國立台灣大學校園無線網路安全及學生密碼安全意識調查

林美君、洪敏菖、邱佑祈、邱繼寬、劉濬銘

摘要

學術網路(TANet)台北區網中心自 2008 年開始，推動以 802.1X PEAP 協定取代過往的開放式校園無線網路以提升校園資訊安全，各個大學院校也逐一將各自的校園無線網路升級為相同協定。不過，早於同年即有資安人員提出警告，沒有正確設定的 PEAP MS-CHAPv2 協定也可能造成嚴重的資安風險。

我們將以實作架設 Rouge AP 的方式，以「教職員帳號密碼流出」這個事件為起點，深入探討第一推手國立台灣大學在無線網路環境上的做法、背後的思維、實際情況中遇到的困難及它們所提供的安全性與所造成的弱點，並提出相對應的可能改善方法，以期提升我們對資安在實務處理上的能力及認知，對校園網路安全盡一份心力。

1. 前言

WPA2 為目前最安全的無線網路安全協定，而 EAP 則是提供了高安全性的使用者身分認證框架，國立台灣大學(以下簡稱台大)目前亦使用 WPA2 和 PEAP-MSCHAPv2 的模式建設校園無線網路。然而，使用了兩個安全機制的無線網路環境，真的就牢不可破了嗎？
我們將試圖在這樣的環境下尋找可能的漏洞，實際進行攻擊，分析漏洞產生的原因，並從中學習可能的漏洞修補方式。

2. 台大選用 PEAP 的原因

在使用目前 WPA2 和 PEAP 的模式前，台大的無線網路環境為開放式 WEP 無線網路，並進行網頁登入認證。

但眾所皆知開放式網路幾乎等於毫無防護，對校園教職員生的資訊安全有極大的威脅，提升校園網路安全日漸成為無線網路建置人員的重要課題。從 WEP 升級為 WPA2 是必然的過程，但我們很好奇，為何另外加入了 EAP？眾多 EAP 方法中，為何選擇 PEAP？
為了解開這個疑惑，我們找到了台北區網中心於民國 97 年 3 月的會議紀錄，其中一項提議便是將網頁式認證「轉為 802.1x 認證，建議使用 Microsoft PEAP 認證」。
訪問了當時提案的人員，他替我們詳細的解說了當時的想法，除了提升 PEAP 協定可以加入跨 AP 漫遊的方便性之外，他也有考慮過其他 EAP 方法的優劣，我們將會在接下來的報告中做出分析。

3. EAP 擴展認證協議

擴展認證協議(Extensible Authentication Protocol)可以但不僅限於在無線網路環境中作為使用者的認證框架，現今行動裝置常見的認證方式有 EAP-TLS、EAP-SIM、EAP-AKA、PEAP、LEAP、EAP-TTLS 等。

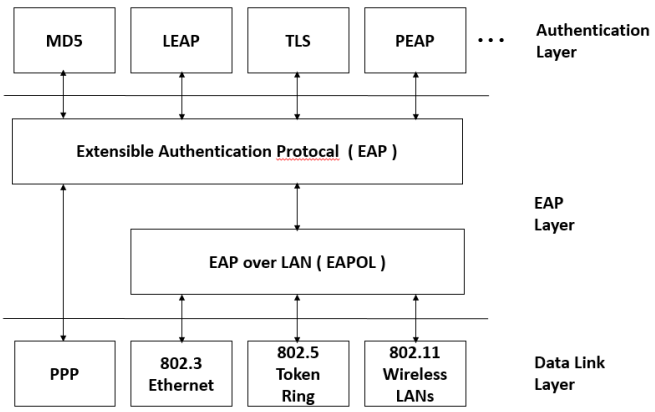

圖 1. EAP 框架各層的關係

EAP 協定類型	連線許可認證	資料傳輸加密
EAP-MD5	密碼，單向認證	
LEAP	密碼，雙向認證	動態更新金鑰
EAP-TLS	憑證，雙向認證	憑證/動態更新金鑰
PEAP	帳號密碼(MSCHAPv2)，可使用公用 CA 憑證，雙向認證	憑證/動態更新金鑰

表 1. EAP 方法的差異

其中 EAP-TLS 和 PEAP 由於在認證過程中加入了伺服器端(EAP-TLS 甚至還有客戶端)的憑證過程，讓資料傳輸過程經過 TLS 通道加密，並且避免中間人攻擊的問題，使得其安全性更加提升。

根據台大網路建置人員的說法：「雖然 TLS 是最安全的作法，但由於必須建置 CA 中心，對於學校這種機構來說較為困難。另外 PEAP 為微軟原生方法，並且支援使用學校行之有年的帳號密碼登入，故在參考外國大學作法及兩相權宜之下，選用了 PEAP 方法。」

4. PEAP-MS-CHAPv2

台大在無線網路環境的 PEAP 方法設置上，經過第一階段的憑證認證產生 TLS 通道後，第二階段驗證(帳號密碼驗證)方法選用了 MS-CHAPv2 方法。

MS-CHAP 為微軟公司設計的認證協議，其特色為使用者身分的認證過程並不是單純的帳號密碼驗證，而是使用獨特的「挑戰/回應」(challenge/response)方式。

圖 2. MS-CHAPv2 驗證過程

其驗證過程如下：

1. Server 端向 client 傳送 EAP-Request/Identity，請求 client 提供使用者名稱。
2. 收到使用者名稱後，server 再發送 EAP-Request/EAP-MS-CHAP-V2 挑戰字串給 client。
3. Client 自身也產生一組挑戰字串，以挑戰字串為基礎，將使用者密碼轉換為 EAP-Response/EAP-MS-CHAPV2 中的回應字串，並且也同時向伺服器提出自己的挑戰字串。
4. Server 端驗證 client response 和伺服器中儲存的密碼經相同運算後是否一致。
5. 驗證成功建立連線。

由上述過程可見，身分驗證期間完全不會有明文密碼傳輸，因此提供了身分驗證上的安全性。

5. 台大無線網路的問題

經由前述的驗證機制，我們可以看出 PEAP-MS-CHAPv2 認證的安全性主要建立在：

1. 伺服器端憑證所建立的 TLS 加密通道
2. MS-CHAPv2 的加密身分驗證過程

雖然乍看之下，PEAP-MS-CHAPv2 的驗證過程非常安全，但這或許也同時提供了攻擊者趁虛而入的空間？

台大使用的伺服器端憑證為臺灣網路認證公司 TWCA 所簽發的，TWCA 是全球網頁瀏覽器及行動裝置所信任的 Root CA 之一，因此在憑證認證上本不應該有任何問題。

不過，實際使用時就會發現，行動裝置會將台大的憑證歸類為不受信任的憑證，並且在台大計資中心發佈的無線網路連線教學中，明確指示了教職員生手動點擊「信任」此憑證。

這衍伸出了第一項問題—**使用者養成了信任有問題的憑證的習慣。**

圖 3. 台大憑證在 iOS 裝置下的狀況

圖 4. 台大計資中心網頁的連線教學

另外一個問題為，**其實 MS-CHAPv2 早於 2012 年即遭破解**，因此這層看似提升安全性的做法也幾乎等同沒有用處了。

6. 憑證問題探究

本應沒有問題的憑證，怎麼會不被行動裝置信任呢？ 這是我們欲了解最重要的事情，畢竟憑證驗證正是 PEAP 方法的精華之所在。

我們發現，該憑證伺服器在以個人電腦連線時，憑證的驗證是沒有問題的。
針對這項議題，我們請教了台大網路建置人員，也寄信至 TWCA 詢問，經過研究後，我們推

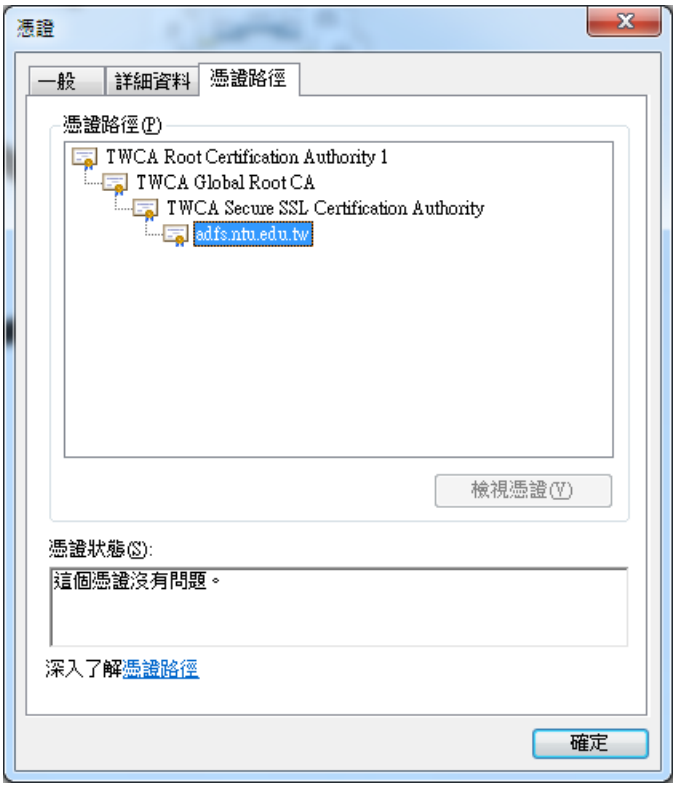

圖 5. 台大憑證階層架構及驗證結果

測原因為行動裝置在欲連線至無線網路時，雖然裝置信任 TWCA 的根憑證，但由於本身處於沒有網路連線的狀態，因此無法驗證中介憑證，最終導致 server 憑證無法驗證，使裝置認為憑證無法信任。
不過，直到撰寫這份文件的時，台大和 TWCA 還未得出真正的結論，因此本文件中無法提供最準確的資訊，還請見諒。

7. MS-CHAPv2 問題探究

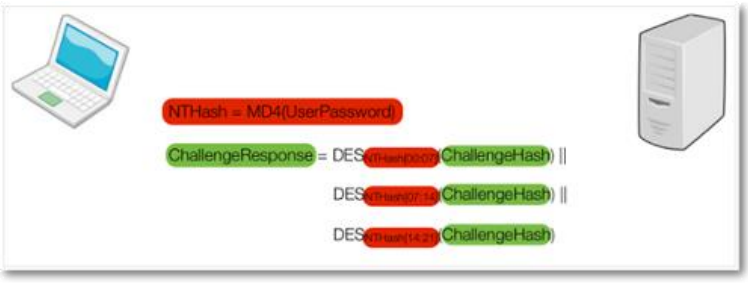

圖 6. ChallengeResponse 產生流程(節錄)

MS-CHAPv2 被認為遭破解的原因，在於其產生密碼 Response 時的機制只使用了現今證實過弱的 MD4 雜湊值演算法，以及有漏洞的 DES 加密法(圖中紅色的部分)，因此，一名攻擊者只要使用足夠演算能力的裝置即可破解出密碼的

原文，現在甚至有提供付費破解 MS-CHAPv2 挑戰回應值的線上服務。

不過，由於本專題只是為了展示 PEAP-MS-CHAPv2 可能造成的漏洞，因此並沒有使用 DES 破解裝置和任何線上服務，而是使用較傳統的字典檔攻擊手法。

8. 攻擊方法

在憑證和 MS-CHAPv2 這兩項問題的存在之下，我們的攻擊作法也相當明確了：

1. 偽造台大 AP 名稱及憑證資訊
2. 擷取 MS-CHAPv2 驗證過程，並破解出帳號及密碼。

利用 hostapd-wpe 這項開源工具即可輕鬆做到這樣的事情。

hostapd-wpe 是基於 hostapd 無線網路架設工具的一種變種工具，專門用在針對 EAP 認證的攻擊上。

hostapd-wpe 能夠利用 openssl 產生自簽憑證，雖然自簽憑證會被任何的憑證驗證機制判別為不受信任，但由於台大無線網路使用者已養成

圖 7. 於 iOS 系統中檢視偽造的憑證

接受有問題的憑證的習慣，再加上多數使用者並沒有自己鑑定憑證真偽的能力，因此我們只需在設定檔中，將特定欄位(如簽發單位名稱、國家、組織名稱等)更改成和台大的憑證一樣，即可達成欺騙的效果。

偽造完憑證後，我們只需要利用 hostapd-wpe 架設一台和台大無線網路一樣 SSID 的 AP 即可開始進行攻擊。

9. 資訊收集及行動規劃

為了將攻擊效果最大化，我們必須提升受害者連線我們偽造的 AP 的意願。

實際攻擊前，我們在台大計資中心的網頁中發現了一項有趣的資訊—台大無線網路訊號分佈圖。

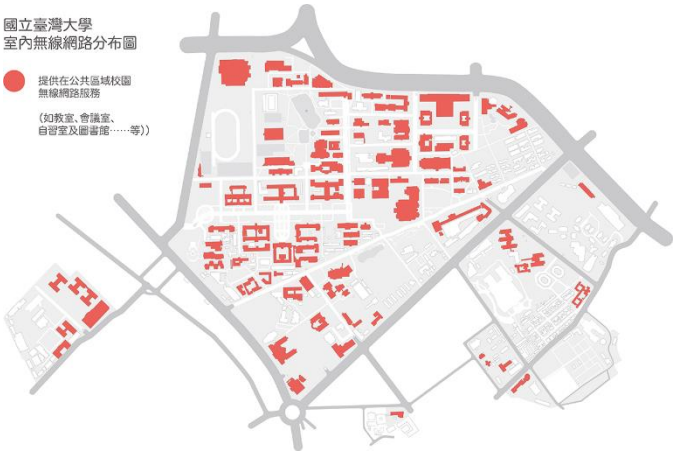

圖 8. 台大室內無線網路分佈圖

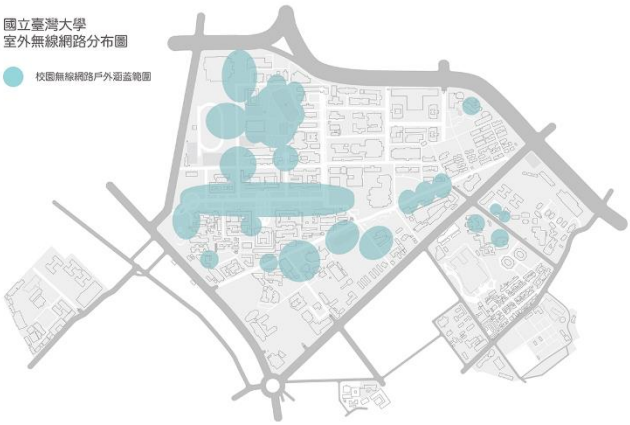

圖 9. 台大室外無線網路分佈圖

為了教職員生使用方便，台大計資中心很貼心的提供了台大校園室外及室內的無線網路訊號分佈圖，然而這也為攻擊者規劃攻擊地點提供了十分有用的資訊。

經由交叉比對和實際探查後，我們發現台大小福是一個非常理想的攻擊地點。
小福是台大的其中一間小型商場，內部設有餐飲區、日用品商店等，為台大學生平日午晚餐時段經常聚集的地方。
其沒有室內無線網路，雖然有被室外無線網路訊號覆蓋，但由於建築物本身為水泥建造，室內訊號極差，再加上人流多及快，便成為了最佳的攻擊地點。

10. 實地攻擊

實作攻擊上，我們利用樹莓派，一種約信用卡大小，能夠以行動電源供電的小型單板電腦配合 hostapd-wpe 建立偽造的台大網路 AP，最終裝置的體型甚至小到可以裝進背包裡帶著四處移動。
本組組員輪班於每日中午至小福，或是針對特殊節慶活動如校慶園遊會等人潮聚集的時刻，混入人群之中進行攻擊。

圖 10. 本專題攻擊用裝置

11. 作業系統對偽造 AP 的反應

在實際攻擊前，我們進行測試時發現了一些有趣的情形。

不同的作業系統如 Windows、Android、iOS、OSX 等，對於憑證有問題的無線 AP 會有不一樣的反應。
如圖 3 所示，iOS 裝置在連線至有問題的 AP 時，會詢問使用者是否要信任該憑證，且在不同的 iOS 版本之下，憑證資訊的詳細程度有很大的差異。本專題實測 iOS8 與 iOS11，後者資訊較為詳細。
OSX 系統和 iOS 相似，也會詢問使用者是否信任該憑證，並且能夠檢視憑證詳細資訊。

Windows 系統方面，本組實測 Windows 7 和 Windows 10 版本在連線到有問題的 AP 時，Windows 7 所提供的資訊較為詳細。

圖 11. Windows 7 安全性警訊

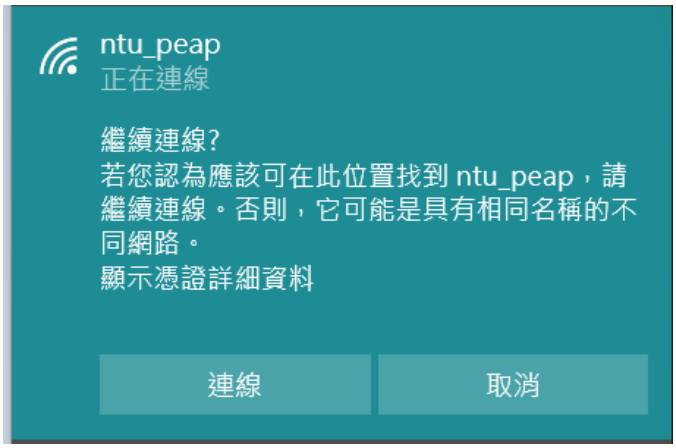

圖 12. Windows 10 安全性警訊

然而，多數人所使用的 Android 作業系統完全不會對使用者提出任何警示，甚至會主動連線至我們偽造的 AP，並在沒有使用者互動的情況下進行身分驗證。

實際測試中我們發現一直到最新的 Android 7.0 版本都有此問題，不過值得一提的是，Samsung A5(2017)型手機所使用的 Android 7.0 系統會直接阻止使用者連接憑證有問題的無線網路，甚至沒有讓使用者手動信任的選項。

圖 13. Samsung A5(2017)連線情形

12. 攻擊結果及分析

截至本文件編寫日之前，我們一共截取了 236 組帳號 ChallengeResponse 值，並且成功使用 John the ripper 密碼破解工具，配合約 20GB 大小的密碼字典檔，破解出了其中 25 組登入帳號的密碼原文，並以”How Secure Is My Password ?”網頁計算其暴力破解所需耗時。

破解出來的密碼，我們將其歸為三類：預設密碼、弱密碼及常見單字。

預設密碼方面，我們經由詢問台大畢業校友得知，台大無線網路帳號的預設密碼由身分證字號第一位英文字母加上最後四位數字所構成，因此我們得以自己建立一個預設密碼字典檔，並且破解出仍在使用預設密碼的帳號。

學院	密碼	檢測結果
電資院	e9377	2 毫秒
醫學院	f3054	2 毫秒
生農院	d4233	2 毫秒
生農院	e3760	2 毫秒

圖 13. 破解出的預設密碼清單

雖然台大系統目前已要求學生在第一次登入學籍系統時必須更改密碼，但是登入無線網路時卻不需要，因此造成了這樣的漏洞存在。

學院	密碼	檢測結果
工學院	1q2w3e4r	即刻
工學院	qwe123asd	42 分鐘
工學院	keavin777	1 分鐘
文學院	a1123581321	1 分鐘
文學院	arbiter1	1 分鐘
文學院	qwerty12345678	五千年
文學院	2wsx1qqz	1 分鐘
文學院	fli2o3n4a5	1 天
生農院	daniel0224	1 天
生農院	eric1204	1 分鐘
社科院	aptx4869	1 分鐘
理學院	wash0831	1 分鐘
電資院	winner11	1 個月
電資院	chun0622	1 個月
電資院	1234qwer	即刻
電資院	winner11	1 個月

圖 14. 弱密碼清單

弱密碼部分則是包含了典型 qwerty 類型密碼，英文名字加上生日、常見詞彙等。
值得注意的是，有些密碼在檢測網站中檢測的結果顯示暴力破解需要非常長的時間，但是卻被我們輕易用字典檔破解出來，因此暴力破解時間長度並不是唯一的安全性指標。

學院	密碼	檢測結果
文學院	William83	4 天
社科院	Hauraki2	2 小時
理學院	Godhand5	2 小時
理學院	Snowflake1	8 個月
理學院	Sophia99	2 小時

圖 15. 長度不足密碼清單

圖 15 的五組密碼雖然有合乎台大安全密碼規範(長度大於 8 位數、含英文大小寫及數字)，但因為長度過短，且使用了常見單字，因此依然容易受到暴力破解或字典檔攻擊破解出原文。

另外一件值得注意的事情是，在所有破解出的 25 組密碼之中，弱密碼就有 16 組，超過一半。
其最大的特色是只有小寫英文加上數字的組合，因此大幅降低了破解的複雜度，由此可見即使在密碼中只加入一個大寫字母，也可以顯著提升密碼安全性。(但依然需要注意常見字元的問題。)

13. 帳號密碼流出所造成的風險

目前台大的設計上，無線網路的帳號密碼和學籍系統是**一樣的**，然而學籍系統為了學生使用方便，將所有的學生資料整合在了一起。
因此，只要擁有了一名學生無線網路登入用的帳號密碼，即可將該學生的學生資料，包含姓名、生日、身分證字號、戶籍地址、家人等資訊，甚至是於大學入學時的體檢資料等一覽無遺。如果攻擊者有這個意願，也可以透過學籍系統進入學生網路信箱，造成社交工程攻擊的風險。

14. 總結與建議

我們認為造成我們成功截取並破解密碼的最主要原因，在於台大官方的憑證無法驗證，**造成學生習慣性信任有問題的憑證**。
因此，修補憑證這塊漏洞並重新教育學生關於憑證安全性的相關知識便成為當務之急。
台大方面目前也已經與 TWCA 聯繫並正著手處理中。

另外，風險管理也是相當重要的一環。
為了提升學生使用方便性，台大的無線網路登入密碼和學籍系統使用同一組帳號密碼，

造成了相當大的重要個資流出風險。因此為了將高風險的無線網路環境所造成的危害降低，我們認為登入無線網路用的帳號密碼應獨立出來不做它用，這樣便可以大幅降低個人資料外流的風險。
台大回應我們，目前台大計資中心也正在推動學生改用跨校園無線網路漫遊 eduroam 服務，其所使用的便是獨立的帳號密碼，因此將來有望逐步降低目前有漏洞的無線網路環境的使用率。

在這份專題中，我們學到資安真的是方便性與安全性之間的取捨，並且看似安全的方法，若是其中一個環節出錯，也可能造成極大的資安風險。
尤其在像台大這種龐大的組織中，如何快速有效地反應資安風險也是一大課題。如何說服龐大的組織成員放棄累積已久的習慣，並且採用安全性較高，但方便性較低的作法；或是尋找另一條路來填補目前面臨的資安漏洞，都是我們資安人員必須面對並積極思考的。