的認證主機軟體後，結合先前開發完成的無線網路管理系統，我們成功的建置了新一代以 IEEE 802.1X 及 PEAP 為認證機制的校園無線區域網路，其架構如圖 1 所示，為校園提供了一個更安全與更方便的無線網路環境。

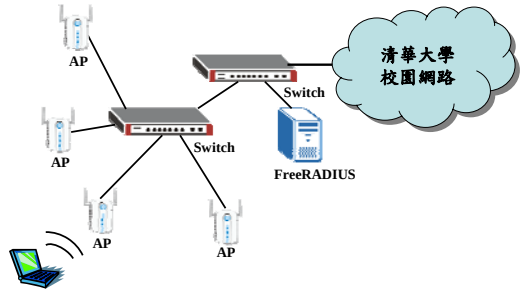

圖 1 以 802.1X 及 PEAP 認證的校園無線網路架構

在下一節中，我們將詳述 IEEE 802.1X 及 PEAP 的運作原理。在第 3 節中，我們將說明系統實際建置的步驟。這次建置更新案所獲得的心得與檢討將在第 4 節中說明，最後則為本文的結論。

2. IEEE 802.1X 及 PEAP 的運作原理

在本節中我們將簡述 IEEE 802.1X 及 PEAP 的簡單運作原理，以作為後續系統實際建置與設定時的基礎。

IEEE 802.1X 是以連接埠為基礎的網路存取控制協定 (Port Based Network Access Control Protocol)，透過現有 EAP (Extensible Authentication Protocol) 封包格式，結合認證主機 (可採用 RADIUS)，提供多種不同之身分驗證機制的包裝方法。因其支援動態 WEP (Wired Equivalent Privacy) 與相互認證(Mutual Authentication)機制，因此 IEEE 802.1X 與 RADIUS 的結合應用，可以提供比以 SSID (Service Set Identifier)、靜態 WEP 或 MAC 卡號過濾等方法更安全的用戶認證機制。

在 IEEE 802.1X 的環境中，無線網路之 AP 會設定為僅允許經 802.1X 認證通過之連線，因此所有未經認證通過的用戶將無法透過 AP 連接網路。此外，認證主機僅接受來自信任 AP 的連線。

在說明 IEEE 802.1X 與 PEAP 的整合運作前，先簡述 PEAP 的運作方式。PEAP 包含兩階段的工作內容，第一階段建立一個 TLS (Transport Layer Security)安全通道，並允許用戶端用主機數位憑證來確認主機端，第二階段則在先前建立的 TLS 安全通道內進行 EAP 協商，並向主機端確認用戶端。這個設計讓 PEAP 在 TLS 安全通道的保護下，可使用各種用戶端的確認方式，包括原先容易遭到離線字典式攻擊的 MS-CHAPv2 認證方式。

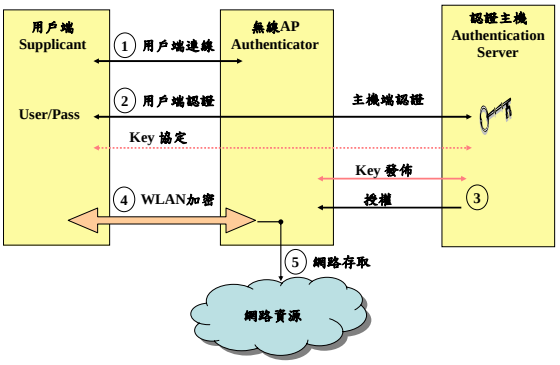

圖 2 WLAN 之 802.1X 及 PEAP 運作原理

當用戶嘗試連線至我們以 IEEE 802.1X 及 PEAP 為認證機制所建立之 WLAN 時，其驗證過程(如圖 2 所示)如下[6]：

1. 當用戶端電腦進入 AP 涵蓋範圍時，它會以 SSID 識別 WLAN 並嘗試連線。
2. 當用 AP 收到用戶端連線嘗試時，AP 會設定限定通道，讓用戶端能與認證主機進行通訊。此時用戶端會嘗試使用 PEAP 與認證主機進行確認。透過 PEAP 所建立 TLS 安全通道，用戶端可以確認主機端憑證，並利用 MS-CHAPv2 與主機端進行認證，並利用 TLS 建立階段所產生的金鑰衍生其他金鑰。
3. 認證主機核可用戶的認證與授權後，會將用戶端主要金鑰傳送給 AP。之後，在動態 WEP 的模式下，用戶端與 AP 會利用這個共用金鑰來加密彼此間傳輸的資料；而認證主機則扮演要求用戶定期重新認證的角色，以達到定期更換金鑰的目的。
4. 認證主機通知 AP 開啟用戶端與 AP LAN 端的連

線，讓用戶端能夠與 LAN 上的系統自由通訊。此時在用戶端及 AP 間傳送的資料都會經過加密。

5. 用戶端可利用 LAN 上 DHCP 主機取得 IP 位址及其他網路連線資訊(如：netmask、default gateway、DNS 等)，之後即可順利進行正常網路通訊。

3. 系統實作

為方便使用者能夠以同時兼顧安全與簡便的方式使用校園無線區域網路，我們採用了目前校園多數用戶作業系統所支援的 IEEE 802.1X 及 PEAP 作為我們的認證協定。考慮校園使用者可能自外部單位漫遊認證，我們選擇目前開放原始碼軟體中，支援多種認證協定的 FreeRADIUS 作為認證主機軟體，配合設定無線 AP 為使用 802.1X 及 PEAP 認證，即可建構一個支援 802.1X 及 PEAP 認證的校園無線區域網路環境。

此環境可讓使用者於電腦開機後，就如同使用固接區域網路(如：Fast Ethernet)一般，自動連線校園無線區域網路，並得以啟動各種開機連網程序(如：Windows Update，防毒軟體病毒碼自動更新，自動網路校時等)，無須再透過其他方式啟用無線區域網路後，如：手動開啟瀏覽器後登入認證畫面，方可進行網路連線。這個設計可以讓校園無線區域網路成功整合融入成為校園網路的一部份，讓使用者無須留意區隔所使用的網路是固接網路或還是無線網路，都能安全便捷的連上網際網路。

以下各小節將詳細說明認證主機建置設定、無線 AP 設定、及用戶作業系統設定方法。

3.1 主機端建置及設定

我們採用 FreeRADIUS v1.0.2 作為我們的 RADIUS server，系統建構在 Linux 作業系統上，硬體則是採用 PC 伺服器架構，成本相當低廉。在軟體的建置上，除安裝 FreeRADIUS 及 OpenSSL 外，主要步驟在於憑證的安裝與系統檔案的設定。

PEAP 只使用主機端的憑證(server certificates)來認證主機端，因此只需產生主機端的憑證即可。主機端的憑證係由 CA (certification authority)所核發，若該 CA 是用戶端信任的憑證核發者，則主機憑證可被自動信任而完成連線，在使用上可說相當方便。若無法從既有信任 CA 得到主機憑證，則可利用 OpenSSL 產生 self-signed certificates。利用 FreeRADIUS 內含之 CA.certs script 可快速產生 RADIUS 主機所需要之 root.pem (CA 憑證)與 cert-srv.pem (主機憑證)，及用戶端確認主機憑證所需之 root.der(DER 格式)。表 1 為清華大學修改 CA.certs 內容的範例。

表 1 FreeRADIUS 之 CA.certs 修改範例

```
COUNTRY="TW"
PROVINCE="TAIWAN"
CITY="Hsinchu"
ORGANIZATION="NTHU"
ORG_UNIT='CCC'
PASSWORD="pw_server"
#-- COMMON_NAME_CLIENT 之內容為 WinXP 在勾選受信任的目錄憑證授權單位時之識別
COMMON_NAME_CLIENT="NTHU WLAN certificate"
EMAIL_CLIENT="wlan@cc.nthu.edu.tw"
```

完成憑證之產生後，即可進行系統檔案之設定，包含 radiusd.conf、eap.conf、clients.conf 及 users 等。之前產生之 root.pem 與 cert-srv.pem 必須存放於 eap.conf 所指定之位置。配合 PEAP 此採用，將 default_eap_type 設定為 peap，並將 peap 之 default_eap_type 設定為 MS-CAHPv2。另外，為讓 FreeRADIUS 於開機啟動時，能驗證主機憑證簽署之密碼，須在 eap.conf 中設定正確之密碼(例如：pw_server)。表 2 為 eap.conf 檔之修改範例。此外，eap.conf 中之 dh_file (Diffie-Hellman parameters file)及 random_file 係用於 TLS 之運作，其設定範例分別如表 3 及表 4 所示。

表 2 FreeRADIUS 之 eap.conf 設定範例

```
#-- eap.conf
eap {
default_eap_type = peap
    tls {
    private_key_password = pw_server
    private_key_file =
    ${raddbdir}/1x/cert-srv.pem
    certificate_file = ${raddbdir}/1x/cert-srv.pem
    CA_file = ${raddbdir}/1x/root.pem
    dh_file = ${raddbdir}/1x/dh
    random_file = ${raddbdir}/1x/random
    fragment_size = 1024
    include_length = yes
    }
    peap {
    default_eap_type = MS-CHAPv2
    }
}
```

表 3 FreeRADIUS 之 dh 檔產生範例

```
openssl dhparam –check –text -5 512 –out dh
或
date > dh
```

表 4 FreeRADIUS 之 random 檔產生範例

```
dd if=/dev/urandom of=random count=2
或
date > random
```

之後將每個 AP 與認證主機之共用密碼及 IP 位址登錄於 clients.conf 檔中，其範例如表 5 所示。

表 5 FreeRADIUS 之 clients.conf 設定範例

```
# clients.conf
client 192.168.0.100      {
        secret          = NASpasswdAuth
        shortname       = nthu-test
}
```

最後進行 users 檔之設定，讓用戶得以通過認證後使用無線區域網路。當認證主機接受用戶端進行存取請求時，系統首先會以 users 檔案之內容進行使用者密碼比對，以表 6 之 users 檔為範例，其使用者 w92001 之對應密碼為 x92001。若身份驗證成功，則會以 Exec-Program-Wait 指定外部程式(此例為 authCheck)進行認證階段之授權處理。授權處理決定用戶之各種使用權限，包括當可上網之日期時間、可上網地點場所、可上網時限、能否同一帳號同時上網或其同時上網個數等。

表 6 FreeRADIUS 之 users 檔設定範例

```
# users 檔案範例（認證與授權）
w92001      User-Password=="x92001"
            Exec-Program-Wait="/aaa/authCheck "
```

當用戶通過認證與授權之後，用戶可經由 DHCP 主機取得 IP 位址及其他網路連線資訊(如：DNS、netmask、default gateway 等)，待個人電腦自動設定完成後即可順利連接校園網路。

在帳務管理方面，假如 AP 設定有帳務服務，當用戶成功連線時，AP 會對 FreeRADIUS (UDP 1813 埠)提出帳務要求 Accounting-Request (start)，此時 FreeRADIUS 會參考如表 7 之 acct_users 檔，以 Exec-Program 指定外部程式(此例為 acctStart)，產生帳務起始紀錄。當用戶要求離線或 AP 發生 Session-Timeout、Idle-Timeout 等情況時，AP 會送出 Accounting-Request (stop)，此時 FreeRADIUS 會以 Exec-Program 指定外部程式(此例為 acctStop)更新帳務紀錄，產生用戶計時或計量之結算記錄。

表 7 FreeRADIUS 之 acct_users 檔案範例

```
# acct_users 檔案範例（帳務收集）
DEFAULT Acct-Status-Type == Start
            Exec-Program = "/aaa/acctStart"
DEFAULT Acct-Status-Type == Stop
            Exec-Program = "/aaa/acctStop "
```

3.2 無線 AP 設定

無線區網路環境所使用之無線 AP 只要有支援 802.1X、PEAP 與動態 WEP 功能即可符合本文之建置需求。以 ZyXel 提供本校之 ZyAIR B-1000v2 無線 AP 為例，在 802.1X 頁面設定 Wireless Port Control=Authentication Required、Authentication Databases=RADIUS Only、Dynamic WEP Key Exchange=128-bit WEP，另在 RADIUS 頁面設定 Authentication Server 及 Accounting Server 之 IP Address、Port Number 及 Shared Secret 即可。其範例如圖 3 及圖 4 所示，整體來說，無線 AP 之設定並不複雜。

圖 3 AP 之 802.1X 設定頁面

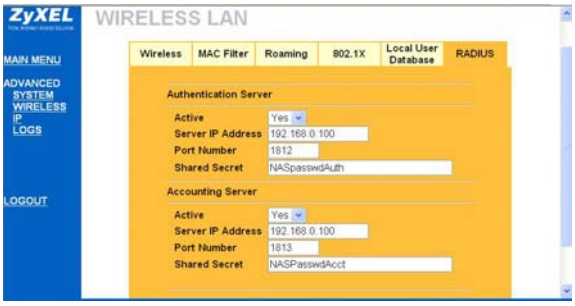

圖 4 AP 之 RADIUS 設定頁面

3.3 用戶端設定

在用戶端無線網路硬體方面，其無線網路卡必須支援 802.1X 及動態 WEP 或 WPA 的功能。目前市面上販售之無線網路卡及符合 Centrino 規範之筆記型電腦多數均符合此一要求。另外，在軟體方面，目前在 Windows 2000 SP4、Windows XP SP2 及 Windows 2003 均內建支援 802.1X 及 PEAP。除此之外，清華大學自行研發之 WIRE1x [8]，也免費提供支援其他平台之 PEAP 軟體。

在連線設定方面，以 Windows XP SP2 為例，使用者初次使用時，因清華大學之主機憑證並非 Windows XP SP2 預置之信任 CA 所核發，因此需下載並安裝校園無線區域網路數位憑證(root.der)，若憑證為信任 CA 所核發則不須事先安裝。之後即可設定無線網路連線之內容，在無線網路頁面，選擇

使用 Windows 來設定無線網路，並新增慣用網路，輸入 nthu 於 SSID 欄位，保持網路驗證為開放系統、資料加密為 WEP (如圖 5)，另外於驗證頁面啟用 802.1X 驗證，並設定 EAP 型態為 PEAP，取消當電腦資訊可用時驗證為電腦(如圖 6)，之後於 EAP 內容部份勾選連線時確認伺服器憑證及受信任的目錄憑證授權單位為先前所安裝之憑證(NTHU)，並選擇驗證方法為 EAP-MSCHAP v2，並設定取消自動使用我的 Windows 登入名稱及密碼(假設不同於無線網路用之帳號及密碼)。完成設定後，即可自動選擇 SSID 為 nthu 之無線網路連上校園無線區域網路。詳細說明範例可參考清華大學校園無線區域網路用戶使用步驟[2]。

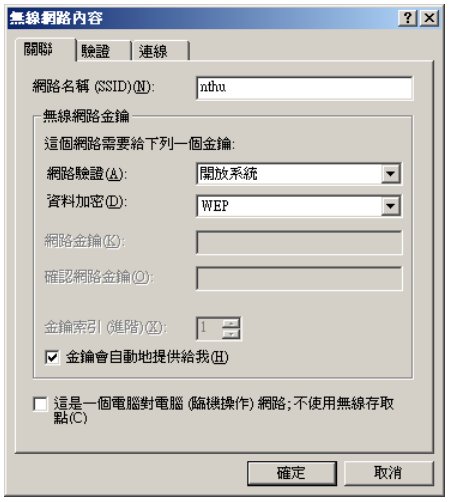

圖 5 新增慣用網路之關聯頁面

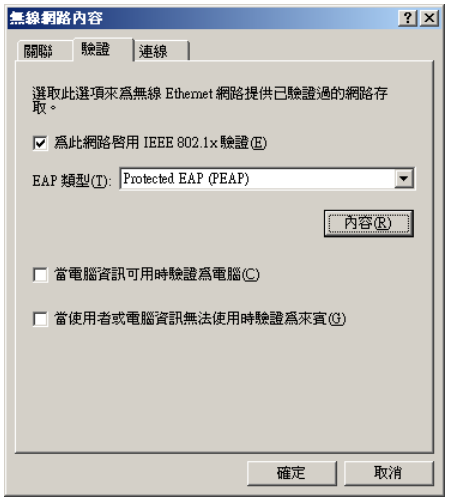

圖 6 設定新增慣用網路之驗證頁面

若用戶想使用 Windows Mobile 2003 之 Pocket PC 連接無線網路，可利用 Windows XP 之 IE 工具將憑證(root.pem)匯出為 CER 格式檔案(IE 工具→網際網路選項→內容憑證→信任的根憑證授權→選擇憑證→匯出→匯出檔案格式為 DER 編碼二進位元 X.509 (CER)→存檔為 root.cer)，再經由同步處理或記憶卡將憑證安裝於 Pocket PC 上，稍作設定之後即可連接無線網路。

4. 心得與檢討

從測試與建置此一採用 IEEE 802.1X 及 PEAP 為認證機制的校園無線區域網路的過程，到建置完成後使用者所反應的各種意見，我們獲得許許多多的寶貴經驗，茲將幾個我們初步獲得心得與檢討條列如下：

1. 若用戶端電腦曾經以 802.1X PEAP (MS-CHAPv2) 帳號密碼認證成功，則當電腦下一次在可用 AP 之涵蓋範圍內開機時，電腦會自動認證後連接上校園網路。相較於 web-based 的認證方式，需要於每次開機後，手動啟動瀏覽器以帳號密碼登入，方能連上校園網路，使用上可說方便許多。
2. 在實際使用上，在 Windows XP SP2 用戶端之 PEAP 內容設定，若取消連線時確認網路伺服器憑證，即可在不需要事先下載安裝校園無線區域網路數位憑證的情況下，透過帳號密碼認證後，連線上網，但這種做法在認證過程中會有 AP 假冒之風險。
3. 目前支援 IEEE 802.11i 之產品尚未普及化，但業界多數產品已經逐漸支援比動態 WEP 更安全之 WPA 協定，待校園內所使用之 AP 能全面更新韌體支援 WPA，且用戶端亦能方便升級支援 WPA 時，即可輕鬆全面建置以 WPA 為基礎之 WLAN，以提供更安全的無線上網環境。而在這樣的更新過程中，主機端的 FreeRADIUS 則無須更改。
4. 考量同時兼顧用戶連線之方便性與安全性，可建置同時支援多種認證機制(如：web-based 及 802.1X)的無線網路環境，以讓使用者能有更多的選擇。目前已有支援多個 SSID 之無線 AP 產品，且每個 SSID 均可設定一種用戶認證方式，用戶可透過 SSID 來選擇所要使用的認證方式以連接無線網路。若建構校園無線網路時選用具備這種功能之無線 AP，則可建置一支援多種認證機制之校園無線網路環境，可照顧到更多的使用者。
5. 採用 802.1X 之認證方式，係先通過認證後再取得 IP 上網，存取控制點在無線 AP；而 web-based 的認證方式，係先取得 IP 後再上網認證，存取控制端在認證閘道器，這在資通安全上會有不同的影響。在未能通過認證的情況下，web-based 的用戶仍可以取得 IP，因此可連線閘道器內的其他電腦。若該電腦係已經感染網路病毒，則在未通過認證的情況下，亦可能感染閘道器內之其他電腦。若採用 802.1X 的認證方式，則可透過關閉帳號的方式，將網路病毒的散播抑制於 AP 端，避免其他無線上網電腦被感染的可能。

5. 結論

本文探討如何以免費開放原始碼為基礎，建置一個同時兼顧方便性與安全性的校園無線區域網路環境。經過分析評估後，我們採用目前多數用戶之電腦系統及無線 AP 設備普遍支援的 802.1X PEAP (MS-CHAPv2)作為認證方式，並採用支援多種認證方式的 FreeRADIUS，搭配 Linux 系統，作為認證主機，配合先前已經建置完成的校園無線網路管理系統，建置了新一代更安全方便之校園無線區域網路系統。目前這個系統已實際應用於清華大學公共區無線區域網路上，除了有效改善早期採用 EAP-MD5 所造成之用戶端不便外，對資訊之安全性及用戶認證、授權、帳務計量之提升改善亦有具體成效。

目前使用 PEAP 建置安全校園無線網路之相關技術已趨成熟，希望透過本文能推廣相關技術，讓無線區域網路在大幅佈建之餘，能提供使用者更便利與更安全之無線網路環境。未來待 WPA 環境成熟時，我們計畫將目前動態 WEP 環境全面升級成 WPA 技術，期能提供更安全方便之無線區域網路環境。

參考文獻

[1] 周文正, 王晉良, “校園無線區域網路 AAA 系統設計與實作,” TANET 2003, pp.173-178.

[2] 校園無線區域網路用戶使用步驟, http://www.wlan.nthu.edu.tw/~wlan/NM/wlanUserStep.html#indoor.

[3] IEEE Standard 802.1X, “IEEE Standard for Local and Metropolitan area networks – Port-Based Network Access Control,” October 2001.

[4] J. Dunn and C. Martin, “PPP EAP TLS Authentication Protocol,” RFC 2716, February 2000.

[5] FreeRADUIS, http://www.FreeRADIUS.org.

[6] Microsoft, “Securing Wireless LANs with PEAP and Passwords,” http://www.microsoft.com/technet/security/topics/cryptographyetc/peap_2.mspx.

[7] A. Palekar et al., “Protected EAP Protocol (PEAP) Version 2,” draft-josefsson-pppext-eap-tls-eap-10.txt, Internet draft (working in progress), October 2004.

[8] WIRE1x, http://wire.cs.nthu.edu.tw/wire1x/.

[9] G. Zorn, “Microsoft PPP CHAP Extensions, Version 2,” RFC 2759, January 2000.