校園無線漫遊認證機制安全與 802.1x PEAP/TTLS 環境建置

唐可忠　黃偉航
國家高速網路與計算中心
kevin@nchc.org.tw ; a00whl00@nchc.org.tw

蔡志宏
國立台灣大學電信工程學研究所
ztsai@cc.ee.ntu.edu.tw

摘要

802.1x EAP-PEAP/TTLS 是兩種頗被看好的無線認證機制，同時兼具線了方便使用與安全特性。EAP 屬於網路第二層的協定，因此也衍生了 IP 無法正確記錄的問題，PEAP/TTLS 的身份隱匿機制更讓管理者難以去追查使用者身份，加上跨校無線漫遊機制的建置，讓相關問題也更為複雜。本文介紹跨校無線漫遊環境常見的無線網路認證環境以及身份認證機制的比較，並且以 PEAP/TTLS 協定為主，介紹可能發生的問題以及相關的處置方式，可作為各界在建置無線網路漫遊認證環境時的參考。

關鍵詞：無線漫遊、802.1x、PEAP/TTLS、憑證

Abstract

EAP-PEAP and EAP-TTLS are the most popular TLS tunneled-based EAP authentication protocols in the 802.1x environment. Normally, PEAP/TTLS are secure and convenient. But there is a big problem that the anonymous login capability supported by PEAP/TTLS may cause some accounting and log problem. The anonymous login capability may be a benefit of users but it's an obstacle to administrators, especially in the cross-campuses WLAN roaming environment. This paper discusses theses problems and some practical solutions that may useful for WLAN administrators.

Keywords：WLAN, 802.1x, PEAP/TTLS, CA

1. 前言

許多學校及單位透過跨校無線漫遊機制*[1]的整合，讓使用者能夠享受原帳號進行無線漫遊的便利，其運作示意圖如圖 1 所示。但由於網路資訊科技的發達，各種駭客工具不斷的出現，進行網路入侵或破解也不再是專門技術人員的專利，雖然無線網路及漫遊機制帶來了更多便利，但也讓使用者及管理者面臨更多的挑戰。

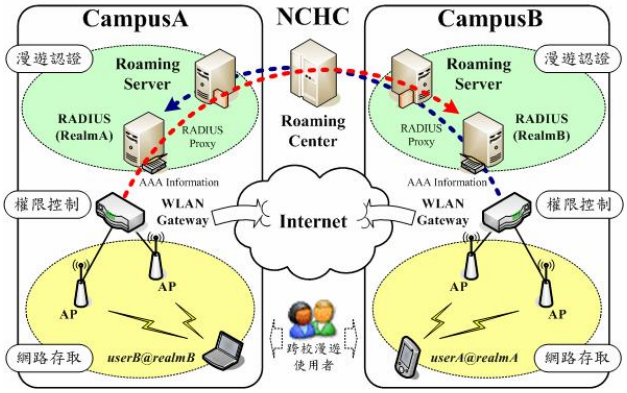

圖 1、跨校無線漫遊認證機制示意圖

2. 常見的校園無線認證架構

目前在各個校園中最常見的無線網路認證方式為 Web-based 網頁認證，少部分單位則採用 802.1x[8] EAP-MD5、EAP-PEAP(Protected EAP)[4]及 TTLS (Tunneled TLS Authentication Protocol)[10]認證方式。大部分單位採用網頁認證的原因主要考量是方便使用，但這卻犧牲了無線網路的安全防護，讓大部分的使用者均暴露在危險的網路環境之中。若要保障無線網路使用者的安全，目前最好的機制莫過於 802.1x，但是安全與方便通常是無法兼顧的。本節將說明無線網路帳號密碼的驗證方式以及校園無線認證架構機制的特性比較。

2.1 密碼驗證方式

在更進一步說明各種認證機制前，我們必須先瞭解使用者帳號與密碼驗證的方式，校園中常用的身份驗證方式基本上可分為兩種：PAP(Password Authentication Protocol)以及 CHAP(Challenge Handshake Authentication Protocol)。

PAP 認證顧名思義就是使用者以密碼來作為主要的身份驗證依據，其流程為認證者(Authenticator)將密碼明文送給認證伺服器(Authentication Server)，認證伺服器再利用使用者所傳來的密碼進行密碼比對。由於伺服器所收到的是密碼原文，因此可以支援多種後端使用者帳號系統，無論使用者

* 本論文由電信國家型科技計畫-「校園無線漫遊網路環境建置與安全升級計畫」所發表，國科會計畫編號：NSC 95-2219-E-492-001，執行期間 95 年 2 月至 95 年 12 月底。

密碼是經過特殊編碼的UNIX shadow/password、或是能夠支援明碼密碼的LDAP、SQL伺服器等。但是 PAP 的缺點是使用者的個人密碼必須透過網路傳送，因此會有被竊聽的風險。

CHAP 主要概念是以 Challenge/Response 的方式來驗證使用者的身份資料，其主要精神在於使用者密碼並不直接在網路上傳送。而是認證者與認證伺服器之間以一問一答的方式進行認證，在這一問一答間彼此都不會直接透露使用者的機密資料，使用者密碼會以單向雜湊函數(One-Way Hash Function)計算出摘要值送給認證伺服器，認證伺服器則同樣以資料庫儲存的密碼原文以相同的演素法計算出摘要，並且比對認證者送來的數值，因此密碼不會有被截聽的危險。CHAP 的缺點是帳號資料庫中的個人密碼必須以明碼儲存才能使用 Challenge-based 認證機制。

表 1、PAP 與 CHAP 比較表

	PAP	CHAP
傳輸安全	不安全	較安全
密碼存放	支援明碼/密碼	僅支援明碼

比較嚴謹的身份驗證機制一般來說都會採用 CHAP 的驗證方式，PAP 驗證由於不安全因此較新的認證標準都不採用，但很弔詭的是偏偏大家都愛用 PAP。探究其原因主要是起因於歷史的包袱，因為早期大部分學校多採用UN*X 系統來建構學生及教職員帳號，因此帳號系統中的使用者密碼會經過不可逆的編碼演算法加密儲存，因此能夠支援此類帳號系統的也只有PAP了。

2.2 網路驗證機制

我們把常用的校園無線網路驗證機制分為網頁認證與 802.1x 兩種，其中 802.1x 在校園中比較常被使用的認證機制為 EAP-MD5、PEAP兩種，但由於 EAP-MD5 具有相當多的弱點，因此在國際間比較被看好的認證機制為PEAP, TTLS。此外 Cisco 提出的 EAP-FAST(Flexible Authentication via Secured Tunnel)[9]也是類似的運作架構，但由於 FAST 需要有具備 PAC(Protected Authentication Credential)的認證伺服器支援，因此在這裡暫不多做介紹。以下針對網頁認證(透過 HTTPS)、PEAP 與 TTLS進行各方面的比較。

表 2、網頁認證 /PEAP/TTLS 比較表

	網頁認證	PEAP	TTLS
認證軟體	瀏覽器	專用軟體	專用軟體
認證協定	PAP	MS-CHAPv2/ EAP-TLS	PAP/CHAP/MS-CHAP v1v2/EAP
漫遊認證	支援	支援	支援
帳號隱藏	無	有	有
傳輸安全	無	動態 WEP	動態 WEP

網頁認證的強處在於支援多種後端帳號系統，使用者只需要網頁瀏覽器便可進行身份認證，但是無法保證使用者認證通過後的資料傳輸安全(但可額外透過 VPN 強化安全性)，且由於其認證協定為 PAP-based，因此密碼將會在網路上被傳送。PEAP 與 TTLS 均屬於 TLS 加密通道式的協定，會先以 TLS 建立加密通道後，再以一般常用的身份驗證機制進行驗證，如 MS-CHAP、PAP 等，因此可以保證使用者個人資料的安全。PEAP 與 TTLS 的差異之處主要在於傳統帳號系統的支援能力，使用 PEAP 時使用者密碼必須以明碼儲存，而 TTLS 則沒有限制。以網路上的傳輸安全來角度說，帳號系統若能夠支援 CHAP 認證機制是較安全的選擇。

下圖 2表現了這三種驗證機制中，使用者密碼明碼可能會被側錄的地方。

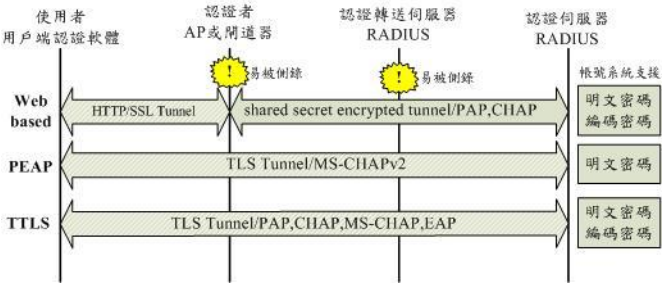

圖 2、網頁認證/PEAP/TTLS 的密碼傳輸

在圖 2中可以觀察到，採用網頁認證時，使用者的個人資料可能在閘道器或認證轉送時被惡意側錄；採用 802.1x EAP-PEAP 或 TTLS 則沒有被側錄的風險，但 PEAP 或 TTLS 能否使用的關鍵則在於後端使用者帳號系統的密碼儲存型態。因此若以安全的角度來評估，802.1x 所整合的動態 WEP 資料加密機制是一般網頁認證無法望其項背的。網頁認證固然方便，但若真的發生了資安事件，雖然說亡羊補牢為時未晚，但發生當時所遭受的損失，也許是無法彌補的。因此未來在建置下一階段的校園無線網路時，應該以802.11i[7]架構為目標，802.11i 中的認證機制採用 802.1x，因此進行網路規劃時應考慮支援802.11i 架構或是802.1x 機制的設備。

PEAP 與 TTLS 有相當大的機會成為下一階段無線網路認證機制的主流，因此接下來我們將針對 PEAP 與 TTLS 進一步分析其安全架構。

3.PEAP與 TTLS 的安全架構

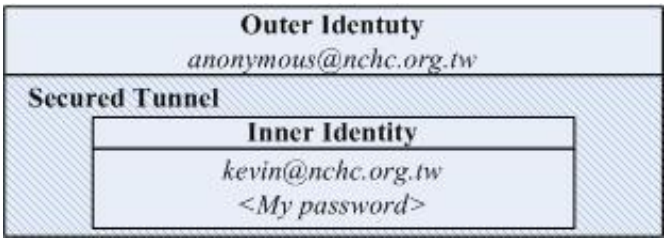

圖 3、Outer 與 Inner Identity

如圖 3所示，PEAP與 TTLS 都是先建立秘密通道，再進行身份驗證的協定(之前提到的FAST 亦是如此)，因此使用者的資料會有兩層：Outer Identity 與 Inner Identity。

當使用者發出 PEAP 或 TTLS 認證請求時，Outer Identity 會明確的寫在認證封包上，該封包途經的設備，例如扮演認證者角色的 AP 或閘道設備以及途經的RADIUS伺服器等，都能夠清楚看到這個資訊。認證封包內所帶的 Inner Identity 則是已經被加密的使用者個人資料，例如帳號、密碼明文或是密碼摘要值，只有建立加密通道的雙方才能夠辨識 Inner Identity，因此途中不會有被攔截的危險。

3.1 Outer Identity與漫遊認證

Inner Identity 包含了使用者帳號與密碼資訊，是使用者身份驗證的最後依據，而 Outer Identity 有兩種功用：身份隱藏或是認證伺服器的導引用途。

PEAP/TTLS 草案標準中並沒有要求對 Outer Identity 進行驗證，因此使用者只要在 Outer Identity 隨便填上一個假名，這時使用者的身份就被隱藏起來了。另外在漫遊認證時，Outer Identity 也扮演著指引認證伺服器方位及建立加密通道的先鋒任務。

如圖 4所示，使用者建立加密通道的對象其實是由 Outer Identity 所指定的，若 Outer Identity 沒有指定帳號領域名稱(realm)，那麼通道僅會建立到上網地點的 RADIUS 伺服器，之後的認證方式則以 Inner Identity 所採用的認證協定繼續進行。若 Outer Identity 指定了帳號領域名稱，那麼加密通道則會經由 RADIUS Proxy一路建立到指定的RADIUS 伺服器，一般來說通常是該帳號所屬的認證伺服器。

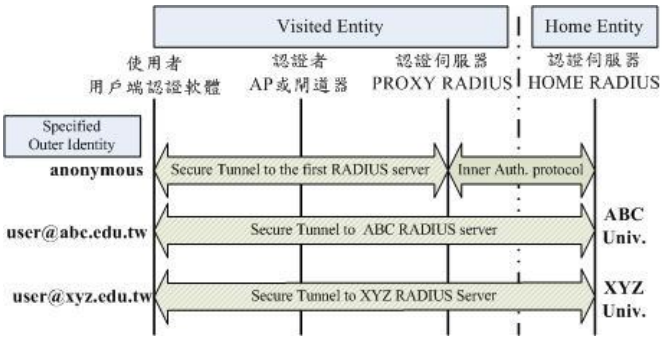

圖 4、加密通道路徑之建立

加密通道式(Tunneled Authentication Protocol)認證機制主要的好處之一是可以避免途經的RADIUS 伺服器側錄使用者個人資料，但是若使用者的 Outer Identity 填寫不當，則可能會造成 TLS 路徑建立不夠長，造成資訊外流的問題。

3.2 PEAP/TTLS用戶端認證軟體

PEAP/TTLS 是在 802.1x 架構下採用的認證機制，因此使用者端必須具備特殊的認證軟體才能夠進行驗證。在 Windows 2000/XP 作業系統下使用 PEAP 認證最簡單的方式的莫過於系統內建的 PEAP 認證軟體了，由於微軟公司為 PEAP 的主要推動者，內建PEAP認證軟體免除了使用者需要額外安裝認證軟體的麻煩，也因此讓PEAP成為校園內 802.1x 認證機制的首選[2]。

要使用 TTLS 認證機制，以目前的狀況來說，並沒有像PEAP那麼方便，使用者必須自行安裝軟體。在 Windows 下專門支援 TTLS 的 Open Source 軟體有 Alfa&Ariss 的 SecureW2。另外有些同時支援 PEAP 與 TTLS 的軟體有支援 Linux 的 Open1x 計畫(XSupplicant)、清華大學的 WIRE1x 以及商業版本的 Juniper Odyssey Access Client 等，在認證操作上都相當方便。

雖然說 PEAP 以及 TTLS 均允許 Outer Identity 的設置，但是在 Windows 2000/XP中內建的 PEAP 認證軟體中卻見不到這個設定選項。Windows 內建的 PEAP認證軟體會直接將使用者所輸入的帳號自動填入 Outer Identity 中，這等於是間接取消了使用者帳號保護的功能。其他的認證軟體如 SecureW2、XSupplicant 以及Odyssey 等軟體均提供讓使用者自行設置 Outer Identity 的功能。

4. PEAP/TTLS的管理問題

PEAP/TTLS 等認證機制提供了保護使用者真實資料的功能，但卻也帶來了管理上的不便。以下將針對三項無線網路管理的問題進行討論。

4.1 Framed-IP-Address 紀錄問題

Framed-IP-Address 是 RADIUS Accounting 中一個很重要的屬性，該屬性用來記錄使用者被分配到的 IP 位址。由於 802.1x 是屬於 Layer2 的協定，因此對於 Layer3 的資訊完全無能為力[5]。

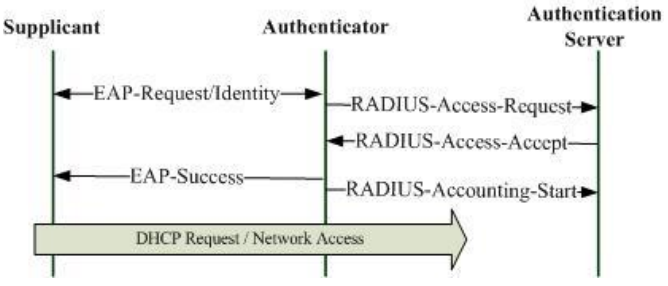

圖 5、EAP 認證流程簡化圖

圖 5 為 802.1x EAP認證的簡圖，一般而言當 Authenticator收到 Access-Accept訊息後，就會立即對使用者發出 EAP-Success 訊息，並且開始進行 RADIUS Accounting，接著使用者自行發出 DHCP 要求分配IP，這時就不是 Authenticator 的管轄範圍了，因此也無法進行IP 位址的記錄，

通常管理者會拿使用者 IP 作為管理使用者的

依據，但是在這樣的機制下，無法正確記錄使用者 IP 將對管理者造成些許困擾。

4.2 User-Name 記錄問題

User-Name 屬性記錄的是使用者在認證軟體中所輸入用來認證的帳號，在 RADIUS 中這個屬性也被用來作為認證及記錄用途。在進行 EAP 認證的情況下，使用者帳號會記錄於 EAP 封包內。使用 PEAP/TTLS 認證時, Authenticator 收到 EAP-Request 後會透過 EAP over RADIIUS 向指定的 RADIUS 伺服器送出要求，為了要與 RADIUS 原始的協定相容，Authenticator 會將 EAP 內記載的 Identity 複製一份到 User-Name 欄位[6]，這項記載於 EAP 封包內的資料其實就是使用者指定的 Outer Identity。

PEAP/TTLS 的 Inner Identity 是受到加密保護的，因此當 Authenticator 發出 RADIUS 封包時，根本沒有辦法獲得 Inner Identity 的真實使用者帳號並填入 User-Name 屬性中，因此也造成了使用者帳號記錄的問題。通常無線網路管理者遇到資安問題時，可能會以帳號找人，但在這種認證環境下可能就不會如此順利了。

4.3 Outer Identity 漫遊問題

這個問題其實與前述的 User-Name 記錄問題的原因相同，都是由 Outer Identity 所造成的，但這在無線漫遊認證的情況下將造成更麻煩的問題。

在 3.1 中有提到，PEAP/TTLS 的 Outer Identity 其實還身負一個開通秘密通道的任務，但這時若一個外來的漫遊使用者，將 Outer Identity 隨意填寫，那麼會出現什麼情況呢？

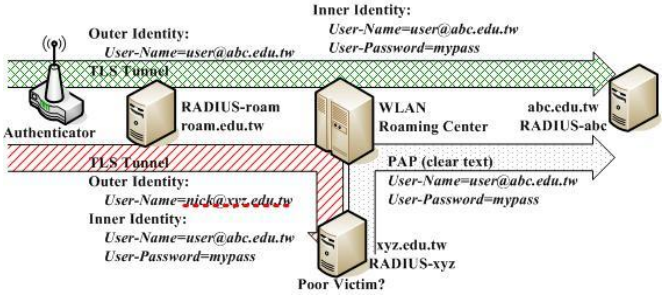

圖 6、TTLS/PAP 漫遊認證示意圖

圖 6 是以 EAP-TTLS/PAP 認證為例所呈現的漫遊認證流程示意圖，若使用者於 roam.edu.tw 進行無線認證時並沒有使用匿名功能，那麼 Authenticator、RADIUS-roam、漫遊中心 RADIUS 以及 RADIUS-abc 都能夠記錄正確的使用者帳號。倘若使用者 *user@abc.edu.tw* 啟用了匿名功能，且刻意將 Outer Identity 設定為 *nick@xyz.edu.tw*，根據 RADIUS Proxy 的規則，這個 TLS 通道將透過漫遊中心伺服器建立到 RADIUS-xyz 上，接著再由 RADIUS-xyz 取出 Inner Identity 獲得真實的帳號與密碼後，以 PAP 認證方式經過漫遊中心再轉送到 RADIUS-abc 進行真正的身份認證程序。

使用者通過認證後，Authenticator 開始發送 Accounting 訊息。很不幸的，由於 User-Name 屬性內容為 *nick@xyz.edu.tw* 的關係，這個 Accounting 資料會轉送送給 RADIUS-xyz，負責轉送的漫遊中心與 RADIUS-xyz 將會忠實的記載這個不實的資料, 而 RADIUS-abc 只會有一筆 *user@abc.edu.tw* 認證記錄，但是不會記載 *user@abc.edu.tw* 這位使用者的統計記錄，因為 Authenticator 根本沒打算，也無法將相關記錄送交給 RADIUS-abc。

這個問題造成管理者無法直接取得使用者的使用行為記錄，當需要裁決一些事項時可能會造成舉證及追蹤上的困難。

5. 解決方案與建議

前述的問題歸咎其原因就是 EAP 與 Outer Identity 的特性所造成，但畢竟這些都已經是國際標準協定，因此若說要更改協定也並非一時三刻的事，相關的標準制訂及因應辦法可以參考 IETF 的 PPPEXT 工作小組[12]所發表的 RFC。然而就算標準文件完成了，但是設備要支援也是得花一番功夫，因此在現有的設備及環境架構下，換個角度思考也還是能夠有不錯的解決方案。

5.1 使用者 IP 記錄方案

由於 EAP 認證下的 Framed-IP-Address 無法由 Authenticator 直接取得而造成無法正確記錄，但至少 Authenticator 會記載 Calling-Station-ID，這個屬性所記錄的是使用者無線網卡的 MAC 位址。配合 DHCP 伺服器的 IP 發放記錄及 MAC 位址，便能夠比對出 IP 位址。

如果要整合到 Accounting 記錄中的話，只要寫一個外部程式定期比對 DHCP IP 發放記錄與 Calling-Station-ID，並將符合條件的 IP 填入 Accounting 資料庫中的 Framed-IP-Address 欄位即可。因此也額外建議 Accounting 盡量以資料庫系統來儲存，取代純文字格式的 Accounting 記錄檔，這樣配合外部程式工作會容易許多。

此外並不是所有 Authenticator 都能夠很完美的支援 RFC2866，因此若打算採用 AP 作為 802.1x 架構的 Authenticator，選用之前應仔細測試其 RADIUS Accounting 的支援程度。若廠商願意修改 AP firmware 支援得更完整，那麼只要升級韌體也能夠順利解決這個問題。

5.2 User-Name 記錄方案

Outer Identity 匿名設置不僅造成 User-Name 無法正確被紀錄，同時在漫遊環境下也產生了

PEAP/TTLS 加密通道建立路徑的問題，並且造成統計資料管理上的麻煩。因此解決方法便是讓 Authenticator 能夠正確送出 User-Name 屬性。由於一般 Authenticator(如啟用 802.1x 的 AP)只能看到 Outer Identity，因此要讓 Authenticator 記錄正確的 User-Name 的方法只有一種：要求使用者正確填寫。

但是使用者通常不願意任管理者宰割，因此這個方法幾乎不可行，不過我們還是能夠用間接的方法取得。首先取得使用者認證時的 Outer Identity，追溯到 RADIUS Accounting 的實際記錄地點，例如圖 4-2 中的 RADIUS-xyz。然後調閱 RADIUS-xyz 的認證記錄，就能夠確認使用者的真正身份。

這邊會有個問題：何時我們會需要這麼大費周章去得知使用者的真實身份及統計資料？通常只有在有外來抱怨或檢舉時管理者才有必要這麼做，但是在非 NAT 環境下被檢舉的通常是一個配發給使用者的 Public IP；NAT 環境下被檢舉的通常是無線網路閘道設備或 NAT 伺服器的 Public IP，這些都造成了追蹤用戶的困難度[3]。

上述的解決方法過程其實有些繁複，且相關的 RADIUS 都必須保留足夠的記錄才可行。不過管理者也可以要求用戶進行無線網路認證前，先行註冊卡號及使用者帳號，那麼有問題發生時也能夠很快的從卡號追 IP，再由 IP 追人。目前有不少加入無線漫遊的單位具備有漫遊使用者卡號註冊的系統，例如暨南大學、聖約翰科技大學等。雖然這種作法除了要建置註冊管理系統外，也會讓使用者覺得有些不便，但這也是一種管理的策略，便利與安全本來就是難以兼顧的。

5.3 Outer Identity 惡意漫遊防止

Windows 2000/XP 內建的 PEAP 認證軟體取消了 Outer Identity 的設置，因此認證時的 Outer/Inner Identity 都是一樣的，雖然這看來有些專制，但也許是件好事，因為這就沒有故意偽造身份的問題。但是一般 Open Source 或商業版本的 802.1x 認證軟體都是按照 PEAP/TTLS 草案文件進行開發，因此也就保留了這項保護使用者隱私的功能，所以要從認證軟體端來掌控全局似乎不可能。

由於此類的漫遊行為是基於 EAP over RADIUS 標準所產生，因此理論上是合法的，雖然 PEAP/TTLS 目前仍屬草案階段，但是這些草案都要求提供使用者的匿名機制，亦即 Outer Identity 的設置功能。既然「官方」袒護使用者，但我們仍可用其他的方式解決這個問題。

由於 PEAP/TTLS 或是 FAST，在進行認證前都會先進行加密通道的建立，建立的對象是一部支援所需加密通道協定(如 TLS)的 RADIUS 伺服器，這個 RADIUS 會由 Outer Identity 來指定，同時該 RADIUS 也能夠取得 Inner Identity。因此只要在 RADIUS 上加入以下認證資料處理規則：「Inner Identity 與 Outer Identity 所設置的 realm 不相符或無法支援，則拒絕或放棄認證程序。」，便可防止有心人使用該 RADIUS 做為認證跳板，當然這也避免了莫名其妙 RADIUS Accounting 記錄的出現。

目前本計畫漫遊中心所採用的 FreeRADIUS[13] 1.1.2 以及早期版本並沒有支援這樣的設置功能，未來也不確定官方是否會支援，但必要時仍可以自行修改 FreeRADIUS 程式碼強制進行檢驗流程以避免此問題出現。

5.4 Early PEAP/TTLS Termination

還有另一種作法可以實作在上網地點，可以避免 Outer Identity 造成的問題。當使用者要求進行 PEAP/TTLS 認證時，強制將加密通道建立到當地的 RADIUS 上，如圖 7 中的 RADIUS-roam，如此一來 RADIUS-roam 將能夠直接解出使用者的認證資訊，並且將 Inner Identity 所指定的認證資訊及協定將認證請求轉送到該使用者所屬的 RADIUS-abc 進行認證，同時使用者的真實帳號也會被紀錄起來。認證資料傳輸過程將透過漫遊中心所建置的 VPN 通道傳輸，因此可避免第三方竊取使用者個人資料。若 Inner Authentication Protocl 能採用 CHAP 機制的協定，例如 MD5-Challeng、MS-CHAPv2 等，將更能夠保障使用者的密碼傳輸安全。

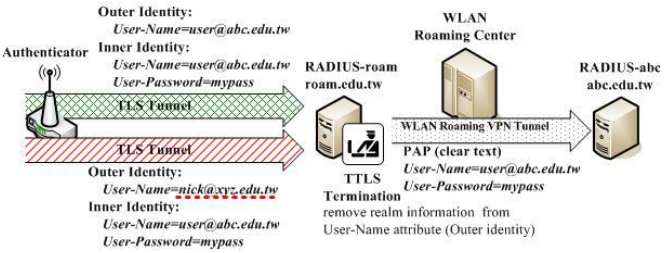

圖 7、TTLS/PAP 使用 TTLS Termination

認證過程完成後，RADIUS-roam、漫遊中心及 RADIUS-abc 都會有一份使用者的實際認證記錄，若要追蹤某位使用者時就不必大費周章的追蹤，只需要在 RADIUS-roam 翻閱認證記錄就能找到相關資料。同時這也避免了 Outer identity 誤用造成的加密通道建立問題。當然這種作法犧牲了使用者的隱私，使加密通道在 RADIUS-roam 便提前停止，Inner Identity 也提早於 RADIUS-roam 被解出，不過這至少保護了使用者在無線傳輸認證資訊時的安全。

在 FreeRADIUS 中只要認證封包不符合 RADIUS Proxy 條件的 Request 都會在本地端處理，很容易就能達成 Early PEAP/TTLS Termination 的功能，但考慮到漫遊環境就沒那麼容易了，因為漫遊環境的基本精神就是要往外 Proxy。

因此還有一種作法是將使用者所填寫的領域名稱濾除，例如 *nick@xyz.edu.tw* 會被修改成 *nick*，造成不符合漫遊條件而將加密通道終止於本地。但 FreeRADIUS 中會根據 RFC2869 的規範檢查

RADIUS Access-Request 中 User-Name 屬性(Outer Identity)與 EAP 訊息中的帳號是否相同，若不相同則會直接拒絕處理，因此我們可以修改程式使其不去檢查，讓加密通道的建立到此為止。這邊我們用了一些手段去解決問題，但是不檢查 User-Name 及 EAP 訊息所造成的安全影響可能還需要經過評估。

5.5 整合式的解決方案

若 Authenticator、RADIUS-roam 與 DHCP 伺服器能夠結合的話，那麼將可解決更多問題。

首先 Authenticator 收到 PEAP/TTLS 認證請求後(取得 MAC 位址/Calling-Station-ID)，利用 PEAP/TTLS Termination 功能將加密通道建立在自身 RADIUS 伺服器上(取得使用者真實帳號/User-Name)，使用者通過 PEAP/TTLS 認證後，以自身的 DHCP 伺服器發放 IP 位址(取得 Framed-IP-Address)，最後將記錄有 User-Name、Calling-Station-ID、Framed-IP-Address 的 RADIUS Accounting 封包送至 User-Name 所屬的帳務伺服器，這一切就被完整的記錄下來了。

此外由於 PEAP/TTLS 在使用者認證軟體端具有驗證 Authentication Server 憑證(Certificate)的選項功能，若使用者強制檢驗伺服器憑證，那麼認證程序將會失敗，因為透過 Early PEAP/TTLS Termination 功能的介入，使用者收到的憑證將會是截斷秘密通道的那一部 RADIUS 伺服器憑證(如圖 7 中的 RADIUS-roam)，而非使用者原本所信賴的伺服器憑證(如圖 7 中的 RADIUS-abc)。當然這問題也有解決方法，就是要求使用者不要確認伺服器憑證，但這又讓使用者處於可能被惡意 Authenticator 以捏造的憑證釣魚(Phising)的危險環境之中。

當然這個問題也是有解決方法的，若能夠以 PKI(Public Key Infrastructure)[11]機制整合無線漫遊環境中所有閘道設備以及 RADIUS 的伺服器憑證，使用者只要信任漫遊憑證中心的「根憑證(Root Certificate)」即可，這同時解決了惡意 Authenticator 以及 PEAP/TTLS 加密通道被提早中止造成的信任問題。透過 Early PEAP/TTLS Termination 及上述其他統計技術，並配合跨校無線漫遊環境提供的 VPN 通道，將能夠有效保障使用者的認證安全。

6. 結論

802.1x EAP-PEAP/TTLS 認證機制提供了使用者認證及一般資訊傳輸時的安全性。PEAP/TTLS 除了保障個人資訊的傳遞外，也提供了匿名功能，以隱藏使用者的個人資訊以及上線地點，但這卻造成了管理上諸多問題。網頁認證機制的建立遠比 802.1x 簡單，但也遠不及 802.1x 能夠提供的安全等級，因此未來建置 802.1x 環境不但勢在必行，同時也是國際間的趨勢。但是兼顧安全也必須考量管理上的便利性，在建置 802.1x EAP-PEAP/TTLS 無線認證環境時，若配合 Early PEAP/TTLS Termination 以及漫遊憑證中心機制，並配合認證平台的 VPN 傳輸支援以及建置完整的 RADIUS Accounting 機制，將能夠強化無線使用者身份認證及網路存取時的安全，並能防止使用偽造憑證的惡意釣魚站台，另外一方面也降低了管理的複雜程度，在使用者安全與資安管理之間取得平衡。

無線網路安全機制是各界必須持續向上提升的，也是本計畫所追求的大方向，在此也期盼本文對於各單位在建置無線認證環境時能夠有所助益。

7.參考文獻

[1] 校園無線漫遊機制整合實驗與推廣計畫網站, Jul. 2006, https://wlanrc.nchc.org.tw

[2] 周文正、賴守全, "建置以802.1X 及 PEAP為基礎的校園無線區域網路", TANET2005 台灣網際網路研討會, Oct. 26-28, 2005.

[3] 唐可忠、楊詠淇、黃偉航、陳偉文, "跨校無線漫遊環境下的使用者監控追蹤機制", TANET2005台灣網際網路研討會, Oct. 26-28, 2005.

[4] Ashwin Palekar, Dan Simon, Joe Salowey, Hao Zhou, Glem Zorn, S. Josefsson, "Protected EAP Protocol (PEAP) Version 2", Oct. 2004,http://www.potaroo.net/ietf/idref/draft-josefsson-pppext-eap-tls-eap

[5] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, "IEEE 802.1X RADIUS Usage Guidelines", RFC 3580, Jun. 2004.

[6] B. Aboba, P. Calhoun, "RADIUS Support for Extensible Authentication Protocol", RFC 2869, Sep. 2003.

[7] IEEE, "802.11i WLAN Security Enhancements", Jul. 2004, http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[8] IEEE, "802.1x Port-Based Network Access Control", Dec. 2004, http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

[9] N. Cam-Winget, D. McGrew, J. Salowey, H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method(EAP-FAST)", Oct. 2005., http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-03.txt

[10] Paul Funk, Simon Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 1(EAP-TTLSv1)", Mar. 2006., http://www.ietf.org/internet-drafts/draft-funk-eap-ttls-v1-01.txt

[11] Public Key Infrastructure(pkix), Mar. 2006, http://www.ietf.org/html.charters/pkix-charter.html

[12] PPP Extensions, Jun. 2005, http://www.ietf.org/html.charters/pppext-charter.html

[13] The FreeRADIUS Server Project, May. 2006, http://www.freeradius.org/